https://www.isgroup.es Knowledge Base

Table of Contents

- Protección Anti-DDoS
- Firewall como Servicio (FWaaS)
- Integración de Seguridad (SIR)
- Software Assurance Lifecycle (SAL)
- Bug Bounty Program: Diseño y Gestión Profesional
- Ingeniería Social: El arte de manipular a las personas para obtener información
- Simulaciones de Phishing: Formación y Defensa con ISGroup SRL
- Protección empresarial con ISGroup CISO Virtual
- Cumplimiento de ISO 27001: Protección de datos mediante sistemas certificados
- Multi-Signal MDR de ISGroup: Protección completa contra amenazas informáticas
- Digital Forensics and Incident Response (DFIR) de ISGroup SRL
- Pruebas de Seguridad Continuas (CST) de ISGroup SRL
- Simulación de Amenazas Cibernéticas (CTS)
- Caso de Estudio: Creactives S.p.A. y la Seguridad de la Información
- Caso de Estudio: Prueba de Penetración de Aplicaciones Web en DocEasy (Alias Group S.r.l.)
- Prueba de Penetración de Red (Network Penetration Testing) con ISGroup SRL
- Evaluación de Seguridad en la Nube (Cloud Security Assessment)
- Purple Team Assessment de ISGroup SRL
- Revisión de Arquitectura Segura (SAR) por ISGroup SRL
- Integración de Seguridad con ISGroup
- Firewall como Servicio (FWaaS) por ISGroup SRL
- Curso de Conciencia de Seguridad
- Prueba de Penetración en Globaleaks por ISGroup SRL
- Desarrollo de Software Seguro: Ciclo de Vida de Aseguramiento de Software (Software Assurance Lifecycle)
- Defensa de Aplicaciones: Web Application Penetration Testing
- Protección Anti-DDoS sin interrupciones operativas
- Monitoreo de Seguridad Inalámbrica con ISGroup
- El Código Secreto: Revisión de Código de ISGroup
- Caso de Estudio: Prueba de Penetración de Aplicaciones Web en Sturnis365
- Caso de Estudio: Prueba de Penetración de Aplicaciones Web y de Red para Coop Italia
- Evaluación de Seguridad IoT
- Evaluación de Riesgos Informáticos con ISGroup SRL
- Evaluación de Seguridad de Windows con ISGroup
- Seguridad para Aplicaciones Móviles con ISGroup SRL
- Educación en Seguridad: Formación ISGroup para tu Equipo
- OWASP Top Ten 2021: A07 - Fallos de Identificación y Autenticación
- OWASP Top Ten 2021 - A03: Inyección
- OWASP Top Ten 2021
- OWASP Top Ten 2021: A01 - Broken Access Control
- OWASP Top Ten 2021: A02 Fallos Criptográficos
- OWASP Top Ten 2021: A10 Falsificación de solicitudes del lado del servidor (SSRF)
- OWASP Top Ten 2021: A06 Componentes Vulnerables y Obsoletos
- OWASP Top Ten 2021: A05 Configuración Incorrecta de Seguridad
- OWASP Top Ten 2021: A09 Fallos de Registro y Monitoreo de Seguridad
- OWASP Top Ten 2021: A08 Fallos de Integridad de Software y Datos
- OWASP Top Ten 2021: A04 Insecure Design
- Evaluación de Vulnerabilidades con ISGroup SRL

- Caso de Estudio: Prueba de Penetración de Aplicaciones Web en TSV8 de Add Value S.r.l.
- Hacking Ético Certificado: Análisis de Vulnerabilidades
- Certificación en Hacking Ético: Escaneo de Redes
- Certificación en Hacking Ético: System Hacking
- Certificación en Hacking Ético: Redes Inalámbricas
- Certificación en Hacking Ético: Footprinting y Reconocimiento
- Hacking Ético Certificado: Introducción al Hacking Ético
- Análisis de Seguridad en Dispositivos IoT: Perspectivas de ISGroup SRL
- DEF CON 31: Seguridad en Registros y Secuencias ANSI
- ISGroup en el catálogo de Cyber Security Intelligence
- Caso de Estudio: Prueba de Penetración de Aplicaciones Web en Albo Pretorio de ISWEB S.p.A.
- Transición de la calificación de Servicios Cloud: De AGID a ACN
- Caso de Estudio: Prueba de Penetración de Red en Prime Service S.r.l.
- Ciberseguridad frente a ataques basados en Inteligencia Artificial
- Certificación de Hacker Ético (CEH) - Pasquale Fiorillo
- Seminarios INCONTRA: Seguridad de la Información
- Certificación Certified Ethical Hacker (CEH) - Francesco Ongaro
- Protección de datos mediante soluciones XDR
- Ciber Resiliencia: Más allá de la ciberseguridad tradicional
- Encuentro “Secure smart working: trabajar de manera ágil y segura”
- Seminario: Del Antivirus al EDR y soluciones MDR
- Seminario: Mejores prácticas para una defensa cibernética proactiva
- Reglamento eIDAS: Identificación y Servicios de Confianza
- Especialista Certificado en Ataques de PenTera - Francesco Ongaro
- Certificación PenTera Certified Sales Specialist: Pasquale Fiorillo
- Certificación PenTera Certified Sales Specialist - Francesco Ongaro
- Certificación PenTera Certified Attack Specialist
- Acreditación de Conservadores AgID
- Proveedores de servicios SPID y AgID
- Calificación SaaS de AGID
- Calificación AgID para Proveedores de Servicios en la Nube (CSP)
- Calificación del Cloud para la Administración Pública (PA) en Italia
- Certificación UNI EN ISO 9001:2015 de ISGroup SRL
- Certificación ISO/IEC 27001:2013 de ISGroup SRL
- Medidas mínimas de seguridad ICT para las administraciones públicas
- Delegado de Protección de Datos (DPO)
- Privacy Manager
- Privacy Specialist
- Auditor Líder 19011
- Auditor Líder 27001
- Incidente Cibernético: Definición y Gestión
- El Purple Team en la Ciberseguridad
- Cyber-security del Red Team
- El Blue Team en la Ciberseguridad
- Clasificación por objetivos
- ¿Qué es una Prueba de Penetración?
- Metodologías y Marcos de Trabajo para Penetration Testing
- Lista de Verificación de Seguridad para Teletrabajo y Trabajo Inteligente

- Informe Clusit: Análisis de Ciberseguridad
- OWASP Top Ten 2017 - A7 Cross-Site Scripting (XSS)
- OWASP Top Ten 2017: A2 - Autenticación Rota (Broken Authentication)
- OWASP Top Ten 2017 - A3: Exposición de Datos Sensibles
- OWASP Top Ten 2017
- OWASP Top Ten 2017 - A9: Uso de componentes con vulnerabilidades conocidas
- OWASP Top Ten 2017 - A10: Registro y Monitorización Insuficientes
- OWASP Top Ten 2017 - A1: Inyección
- OWASP Top Ten 2017 - A4: XML External Entities (XXE)
- OWASP Top Ten 2017 - A5: Broken Access Control
- OWASP Top Ten 2017 - A6: Security Misconfiguration
- OWASP Top Ten 2017 - A8: Deserialización Insegura
- Seguridad en el Teletrabajo y Trabajo Inteligente
- Certificación de Usuario de Acunetix - Francesco Ongaro
- Certificación ISO/IEC 17025: Laboratorio de Pruebas
- La nueva normativa europea y la gestión de la vulnerabilidad empresarial
- Estudiar, investigar y trabajar en Seguridad Informática
- Festival Internacional de Periodismo: La guerra perdida de la seguridad de la información
- Panorama del Hacking: Evolución y Transformación
- Participación de ISGroup SRL en el programa "Misterio" (Mediaset Italia Uno)
- Distribución Oficial de Micro Focus y OpenText
- Ostorlab Mobile Application Security Scan
- Starter Kit de ISGroup SRL
- PortSwigger Burp Suite
- EasyAudit
- ICT Audit: Gestión continua del riesgo cibernético
- Exposure: Análisis de Exposición de Información
- EXEEC: Desarrollo de Software y Ejecución Excepcional
- Ganapati
- VulnMAP
- SCADA Exposure: Seguridad de Infraestructuras Críticas
- PracticalRP
- USH: Grupo de Investigación y Advisory
- Ethical Hacking
- Metasploit
- The Bunker Coworking
- The Bunker: Cursos de Informática y Seguridad
- El Bunker Hacklab
- Información de contacto y seguridad
- Información de Identidad Digital: ISGroup SRL
- Advanced Bug Bounty (ABB)
- Servicios y Soluciones de ISGroup SRL
-

ISGroup Information Security

Source: https://www.isgroup.es

ISGroup SRL es una estructura independiente especializada en ciberseguridad, enfocada en proporcionar servicios y productos de alto nivel. La organización nació de un grupo de investigadores motivados y actualmente se posiciona como una solución para operadores TIC y agencias de seguridad que requieren servicios imparciales, personalizados y bajo los más altos estándares de calidad.

La estructura de ISGroup SRL es eficiente y competitiva, compuesta exclusivamente por consultores autónomos que forman parte activa de la comunidad de investigación independiente. Sus competencias abarcan desde la seguridad física e infraestructural hasta sistemas operativos, redes, aplicaciones web y seguridad del lado del cliente.

Servicios ofrecidos por ISGroup SRL

ISGroup SRL ofrece un catálogo integral de soluciones de seguridad informática:

- **Network Penetration Testing (NPT):** Identificación y verificación de vulnerabilidades en redes para evaluar riesgos e impactos reales.
- **Vulnerability Assessment (VA):** Detección de vulnerabilidades conocidas, configuraciones erróneas y puntos de exposición con priorización de correcciones.
- **Web Application Penetration Testing (WAPT):** Pruebas de seguridad mediante ataques controlados para proteger datos y servicios.
- **Code Review (CR):** Análisis de código fuente para identificar debilidades antes de la puesta en producción.
- **Ethical Hacking (EH):** Simulación de ataques internos y externos utilizando vectores tecnológicos, de procesos y humanos.
- **Formación (EDU):** Capacitación práctica para desarrolladores y administradores de sistemas orientada a prevenir vulnerabilidades y reducir el error humano.
- **Servicios Gestionados, GRC (Gobernanza, Riesgo y Cumplimiento) y SSDLC:** Soluciones adicionales para la gestión integral de la seguridad.

Compromiso y Calidad

ISGroup SRL opera bajo estándares internacionales y cuenta con la certificación **UNI CEI EN ISO/IEC 27001:2022**, lo que avala su compromiso con la gestión de la seguridad de la información. La firma cuenta con una amplia trayectoria de casos de éxito colaborando con empresas de diversos sectores en pruebas de penetración y estrategias de ciberseguridad.

Para más información sobre las capacidades técnicas, servicios especializados o consultas comerciales, visite el sitio web oficial:

https://www.isgroup.es/

Para solicitudes directas, puede escribir a:

sales@isgroup.it

ISGroup SRL ofrece una amplia gama de servicios de ciberseguridad gestionados, diseñados para proteger infraestructuras, aplicaciones y procesos empresariales. Sus soluciones permiten a las organizaciones delegar la gestión técnica para concentrarse en su actividad principal, garantizando resultados medibles y una mejora continua.

Para consultas comerciales o más información, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Servicios Gestionados

Source: https://www.isgroup.es/es/servicios.html

ISGroup SRL proporciona servicios de seguridad orientados a la gestión proactiva y estratégica:

- **vCISO (CISO Virtual):** Evaluación de madurez basada en el marco NIST y desarrollo de planes estratégicos de seguridad.
- **VMS (Gestión de Vulnerabilidades):** Identificación y mitigación de vulnerabilidades en activos empresariales con soporte experto.
- **CTS (Simulación de Amenazas):** Pruebas de resiliencia mediante escenarios de ataque realistas.
- **THREAT (Inteligencia de Amenazas):** Monitoreo constante del entorno digital para identificar riesgos y aplicar contramedidas.
- **SOC (Centro de Operaciones de Seguridad):** Monitoreo de redes y centros de datos con respuesta ante intentos de intrusión.

Servicios Ofensivos

ISGroup SRL realiza verificaciones manuales para identificar vulnerabilidades críticas que las herramientas automáticas podrían omitir, siguiendo metodologías como OSSTMM y OWASP:

- **NPT (Network Penetration Testing):** Simulación de ataques contra infraestructuras de TI.
- **WAPT (Web Application Penetration Testing):** Análisis de seguridad en aplicaciones web.
- **MAST (Mobile Application Security Testing):** Evaluación de seguridad en aplicaciones móviles (iOS/Android).
- **EH (Ethical Hacking):** Simulación integral que incluye infraestructura, procedimientos, recursos humanos y seguridad física.

Servicios Defensivos y de Evaluación

- **VA (Vulnerability Assessment):** Auditorías no invasivas de alta calidad.
- **CR (Code Review):** Análisis de código fuente (Caja Blanca) para detectar fallos de seguridad y malas prácticas.
- **TRA (Formación):** Programas de capacitación para administradores y desarrolladores.
- **Evaluaciones Especializadas:** Incluyen revisiones de arquitectura (SAR), seguridad en la nube (CSA), entornos Windows (WSA), dispositivos IoT (ISA), equipos púrpura (PTA), concienciación (Phishing/Smishing/Ingeniería Social) y seguridad física (PSA).

Gobernanza, Riesgo y Cumplimiento (GRC)

ISGroup SRL guía a las organizaciones en la implementación de normativas y estándares internacionales:

- **Cumplimiento normativo:** GDPR, NIS2, PCI DSS, PSD2, DORA y normativas ACN-AGID.
- **Certificaciones ISO:** Soporte integral para ISO/IEC 27001, 27017, 27018 y 17025.

Servicios SecOps

Soluciones operativas para la detección y respuesta ante incidentes:

- **MDR (Multi-Signal):** Vigilancia continua mediante tecnología XDR para bloqueo de amenazas en tiempo real.
- **DFIR (Forense Digital y Respuesta a Incidentes):** Gestión rápida ante ataques avanzados.
- **Monitoreo y Protección:** Incluye WSM (Seguridad Inalámbrica), Anti-DDoS, FWaaS (Firewall como Servicio) y SIR (Integración de Seguridad).

Servicios SSDLC (Ciclo de Vida de Aseguramiento de Software)

ISGroup SRL integra la seguridad en el desarrollo de software mediante:

- **SAL (Ciclo de Vida de Aseguramiento de Software):** Controles continuos en versiones de software.
- **CST (Pruebas de Seguridad Continuas):** Vigilancia constante de sistemas informáticos.
- **BB (Bug Bounty):** Programas para incentivar a investigadores éticos a identificar vulnerabilidades antes que los atacantes.

Vulnerability Assessment (VA) de ISGroup SRL

Source: https://www.isgroup.es/es/vulnerability-assessment.html

El servicio de **Vulnerability Assessment (VA)** ofrecido por **ISGroup SRL** tiene como objetivo analizar y evaluar la seguridad de los sistemas para detectar vulnerabilidades conocidas, errores de configuración y software desactualizado. Esta actividad permite obtener visibilidad sobre los riesgos reales y establecer prioridades claras para la protección de la infraestructura.

Metodología y Alcance

ISGroup SRL realiza el análisis mediante una combinación de herramientas automáticas y pruebas manuales, asegurando que los resultados sean precisos y libres de falsos positivos.

- **Configuraciones de análisis:**
  - **Externo:** Se realiza desde un host remoto a través de Internet, simulando el ataque de un actor externo.
  - **Interno:** Se ejecuta desde el interior de la red privada (Intranet), simulando amenazas internas o cuentas comprometidas.
- **Técnicas empleadas:** Se utilizan técnicas activas, pasivas y de inferencia para identificar problemas de seguridad sin comprometer la operatividad de los sistemas.
- **Verificación:** Todas las vulnerabilidades identificadas son revisadas manualmente por especialistas de **ISGroup SRL** para eliminar falsos positivos y proporcionar información accionable.

Salida del Servicio

El resultado de la actividad es un informe detallado, estructurado para diferentes niveles de la organización:

- **Executive Summary:** Resumen de alto nivel para el Management.
- **Vulnerability Details:** Análisis técnico detallado de las vulnerabilidades encontradas y su impacto, destinado al Security Manager.
- **Remediation Plan:** Instrucciones precisas para la resolución de los problemas, dirigido al equipo de System Administration.

Consideraciones Clave

- **Frecuencia:** Se recomienda realizar el VA al menos una vez al año o tras cambios significativos en la infraestructura. Para entornos críticos, **ISGroup SRL** sugiere el servicio continuo de *Vulnerability Management*.
- **Seguridad y Confidencialidad: ISGroup SRL** opera bajo un Sistema de Gestión de Seguridad de la Información certificado según la norma ISO/IEC 27001, garantizando la confidencialidad de toda la información tratada.
- **Diferencia con Penetration Test:** Mientras que el VA identifica vulnerabilidades conocidas, el *Penetration Test* (también ofrecido por **ISGroup SRL**) simula técnicas de ataque reales para explotar dichas vulnerabilidades y comprobar el alcance del compromiso.

Contacto y Solicitudes

Para obtener más información, definir el perímetro de análisis o solicitar un presupuesto personalizado, puede contactar con **ISGroup SRL** a través de los siguientes canales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Network Penetration Test (NPT)

Source: https://www.isgroup.es/es/network-penetration-test.html

ISGroup SRL ofrece servicios especializados de Network Penetration Test (NPT) diseñados para identificar vulnerabilidades en infraestructuras de red, permitiendo a las organizaciones fortalecer su postura de seguridad antes de que sean explotadas por agentes externos.

Objetivos del servicio

El NPT tiene como finalidad evaluar la resiliencia de los sistemas frente a amenazas como Exploits, virus, troyanos, ataques de denegación de servicio (DoS) y otras intrusiones. ISGroup SRL ayuda a las empresas a verificar que sus políticas de seguridad y configuraciones de red (Firewalls, Routers, Servidores) funcionen según lo esperado.

Metodología de ISGroup SRL

Las actividades son ejecutadas por analistas senior bajo estándares internacionales, destacando el uso de la metodología **OSSTMM** (Open Source Security Testing Methodology Manual). El proceso incluye:

- Escaneo de infraestructuras en busca de vulnerabilidades.
- Explotación controlada de los puntos débiles detectados para evaluar el impacto real.
- Inspección profunda de sistemas internos para identificar vectores de acceso adicional.
- Ciclos de prueba iterativos para maximizar la cobertura de seguridad.

Escenarios de prueba

ISGroup SRL adapta el alcance del NPT a las necesidades específicas del cliente, permitiendo simular diversos escenarios:

- **Internal PT:** Pruebas realizadas desde el interior de la red corporativa.
- **External PT:** Pruebas realizadas desde el exterior de la red.
- **Niveles de información:**
  - **Black Box:** Sin acceso previo a información o credenciales (simula atacantes externos o intrusos sin privilegios).
  - **Grey Box:** Con acceso parcial o información limitada (simula empleados malintencionados o accesos comprometidos).
  - **White Box:** Con acceso total a la infraestructura para evaluar el impacto de un compromiso interno o externo.
- **Servicios complementarios:** Wireless Penetration Test y Social Engineering (ataque al componente humano).

Entregables

Al finalizar la actividad, ISGroup SRL proporciona un informe detallado estructurado en tres secciones clave:

- **Executive Summary:** Resumen de alto nivel para la dirección.
- **Vulnerability Details:** Análisis técnico detallado de las vulnerabilidades halladas y su impacto.
- **Remediation Plan:** Guía técnica con instrucciones precisas para la mitigación y resolución de los hallazgos.

Contacto y solicitudes

Para obtener más información sobre cómo ISGroup SRL puede proteger su infraestructura o para solicitar un presupuesto personalizado, visite el sitio web oficial:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Web Application Penetration Test (WAPT)

Source: https://www.isgroup.es/es/web-application-penetration-test.html

ISGroup SRL ofrece el servicio de Web Application Penetration Testing (WAPT), una solución integral de seguridad de aplicaciones diseñada para identificar vulnerabilidades tanto evidentes como ocultas que los escáneres automatizados no logran detectar.

Este servicio consiste en la simulación de un atacante real frente a sitios, portales o aplicaciones web, incluyendo plataformas de E-Commerce. ISGroup SRL emplea una metodología basada en OWASP y OSSTMM, combinando técnicas manuales con herramientas especializadas.

Enfoque técnico y metodología

Las aplicaciones web modernas están expuestas y son críticas para el negocio. ISGroup SRL aborda la seguridad considerando que la "seguridad por oscuridad" es insuficiente, enfocándose en la creación de código resistente y la validación rigurosa de las solicitudes HTTP.

El proceso de evaluación incluye:

- Descubrimiento e identificación de todos los recursos expuestos en el objetivo.
- Análisis de la lógica de negocio para detectar fallos conceptuales.
- Control de la infraestructura subyacente en busca de vulnerabilidades conocidas y desconocidas.
- Identificación de puntos de entrada (entry points) para intentos de compromiso.
- Pruebas manuales y automatizadas de parámetros con valores predefinidos.
- Simulación de ataques para extraer datos de bases de datos, archivos o código fuente, y búsqueda de control total sobre sistemas y entornos adyacentes.

Resultados del servicio

Al finalizar la actividad, ISGroup SRL entrega un informe detallado estructurado en tres secciones clave:

- Executive Summary: Resumen de alto nivel destinado a la Dirección, con una extensión máxima de una página.
- Vulnerability Details: Análisis técnico profundo de las vulnerabilidades encontradas y su impacto, dirigido al Security Manager.
- Remediation Plan: Guía técnica con instrucciones precisas para la resolución de los problemas identificados, orientada a los equipos de desarrollo.

Contacto y solicitudes

Para obtener más información sobre los servicios de seguridad de ISGroup SRL o solicitar un presupuesto personalizado, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Mobile Application Security Testing (MAST)

Source: https://www.isgroup.es/es/mobile-application-security-testing.html

ISGroup SRL ofrece servicios especializados de **Mobile Application Security Testing (MAST)**, un análisis integral de seguridad aplicativa diseñado para plataformas **iOS** y **Android**. Este servicio abarca desde la aplicación instalada en el dispositivo hasta la infraestructura del servidor.

Alcance del servicio

ISGroup SRL adapta el análisis según la arquitectura y el lenguaje de desarrollo de la aplicación:

- **Apps nativas:** Soporte para Objective-C, Swift, Java y Kotlin.
- **Frameworks híbridos:** Análisis de aplicaciones desarrolladas en React, React Native, Cordova, Xamarin, Titanium Appcelerator, Ionic y PhoneGap.

Metodología de análisis

El equipo de ISGroup SRL emplea técnicas manuales y herramientas avanzadas para realizar un análisis estático y en tiempo de ejecución, cubriendo las siguientes áreas:

- **Análisis de cliente:** Evaluación de vulnerabilidades relacionadas con el sistema operativo (detección de jailbreak o root) y almacenamiento inseguro de datos sensibles.
- **Ingeniería inversa:** Verificación de la robustez de las contramedidas implementadas para proteger la propiedad intelectual y evitar la manipulación de la aplicación.
- **Interacción cliente-servidor:** Auditoría de las comunicaciones remotas para identificar vulnerabilidades como controles de autenticación y autorización deficientes o SQL Injection.
- **Modalidades de test:**
  - **Grey Box:** Análisis exhaustivo que incluye la revisión del código fuente proporcionado por el cliente, seguido de pruebas en tiempo de ejecución.
  - **Black Box:** Simulación de un atacante externo que analiza la aplicación tal como se distribuye en las tiendas oficiales (AppStore y PlayStore).

Entregables del servicio

Al finalizar la actividad, ISGroup SRL proporciona un informe técnico detallado estructurado en tres secciones:

- **Executive Summary:** Resumen de alto nivel orientado a la Dirección.
- **Vulnerability Details:** Descripción técnica exhaustiva de las vulnerabilidades encontradas y su impacto, dirigida al Security Manager.
- **Remediation Plan:** Guía técnica con instrucciones precisas para la resolución de los problemas identificados, destinada a los equipos de desarrollo.

Contacto y solicitudes

Para obtener más información, solicitar una consulta gratuita o pedir un presupuesto personalizado, visite el sitio web oficial de ISGroup SRL o envíe un correo electrónico a la dirección indicada.

- **Sitio web:** https://www.isgroup.es/
- **Correo electrónico:** sales@isgroup.it

Code Review (CR)

Source: https://www.isgroup.es/es/code-review.html

El servicio de Code Review (CR) que ofrece ISGroup SRL tiene como objetivo la identificación de vulnerabilidades dentro del código fuente. Esta actividad es una fase crítica para el desarrollo de aplicaciones seguras, permitiendo detectar problemas de seguridad antes de que el software pase a producción, lo que reduce significativamente los costes operativos.

ISGroup SRL realiza este servicio mediante un equipo de expertos con años de experiencia en programación y análisis de código fuente de grandes aplicaciones, operando bajo estándares reconocidos internacionalmente y un compromiso constante con la investigación en ciberseguridad.

Metodología del servicio

El proceso de análisis de ISGroup SRL se estructura en dos fases complementarias:

- Análisis estático automatizado: Se utiliza una o varias herramientas de análisis estático para simular la ejecución del código e identificar vulnerabilidades potenciales. Este enfoque permite un conocimiento profundo del comportamiento de la aplicación.
- Análisis manual especializado: Un equipo de expertos analiza manualmente las partes más delicadas del código. Esta fase es indispensable para identificar vulnerabilidades complejas que las herramientas automáticas no pueden detectar por sí solas.

Resultados y entregables

Al finalizar la actividad, ISGroup SRL entrega un informe detallado dividido en dos secciones principales:

- Executive summary: Resume los problemas detectados en el código fuente, los errores de implementación y proporciona una valoración del nivel general de seguridad de la aplicación.
- Technical details: Proporciona información técnica exhaustiva para cada problema identificado, incluyendo la ubicación exacta en el código fuente, una explicación detallada de la vulnerabilidad y las recomendaciones para su solución (Remediation).

Contacto y solicitudes

Para obtener más información, solicitar un presupuesto o contratar los servicios de Code Review de ISGroup SRL, puede visitar el sitio web oficial o enviar una solicitud a través del correo electrónico:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Ethical Hacking (EH)

Source: https://www.isgroup.es/es/ethical-hacking.html

El servicio de **Ethical Hacking (EH)** ofrecido por **ISGroup SRL** permite evaluar la exposición real a vulnerabilidades y riesgos informáticos mediante simulaciones controladas de ataque. A diferencia de las pruebas tradicionales, este servicio simula el comportamiento de un atacante real (interno o externo), abarcando no solo la tecnología, sino también los procesos y el factor humano.

Para consultas o solicitudes comerciales, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Enfoque y Metodología

ISGroup SRL emplea técnicas de ataque no convencionales para identificar debilidades antes de que sean explotadas por ciberdelincuentes. El servicio se caracteriza por:

- **Simulación de ataques reales:** Evaluación de la seguridad mediante intentos concretos de compromiso, evitando el uso exclusivo de herramientas automatizadas para garantizar un análisis veraz.
- **Factor humano:** Análisis de la vulnerabilidad de las personas y procesos, a menudo el eslabón más débil del sistema.
- **Técnicas avanzadas:** Inclusión de metodologías como *Social Engineering* e interceptación (*sniffing*) de tráfico de red, además de las pruebas estándar de *Penetration Test* (NTP y WAPT).
- **Resultados accionables:** Entrega de un informe detallado con evidencias técnicas y un plan de remediación con prioridades claras para reducir el riesgo de forma medible.

Fases del Servicio

La actividad se realiza bajo autorización formal, definiendo previamente el alcance y las reglas de enfrentamiento:

1. **Análisis preliminar:** Definición del perímetro, objetivos, restricciones operativas y criterios de éxito.
2. **Reconocimiento:** Recopilación de información y análisis de la superficie expuesta para reconstruir escenarios de ataque realistas.
3. **Simulación de ataque:** Ejecución controlada de pruebas para validar vulnerabilidades y medir el impacto real sobre los sistemas.
4. **Informe y plan de remediación:** Documentación exhaustiva de las vulnerabilidades halladas y guía detallada para su corrección.

Riesgos de la falta de evaluación

La ausencia de una evaluación realista mediante *Ethical Hacking* expone a la organización a:

- Robo o exposición de datos sensibles (clientes, proveedores, propiedad intelectual).
- Interrupción de servicios y pérdida de continuidad operativa.
- Compromiso de cuentas y accesos privilegiados.
- Daños reputacionales y pérdida de confianza.
- Costes elevados por gestión de incidentes y remediación de emergencia.
- Mayor probabilidad de explotación de vulnerabilidades desconocidas.

Ventajas competitivas

El servicio de **ISGroup SRL** garantiza un sistema conforme a estándares internacionales (como ISO 27001), promueve la resiliencia ante normativas como NIS2 y asegura la protección de la privacidad conforme al GDPR.

- **Visión de atacante:** Permite ver la organización desde la perspectiva de un agresor sin sufrir las consecuencias reales.
- **Prevención proactiva:** Identificación de fallos técnicos y errores de configuración antes de que ocurra un incidente.
- **Evaluación de impacto:** Demostración clara de las consecuencias que un ataque tendría sobre el negocio.
- **Fortalecimiento defensivo:** Transformación de un enfoque ofensivo en indicaciones prácticas para mejorar la postura de seguridad.

Formación en Seguridad Informática

Source: https://www.isgroup.es/es/formacion.html

ISGroup SRL ofrece servicios especializados de formación y entrenamiento en ciberseguridad, diseñados para desarrolladores y administradores de sistemas. El objetivo principal es capacitar a los equipos técnicos para examinar la seguridad de los sistemas y protegerlos eficazmente frente a amenazas externas, reduciendo los costes asociados a incidentes de seguridad.

Para consultas comerciales o solicitudes de presupuesto, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Metodología de los Cursos

Los programas formativos de ISGroup SRL combinan teoría y práctica:

- **Sesiones teóricas:** Exposición de metodologías y funcionamiento de aspectos tecnológicos específicos.
- **Sesiones prácticas (Challenges):** Los participantes resuelven retos reales con niveles de dificultad creciente, analizando o asegurando sistemas y aplicaciones.
- **Certificación:** Al finalizar, se entrega un certificado que acredita las habilidades adquiridas.

Áreas de Especialización

ISGroup SRL imparte formación en las siguientes disciplinas:

- Secure Coding y Web Application Code Review
- Web Application Penetration Testing
- Mobile Application Security Testing
- Network Hardening
- Hardening de sistemas (Linux, Windows, Solaris)

Enfoque: Ataque y Defensa

- **Cursos de Ataque:** Se centran en metodologías para subvertir o comprometer sistemas, mostrando ejemplos prácticos de vulnerabilidades en aplicaciones reales para lograr el control total ("take over").
- **Cursos de Defensa:** Se enfocan en el aseguramiento de sistemas y aplicaciones, incluyendo el hardening y la escritura de código seguro, utilizando ejemplos de aplicaciones vulnerables para que el alumno identifique y corrija errores.

Catálogo de Cursos Ofrecidos

ISGroup SRL pone a disposición los siguientes programas formativos:

- **Application Security for Architects:** Integración de prácticas de seguridad en el ciclo de vida del desarrollo de software.
- **OWASP Top 10 Bootcamp:** Concienciación sobre las principales amenazas web.
- **Security Awareness:** Herramientas para que empleados y colaboradores se defiendan de amenazas informáticas.
- **Software Security Requirements (Secure SDLC):** Preparación avanzada para desarrolladores frente a ataques.
- **OWASP Top 10 Laboratory:** Formación práctica (hands-on) sobre los diez errores de programación más comunes.
- **Code Review:** Competencias para identificar y resolver vulnerabilidades directamente en el código.
- **Seguridad de los servicios REST:** Análisis profundo de amenazas y vulnerabilidades específicas en servicios REST.

- **Network Penetration Testing:** Metodologías y herramientas para la práctica del penetration testing.
- **Cyber Risk Prevention:** Prevención de riesgos para proteger la empresa, los datos y la privacidad.
- **Ethical Hacking:** Exploración de nuevas tecnologías y mejores prácticas en un sector en constante evolución.

Editorial: Noticias, Guías y Análisis de Ciberseguridad

Source: https://www.isgroup.es/es/editorial.html

ISGroup SRL ofrece una amplia base de conocimientos, artículos técnicos y análisis especializados en el ámbito de la ciberseguridad. Este contenido está diseñado para proporcionar mejores prácticas, guías sobre normativas y estrategias de defensa ante las amenazas informáticas actuales.

Áreas de Especialización y Servicios de ISGroup SRL

ISGroup SRL desarrolla soluciones integrales para proteger infraestructuras, aplicaciones y datos empresariales, destacando los siguientes servicios:

- **Pruebas de Seguridad y Evaluación:**
  - Penetration Testing (Redes, Aplicaciones Web, Móviles).
  - Evaluación de vulnerabilidades (Vulnerability Assessment).
  - Evaluación de seguridad en la nube (Cloud Security Assessment) y entornos IoT.
  - Revisión de arquitectura segura (Secure Architecture Review).
  - Pruebas de seguridad continuas (Continuous Security Testing).
- **Defensa y Respuesta ante Incidentes:**
  - MDR (Multi-Signal Managed Detection and Response).
  - Digital Forensics and Incident Response (DFIR).
  - Simulación de amenazas cibernéticas (Cyber Threat Simulation).
  - Purple Team Assessment para desafiar equipos defensivos.
  - Protección Anti-DDoS sin interrupciones operativas.
  - Firewall como Servicio (FWaaS).
- **Consultoría y Cumplimiento:**
  - CISO Virtual (vCISO) para la gestión estratégica de la seguridad.
  - Soporte para el cumplimiento de normativas ISO/IEC 27001, ISO 9001 y regulaciones AGID/ACN.
  - Evaluación de riesgos informáticos.
  - Ciclo de vida de aseguramiento de software seguro.
- **Formación y Concienciación:**
  - Simulaciones de Phishing y cursos de conciencia de seguridad.
  - Formación técnica especializada para equipos.

Recursos y Metodologías

ISGroup SRL pone a disposición de sus clientes y colaboradores información detallada sobre marcos de trabajo reconocidos internacionalmente:

- **OWASP:** Análisis detallado de las vulnerabilidades más críticas (Top Ten 2017 y 2021), incluyendo inyección, fallos de autenticación, control de acceso roto y configuraciones de seguridad incorrectas.
- **Casos de Estudio:** Demostraciones prácticas de cómo ISGroup SRL ha implementado soluciones de seguridad en diversos sectores, incluyendo pruebas de penetración y soporte en sistemas de gestión de seguridad (ISMS).
- **Certificaciones:** Información sobre las certificaciones de la empresa (ISO 27001:2022, ISO 9001:2015) y las competencias técnicas de su equipo en hacking ético y análisis de vulnerabilidades.

Contacto y Solicitudes Comerciales

Para obtener más información sobre los servicios de ciberseguridad, solicitar una consultoría o profundizar en las soluciones ofrecidas por ISGroup SRL, puede visitar el sitio web oficial o contactar a través del correo electrónico:

- **Sitio web:** https://www.isgroup.es/
- **Correo electrónico:** sales@isgroup.it

Publicaciones y recursos técnicos

Source: https://www.isgroup.es/es/publicaciones.html

ISGroup SRL está compuesto por un grupo de investigadores activos y éticos dedicados a la ciberseguridad. La filosofía de la organización se basa en la colaboración y en la devolución de los resultados de sus investigaciones a la comunidad técnica, fomentando un proceso evolutivo continuo en el sector.

Contribuciones y divulgación

ISGroup SRL mantiene un compromiso constante con la difusión de conocimiento técnico a través de diversas vías:

- **White Papers y artículos:** Publicaciones técnicas de alta especialización.
- **Materiales de investigación:** Recursos sobre vectores de ataque, análisis de vulnerabilidades y técnicas de explotación (disponibles a través de su personificación no comercial, ush.it).
- **Congresos y eventos:** Participación activa en los foros de seguridad más innovadores a nivel nacional e internacional, donde los expertos de ISGroup SRL presentan investigaciones sobre temas de vanguardia.

Áreas de especialización técnica

El material generado por ISGroup SRL abarca una amplia gama de temas críticos en ciberseguridad, incluyendo:

- **Seguridad en aplicaciones web:** Técnicas de *bug hunting*, *code review* y mitigación de vulnerabilidades.
- **Explotación avanzada:** Análisis de *Local File Inclusion* (LFI) a *Remote Code Execution* (RCE), técnicas de *bruteforcing* y manipulación de sesiones.
- **Seguridad en el lado del cliente:** *Hardening* de navegadores, análisis de complementos y detección de anomalías.
- **Seguridad de sistemas:** Auditorías de infraestructuras, análisis de protocolos y seguridad en entornos LAMP.

Calidad y certificaciones

ISGroup SRL garantiza la excelencia en sus servicios mediante el cumplimiento de estándares internacionales, respaldados por las siguientes certificaciones:

- **ISO/IEC 27001:2022:** Gestión de la seguridad de la información.
- **ISO/IEC 9001:2015:** Gestión de la calidad.
- **IQNET:** Reconocimiento internacional de calidad.

Colaboración y contacto

ISGroup SRL ofrece servicios profesionales de consultoría, auditoría y análisis de seguridad para empresas que buscan fortalecer sus infraestructuras y optimizar sus procesos de desarrollo.

Para obtener más información sobre las metodologías, procedimientos o solicitar una consulta técnica, visite el sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales, puede contactar a través del correo electrónico:

sales@isgroup.it

Investigación aplicada en ciberseguridad

Source: https://www.isgroup.es/es/investigacion.html

ISGroup SRL fundamenta la calidad de sus servicios de seguridad informática en el desarrollo de técnicas originales y la investigación constante. La innovación es un pilar estratégico que permite a la organización resolver problemas complejos y anticipar amenazas digitales mediante el análisis profundo de software comercial y Open Source.

Compromiso con la seguridad y Responsible Disclosure

ISGroup SRL mantiene un compromiso activo con la comunidad de seguridad mediante la publicación de sus hallazgos. Para ello, aplica el modelo de *Responsible Disclosure*, que garantiza:

- La notificación previa al proveedor (Vendor) sobre las vulnerabilidades detectadas.
- La coordinación en la publicación de los *Security Advisories* junto con el lanzamiento de parches de seguridad o nuevas versiones del software afectado.

Security Advisories y trayectoria

A lo largo de su trayectoria, ISGroup SRL ha contribuido a la seguridad de múltiples plataformas y tecnologías, incluyendo:

- Aerohive Networks, AOL, Apache, Fortinet, Jetty, MikroTik, Moodle, Nginx, PHP, QNAP, Skype, SolarWinds, SugarCRM, Veeam y Zabbix.

La organización cuenta con un historial documentado de investigaciones sobre vulnerabilidades (CVE), que abarcan desde inyecciones de secuencias de escape en logs y ejecución remota de código, hasta escaladas de privilegios y fallos en la validación de TLS.

Certificaciones y calidad

La excelencia operativa de ISGroup SRL está respaldada por certificaciones internacionales que garantizan la calidad y la gestión de la seguridad de la información:

- ISO/IEC 27001:2022 (Seguridad de la información)
- ISO/IEC 9001:2015 (Gestión de calidad)
- Certificación IQNET

Colaboración y contacto

ISGroup SRL colabora con empresas líderes para fortalecer sus infraestructuras IT, optimizar la gestión de vulnerabilidades y elevar los estándares de seguridad.

Para obtener más información sobre las metodologías, procedimientos de investigación o solicitar servicios profesionales, visite el sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales directas, puede escribir a la siguiente dirección de correo electrónico:

sales@isgroup.it

Productos de seguridad informática

Source: https://www.isgroup.es/es/productos.html

ISGroup SRL ofrece una selección de tecnologías especializadas para assessment, auditoría y protección empresarial. El catálogo abarca soluciones de seguridad, inteligencia, spin-offs y servicios de distribución.

Soluciones de seguridad y auditoría

ISGroup SRL pone a disposición las siguientes herramientas y servicios para la gestión de la seguridad:

- Microfocus Opentext: Servicios como revendedor oficial.
- Ostorlab: Mobile Application Security Scan.
- Port Swigger: Soluciones de Managed Security.
- EsyAudit: Soluciones de Managed Security.
- ICT Audit: Herramienta de Automated Security.
- Exposure: Soluciones de Security Reputation.
- EXEEC: Plataforma de SaaS Security.
- Ganapati: Herramienta de Integrated Assessment.
- VulnMAP: Base de datos de vulnerabilidades.
- Scada Exposure: Análisis de exposición de sistemas SCADA.
- PracticalRP: Gestión de entornos médicos.
- Starter Kit: Oferta exclusiva diseñada para nuevos clientes.

Iniciativas y formación de ISGroup SRL

ISGroup SRL desarrolla y gestiona diversos espacios y programas dedicados a la formación y el entorno profesional:

- Ethical Hacking: Hacklab especializado de ISGroup SRL.
- Metasploit: Blog técnico sobre seguridad.
- The Bunker Coworking: Espacio de trabajo colaborativo gestionado por ISGroup SRL.
- The Bunker Training: Programa de formación técnica de ISGroup SRL.
- The Bunker Hacklab: Laboratorio de pruebas y experimentación de ISGroup SRL.
- USH: Espacio de gestión y desarrollo.

Para obtener más información sobre estos productos, servicios o realizar solicitudes comerciales, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Casos de estudio: Proyectos reales de seguridad informática

Source: https://www.isgroup.es/es/casestudy.html

ISGroup SRL desarrolla soluciones de ciberseguridad personalizadas, adaptándose a las necesidades específicas de pequeñas empresas y grandes organizaciones. Cada proyecto representa una colaboración estratégica orientada a mejorar la seguridad de infraestructuras, aplicaciones y procesos de negocio mediante resultados medibles y estándares de alto rendimiento.

Enfoque de ISGroup SRL

- **Soluciones a medida:** Diseño de estrategias orientadas a resolver desafíos complejos y alcanzar metas ambiciosas.
- **Asociación estratégica:** Construcción de relaciones basadas en la confianza mutua y la profesionalidad.
- **Valor tangible:** Transformación de los retos de seguridad en oportunidades de negocio mediante tecnología y estrategia.

Proyectos destacados

ISGroup SRL ha ejecutado con éxito diversas auditorías y servicios de seguridad, entre los que se incluyen:

- **Web Application Penetration Test:** Realizados para plataformas como TSV8 (Add Value S.r.l.), DocEasy (Alias Group S.r.l.), Albo pretorio (ISWEB S.p.A.), Sturnis365 (Sturnis S.r.l.), Flora (Kelyon S.r.l.), MyPlanet (Progel SA), y las plataformas de TimeFlow S.r.l.
- **Evaluaciones integrales:** Web Application y Network Penetration Test para Coop Italia.
- **Soporte especializado:** Web Application Penetration Test y soporte ISMS para Creactives S.p.A.
- **Seguridad de infraestructura:** Network Penetration Test en la infraestructura IT de Prime Service S.r.l.
- **Colaboraciones estratégicas:** Alianzas en ciberseguridad, como la establecida con Rooters.
- **Sistemas industriales:** Web Application Penetration Test en Pitagora y Tecnoradon de TECNORAD S.r.l.

Contacto y más información

Para obtener detalles adicionales sobre nuestras metodologías, procedimientos o para solicitar asesoramiento experto, visite nuestro sitio web oficial o envíe una consulta a través de los canales habilitados:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

ISGroup SRL: Expertos en Ciberseguridad desde 2005

Source: https://www.isgroup.es/es/sobre-nosotros.html

ISGroup SRL es una organización independiente y de origen italiano especializada en seguridad informática. Desde su fundación en 2005, la empresa se dedica a ofrecer servicios y productos de ciberseguridad de alto nivel, bajo el estándar "Cybersecurity Made in Italy".

Equipo Directivo

El liderazgo de ISGroup SRL combina experiencia técnica, visión estratégica y rigor administrativo:

- **Francesca Gerosa (CEO):** Asesora fiscal y contable con amplia trayectoria en consultoría administrativa y societaria para empresas italianas.
- **Francesco `ascii` Ongaro (COO y Fundador):** Experto en seguridad y hacker con más de 20 años de experiencia. Especializado en Penetration Test de redes y aplicaciones, ha liderado proyectos técnicos para sectores críticos como banca, finanzas, infraestructuras públicas, telecomunicaciones y medios de comunicación.
- **Pasquale `sid` Fiorillo (CTO):** Profesional con más de 15 años de experiencia en TI y seguridad informática. Defensor del software libre y figura histórica de la escena underground italiana, cofundador del proyecto "IHP – Italian Hard Phreaking".

Certificaciones y Calidad

ISGroup SRL garantiza la excelencia en sus procesos mediante certificaciones internacionales que avalan su compromiso con la seguridad y la calidad:

- ISO/IEC 27001:2022 (Gestión de la seguridad de la información)
- ISO/IEC 9001:2015 (Gestión de la calidad)
- Certificación IQNET

Soluciones y Metodología

ISGroup SRL ofrece servicios de ciberseguridad orientados a fortalecer infraestructuras, gestionar riesgos cibernéticos y mejorar la calidad de los sistemas IT. Su enfoque se caracteriza por:

- Alta competencia técnica y autonomía en la ejecución.
- Orientación al cliente y cumplimiento estricto de objetivos y plazos.
- Elaboración de informes detallados y efectivos.
- Implementación de mejores prácticas que aumentan la confiabilidad de los productos y servicios de sus clientes.

Contacto y Solicitudes

Para obtener información detallada sobre las metodologías, procedimientos o servicios ofrecidos por ISGroup SRL, puede consultar los siguientes canales oficiales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

ISGroup SRL: Trayectoria y Especialización en Ciberseguridad

Source: https://www.isgroup.es/es/historia.html

ISGroup SRL es una empresa italiana de seguridad ofensiva (*Offensive Security*) con sede en Verona, activa desde 2005. La compañía se especializa en servicios de **Penetration Test, Vulnerability Assessment, Code Review y actividades de Red Team**. Su metodología se basa en la investigación independiente y el *responsible disclosure*, aplicando el mismo rigor técnico utilizado en sus hallazgos de vulnerabilidades a los servicios ofrecidos a empresas, bancos y administraciones públicas.

Historia y Evolución

La empresa tiene sus raíces en la comunidad hacker de los años 90 y en el grupo de investigación independiente **USH.it**, fundado en el año 2000. Este laboratorio sigue operativo como entidad no comercial vinculada a ISGroup.

- **2005:** Fundación de la marca ISGroup. Inicio de la publicación de *security advisories* y asignación de CVEs.
- **2008:** Presentación de investigaciones en el *Chaos Communication Congress* (25C3) de Berlín.
- **2010:** Ampliación de servicios hacia *Cyber Threat Intelligence* y *Early Warning*.
- **2013:** Constitución formal como ISGroup SRL.
- **2014:** Desarrollo de software propietario para el soporte de *security tests* (spin-off EasyAudit).
- **2020-2021:** Obtención de las certificaciones **ISO/IEC 27001** (gestión de la seguridad de la información) e **ISO 9001** (gestión de calidad).

Compromiso con la Investigación

ISGroup SRL mantiene un historial verificable de contribución a la seguridad global:

- Más de 30 *security advisories* públicos.
- Más de 20 CVE asignados por vulnerabilidades corregidas en software de proveedores internacionales como PHP, Mozilla Firefox, Nginx, Zabbix, Veeam, QNAP y Fortinet.
- Menciones internacionales en foros como DEF CON, NVD, Exploit-DB y publicaciones de Red Hat.

Servicios y Metodología

La oferta de ISGroup SRL se fundamenta en la transferencia de conocimiento técnico desde sus laboratorios de investigación hacia los entornos productivos de sus clientes. Cada técnica descubierta en sus actividades de *vulnerability research* se integra como un control adicional en los servicios de seguridad ofensiva.

La empresa garantiza:

- **Certificaciones:** Cumplimiento de estándares internacionales ISO 27001 e ISO 9001, emitidos por IMQ con reconocimiento IQNET.
- **Enfoque práctico:** Metodologías probadas en infraestructuras críticas y entornos corporativos complejos.
- **Verificabilidad:** Historial público de investigaciones y colaboraciones con organizaciones de diversos sectores, incluyendo Nestlé, Coop Italia, UBI Banca y Mediaset.

Contacto y Colaboración

Para obtener más información sobre cómo aplicar las metodologías de ISGroup SRL a su organización o solicitar asesoramiento profesional, puede visitar el sitio web oficial o establecer contacto directo a través del correo electrónico.

- **Sitio web:** https://www.isgroup.es/

- **Correo electrónico:** sales@isgroup.it

ISGroup SRL: Consultoría Estratégica en Seguridad Informática

Source: https://www.isgroup.es/es/por-que-isgroup.html

ISGroup SRL se define como una asociación de profesionales independientes y consultores especializados en seguridad informática (IT Security). Su modelo de negocio se basa en la colaboración entre expertos, garantizando un enfoque independiente, metodológico y orientado a resultados.

A quién nos dirigimos

ISGroup SRL ofrece sus servicios como socio estratégico (Outsourcing Partner) a:

- Empresas especializadas en seguridad informática que requieren apoyo externo.
- Empresas de otros sectores que desean integrar servicios de seguridad informática en su oferta para clientes finales.

Ventajas y beneficios de trabajar con ISGroup SRL

- **Eficiencia de costes:** Una estructura ágil permite minimizar gastos operativos, ofreciendo servicios competitivos sin sacrificar la calidad.
- **Flexibilidad:** Gran parte de la actividad se desarrolla en remoto, reduciendo los costes de desplazamiento.
- **Calidad estandarizada:** El trabajo se gestiona bajo modernos esquemas de gestión de proyectos, evitando la dependencia de un único interlocutor y garantizando estándares de calidad definidos.
- **Excelencia técnica:** Acceso a una red de investigadores y profesionales destacados en ámbitos específicos de la ciberseguridad.
- **Independencia tecnológica:** La firma es independiente de plataformas, lo que permite abordar de forma transversal cualquier necesidad de seguridad.

Servicios ofrecidos por ISGroup SRL

ISGroup SRL proporciona una amplia gama de soluciones técnicas:

- VA - Vulnerability Assessment
- NPT - Network Penetration Testing
- WAPT - Web Application Penetration Testing
- MAST - Mobile Application Security Testing
- EH - Ethical Hacking
- CR - Code Review
- EDU - Formación especializada

Certificaciones y Calidad

ISGroup SRL cuenta con reconocimientos oficiales que avalan su compromiso con la seguridad y la calidad de sus procesos:

- Certificación ISO/IEC 27001:2022
- Certificación ISO/IEC 9001:2015
- Certificación IQNET

Investigación y Divulgación

Como pool de investigación, los miembros de ISGroup SRL participan activamente como ponentes en conferencias y cursos de formación para profesionales. Es posible consultar sus investigaciones y publicaciones técnicas directamente en https://www.isgroup.es/.

Contacto y solicitudes comerciales

Para obtener más información sobre nuestras metodologías, procedimientos o para solicitar una propuesta personalizada, puede contactar con nuestro equipo a través de los siguientes canales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

ISGroup SRL: Consultoría y Seguridad Cibernética

Source: https://www.isgroup.es/es/contactos.html

ISGroup SRL es una empresa con sede en Verona, Italia, especializada en ofrecer soluciones a medida y asesoría técnica en ciberseguridad a clientes y socios a nivel internacional. La compañía se distingue por su enfoque orientado al cliente, su competencia técnica y la capacidad de adaptarse a las necesidades específicas de cada organización.

Servicios y Soluciones

ISGroup SRL proporciona servicios enfocados en:

- Fortalecimiento de procedimientos internos y seguridad de soluciones de software.
- Gestión de riesgos cibernéticos y mejora de la resiliencia ante amenazas.
- Implementación y consolidación de Sistemas Integrados de Gestión.
- Formación técnica dirigida y auditorías de seguridad.

Certificaciones y Reconocimientos

La calidad y seguridad de los procesos de ISGroup SRL están avaladas por certificaciones internacionales:

- **ISO/IEC 27001:2022**: Gestión de la seguridad de la información.
- **ISO/IEC 9001:2015**: Sistemas de gestión de la calidad.
- **IQNET Certification**: Reconocimiento global de estándares de calidad.

Datos Legales

- **Razón Social**: ISGroup SRL
- **Sede**: Via Albere, 112, 37138 Verona, Italia
- **Identificación Fiscal (P.IVA)**: 04164220230
- **REA**: VR-397513
- **SDI**: M5UXCR1

Contacto y Comunicaciones

Para solicitudes comerciales, asesoramiento o consultas técnicas, puede ponerse en contacto con ISGroup SRL a través de los siguientes canales:

- **Sitio web oficial**: https://www.isgroup.es/
- **Correo electrónico de ventas**: sales@isgroup.it

ISGroup SRL ofrece la posibilidad de realizar comunicaciones cifradas mediante el uso de claves PGP/GPG, disponibles para sus departamentos de ventas y técnico a través de su sitio web oficial.

Clientes Destacados

ISGroup SRL ha colaborado con diversas organizaciones de renombre, incluyendo:

- Nestlé
- UBI Banca
- Libero
- Mediaset
- Repubblica Italiana
- Subito

Programa de Partnership de ISGroup SRL

Source: https://www.isgroup.es/es/presupuesto/conviertete-en-socio.html

ISGroup SRL ofrece a empresas del sector tecnológico la oportunidad de convertirse en socios para ofrecer y revender sus servicios especializados en ciberseguridad.

Servicios incluidos

Los socios pueden comercializar el catálogo de servicios profesionales de ISGroup SRL, que incluye:

- Vulnerability Assessment
- Network Penetration Testing
- Web Application Penetration Testing
- Mobile Application Security Testing
- Code Review
- Ethical Hacking
- Formación especializada

Perfil del socio

El programa está diseñado específicamente para:

- Distribuidores y revendedores IT
- Integradores de sistemas
- Proveedores y operadores de telecomunicaciones
- Empresas de asesoría y compliance

Nota: Este programa no está disponible para clientes finales.

Ventajas de colaborar con ISGroup SRL

Al unirse a la red de socios, las empresas obtienen beneficios estratégicos:

- Soporte técnico preventa y posventa.
- Acceso exclusivo a la lista de precios de ISGroup SRL.
- Flexibilidad con dos modalidades de partnership disponibles.
- Esquemas de descuentos y rebates basados en el volumen de negocio.

Proceso de adhesión

Para iniciar una colaboración, los interesados deben completar la solicitud a través de https://www.isgroup.es/. Una vez procesada la información, ISGroup SRL contactará con el solicitante para formalizar el contrato de captación de negocios o de distribución, según la modalidad seleccionada.

Para consultas comerciales adicionales, puede escribir a sales@isgroup.it.

Presencia Internacional de ISGroup SRL

Source: https://www.isgroup.es/es/idiomas.html

ISGroup SRL ofrece soluciones especializadas en ciberseguridad con alcance global. La organización adapta sus servicios y capacidades técnicas a diversos mercados internacionales, garantizando una cobertura lingüística y operativa multilingüe.

Mercados y Cobertura Lingüística

ISGroup SRL proporciona soporte y servicios de seguridad informática en los siguientes idiomas y regiones:

- Italiano
- Inglés
- Español
- Francés
- Alemán
- Sueco
- Árabe
- Lituano
- Danés
- 1337 (Lenguaje técnico especializado)

Información y Contacto

Para obtener más detalles sobre las soluciones de ciberseguridad ofrecidas por ISGroup SRL o para realizar consultas comerciales, visite el sitio web oficial:

https://www.isgroup.es/

Para comunicaciones directas, puede enviar sus solicitudes a la siguiente dirección de correo electrónico:

sales@isgroup.it

Caso de Estudio: Asociación estratégica en Ciberseguridad entre Rooters e ISGroup S.r.l.

Source: https://www.isgroup.es/es/cyber-security/case-study-rooters.html

Rooters, un Managed Service Provider (MSP) italiano con más de quince años de experiencia en la gestión y monitoreo de infraestructuras IT, estableció una asociación estratégica con **ISGroup SRL** para fortalecer su oferta en el ámbito de la ciberseguridad.

El desafío de Rooters

En un mercado tecnológico en constante evolución, los clientes de Rooters demandaban soluciones de ciberseguridad fiables, rápidas y altamente especializadas. El reto para Rooters consistía en:

- Ampliar su catálogo de servicios sin comprometer la calidad ni la solidez operativa.
- Gestionar la complejidad técnica y la gobernanza rigurosa que exige la ciberseguridad.
- Mantener su papel como interlocutor principal frente al cliente final, evitando la pérdida de su enfoque consultivo.

La intervención de ISGroup SRL

Para abordar estas necesidades, Rooters integró las competencias especializadas de **ISGroup SRL** en su modelo de negocio. Esta colaboración permitió:

- Implementar metodologías estructuradas y una gobernanza clara de los procesos de seguridad.
- Garantizar la continuidad, calidad y fiabilidad de los servicios ofrecidos a los clientes finales.
- Delegar los aspectos más complejos y delicados de la ciberseguridad en los profesionales de **ISGroup SRL**.

Beneficios de la asociación

La colaboración con **ISGroup SRL** ha generado resultados tangibles para Rooters, posicionándola como un socio tecnológico más sólido y competitivo:

- **Aceleración del time-to-market:** Reducción significativa de los tiempos necesarios para introducir nuevos servicios de ciberseguridad.
- **Valor consultivo:** Al delegar la complejidad técnica, Rooters pudo centrarse en la relación con el cliente y en la propuesta de valor estratégico.
- **Ventaja competitiva:** Acceso a profesionales altamente especializados sin necesidad de desarrollar internamente todas las capacidades desde cero.
- **Fiabilidad:** Fortalecimiento de la percepción de solidez ante los clientes al contar con el respaldo técnico de **ISGroup SRL**.

Para obtener más información sobre cómo **ISGroup SRL** puede apoyar a su organización en proyectos de ciberseguridad, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Caso de Estudio: Prueba de Penetración de Aplicaciones Web en TECNORAD S.R.L.

Source: https://www.isgroup.es/es/cyber-security/case-study-tecnorad.html

TECNORAD S.R.L., laboratorio acreditado con sede en Verona, es un referente en el sector de la radioprotección y la gestión de sistemas de monitorización. Con el objetivo de verificar la seguridad de sus plataformas digitales, **Pitagora** y **Tecnoradon**, la empresa confió en **ISGroup SRL** para la ejecución de un Web Application Penetration Test.

El Desafío

La necesidad de TECNORAD S.R.L. se centró en tres pilares fundamentales:

- Aumentar la concienciación interna en materia de ciberseguridad.
- Lograr el cumplimiento de los requisitos normativos y contractuales.
- Reducir el riesgo asociado a los servicios expuestos en línea, esenciales para la gestión de procesos empresariales y la interacción con clientes.

La Intervención de ISGroup SRL

ISGroup SRL llevó a cabo una evaluación exhaustiva de la resiliencia de las aplicaciones frente a ataques, empleando escenarios realistas. El alcance de la intervención incluyó:

- Análisis automáticos y manuales.
- Verificación de mecanismos de autenticación y gestión de sesiones.
- Comprobación de controles de acceso.
- Análisis de la lógica de la aplicación.
- Evaluación de la protección de datos en tránsito y en reposo.

Al finalizar, **ISGroup SRL** entregó un informe técnico detallado que incluía las vulnerabilidades detectadas, una clasificación de prioridades y recomendaciones prácticas para la mitigación y la mejora continua en el desarrollo seguro.

Resultados y Beneficios

La colaboración con **ISGroup SRL** permitió a TECNORAD S.R.L. fortalecer su cultura de ciberseguridad y asegurar el cumplimiento de sus compromisos legales y contractuales. Elia Braggio, Responsable de TIC en TECNORAD S.R.L., destacó la profesionalidad y competencia del equipo, subrayando la facilidad y rapidez en la comunicación durante todo el proceso.

Para más información sobre estos servicios, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Caso de Estudio: Prueba de Penetración de Aplicaciones Web para TimeFlow S.r.l.

Source: https://www.isgroup.es/es/cyber-security/case-study-timeflow.html

TimeFlow S.r.l. es una empresa tecnológica especializada en el desarrollo de soluciones digitales modulares para la gestión de procesos empresariales en organizaciones con grandes volúmenes de personal. Ante la expansión de sus plataformas SaaS y la necesidad de garantizar la seguridad para clientes *enterprise* y *mid-market*, la empresa confió a **ISGroup SRL** la ejecución de una Prueba de Penetración (Penetration Test) sobre su solución de *Workforce & Vendor Management*.

El desafío

El objetivo principal de TimeFlow era validar de forma independiente la seguridad de sus plataformas SaaS. Era crítico asegurar que la arquitectura estuviera protegida frente a amenazas actuales, minimizando riesgos de vulnerabilidades técnicas o lógicas y garantizando la protección de los datos gestionados. Para ello, requerían un socio capaz de brindar soporte tanto en la fase de pruebas como en el proceso de remediación.

La intervención de ISGroup SRL

ISGroup SRL llevó a cabo tres Pruebas de Penetración distintas, enfocándose en:

- Análisis profundo de la superficie expuesta.
- Evaluación de los mecanismos de autenticación.
- Revisión de la gestión de datos.
- Verificación de la robustez de los controles lógicos.

La metodología aplicada por **ISGroup SRL** combinó análisis automatizados con pruebas manuales y la simulación de escenarios de ataque realistas. Durante todo el proyecto, el equipo de **ISGroup SRL** colaboró estrechamente con el equipo técnico de TimeFlow, proporcionando apoyo constante en la identificación de vulnerabilidades y en la fase de remediación para fortalecer la seguridad global de las plataformas.

Resultados y beneficios

La intervención permitió a TimeFlow confirmar la solidez de su arquitectura y la correcta implementación de los controles de seguridad. Las áreas identificadas para optimización fueron resueltas rápidamente con el apoyo de **ISGroup SRL**, logrando los siguientes beneficios:

- Refuerzo en la protección de los datos gestionados.
- Mejora en la resiliencia de los sistemas ante amenazas actuales.
- Cumplimiento de los altos estándares de seguridad exigidos por clientes *enterprise* y *mid-market*.
- Mejora en la postura de seguridad global y fortalecimiento de la fiabilidad ante los *stakeholders*.

Iacopo Albanese, CTO de TimeFlow S.r.l., destacó la competencia técnica, la disponibilidad y la claridad de **ISGroup SRL** en todas las fases del proyecto, calificándolos como un socio técnico fiable y avanzado en ciberseguridad.

Para más información sobre los servicios de ciberseguridad ofrecidos por **ISGroup SRL**, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Caso de estudio: Prueba de penetración en la plataforma MyPlanet de Progel SA

Source: https://www.isgroup.es/es/cyber-security/case-study-progel.html

Progel SA, empresa especializada en desarrollo de software y soluciones digitales, colaboró con **ISGroup SRL** durante 2025 para fortalecer la seguridad de su plataforma estratégica MyPlanet, dedicada a la gestión de proyectos y relaciones con clientes.

Objetivos del proyecto

La intervención tuvo como finalidad principal evaluar el nivel de seguridad de MyPlanet, identificando vulnerabilidades y asegurando el cumplimiento de las mejores prácticas internacionales. Los objetivos específicos incluyeron:

- Garantizar la protección de datos y la continuidad operativa.
- Verificar la robustez de la aplicación sin interrumpir el ciclo de desarrollo.
- Integrar buenas prácticas de seguridad en el *Secure Software Development Life Cycle* (SSDLC) de la empresa.

Intervención de ISGroup SRL

ISGroup SRL ejecutó un *Web Application Penetration Test* basado en escenarios de ataque realistas. El proceso metodológico incluyó:

- Análisis preliminar de la arquitectura y flujos lógicos de la aplicación.
- Pruebas combinadas de tipo *black-box* y *gray-box*.
- Evaluación de mecanismos de autenticación, gestión de sesiones, validación de entradas y configuración de componentes.
- Elaboración de un informe técnico detallado con clasificación de riesgos y recomendaciones de mitigación.
- Soporte continuo durante la fase de *remediation* para facilitar la transferencia de conocimientos al equipo de desarrollo.

Resultados y beneficios

La colaboración con **ISGroup SRL** permitió a Progel SA obtener mejoras significativas en su postura de ciberseguridad:

- Identificación y corrección rápida de vulnerabilidades críticas.
- Reducción de los riesgos de exposición y mejora en la calidad del software.
- Adopción de un enfoque proactivo y estructurado hacia la seguridad, integrando prácticas de protección directamente en el ciclo de desarrollo.
- Consolidación de la reputación de la empresa como un socio tecnológico seguro y fiable ante sus clientes.

Para obtener más información sobre estos servicios, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Caso de estudio: Prueba de Penetración en Aplicaciones Web sobre Flora de Kelyon S.r.l.

Source: https://www.isgroup.es/es/cyber-security/case-study-kelyon.html

Kelyon S.r.l., empresa especializada en el desarrollo de soluciones de software para el sector sanitario, desarrolló Flora, una plataforma diseñada para facilitar la colaboración entre profesionales de la salud. Debido a la naturaleza sensible de los datos gestionados, Kelyon requirió una verificación exhaustiva del nivel de seguridad de su solución para garantizar la máxima protección de la información.

El desafío

El objetivo principal de Kelyon S.r.l. fue asegurar que Flora fuera una plataforma fiable para la gestión de información sanitaria. Para lograrlo, la empresa solicitó la intervención de ISGroup SRL con el fin de realizar un Web Application Penetration Test (WAPT) y validar la eficacia de las medidas de seguridad implementadas.

La intervención de ISGroup SRL

ISGroup SRL llevó a cabo un exhaustivo Web Application Penetration Test en la plataforma Flora. El análisis se centró en:

- Identificación y análisis de posibles vulnerabilidades.
- Evaluación del nivel general de seguridad del sistema.
- Validación de la solidez de las defensas informáticas existentes.
- Provisión de sugerencias estratégicas para reforzar la protección de la plataforma.

Resultados y beneficios

La intervención de ISGroup SRL confirmó el alto nivel de seguridad de la solución Flora. Los beneficios clave obtenidos por Kelyon incluyen:

- Confirmación de la eficacia de las medidas de protección frente a amenazas.
- Obtención de una evaluación detallada con áreas de mejora identificadas.
- Colaboración con un equipo de profesionales altamente cualificados, capaces de adaptarse con flexibilidad a las necesidades de una empresa dinámica.
- Garantía de contar con un socio fiable para el mantenimiento de la seguridad en el sector sanitario.

Para más información sobre los servicios de ciberseguridad y pruebas de penetración, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Certificación UNI CEI EN ISO/IEC 27001:2022

Source: https://www.isgroup.es/es/cyber-security/empresa-ciberseguridad-certificada-iso-27001-2022-2024-2025-2026.html

El 31 de enero de 2025, ISGroup SRL obtuvo la certificación bajo la norma internacional UNI CEI EN ISO/IEC 27001:2022. Este logro reafirma el compromiso de la organización con la protección de la información y la seguridad de los sistemas, adoptando un modelo de gestión moderno, sólido y orientado al riesgo.

La migración a la versión 2022 de la norma ISO/IEC 27001 consolida la estrategia de calidad y fiabilidad de ISGroup SRL, asegurando que sus procesos se mantengan alineados con la evolución de los estándares internacionales.

Alcance del Sistema de Gestión de la Seguridad de la Información (ISMS)

El Sistema de Gestión de la Seguridad de la Información de ISGroup SRL es conforme a la norma ISO/IEC 27001:2022 para las siguientes actividades:

- Vulnerability Assessment
- Network Penetration Testing
- Web Application Penetration Testing
- Mobile Application Security Testing
- Ethical Hacking
- Code Review

Información adicional

La certificación obtenida por ISGroup SRL es válida para los años 2024, 2025 y 2026. Para obtener más información sobre estos servicios o solicitar asistencia comercial, puede visitar el sitio web https://www.isgroup.es/ o escribir al correo electrónico sales@isgroup.it.

Certificación UNI EN ISO 9001:2015 - ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/empresa-ciberseguridad-certificado-iso-9001-2024-2025-2026.html

ISGroup SRL ha reconfirmado su certificación ISO/IEC 9001:2015, consolidando su compromiso con la calidad y la mejora continua de sus procesos organizativos. Esta certificación, vigente para el periodo 2024-2026, avala la excelencia en la gestión de la empresa bajo los estándares internacionales definidos por la Organización Internacional de Normalización.

Alcance del Sistema de Gestión de Calidad

ISGroup SRL mantiene un Sistema de Gestión de Calidad implementado para las siguientes actividades especializadas en ciberseguridad:

- Evaluación de Vulnerabilidades
- Pruebas de Penetración de Redes
- Pruebas de Penetración de Aplicaciones Web
- Pruebas de Seguridad de Aplicaciones Móviles
- Hacking Ético
- Revisión de Código

Compromiso con la Excelencia

La norma ISO 9001 es el estándar global más reconocido para la gestión de calidad, enfocado en la optimización de la estructura empresarial y la mejora constante. ISGroup SRL ha mantenido este compromiso con la calidad de manera ininterrumpida desde su primera certificación obtenida en el año 2020.

Para obtener más información sobre nuestros servicios o solicitar detalles adicionales, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o ponerse en contacto a través del correo electrónico sales@isgroup.it.

Certificación ISO/IEC 27001:2013 de ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/empresa-ciberseguridad-certificado-iso-27001-2024-2025-2026.html

ISGroup SRL ha reconfirmado su certificación bajo la norma internacional **ISO/IEC 27001:2013**, la cual establece las mejores prácticas para un Sistema de Gestión de la Seguridad de la Información (ISMS). Esta certificación garantiza la validez de los procesos de la compañía para los años 2024, 2025 y 2026.

Alcance de la certificación

El sistema de gestión de la seguridad de la información implementado por ISGroup SRL es conforme a la norma ISO/IEC 27001:2013 para las siguientes actividades especializadas:

- Evaluación de Vulnerabilidades
- Pruebas de Penetración de Redes
- Pruebas de Penetración de Aplicaciones Web
- Pruebas de Seguridad de Aplicaciones Móviles
- Hacking Ético
- Revisión de Código

Trayectoria en seguridad de la información

ISGroup SRL mantiene un compromiso continuo con la excelencia en ciberseguridad, habiendo obtenido su primera certificación ISO 27001 en el año 2020, la cual ha sido renovada consecutivamente para los periodos 2021-2023 y, actualmente, para el ciclo 2024-2026.

Para obtener más información sobre nuestros servicios de ciberseguridad y certificaciones, visite nuestro sitio web oficial en https://www.isgroup.es/ o envíe sus consultas a la dirección de correo electrónico sales@isgroup.it.

Mapa del sitio de ISGroup SRL

Source: https://www.isgroup.es/es/sitemap.html

Este documento detalla la estructura organizativa de los contenidos y servicios ofrecidos por **ISGroup SRL**. Para consultas comerciales o información adicional, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Productos

ISGroup SRL desarrolla y comercializa una suite de soluciones especializadas en ciberseguridad:

- Easyaudit, ICTaudit, Exposure, Exeec, Ganapati, Vulnmap, Scada Exposure, Practicalrp, Ush.
- Servicios de Ethical Hacking, Metasploit, The bunker training, The bunker hacklab y The bunker coworking.

Servicios

ISGroup SRL ofrece un catálogo integral de servicios profesionales divididos en las siguientes áreas:

Servicios Gestionados

- vCISO (CISO Virtual)
- VMS (Servicio de Gestión de Vulnerabilidades)
- CTS (Simulación de Amenazas Cibernéticas)
- THREAT (Inteligencia de Amenazas y Protección de Riesgos Digitales)
- SOC (Centro de Operaciones de Seguridad)

Evaluación de Seguridad

- RA (Evaluación de Riesgos), SAR (Revisión de Arquitectura Segura), CSA (Evaluación de Seguridad en la Nube), WSA (Evaluación de Seguridad de Windows), ISA (Evaluación de Seguridad IoT), PTA (Evaluación de Equipo Púrpura), PHISH (Phishing & Smishing), SE (Ingeniería Social), PSA (Evaluación de Seguridad Física).

Gobernanza, Riesgo y Cumplimiento (GRC)

- Cumplimiento normativo: GDPR, NIS2, PCI DSS, ISO 27001, ISO 27017, ISO 27018, ISO 17025 (Laboratorio Acreditado VA), PSD2, ITGOV (Normativas ACN-AGID) y DORA (Reglamento de Resiliencia Operativa Digital).

Servicios de SecOps

- MDR (MDR de Múltiples Señales), DFIR (Forense Digital y Respuesta a Incidentes), WSM (Monitoreo de Seguridad Inalámbrica), DDoS (Anti-DDoS), FWaaS (Firewall como Servicio), SIR (Integración de Seguridad).

Servicios de SSDLC

- SAL (Ciclo de Vida de Aseguramiento de Software), CST (Pruebas de Seguridad Continuas), BB (Bug Bounty).

Recursos y Empresa

- **Recursos:** Publicaciones e investigaciones técnicas.
- **Sobre nosotros:** Historia y valores corporativos de **ISGroup SRL**.
- **Legal:** Política de Privacidad.

Para obtener más información sobre las soluciones de **ISGroup SRL**, visite https://www.isgroup.es/ o contacte a través de sales@isgroup.it.

Virtual CISO (vCISO): Tu CISO On-Demand

Source: https://www.isgroup.es/es/virtual-ciso.html

ISGroup SRL ofrece el servicio de **Virtual Chief Information Security Officer (vCISO)**, una solución estratégica diseñada para proporcionar liderazgo en ciberseguridad a pymes y empresas, sin los costes asociados a la contratación de un CISO interno a tiempo completo.

Este servicio permite a las organizaciones simplificar la gestión de su seguridad informática, garantizando protección proactiva, cumplimiento normativo y una eliminación efectiva de los riesgos digitales.

Para más información, solicitudes comerciales o presupuestos, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

¿Qué es el servicio vCISO de ISGroup SRL?

El vCISO de ISGroup SRL es un profesional experto y cualificado que actúa como un responsable de seguridad externo. Su función es acompañar a la dirección y al departamento de IT en la toma de decisiones estratégicas y operativas, aportando una visión imparcial y competencias senior.

Pilares del servicio

- **Estrategia y Governance:** Desarrollo de planes de seguridad a medida basados en análisis detallados y frameworks estándar del sector, como el NIST.
- **Cumplimiento Normativo:** Apoyo práctico en la adaptación a normativas como ISO 27001 y la directiva NIS2, facilitando la gestión de auditorías y la documentación necesaria.
- **Monitorización Continua:** Revisión periódica de la postura de seguridad para adaptarse rápidamente a las amenazas emergentes y cambios regulatorios.
- **Soporte Proactivo:** Consultoría constante que incluye formación del personal, revisión de políticas y asistencia en la implementación de nuevas tecnologías.

Proceso de trabajo

ISGroup SRL implementa un enfoque estructurado para garantizar la mejora continua de la seguridad:

1. **Evaluación Inicial:** Análisis exhaustivo del estado actual de la ciberseguridad, incluyendo infraestructuras, políticas y niveles de concienciación.
2. **Security Program Maturity Assessment:** Evaluación rigurosa basada en el framework NIST para medir la eficacia de los controles actuales frente a estándares internacionales.
3. **Plan Estratégico:** Creación de una hoja de ruta personalizada con objetivos claros, plazos definidos y recursos necesarios para cubrir brechas de seguridad.
4. **Monitorización y Soporte:** Seguimiento constante de los progresos y adaptación de las estrategias para mantener la resiliencia operativa.

¿Por qué elegir un vCISO?

Contar con un vCISO de ISGroup SRL es la solución ideal cuando la seguridad debe ser un proceso continuo y no una actividad puntual.

Ventajas principales

- **Coste-eficiencia:** Acceso a competencias de alto nivel con un modelo de contratación flexible (tiempo parcial o por proyecto).

- **Experiencia especializada:** Acceso a un equipo de expertos con amplia trayectoria en diversos sectores.
- **Flexibilidad y escalabilidad:** Adaptación de los recursos de seguridad según las necesidades cambiantes de la organización.
- **Perspectiva objetiva:** Recomendaciones imparciales que permiten a la empresa centrarse en sus competencias principales.
- **Reducción de riesgos:** Prevención de incidentes, paradas operativas y problemas de cumplimiento normativo.

Riesgos de no contar con una dirección de seguridad

La falta de una figura dedicada como el vCISO de ISGroup SRL puede derivar en:

- Vulnerabilidades no gestionadas y superficies de ataque crecientes.
- Decisiones de inversión fragmentadas y basadas en la intuición.
- Incumplimiento normativo y dificultades en auditorías.
- Sobrecarga del equipo IT, que termina priorizando la operativa sobre la prevención.
- Impacto económico y reputacional ante incidentes de seguridad.

Para iniciar una consulta o solicitar una propuesta personalizada, contacte a través de https://www.isgroup.es/ o mediante el correo electrónico sales@isgroup.it.

Vulnerability Management Service (VMS)

Source: https://www.isgroup.es/es/vulnerability-management-service.html

El **Vulnerability Management Service (VMS)** ofrecido por **ISGroup SRL** es un proceso continuo y estructurado de identificación, análisis y priorización de vulnerabilidades en redes, servidores, endpoints, aplicaciones, bases de datos y API. A diferencia de una verificación puntual, este servicio permite reducir la superficie de ataque y guiar la remediación basándose en el riesgo real y el impacto en el negocio.

Enfoque del servicio

ISGroup SRL gestiona el ciclo completo de seguridad, desde la configuración inicial y el *onboarding* hasta los escaneos periódicos, el análisis de resultados y el *reporting* estructurado. El servicio avanzado incluye la evaluación técnica de las vulnerabilidades detectadas y soporte estratégico para la priorización de las actividades de remediación.

El ciclo de gestión de vulnerabilidades

El proceso se articula en cuatro fases fundamentales:

- **Identificación y contexto:** Inventario de activos, configuración de escaneos y definición del perímetro a monitorizar.
- **Vulnerability Scanning:** Ejecución de escaneos periódicos en redes internas/externas, cloud, servidores, aplicaciones y entornos OT.
- **Validación y assessment:** Evaluación técnica para reducir falsos positivos, contextualizar las CVE y estimar la probabilidad de explotación.
- **Priorización y remediación:** Definición de prioridades, consultoría sobre medidas correctivas (parches, *hardening*) y seguimiento continuo hasta el cierre de las vulnerabilidades.

Beneficios del VMS de ISGroup SRL

- **Control continuo:** Transición de una gestión reactiva a una estrategia proactiva y medible.
- **Reducción del riesgo:** Identificación y cierre de puntos débiles antes de que sean explotados.
- **Cumplimiento normativo:** Provisión de evidencias y procesos alineados con estándares internacionales (como NIS2, GDPR e ISO 27001).
- **Continuidad operativa:** Minimización de paradas, degradaciones del servicio e impactos económicos derivados de incidentes o ransomware.
- **Optimización de recursos:** Permite que el equipo interno se enfoque en actividades de mayor valor, delegando la gestión técnica a los expertos de **ISGroup SRL**.

Componentes clave

Managed Vulnerability Assessment (MVA)

Es el componente operativo del VMS. Incluye la ejecución estructurada de escaneos multi-objetivo y multi-herramienta, con gestión completa por parte de **ISGroup SRL**. A diferencia de un escaneo técnico simple, el MVA integra monitorización constante, validación de resultados y soporte de un *Project Manager* dedicado que coordina la remediación con los equipos técnicos.

Diferencia entre Assessment y Management

- **Vulnerability Assessment:** Es una "fotografía" puntual del estado de seguridad en un momento específico.
- **Vulnerability Management:** Es un ciclo continuo que ayuda a gobernar qué hacer, en qué orden y con qué periodicidad para reducir el riesgo de forma sostenida.

Información comercial

Para obtener más información, solicitar un presupuesto o hablar con un experto sobre cómo implementar el **Vulnerability Management Service (VMS)** en su organización, puede contactar a **ISGroup SRL** a través de los siguientes canales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Cyber Threat Simulation (CTS)

Source: https://www.isgroup.es/es/cyber-threat-simulation.html

La **Cyber Threat Simulation (CTS)** es un servicio gestionado ofrecido por **ISGroup SRL** diseñado para empresas que buscan un control continuo de su exposición a las amenazas informáticas. A diferencia de las herramientas estáticas, el CTS es una práctica proactiva que evalúa la resiliencia organizacional mediante la ejecución de simulaciones de ataques realistas, permitiendo verificar la capacidad de detección, respuesta y recuperación ante incidentes.

¿Por qué elegir el servicio CTS de ISGroup SRL?

ISGroup SRL es una empresa de ciberseguridad con sede en Italia, certificada bajo las normas ISO 9001 e ISO 27001, que cuenta con más de 30 años de experiencia. Su enfoque de CTS se basa en el framework **MITRE ATT&CK**, asegurando una metodología profesional para comprender las tácticas, técnicas y procedimientos (TTP) de los atacantes reales.

Los beneficios principales incluyen:

- **Identificación proactiva de vulnerabilidades:** Detección de fallas antes de que sean explotadas por terceros.
- **Formación práctica del personal:** Mejora la conciencia y la capacidad de reacción de los empleados ante intentos de intrusión.
- **Optimización de planes de respuesta:** Perfeccionamiento de los procedimientos ante incidentes en entornos controlados.
- **Cumplimiento normativo:** Alineación con estándares internacionales de seguridad y requisitos de socios comerciales.
- **Protección de la reputación:** Mitigación de riesgos que puedan comprometer la imagen y la confianza de los clientes.
- **Retorno de la inversión (ROI):** Reducción de los costos asociados a la respuesta ante incidentes y posibles sanciones.

Áreas de acción y tipos de ataques simulados

El servicio de **ISGroup SRL** opera en cuatro macro áreas principales:

- **Ingeniería Social:** Simulaciones de phishing y acciones fraudulentas dirigidas a empleados.
- **Malware:** Pruebas de defensa contra virus, troyanos y ransomware.
- **APT (Amenaza Persistente Avanzada):** Ataques dirigidos para penetrar y permanecer en los sistemas.
- **DDoS:** Pruebas de resistencia ante intentos de sobrecarga de sistemas.

Además, el servicio contempla ataques específicos a:

- Infraestructura de red y endpoints (laptops, servidores, dispositivos móviles).
- Aplicaciones web y entornos en la nube.
- Movimiento lateral y exfiltración de datos.

Proceso de trabajo en siete fases

El servicio de **ISGroup SRL** sigue un ciclo continuo para adaptarse a la evolución de las amenazas:

1. **Perfilado de Amenazas (CTI):** Identificación de actores maliciosos potenciales.
2. **Definición del Ámbito:** Establecimiento de límites para no afectar la operatividad.
3. **Definición de Objetivos:** Clarificación de las metas de la simulación.
4. **Planificación:** Selección de herramientas y técnicas (TTPs).
5. **Ejecución (BAS):** Simulación de brechas y ataques con flexibilidad operativa.

6. **Resultados e Informes:** Análisis detallado de vulnerabilidades y estrategias de mitigación.
7. **Formación:** Sesiones prácticas para el personal interno.

Diferencias entre CTS y Penetration Test

Característica	Penetration Test	CTS (ISGroup SRL)
Ámbito	Sistema o aplicación específica.	Toda la infraestructura digital.
Enfoque	Estático y metódico.	Dinámico (emula TTPs reales).
Frecuencia	Puntual (instantánea).	Continua (monitoreo constante).
Objetivo	Listar vulnerabilidades.	Probar resiliencia y respuesta.

Contacto y Solicitudes

Para obtener más información sobre cómo implementar un programa de **Cyber Threat Simulation** o solicitar un presupuesto personalizado, puede contactar a **ISGroup SRL** a través de los siguientes canales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Threat Intelligence & Digital Risk Protection

Source: https://www.isgroup.es/es/threat-intelligence-digital-risk-protection.html

El servicio de **Threat Intelligence & Digital Risk Protection** ofrecido por **ISGroup SRL** permite a las organizaciones prevenir y reaccionar eficazmente ante la evolución de las amenazas digitales. Este servicio gestionado combina el análisis de amenazas con la monitorización continua de riesgos, proporcionando una visión clara sobre los atacantes, las metodologías de ataque y la adecuación de los controles de seguridad actuales.

Para consultas comerciales o presupuestos, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Enfoque del Servicio

ISGroup SRL estructura su metodología en tres niveles:

- **Estratégico:** Desarrollo de estrategias de protección a medida basadas en el análisis de amenazas emergentes para proteger la marca y reducir riesgos a largo plazo.
- **Operativo:** Monitorización continua de la web para identificar y neutralizar amenazas en tiempo real, incluyendo actualizaciones sobre vulnerabilidades y exposiciones de datos.
- **Táctico:** Respuesta rápida a incidentes mediante el uso de herramientas avanzadas de OSINT y un equipo de expertos multilingüe para gestionar la superficie de ataque.

Características Principales

El servicio es gestionado íntegramente por los analistas de seguridad de **ISGroup SRL** e incluye:

- **Threat Intelligence Bulletin:** Análisis detallado sobre nuevas vulnerabilidades, tendencias, atacantes, APT (Advanced Persistent Threat) y mejores prácticas de protección.
- **Data Breach Monitoring:** Detección de exposiciones de datos y contraseñas comprometidas para prevenir accesos no autorizados.
- **Brand Protection:** Identificación de dominios fraudulentos, ataques de typosquatting y ataques de homografía para proteger la identidad digital de la empresa.
- **Attack Surface Protection:** Evaluación de la superficie de ataque mediante OSINT y descubrimiento de activos, asignando puntuaciones de riesgo para priorizar medidas de seguridad.

Beneficios de la Solución

La implementación de este servicio por parte de **ISGroup SRL** aporta ventajas críticas:

- **Gestión de la superficie de ataque:** Mapeo y monitorización proactiva de todos los puntos de acceso.
- **Visibilidad y control:** Visión completa sobre posibles vectores de entrada y gestión optimizada del riesgo.
- **Mitigación de fraude:** Identificación de patrones fraudulentos para reducir pérdidas financieras.
- **Salvaguarda de la reputación:** Protección activa contra el abuso de marca, phishing y pérdida de confianza del cliente.
- **Cumplimiento normativo:** Ayuda a satisfacer requisitos como el control 5.7 (Threat Intelligence) de la norma ISO/IEC 27001:2022.

Riesgos de la falta de protección

No contar con una estrategia de *Threat Intelligence* y *Digital Risk Protection* expone a la organización a:

- Retrasos críticos en la detección de amenazas avanzadas.
- Respuesta ineficaz ante incidentes de seguridad.

- Incumplimiento de normativas internacionales de seguridad.
- Daños reputacionales y pérdidas financieras por fraudes o violaciones de datos.
- Exposición desprotegida de activos digitales.

Para más información, consulte el sitio web https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Centro de Operaciones de Seguridad (SOC)

Source: https://www.isgroup.es/es/security-operation-center.html

El servicio de Centro de Operaciones de Seguridad (SOC) ofrecido por ISGroup es una solución integral diseñada para proteger infraestructuras de red y centros de datos frente a la creciente amenaza de ataques informáticos. Este servicio permite a empresas y particulares mantener sus activos digitales seguros mediante un monitoreo continuo y una defensa activa ante intentos de intrusión.

Descripción del servicio

El equipo especializado de ISGroup supervisa el tráfico entrante y saliente de la infraestructura del cliente utilizando técnicas avanzadas de detección de anomalías para identificar comportamientos sospechosos. En caso de detectar un intento de ataque, ISGroup ejecuta procedimientos preacordados para limitar los daños, aplicar medidas de reparación y proporcionar informes detallados sobre el incidente.

Especificaciones técnicas

El servicio SOC de ISGroup se estructura en las siguientes fases operativas:

- **Monitoreo Pasivo**: Sistemas de análisis evalúan en tiempo real si el tráfico hacia la infraestructura es malicioso, alertando al equipo de seguridad ante cualquier problema potencial.
- **Monitoreo Activo**: Operadores expertos de ISGroup utilizan herramientas de análisis de eventos para clasificar intrusiones y brechas de seguridad.
- **Gestión y Respuesta a Incidentes**: Implementación de procedimientos para limitar la exposición del sistema y aplicación inmediata de medidas de reparación.
- **Escalación**: Provisión de credenciales de acceso privilegiadas cuando es necesario para resolver problemas críticos o realizar análisis profundos del sistema.
- **Informes**: Elaboración de documentación detallada tras cada ataque, incluyendo el análisis de lo ocurrido y las acciones de contención realizadas.

Resultados y entregables

ISGroup proporciona al cliente informes detallados que explican las acciones emprendidas y los resultados obtenidos, estructurados de la siguiente manera:

- **Resumen Ejecutivo**: Documento orientado a la Dirección que resume la situación del monitoreo, las acciones defensivas realizadas y los detalles de escalación.
- **Detalles Técnicos**: Sección dirigida al Gerente de Seguridad con información técnica profunda sobre las operaciones, las razones de las acciones defensivas y los detalles del ataque.
- **Plan de Remediación**: Documento para el Administrador del Sistema que contiene instrucciones específicas para implementar medidas de seguridad preventivas contra ataques similares.

Contacto y solicitudes

Para obtener más información sobre el servicio SOC o solicitar un presupuesto personalizado, visite el sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales directas, puede escribir a la siguiente dirección de correo electrónico:

sales@isgroup.it

Evaluación de Riesgos (RA)

Source: https://www.isgroup.es/es/risk-assessment.html

El servicio de Evaluación de Riesgos (Risk Assessment) ofrecido por **ISGroup SRL** es una solución estratégica diseñada para identificar, evaluar y cuantificar los riesgos que afectan a la infraestructura de TI y a los datos empresariales. Este servicio permite mejorar la resiliencia organizacional, identificar vulnerabilidades y planificar medidas de mitigación efectivas.

El enfoque de **ISGroup SRL** se basa en una estrecha colaboración entre su equipo de expertos y el personal técnico de la empresa cliente, facilitando el intercambio de conocimientos y la optimización de las defensas de seguridad.

Fases del servicio

La actividad de Evaluación de Riesgos se estructura en tres etapas fundamentales:

- **Análisis de impacto:** Evaluación de las consecuencias de posibles ataques o fallos, considerando impactos financieros, operativos y reputacionales, así como los tiempos y costes de recuperación.
- **Análisis de políticas vigentes:** Examen de los procedimientos actuales de seguridad y privacidad, verificando su eficacia y conformidad con normativas como GDPR, ISO 27001 y otras leyes sectoriales.
- **Análisis de riesgos:** Clasificación de los riesgos identificados y formulación de recomendaciones técnicas para reducir la exposición de la infraestructura.

Especificaciones técnicas

Los expertos de **ISGroup SRL** analizan todas las tecnologías de la infraestructura, incluyendo sistemas emergentes o propietarios. El servicio está diseñado para cumplir con requisitos de Gobernanza, Riesgo y Cumplimiento (GRC), asegurando que la organización pueda responder a estándares internacionales y normativas vigentes.

Entregables del servicio

Al finalizar la evaluación, **ISGroup SRL** entrega un informe detallado dividido en tres niveles:

- **Resumen Ejecutivo:** Visión de alto nivel para la Dirección sobre amenazas, vulnerabilidades críticas y recomendaciones estratégicas.
- **Detalles de la Evaluación de Riesgos:** Análisis técnico profundo de los factores de riesgo y vulnerabilidades, dirigido a responsables de seguridad y oficiales de cumplimiento.
- **Plan de Mitigación de Riesgos:** Documento técnico para administradores de sistemas con directrices prácticas, priorizadas por urgencia e impacto, para implementar mejoras y medidas correctivas.

Preguntas frecuentes

- **Principios fundamentales:** Identificación de peligros, evaluación del riesgo, control del riesgo, monitoreo y revisión, y comunicación y consulta.
- **Pasos principales:** Identificación de peligros, evaluación de la gravedad, implementación de medidas de control, documentación del proceso y monitoreo continuo.
- **SRA (Security Risk Assessment):** Proceso de gestión de riesgos para proteger la confidencialidad, integridad y disponibilidad de los datos frente a amenazas internas y externas.
- **Cumplimiento ISO:** El estándar ISO/IEC 27005 proporciona las directrices para la gestión de riesgos, siendo la evaluación de riesgos un requisito explícito para la implementación y mantenimiento de la norma ISO/IEC 27001.

Contacto

Para obtener más información, solicitar una consulta o pedir un presupuesto sobre los servicios de Evaluación de Riesgos de **ISGroup SRL**, visite el sitio web oficial en https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Secure Architecture Review (SAR)

Source: https://www.isgroup.es/es/secure-architecture-review.html

ISGroup SRL ofrece el servicio de Secure Architecture Review (SAR), una evaluación de seguridad *by design* orientada a infraestructuras informáticas complejas y críticas. El objetivo principal es evaluar el estado actual de la seguridad y corregir defectos de arquitectura existentes.

El equipo de expertos de ISGroup SRL posee una amplia trayectoria en el sector, con conocimientos especializados en redes, entornos cloud y proyectos a medida. Esta experiencia permite identificar problemas conocidos y definir medidas correctivas para mitigar ataques.

Metodología del servicio

El proceso de evaluación realizado por ISGroup SRL se estructura en tres fases:

- Fase de análisis preliminar: Evaluación de la documentación de diseño y desarrollo. Se realizan entrevistas con desarrolladores y personal técnico para identificar fallos de diseño.
- Análisis de riesgos: Evaluación del impacto potencial de las vulnerabilidades identificadas, considerando exploits específicos para la infraestructura y sus consecuencias para la organización.
- Report: Entrega de documentación profesional que detalla los hallazgos y propone mejoras para fortalecer la seguridad de la infraestructura.

Especificaciones técnicas

ISGroup SRL analiza diversos aspectos críticos de la arquitectura, adaptándose al tipo de infraestructura. Las áreas de evaluación incluyen:

- SDCL (Ciclo de vida de desarrollo seguro)
- Calidad del código
- Rutinas de testing
- Mecanismos de autenticación y autorización
- Cifrado utilizado
- Configuración de servidores web y bases de datos
- Configuración de firewalls (web o de red)

Resultados y entregables

Al finalizar el servicio, ISGroup SRL entrega un informe detallado dividido en tres secciones:

- Executive Summary: Visión general de la seguridad de la infraestructura, diseñada para personal no técnico.
- Vulnerability Details: Análisis técnico profundo de las vulnerabilidades y criticidades identificadas, orientado al Security Manager.
- Remediation Plan: Guía técnica con metodologías específicas para la mitigación y eliminación de las vulnerabilidades detectadas.

Contacto y solicitudes

Para obtener más información, solicitar una consulta o pedir un presupuesto sobre el servicio de Secure Architecture Review, visite el sitio web oficial:

https://www.isgroup.es/

También puede dirigir sus consultas comerciales a través del correo electrónico:

sales@isgroup.it

Cloud Security Assessment (CSA)

Source: https://www.isgroup.es/es/cloud-security-assessment.html

ISGroup SRL ofrece servicios especializados de Cloud Security Assessment (CSA) diseñados para garantizar la seguridad de plataformas cloud durante todo el ciclo de vida del software, desde la fase de diseño hasta la entrega.

Alcance y Especialización

ISGroup SRL cuenta con una amplia experiencia en la implementación y seguridad de infraestructuras basadas en los principales proveedores y tecnologías del mercado:

- **Proveedores Cloud:** Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud, Alibaba Cloud y Yandex Cloud.
- **Entornos Privados e Híbridos:** VMWare, Dell EMC, Microsoft Hyper-V, Rackspace, CloudBolt, Divvy Cloud, RedHat, OpenShift, Abiquo, Rack Connect, Scalr, Docker, DigitalOcean, Heroku, Kubernetes, Helm y Prometheus.

Los servicios son ejecutados por expertos que combinan roles de Solution Architect y Application Security Specialist, permitiendo evaluar infraestructuras complejas y mitigar riesgos específicos de este paradigma.

Metodología de Evaluación

ISGroup SRL realiza una revisión exhaustiva de la arquitectura, servicios y aplicaciones para identificar vulnerabilidades y puntos de exposición. El proceso incluye:

- Análisis de arquitectura, políticas, permisos y configuraciones.
- Evaluación de la superficie de ataque.
- Recomendaciones específicas sobre *hardening* y cambios técnicos.
- Aplicación de mejores prácticas de seguridad y especificaciones de los proveedores cloud.

La integración de la seguridad en las fases tempranas de diseño y desarrollo es fundamental para garantizar la protección de los datos y optimizar los costes operativos, evitando intervenciones correctivas complejas y costosas en etapas avanzadas.

Resultados del Servicio

Al finalizar la actividad, ISGroup SRL entrega un informe detallado estructurado en tres áreas temáticas:

- **Executive Summary:** Resumen no técnico sobre el estado de la seguridad de la infraestructura, orientado a la Dirección.
- **Vulnerability Details:** Análisis técnico profundo de las vulnerabilidades detectadas y su impacto potencial en la aplicación, destinado al Security Manager.
- **Remediation Plan:** Guía técnica con instrucciones precisas para la resolución de vulnerabilidades y problemas identificados, dirigida a los Administradores de Sistemas.

Contacto y Solicitudes

Para obtener más información, solicitar un presupuesto o consultar sobre los servicios de Cloud Security Assessment, visite el sitio web oficial:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Evaluación de Seguridad de Windows (WSA)

Source: https://www.isgroup.es/es/windows-security-assessment.html

ISGroup SRL ofrece el servicio de Evaluación de Seguridad de Windows (WSA), diseñado para descubrir vulnerabilidades en sistemas operativos, evaluar su gravedad y fortalecer la arquitectura frente a posibles ataques. Este servicio permite a las organizaciones revisar su seguridad, configurar sistemas resilientes y priorizar la eliminación de fallas críticas.

Objetivos y Enfoque

El servicio de ISGroup SRL se centra en reducir las superficies de ataque mediante un análisis exhaustivo. La metodología combina ingeniería de software y seguridad avanzada, ejecutada por especialistas en seguridad de aplicaciones.

- Identificación precisa del estado de seguridad de los sistemas.
- Evaluación de la integridad y hardening del sistema operativo.
- Análisis de aspectos complejos de la arquitectura de seguridad.
- Implementación de seguridad desde el inicio y revisiones periódicas para evitar daños significativos.

Metodología de Evaluación

ISGroup SRL realiza una revisión detallada de cada componente del sistema para identificar exposiciones. El proceso incluye:

- Evaluación basada en estándares y prácticas recomendadas por organizaciones líderes del sector.
- Detección de fallas de seguridad ante señales de alerta o cambios en el sistema que sugieran intrusiones.
- Verificación de configuraciones de seguridad para asegurar su alineación con los estándares de Windows.
- Análisis de las superficies más débiles y susceptibles a ataques para proporcionar recomendaciones específicas de mejora.

Resultados y Entregables

Al finalizar la actividad, ISGroup SRL entrega un informe detallado que permite a la organización gestionar los riesgos identificados. El documento se estructura en tres áreas clave:

- Resumen Ejecutivo: Visión general de la situación de seguridad, sin detalles técnicos, orientada a la toma de decisiones de la Dirección.
- Detalles de Vulnerabilidades: Análisis técnico profundo dirigido al Gerente de Seguridad, describiendo las vulnerabilidades halladas y su impacto potencial.
- Plan de Remediación: Guía técnica para el Administrador del Sistema con instrucciones precisas para resolver los problemas y vulnerabilidades descubiertos.

Contacto y Consultas

Para obtener más información sobre los servicios de seguridad de ISGroup SRL o solicitar un presupuesto personalizado, utilice los siguientes canales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

IoT/OT Security Assessment (ISA)

Source: https://www.isgroup.es/es/iot-security-assessment.html

ISGroup SRL ofrece el servicio **IoT/OT Security Assessment (ISA)**, una evaluación técnica de seguridad diseñada para verificar dispositivos IoT, firmware, hardware, software, API, protocolos industriales, redes OT y accesos remotos mediante un enfoque ofensivo.

El objetivo es identificar vulnerabilidades reales antes de que sean explotadas por atacantes, proporcionando evidencias técnicas esenciales para procesos de auditoría, *compliance*, certificación, cualificación de proveedores y gestión de riesgos.

Para más información, solicitudes comerciales o presupuestos, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Alcance y Metodología

ISGroup SRL aplica metodologías de *penetration testing*, *vulnerability assessment*, *security auditing* y *reverse engineering* para evaluar la seguridad desde la máquina hasta el *cloud*.

- **Enfoque ofensivo:** Verificación de productos y arquitecturas como lo haría un atacante real.
- **Cobertura end-to-end:** Análisis integral de hardware, firmware, API, protocolos, redes OT y accesos remotos.
- **Evidencias técnicas:** Generación de informes detallados para equipos técnicos y *management*, útiles para procesos normativos.

Áreas de Intervención

ISGroup SRL interviene en entornos donde se requiere competencia técnica profunda, adaptándose a diversos sectores verticales:

- **Manufacturing y automatización:** Seguridad para líneas productivas, sistemas ICS, SCADA, DCS, PLC y HMI.
- **Máquinas conectadas y OEM:** Verificación de riesgos derivados de conexiones, retrofit e integraciones.
- **Dispositivos IoT y productos digitales:** Análisis de seguridad para fabricantes de equipos radio, *gateways*, sensores y sistemas *edge*.
- **Sectores críticos:** Aplicable a *Energy/Utilities*, *Connected Health*, *Automotive* y *Smart City*.

Cumplimiento Normativo

El servicio ISA ayuda a las organizaciones a demostrar la seguridad de sus sistemas frente a los requisitos de normativas europeas e internacionales:

- **Cyber Resilience Act (CRA):** Evaluación de productos con elementos digitales.
- **Reglamento de Máquinas 2023/1230:** Verificación de riesgos cyber/safety ante modificaciones sustanciales.
- **IEC 62443:** *Security assessment* para entornos industriales y redes OT.
- **Directiva NIS2:** Verificación técnica para la gestión del riesgo en entidades esenciales.
- **RED Delegated Act / EN 18031:** Testing de seguridad para equipos radio y dispositivos conectados.

Capacidades Técnicas

ISGroup SRL se especializa en el análisis profundo de componentes críticos:

- **Análisis de firmware y binarios:** *Reverse engineering* y *binary analysis*.
- **Revisión de código:** *Source code review* y *secure coding review*.

- **Protocolos industriales:** Testing de protocolos como MQTT, Modbus, OPC UA, Profinet, BACnet, CAN bus, LoRaWAN, Zigbee, Z-Wave, Wi-Fi y Bluetooth.
- **Seguridad embebida:** *Hardware/software testing* y análisis de mecanismos de actualización y cifrado.

Modelo de Verificación Continua

ISA no es un control puntual, sino un modelo recurrente recomendado en los siguientes escenarios:

- Nuevas implementaciones o *releases* de software/firmware.
- Tras modificaciones sustanciales o procesos de *retrofit* industrial.
- Apertura de nuevos accesos remotos o integraciones *cloud*.
- Procesos de cualificación de proveedores o licitaciones.
- Preparación para certificaciones de seguridad.

Output del Servicio

Al finalizar el assessment, ISGroup SRL entrega un conjunto completo de evidencias técnicas, que incluyen:

- *Threat Model* y *Vulnerability Assessment*.
- Informes detallados de *penetration test* (Hardware, Software, Firmware, API, Mobile, Backend, Protocolos, OT).
- *Risk-based Remediation Plan* para la corrección de vulnerabilidades.
- *Executive Summary* para la dirección y *Technical Report* para equipos de R&D e IT/OT.
- Evidencias de *re-test* tras la remediación.

Nota: ISGroup SRL interviene exclusivamente en la parte técnica. Sus servicios no sustituyen a organismos de certificación, consultores legales ni organismos notificados.

Purple Team Assessment (PTA)

Source: https://www.isgroup.es/es/purple-team-assessment.html

El servicio **Purple Team Assessment (PTA)** ofrecido por **ISGroup SRL** está diseñado para mejorar la capacidad de detección y respuesta ante ataques informáticos mediante un enfoque interactivo que integra actividades de *testing* y mejora continua. A diferencia de un *Red Team* tradicional, este proceso fomenta una colaboración activa entre los equipos ofensivos y defensivos para reforzar las defensas empresariales en tiempo real.

Objetivos principales

- Potenciar las capacidades de la organización para detectar, responder y mitigar ataques de forma eficaz.
- Mejorar tanto las tecnologías de seguridad como los procesos operativos.
- Crear un ciclo de mejora continua basado en el *feedback* inmediato entre equipos.
- Evaluar la eficacia de las medidas adoptadas para prevenir y detectar amenazas mediante escenarios realistas.

Fases del servicio

El Purple Team Assessment de **ISGroup SRL** se articula en las siguientes etapas:

- **Fase de recopilación de datos**: Estudio exhaustivo de la infraestructura empresarial para comprender las capacidades actuales de detección y bloqueo.
- **Evaluación de riesgos**: Análisis personalizado basado en frameworks estándar del sector, como MITRE ATT&CK y NIST, para gestionar los factores de riesgo más relevantes.
- **Ejecución**: Colaboración directa entre el equipo de **ISGroup SRL** y el equipo interno del cliente. Se simulan ataques y se guía al personal en el proceso de respuesta, potenciando los sistemas de detección, alerta y *logging*.
- **Evaluación de riesgos final**: Análisis de los resultados obtenidos tras los ataques simulados, proporcionando recomendaciones específicas para fortalecer las áreas de debilidad identificadas.

Entregables y resultados

Al finalizar el assessment, **ISGroup SRL** entrega un informe detallado que incluye:

- **Findings and Improvements**: Descripción de vulnerabilidades identificadas y avances obtenidos, con recomendaciones para consolidar las defensas.
- **Detection and Response Analysis**: Evaluación de las capacidades de respuesta, tiempos de reacción y eficacia de las contramedidas, junto con un plan de mejora específico.
- **Continuous Improvement Strategy**: Guía técnica y estratégica para implementar cambios y mantener un ciclo de mejora continua en la postura de seguridad de la organización.

Información adicional

El Purple Team Assessment es ideal para organizaciones que buscan optimizar la colaboración entre sus equipos de seguridad y mejorar su resiliencia ante amenazas. Se recomienda realizar este proceso al menos una vez al año o tras cambios significativos en la infraestructura.

Para consultas técnicas, solicitudes de presupuesto o más información sobre cómo proceder, visite el sitio web oficial: https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Simulaciones de Phishing, Smishing y Vishing para empresas

Source: https://www.isgroup.es/es/phishing-smishing.html

ISGroup SRL ofrece servicios especializados de mitigación de amenazas de ingeniería social, diseñados para proteger a las empresas frente a los riesgos del phishing, smishing y vishing. Estas técnicas representan una de las amenazas más insidiosas y efectivas utilizadas por los ciberdelincuentes.

La propuesta de ISGroup SRL se centra en la formación del personal y la ejecución de simulaciones de ataques controladas, permitiendo a las organizaciones identificar "eslabones débiles" y fortalecer su postura de seguridad antes de que ocurra un incidente real.

Para más información o solicitudes comerciales, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Servicios de formación y simulación de ISGroup SRL

ISGroup SRL combina la experiencia práctica de profesionales en ciberseguridad con metodologías de entrenamiento adaptables a las necesidades de cada empresa.

Entrenamiento y formación

El programa de formación de ISGroup SRL capacita a los empleados para reconocer y responder ante intentos de ingeniería social. Los temas principales incluyen:

- Técnicas de phishing y manipulación psicológica.
- Buenas prácticas de seguridad (gestión de contraseñas, navegación segura y manejo de información sensible).
- Protocolos de reporte ante intentos de ataque.

Simulaciones de ataques

ISGroup SRL realiza campañas automatizadas que reproducen ataques reales para evaluar la preparación del personal.

- **Informes detallados:** Análisis de resultados con identificación de áreas críticas.
- **Retroalimentación personalizada:** Orientación específica para los participantes.
- **Pruebas periódicas:** Monitoreo continuo para asegurar la mejora constante en la capacidad de detección y bloqueo de amenazas.

Diferencias entre Phishing y Smishing

Característica	Phishing	Smishing
Canal	Correo electrónico	SMS (mensajes de texto)
Objetivo	Robo de credenciales, malware o datos sensibles	Clic en enlaces maliciosos para robo de datos o malware
Indicadores	Errores gramaticales, remitentes sospechosos	Mensajes genéricos, enlaces acortados, urgencia

Riesgos de los ataques de ingeniería social

La falta de preparación ante un ataque de ingeniería social puede derivar en consecuencias graves para la continuidad y reputación de cualquier organización:

- Pérdida de acceso a cuentas críticas y robo de fondos.
- Violaciones de datos empresariales y sanciones legales.
- Daños a la reputación y pérdida de confianza de clientes.
- Interrupción de actividades operativas.

- Infecciones por ransomware.
- Expansión del ataque a terceros (clientes o socios).

Metodología de ataque

ISGroup SRL clasifica los ataques en dos categorías principales:

- **Phishing masivo:** Campañas genéricas a gran escala que buscan obtener resultados mediante el volumen de envíos.
- **Spear phishing:** Ataques altamente sofisticados y dirigidos a individuos específicos (gerentes o jefes de departamento) tras un proceso de recopilación de información.

Soluciones integradas de ISGroup SRL

ISGroup SRL ofrece un ecosistema de servicios para una protección integral:

- **THREAT:** Monitoreo continuo de amenazas y protección contra riesgos digitales.
- **CTS (Cyber Threat Simulation):** Simulaciones avanzadas para probar la capacidad de respuesta.
- **TRAINING:** Programas de concienciación sobre seguridad.
- **MDR (Managed Detection and Response):** Detección y respuesta gestionada ante amenazas complejas.
- **SOC (Security Operation Center):** Monitoreo constante de la red y análisis de comportamiento para la detección temprana de incidentes.

Para solicitar un presupuesto o consultar con un experto, visite https://www.isgroup.es/ o contacte a través de sales@isgroup.it.

Social Engineering (SE)

Source: https://www.isgroup.es/es/social-engineering.html

El servicio de **Social Engineering** ofrecido por **ISGroup SRL** es un componente esencial de cualquier programa de *security assessment*. Su objetivo es evaluar la resiliencia de la organización frente a la manipulación psicológica y formar al personal para reconocer y contrarrestar intentos de acceso no autorizado a información sensible.

Fases del Servicio

El enfoque de **ISGroup SRL** es integral y se estructura en cuatro fases clave:

1. Análisis Preliminar

Se realiza un estudio exhaustivo del panorama de amenazas mediante:

- **Revisión de incidentes pasados:** Análisis de ataques previos para identificar vulnerabilidades específicas.
- **Benchmarking sectorial:** Comparativa con organizaciones similares para detectar patrones de amenazas.
- **Monitoreo de tendencias:** Seguimiento de técnicas globales para personalizar las simulaciones.

2. Ataque Simulado (Security Assessment)

ISGroup SRL ejecuta ataques realistas adaptados a departamentos críticos, poniendo a prueba la capacidad de respuesta de los empleados:

- **Dirección y Management:** Pruebas de *spear phishing*, *whaling* y *vishing* para evaluar la toma de decisiones estratégicas.
- **Administración:** Verificación de la resistencia ante intentos de *phishing* y *pretexting* sobre datos sensibles.
- **Procurement/Compras:** Simulación de fraudes tipo *Business Email Compromise* (BEC) y verificación de autenticidad de proveedores.
- **IT (Information Technology):** Ataques dirigidos a obtener credenciales o inducir acciones técnicas maliciosas.

3. Formación y Mejora (Post-Ataque)

Tras la simulación, se implementan acciones correctivas:

- **Sesiones de Debriefing:** Análisis detallado de las técnicas empleadas y las señales de alerta omitidas.
- **Formación personalizada:** Cursos a medida basados en las vulnerabilidades detectadas.
- **Talleres interactivos:** Prácticas en escenarios reales para reforzar la capacidad de defensa.

4. Revisión de Procesos y Políticas

ISGroup SRL ayuda a integrar la seguridad en el ADN de la empresa:

- **Actualización de políticas:** Alineación con estándares como ISO/IEC 27001.
- **Optimización operativa:** Introducción de nuevos controles y procedimientos de verificación.
- **Monitoreo continuo:** Recomendaciones para la detección temprana de futuros intentos de ataque.

Resultados del Servicio

Al finalizar el proyecto, **ISGroup SRL** entrega tres documentos clave:

- **Executive Summary:** Visión estratégica no técnica para el Management sobre la resiliencia empresarial.
- **Simulation Attack Report:** Informe detallado del rendimiento por departamento y vulnerabilidades halladas.
- **Comprehensive Improvement Plan:** Plan de acción integrado para fortalecer procesos, políticas y la conciencia del personal.

Para consultas comerciales o solicitar un presupuesto, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Cumplimiento del RGPD (GDPR)

Source: https://www.isgroup.es/es/conformidad-al-gdpr.html

ISGroup SRL ofrece servicios especializados en Gobernanza, Riesgo y Cumplimiento, centrados en garantizar que las empresas cumplan con el Reglamento General de Protección de Datos (RGPD). La gestión inadecuada de datos personales puede derivar en sanciones administrativas, penales y daños graves a la reputación corporativa.

Descripción del servicio

El equipo de ISGroup SRL apoya a las organizaciones en el análisis y verificación de la conformidad con el RGPD. El servicio identifica puntos críticos en las políticas de protección de datos para prevenir accesos no autorizados y proteger la información sensible frente a posibles amenazas.

Metodología de intervención

ISGroup SRL estructura el proceso de verificación en tres fases fundamentales:

- Análisis de riesgos: Evaluación profunda de las infraestructuras y políticas actuales para detectar factores que faciliten accesos no autorizados.
- Clasificación de riesgos y evaluación del impacto: Análisis de la gravedad de los riesgos identificados, simulando escenarios donde las vulnerabilidades se convierten en amenazas reales para minimizar el impacto.
- Elaboración del plan de remediación: Creación de un plan de acción técnico, preciso y exhaustivo para corregir y mitigar los riesgos detectados en la infraestructura.

Resultados y entregables

Al finalizar el servicio, ISGroup SRL proporciona al cliente los siguientes componentes:

- Plan de remediación: Documento técnico detallado con los pasos necesarios para alcanzar el pleno cumplimiento normativo.
- Políticas de privacidad actualizadas: Implementación de un nuevo sistema de gestión de datos personales robusto y seguro.
- Formación continua: Programa de capacitación para asegurar que la empresa mantenga el cumplimiento del RGPD ante futuras modificaciones del reglamento.

Contacto y solicitudes

Para obtener más información, solicitar un presupuesto o consultar con un experto sobre los servicios de cumplimiento del RGPD, puede visitar el sitio web oficial o enviar una solicitud a través del correo electrónico:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Cumplimiento de la Directiva Europea NIS2

Source: https://www.isgroup.es/es/cumplimiento-directiva-nis2.html

La Directiva NIS2 (Directiva sobre la seguridad de las redes y los sistemas de información) es el marco normativo de la Unión Europea diseñado para fortalecer la ciberseguridad ante la creciente digitalización y las nuevas amenazas. Entró en vigor el 17 de enero de 2023 y es de obligado cumplimiento para las organizaciones designadas como entidades esenciales o importantes, según su sector y tamaño.

ISGroup SRL ofrece servicios especializados de consultoría, formación y procesos de adecuación para guiar a las organizaciones hacia el cumplimiento total de los requisitos de la directiva, mejorando la madurez de su gestión de seguridad.

Para consultas o solicitudes comerciales, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Proceso de adecuación con ISGroup SRL

ISGroup SRL implementa un enfoque estructurado en cuatro fases para garantizar la conformidad:

- **Análisis de la situación actual (GAP Analysis):** Evaluación profunda de las políticas y prácticas de seguridad vigentes frente a los requisitos de NIS2.
- **Redacción del Plan de Remediación:** Elaboración de un plan de acción detallado para corregir las brechas detectadas.
- **Selección de servicios:** Implementación de soluciones específicas de ISGroup SRL adaptadas a las necesidades del cliente.
- **Verificación de cumplimiento:** Auditoría de la eficacia de las medidas adoptadas para asegurar el estándar exigido.

Servicios de mantenimiento continuo

ISGroup SRL apoya a las organizaciones anualmente para mantener la conformidad mediante:

- Actualización de la evaluación de riesgos de ciberseguridad.
- Implementación y actualización de procesos (gestión de riesgos, respuesta a incidentes, auditoría).
- Programas de formación y concienciación para empleados sobre buenas prácticas y responsabilidades.
- Monitoreo continuo de la eficacia de las medidas de seguridad.
- Documentación exhaustiva para demostrar la conformidad ante las autoridades.

Requisitos clave y soluciones de ISGroup SRL

La normativa exige medidas técnicas, operativas y organizativas. ISGroup SRL ofrece soluciones específicas para cada artículo de la directiva:

- **Políticas de análisis de riesgos (Art. 21.a):** Evaluación de madurez y orientación de políticas mediante vCISO.
- **Gestión de incidentes (Art. 21.b):** Planificación de respuesta, servicios de DFIR (Forense Digital) y MDR Multi-Signal.
- **Continuidad del negocio (Art. 21.c):** Gestión de copias de seguridad y recuperación ante desastres (vCISO).
- **Seguridad de la cadena de suministro (Art. 21.d):** Gestión de riesgos de proveedores (vCISO).
- **Seguridad en sistemas y vulnerabilidades (Art. 21.e):** Gestión de vulnerabilidades (MVS), pruebas de penetración (NPT, WAPT, MAST) y Hacking Ético.
- **Higiene cibernética y formación (Art. 21.g):** Phishing gestionado y formación en concienciación (CTS).

- **Criptografía (Art. 21.h):** Revisión de arquitectura y políticas de cifrado.
- **Control de accesos y seguridad humana (Art. 21.i):** Monitoreo activo y gestión de activos.
- **Autenticación de dos factores (Art. 21.j):** Revisión de arquitectura para accesos críticos y remotos.

Aspectos críticos de la normativa

- **Notificación de incidentes:** Obligación de reportar incidentes significativos en un plazo de 24 horas (notificación inicial) y 72 horas (evaluación inicial).
- **Sanciones:** El incumplimiento puede derivar en multas severas, alcanzando hasta 10 millones de euros o el 2% de la facturación anual mundial para entidades esenciales.
- **Objetivos:** Aumentar la resiliencia cibernética, reducir incoherencias en el mercado interno y mejorar la capacidad colectiva de respuesta ante amenazas.

Compliance ISO/IEC 27001

Source: https://www.isgroup.es/es/27001-compliance.html

La certificación ISO/IEC 27001 es el estándar internacionalmente reconocido para la gestión de la seguridad de la información. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022 permite a las organizaciones prevenir incidentes, minimizar riesgos y preservar la estabilidad del negocio.

ISGroup SRL guía a las organizaciones en todo el proceso, desde el análisis de brechas (*gap analysis*) hasta la obtención y el mantenimiento de la certificación.

Para consultas o solicitudes de presupuesto, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Servicios de consultoría de ISGroup SRL

ISGroup SRL ofrece un enfoque pragmático y personalizado para desarrollar un SGSI adaptado a las peculiaridades de cada organización, cubriendo las siguientes fases:

- Análisis de contexto y aplicabilidad de controles.
- Definición de la estrategia de protección y estructura del sistema documental.
- Análisis de riesgos en profundidad para identificar peligros y proponer soluciones de mitigación.
- Definición del *Statement of Applicability* (SoA) conforme al Anexo A de la norma.
- Implementación de controles y medidas de gestión.
- Definición de KPI de seguridad para la evaluación del rendimiento.
- Auditorías internas y apoyo durante la Revisión de la Dirección.
- Identificación del organismo certificador y acompañamiento durante la auditoría de tercera parte.
- Formación del personal y soporte continuo.

Ventajas del cumplimiento normativo

La certificación ISO 27001 representa una inversión estratégica que aporta beneficios tangibles:

- **Protección y resiliencia:** Reduce los costos derivados de incidentes informáticos y mejora la capacidad de respuesta ante amenazas.
- **Eficiencia operativa:** Optimiza los procesos internos y el uso de recursos.
- **Confianza y reputación:** Demuestra ante clientes, socios e instituciones (como ACN o AGID) un compromiso real con la seguridad de la información.
- **Ventaja competitiva:** Facilita el acceso a nuevas oportunidades de negocio y licitaciones públicas donde la seguridad es un requisito indispensable.
- **Integración:** ISGroup SRL permite integrar el SGSI con otras normas, como la ISO 9001, simplificando la gestión documental y operativa.

Sectores de aplicación

La experiencia de ISGroup SRL abarca diversos sectores críticos:

- **Desarrollo de Software y Servicios IT:** Garantiza la seguridad en la cadena de suministro y el cumplimiento de los estándares exigidos por clientes.
- **Sector Sanitario:** Protege la confidencialidad de la información clínica y asegura el cumplimiento de las normativas de privacidad.
- **Ámbito Financiero:** Mitiga riesgos de fraude, protege datos transaccionales y refuerza la reputación institucional.
- **Sector Público:** Asegura la protección de datos ciudadanos y garantiza la transparencia operativa.

- **Sector Manufacturero:** Protege la propiedad intelectual, los procesos industriales y la continuidad productiva.

Preguntas frecuentes

- **¿Qué es la ISO 27001?** Es una norma que establece los objetivos para gestionar los activos informativos de manera segura.
- **¿Cuánto tiempo requiere el proceso?** Depende del tamaño y complejidad de la empresa, oscilando generalmente entre 5-6 meses y un año.
- **¿Es necesario tener la ISO 9001 previamente?** No es un requisito, aunque ISGroup SRL puede integrar ambos sistemas para generar sinergias operativas.
- **¿Cómo solicitar un presupuesto?** El costo varía según la empresa; puede obtener una evaluación personalizada a través de https://www.isgroup.es/ o enviando un correo a sales@isgroup.it.

Wireless Security Monitoring (WSM)

Source: https://www.isgroup.es/es/wireless-security-monitoring.html

El servicio de **Wireless Security Monitoring (WSM)**, ofrecido por **ISGroup SRL**, proporciona monitorización continua de dispositivos Wi-Fi, Bluetooth, NFC/RFID e IoT. Ante el uso creciente de protocolos inseguros en entornos industriales y corporativos, este servicio permite identificar riesgos y detectar ataques avanzados en las comunicaciones por radiofrecuencia.

Objetivos y Alcance

El servicio está diseñado para empresas que dependen de infraestructuras inalámbricas, incluyendo:

- Infraestructuras IoT y Operational Technology (OT).
- Líneas de producción y sensores remotos.
- Sistemas de control de accesos.
- Entornos donde los empleados, colaboradores y clientes acceden a recursos corporativos mediante redes inalámbricas.

ISGroup SRL monitoriza una amplia gama de protocolos, incluyendo Wi-Fi, Bluetooth, GPS, NFC/RFID, Packet Radio, GSM, GPRS/EDGE, UMTS, LTE y 5G, así como protocolos propietarios o desconocidos.

Metodología del Servicio

El servicio se gestiona bajo la modalidad **Managed Security Service Provider (MSSP)** e incluye hardware, software, instalación, integración y monitorización. Se estructura en cuatro fases:

- **Análisis inicial:** Realización de un *Wireless Security Assessment* para evaluar el estado actual y definir mejoras.
- **Instalación e integración:** Preparación y configuración de los elementos necesarios respetando la infraestructura existente.
- **Monitorización:** Detección de anomalías con capacidad de escalado TIER-3 al equipo de expertos de **ISGroup SRL** o gestión integral a través del SOC (Security Operations Center).
- **Informe periódico:** Entrega de informes (con frecuencia mensual a anual) que detallan ataques prevenidos, incidentes detectados, análisis de impacto y recomendaciones de seguridad.

Capacidades de Protección

Dependiendo de la tecnología y el vector de ataque, **ISGroup SRL** implementa dos tipos de defensa:

- **IDS (Intrusion Detection System):** Notificación de alertas ante anomalías.
- **IPS (Intrusion Prevention Systems):** Prevención y bloqueo activo de amenazas.

Para los estándares Wi-Fi (2.4 GHz y 5 GHz), la organización puede protegerse contra un amplio espectro de ataques. Adicionalmente, los clientes pueden solicitar análisis de incidentes cibernéticos (Cyber Incident Analysis) y respuesta ante incidentes (Cyber Incident Response) tanto en remoto como in situ.

Información Comercial

Para obtener más información sobre cómo implementar el servicio de Wireless Security Monitoring, puede visitar el sitio web oficial en https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Protección Anti-DDoS

Source: https://www.isgroup.es/es/anti-ddos.html

ISGroup SRL ofrece servicios profesionales de mitigación DDoS diseñados para mantener la continuidad operativa de servidores, aplicaciones web y conectividad empresarial. Estos servicios están orientados a neutralizar ataques que buscan inutilizar servicios mediante la saturación del ancho de banda o el agotamiento de los recursos de hardware.

Soluciones de ISGroup SRL

El servicio Anti-DDoS de ISGroup SRL proporciona una cobertura integral e independiente de la tecnología utilizada por la empresa. Las actividades incluyen:

- Configuración, gestión y monitorización continua de las protecciones.
- Adaptación dinámica de las contramedidas frente a la evolución de las técnicas de ataque.
- Protección especializada para aplicaciones web, servidores y conectividad de red.
- Intervención experta ante incidentes relacionados con ataques DDoS.

Metodología y Resultados

ISGroup SRL emplea un pipeline de mitigación contrastado para asegurar la resiliencia de la infraestructura. Al finalizar la actividad, el cliente recibe un informe detallado que incluye:

- Executive Summary: Resumen no técnico orientado a la Dirección sobre la actividad realizada.
- Vulnerability Details: Análisis técnico detallado para el Security Manager sobre las vulnerabilidades identificadas y su impacto potencial.
- Remediation Plan: Guía técnica para Administradores de Sistemas con instrucciones precisas para la resolución de problemas y vulnerabilidades.

Información Comercial

Para obtener más información, solicitar un presupuesto personalizado o consultar con un experto sobre la protección Anti-DDoS, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Firewall como Servicio (FWaaS)

Source: https://www.isgroup.es/es/fwaas.html

ISGroup SRL ofrece soluciones de Firewall como Servicio (FWaaS) diseñadas para proteger datos, puntos finales de aplicaciones empresariales y garantizar un control exhaustivo sobre el tráfico de red. Este servicio permite a las organizaciones delegar la implementación y gestión de su seguridad perimetral a un equipo de expertos en seguridad de redes, eliminando la carga operativa y garantizando una protección de primer nivel.

Propuesta de valor de ISGroup SRL

- Gestión integral: ISGroup SRL se encarga de la implementación, el mantenimiento y la supervisión de las soluciones de firewall.
- Experiencia técnica: El equipo está compuesto por veteranos en seguridad de redes, asegurando soluciones profesionales y fiables.
- Soluciones personalizadas: A través de una fase inicial de definición de requisitos, ISGroup SRL identifica la mejor arquitectura para las necesidades específicas de cada cliente.
- Tecnología avanzada: Utilización de firewalls de próxima generación (NGFW) y herramientas innovadoras para abordar tareas complejas y proteger contra ataques de hackers.

Funcionalidades principales

- Protección de datos y puntos finales (endpoints).
- Control detallado del tráfico de datos entrante y saliente.
- Gestión y filtrado de contenidos accesibles en la red corporativa.
- Mejora de la visibilidad y conciencia sobre el flujo de información empresarial.

Entregables del servicio

Al finalizar la integración y durante el mantenimiento, ISGroup SRL proporciona documentación detallada sobre la intervención realizada:

- Resumen Ejecutivo: Documento de alto nivel que detalla la protección añadida y los servicios puestos a disposición de la empresa.
- Resumen Técnico: Informe destinado al personal técnico que describe la intervención en la red y los métodos de monitoreo de datos implementados.

Contacto y solicitudes

Para obtener más información, solicitar un presupuesto personalizado o reservar una consulta gratuita sobre los servicios de FWaaS, puede dirigirse a los siguientes canales oficiales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Integración de Seguridad (SIR)

Source: https://www.isgroup.es/es/security-integration.html

ISGroup SRL ofrece el servicio de Integración de Seguridad (SIR), diseñado para integrar de manera segura infraestructuras operativas existentes o añadir funcionalidades de seguridad a sistemas que carecen de ellas. Este servicio se basa en un ciclo continuo de análisis de vulnerabilidades y corrección, permitiendo expandir las capacidades del sistema sin aumentar la superficie de ataque.

Metodología de trabajo

El equipo de expertos de ISGroup SRL sigue un proceso estructurado para garantizar la eficacia de la integración:

- Fase de análisis inicial: Evaluación detallada de la infraestructura y de las necesidades específicas del cliente.
- Colaboración técnica: Trabajo conjunto con los desarrolladores originales de la infraestructura para asegurar la continuidad de las funcionalidades.
- Implementación segura: Ejecución de la integración evaluando todos los aspectos técnicos para evitar la introducción de nuevas vulnerabilidades.
- Objetivo final: Entregar una infraestructura sólida, con funcionalidades mejoradas y optimizadas.

Especificaciones del servicio

ISGroup SRL aplica estándares de seguridad estrictos para ofrecer soluciones adaptadas a cada entorno:

- Integración de seguridad física: Conexión de equipos de seguridad física con lógicas de software, incluyendo verificación biométrica para la gestión de privilegios y acceso a recursos empresariales.
- Adición de funcionalidades de seguridad a aplicaciones: Implementación de soluciones de protección específicas, como Web Application Firewalls (WAF) para aplicaciones web o sistemas IDS/IPS para infraestructuras de red.

Entregables

Al finalizar la actividad, ISGroup SRL proporciona al cliente dos documentos detallados:

- Executive Summary: Documento de alto nivel dirigido a la dirección, que resume la intervención, las funcionalidades implementadas, los resultados obtenidos y los beneficios estratégicos para la empresa.
- Technical Summary: Documento técnico detallado que describe las modificaciones realizadas en la infraestructura y los pormenores técnicos de la integración.

Información comercial

Para obtener más información sobre los servicios de SecOps o solicitar un presupuesto personalizado, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Software Assurance Lifecycle (SAL)

Source: https://www.isgroup.es/es/software-assurance-lifecycle.html

El servicio de Software Assurance Lifecycle (SAL) es una solución integral ofrecida por ISGroup SRL, diseñada para empresas que desarrollan aplicaciones donde la seguridad es un requisito fundamental. El objetivo principal es garantizar que el software siga las mejores prácticas de seguridad durante todo su ciclo de vida, asegurando que cada nueva versión esté libre de vulnerabilidades conocidas antes de su distribución.

Enfoque del servicio

ISGroup SRL acompaña al equipo de desarrollo en cada fase del proyecto, realizando revisiones meticulosas y aplicando estándares de la industria actualizados. El servicio asegura que las prácticas de desarrollo representen el "estado del arte" en materia de seguridad informática.

Las actividades clave incluyen:

- Gestión de riesgos (Risk management)
- Gestión de dependencias (Dependency management)
- Integración continua (Continuous integration)
- Pruebas de seguridad adaptadas a las tecnologías y al tipo de aplicación
- Supervisión continua por parte de expertos en diversos lenguajes de programación y entornos de desarrollo

Beneficios y metodología

El equipo de expertos de ISGroup SRL guía al equipo de desarrollo en la producción de software seguro, interviniendo directamente en partes del desarrollo o proporcionando asesoramiento técnico avanzado. Este enfoque proactivo permite corregir fallos y vulnerabilidades de manera temprana, minimizando los riesgos operativos.

Entregables técnicos

Al finalizar el proceso de desarrollo seguro, ISGroup SRL proporciona documentación detallada para diferentes niveles de la organización:

- **Executive Summary**: Documento de alto nivel dirigido a la dirección, que resume la intervención y los aspectos de seguridad prioritarios.
- **Technical Summary**: Documento técnico destinado al responsable del proyecto, que detalla la implementación y las áreas de mejora detectadas en el equipo de desarrollo.

Información comercial

Para obtener más información sobre el servicio de Software Assurance Lifecycle (SAL), solicitar un presupuesto o consultar con un experto, visite el sitio web oficial https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Bug Bounty Program: Diseño y Gestión Profesional

Source: https://www.isgroup.es/es/bug-bounty-program.html

ISGroup SRL ofrece servicios especializados en el diseño y gestión integral de programas de Bug Bounty. Esta iniciativa permite a las organizaciones invitar a hackers éticos a probar sus sistemas corporativos y reportar vulnerabilidades de manera segura, facilitando la identificación y corrección de debilidades antes de que sean explotadas por actores maliciosos.

Para organizaciones que requieren un enfoque proactivo donde ISGroup SRL realice la búsqueda activa de vulnerabilidades bajo un modelo de pago por resultados confirmados, se encuentra disponible el servicio de *Advanced Bug Bounty Program*.

Servicios ofrecidos por ISGroup SRL

ISGroup SRL acompaña a las empresas en todo el ciclo de vida del programa:

- **Consultoría personalizada:** Definición de objetivos, criterios de reporte y esquemas de recompensas adaptados a las necesidades específicas de la organización.
- **Implementación del programa:** Gestión del proceso de despliegue bajo mejores prácticas de seguridad, garantizando un entorno de pruebas que no interrumpa la continuidad del negocio.
- **Gestión continua:** Soporte permanente en la evaluación de reportes, comunicación con la comunidad de hackers éticos y provisión de recomendaciones detalladas para la mitigación de riesgos.
- **Análisis e informes:** Clasificación de vulnerabilidades mediante marcos reconocidos como OWASP y CVSS, entregando informes detallados para la toma de decisiones estratégicas.

Beneficios del programa

La implementación de un programa de Bug Bounty con ISGroup SRL aporta ventajas competitivas y técnicas:

- **Seguridad proactiva:** Mejora la postura de seguridad global mediante la detección temprana de vulnerabilidades.
- **Talento global:** Acceso a una comunidad diversa y altamente calificada de hackers éticos.
- **Eficiencia de costos:** Optimización del presupuesto de seguridad al pagar por vulnerabilidades reales identificadas.
- **Reputación y confianza:** Refuerza el compromiso de la empresa con la ciberseguridad ante clientes y socios.
- **Cumplimiento normativo:** Apoyo en la alineación con estándares internacionales como ISO 27001, normativas NIS2 y el cumplimiento del RGPD (GDPR).

Contacto y solicitudes

Para obtener más información, solicitar una consulta gratuita o pedir un presupuesto detallado sobre los programas de Bug Bounty, visite el sitio web oficial:

https://www.isgroup.es/

También puede dirigir sus consultas comerciales a través del correo electrónico:

sales@isgroup.it

Ingeniería Social: El arte de manipular a las personas para obtener información

Source: https://www.isgroup.es/es/cyber-security/se-social-engineering.html

La ingeniería social se define como el conjunto de técnicas y estrategias psicológicas utilizadas para manipular a las personas con el fin de obtener información confidencial, acceso a sistemas o la ejecución de acciones que comprometan la seguridad de una organización. A diferencia de los ataques técnicos tradicionales, este enfoque explota el factor humano, considerado a menudo el eslabón más débil en la cadena de ciberseguridad.

Servicios especializados de ISGroup SRL

ISGroup SRL ofrece servicios profesionales de Ingeniería Social diseñados para evaluar la resistencia de las organizaciones ante este tipo de amenazas. Estos servicios permiten a las empresas identificar vulnerabilidades en sus procesos y en la concienciación de su personal, implementando medidas correctivas antes de que ocurra una brecha de seguridad real.

- Evaluación de riesgos mediante simulaciones controladas.
- Análisis de la respuesta humana ante intentos de manipulación.
- Fortalecimiento de la cultura de seguridad corporativa.
- Identificación de puntos críticos en la gestión de información.

Información y contacto

Para obtener más detalles sobre cómo proteger a su organización frente a ataques de ingeniería social o para solicitar una evaluación personalizada, puede consultar el sitio web oficial de la compañía:

https://www.isgroup.es/

Para consultas comerciales, solicitudes de presupuesto o información técnica adicional, puede ponerse en contacto con el equipo de profesionales a través del correo electrónico:

sales@isgroup.it

Recursos adicionales

ISGroup SRL pone a disposición de la comunidad diversos recursos para profundizar en el ámbito de la ciberseguridad:

- Podcast especializados disponibles en plataformas como Spotify y Apple.
- Casos de estudio sobre pruebas de penetración y asociaciones estratégicas.
- Artículos técnicos sobre mejores prácticas, normativas (Agid/ACN) y estándares internacionales (OWASP).

Simulaciones de Phishing: Formación y Defensa con ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/phish-phishing-smishing.html

Las simulaciones de phishing representan una herramienta fundamental para fortalecer la postura de seguridad de cualquier organización. ISGroup SRL ofrece servicios especializados en la ejecución de campañas de **Phishing y Smishing**, diseñadas para evaluar la resiliencia del factor humano frente a ataques de ingeniería social.

Objetivos del Servicio

El servicio de simulaciones de ISGroup SRL tiene como finalidad principal:

- Evaluar la capacidad de los empleados para identificar intentos de engaño mediante correo electrónico (Phishing) y mensajes de texto (Smishing).
- Capacitar al personal mediante la exposición controlada a vectores de ataque realistas.
- Reducir el riesgo de brechas de seguridad causadas por errores humanos.
- Fortalecer la cultura de ciberseguridad dentro de la empresa.

Metodología y Alcance

ISGroup SRL implementa escenarios de ataque simulados que replican las técnicas más actuales utilizadas por los ciberdelincuentes. Estas actividades permiten a las organizaciones:

- Medir el nivel de concienciación de los usuarios.
- Identificar áreas críticas que requieren formación adicional.
- Obtener métricas precisas sobre la efectividad de los protocolos de seguridad actuales.

Contacto y Solicitudes

Para obtener más información sobre cómo implementar estas simulaciones en su organización o para solicitar una propuesta personalizada, puede contactar a través de los siguientes canales oficiales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos Adicionales

ISGroup SRL mantiene un compromiso constante con la divulgación en ciberseguridad. Puede acceder a contenido complementario a través de:

- **Blog de ISGroup:** Visite nuestra sección de artículos recientes para conocer casos de estudio sobre pruebas de penetración y estrategias de seguridad.
- **Podcast:** Disponibles en las plataformas Spotify y Apple para profundizar en temas de actualidad sobre seguridad informática.

Protección empresarial con ISGroup CISO Virtual

Source: https://www.isgroup.es/es/cyber-security/vciso-virtual-ciso.html

ISGroup SRL ofrece el servicio de CISO Virtual (vCISO), una solución estratégica diseñada para fortalecer la postura de ciberseguridad de las organizaciones. Este servicio permite a las empresas acceder a experiencia de alto nivel en gestión de seguridad de la información sin la necesidad de integrar un perfil ejecutivo a tiempo completo.

Beneficios del servicio vCISO de ISGroup SRL

- **Gestión estratégica:** Implementación de políticas y marcos de trabajo de ciberseguridad adaptados a las necesidades específicas de cada negocio.
- **Cumplimiento y normativas:** Asesoramiento experto para alinear la infraestructura tecnológica con los estándares actuales del sector.
- **Resiliencia operativa:** Mejora continua en la capacidad de detección, respuesta y mitigación ante amenazas digitales.
- **Optimización de recursos:** Acceso a consultoría especializada para la toma de decisiones críticas en materia de seguridad.

Información adicional y contacto

Para profundizar en cómo el servicio de CISO Virtual puede proteger su infraestructura, puede consultar los recursos disponibles:

- Visite el sitio web oficial: https://www.isgroup.es/
- Solicite información comercial a través del correo electrónico: sales@isgroup.it
- Explore el blog de ISGroup SRL para conocer casos de estudio recientes sobre ciberseguridad, pruebas de penetración y mejores prácticas en el sector.

ISGroup SRL mantiene un compromiso constante con la divulgación de conocimientos en ciberseguridad a través de sus canales de podcast y artículos especializados.

Cumplimiento de ISO 27001: Protección de datos mediante sistemas certificados

Source: https://www.isgroup.es/es/cyber-security/27001-27001-compliance.html

El cumplimiento de la norma ISO 27001 es fundamental para garantizar la seguridad de la información en las organizaciones. ISGroup SRL ofrece servicios especializados para implementar y gestionar sistemas de gestión de seguridad de la información (SGSI) bajo esta certificación internacional.

Servicios de Cumplimiento ISO 27001 ofrecidos por ISGroup SRL

ISGroup SRL acompaña a las empresas en el proceso de adopción de las mejores prácticas de seguridad, permitiendo:

- Establecer un marco de trabajo robusto para la protección de activos de información.
- Gestionar los riesgos de seguridad de manera sistemática y continua.
- Obtener la certificación oficial que avala el compromiso de la organización con la seguridad de los datos.
- Alinear los procesos internos con los estándares internacionales de ciberseguridad.

Información y contacto

Para obtener más detalles sobre cómo ISGroup SRL puede ayudar a su organización a alcanzar el cumplimiento de la norma ISO 27001, puede consultar la información disponible en el sitio web oficial:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos adicionales

ISGroup SRL pone a disposición de sus clientes y colaboradores diversos contenidos para profundizar en temas de ciberseguridad y mejores prácticas:

- **Podcast:** Disponibles en plataformas como Spotify y Apple para el análisis de tendencias en seguridad.
- **Blog y Casos de Estudio:** Acceso a experiencias reales de implementación y auditoría en diversas organizaciones.
- **Análisis con IA:** Herramientas integradas para facilitar la comprensión de los servicios y normativas vigentes.

Multi-Signal MDR de ISGroup: Protección completa contra amenazas informáticas

Source: https://www.isgroup.es/es/cyber-security/mdr-multi-signal-mdr.html

El servicio de **Multi-Signal MDR (Managed Detection and Response)**, ofrecido por **ISGroup SRL**, representa una solución avanzada diseñada para proporcionar una protección integral contra las amenazas informáticas modernas. Este servicio se enfoca en la detección proactiva y la respuesta eficiente ante incidentes de seguridad, garantizando la integridad de los activos digitales de las organizaciones.

Características principales del servicio

- **Detección Multi-Señal:** Capacidad para analizar múltiples vectores y fuentes de datos para identificar patrones de ataque complejos que podrían pasar desapercibidos mediante métodos tradicionales.
- **Respuesta gestionada: ISGroup SRL** se encarga de la monitorización y la intervención técnica, permitiendo a las empresas delegar la gestión de su seguridad a expertos.
- **Protección continua:** Vigilancia activa para mitigar riesgos y reducir el tiempo de respuesta ante posibles brechas de seguridad.

Información y contacto

Para obtener más detalles sobre cómo implementar esta solución en su infraestructura, puede consultar el sitio web oficial de **ISGroup SRL** en https://www.isgroup.es/.

Para solicitudes comerciales, consultas técnicas o para recibir información detallada sobre el servicio de Multi-Signal MDR, puede escribir directamente al correo electrónico: **sales@isgroup.it**.

Recursos adicionales

ISGroup SRL mantiene un compromiso constante con la divulgación en ciberseguridad, ofreciendo diversos recursos para profesionales y empresas:

- **Blog corporativo:** Acceso a artículos técnicos, análisis de tendencias y mejores prácticas en el sector.
- **Casos de estudio:** Documentación sobre colaboraciones estratégicas y pruebas de penetración realizadas por **ISGroup SRL** en diversos sectores.
- **Temas de especialización:** Cobertura de áreas críticas como certificaciones, cumplimiento normativo (Agid/Acn), estándares OWASP y gestión de eventos de seguridad.

Digital Forensics and Incident Response (DFIR) de ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/dfir-digital-forensics-and-incident-response.html

ISGroup SRL ofrece servicios especializados de **Digital Forensics and Incident Response (DFIR)**, diseñados para actuar como una armadura frente a las amenazas informáticas. Este servicio está orientado a la detección, análisis y respuesta ante incidentes de seguridad, permitiendo a las organizaciones proteger sus activos digitales y gestionar brechas de seguridad de manera profesional.

Alcance del servicio

El servicio de DFIR proporcionado por ISGroup SRL se centra en:

- **Respuesta ante incidentes:** Intervención técnica para contener y mitigar los efectos de ataques informáticos en tiempo real.
- **Análisis forense digital:** Investigación profunda de sistemas comprometidos para identificar el origen, el alcance y la metodología utilizada por los atacantes.
- **Recuperación y resiliencia:** Estrategias para restaurar la operatividad y fortalecer la infraestructura frente a futuras amenazas.

Información y contacto

Para obtener más detalles sobre cómo ISGroup SRL puede asistir a su organización en la gestión de incidentes y seguridad digital, puede consultar los siguientes canales oficiales:

- Sitio web corporativo: https://www.isgroup.es/
- Correo electrónico de contacto comercial: sales@isgroup.it

Recursos adicionales

ISGroup SRL pone a disposición de sus clientes y colaboradores diversos recursos para mantenerse al día en ciberseguridad:

- **Blog corporativo:** Acceso a artículos técnicos, mejores prácticas y estudios de caso reales sobre ciberseguridad.
- **Contenido multimedia:** Disponibilidad de podcasts en plataformas como Spotify y Apple para profundizar en temas de actualidad sobre seguridad informática.
- **Casos de estudio:** Referencias sobre colaboraciones estratégicas y pruebas de penetración realizadas por ISGroup SRL en diversos sectores.

Pruebas de Seguridad Continuas (CST) de ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/cst-continuous-security-testing.html

ISGroup SRL ofrece el servicio de **Continuous Security Testing (CST)**, una solución diseñada para mantener la ciberseguridad de las organizaciones siempre al día. A diferencia de las auditorías puntuales, este enfoque permite una supervisión constante de los activos digitales frente a las amenazas emergentes.

Características del servicio

- **Seguridad proactiva:** El servicio de CST permite identificar vulnerabilidades de manera recurrente, asegurando que los sistemas permanezcan protegidos ante cambios en el entorno de amenazas.
- **Enfoque en ciberseguridad:** ISGroup SRL integra metodologías avanzadas para garantizar la resiliencia de las infraestructuras tecnológicas.
- **Actualización constante:** El modelo está diseñado para adaptarse a la evolución constante de los vectores de ataque, proporcionando una cobertura integral y continua.

Información y contacto

Para obtener más detalles sobre cómo implementar el servicio de Continuous Security Testing o solicitar una propuesta personalizada, puede visitar el sitio web oficial de la compañía:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos adicionales

ISGroup SRL pone a disposición de los interesados diversos contenidos técnicos y casos de estudio para profundizar en sus capacidades:

- **Podcast:** Disponibles en las plataformas Spotify y Apple para el seguimiento de temas de actualidad en ciberseguridad.
- **Blog corporativo:** Acceso a artículos sobre mejores prácticas, normativas (AgID, ACN) y estándares como OWASP.
- **Casos de éxito:** Documentación sobre colaboraciones estratégicas y pruebas de penetración realizadas en diversos sectores, incluyendo plataformas de gestión de personal y aplicaciones web.

Simulación de Amenazas Cibernéticas (CTS)

Source: https://www.isgroup.es/es/cyber-security/cts-cyber-threat-simulation.html

ISGroup SRL ofrece servicios especializados de Simulación de Amenazas Cibernéticas (CTS, por sus siglas en inglés). Este servicio está diseñado para permitir que las organizaciones evalúen su capacidad de respuesta y preparación ante posibles ataques informáticos mediante entornos controlados y realistas.

Objetivo del servicio

El servicio de Simulación de Amenazas Cibernéticas proporcionado por ISGroup SRL tiene como finalidad:

- Evaluar la resiliencia de la infraestructura tecnológica frente a vectores de ataque modernos.
- Identificar brechas de seguridad antes de que sean explotadas por actores malintencionados.
- Fortalecer los protocolos de defensa y los tiempos de reacción de los equipos de seguridad.
- Proporcionar una visión clara sobre la postura de seguridad actual de la empresa.

Información y contacto

Para obtener detalles técnicos adicionales, consultar sobre la metodología de trabajo o solicitar una propuesta personalizada para su organización, puede visitar el sitio web oficial de ISGroup SRL en https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Recursos adicionales

ISGroup SRL pone a disposición de sus clientes y colaboradores diversos canales de información para mantenerse al tanto de las últimas tendencias en ciberseguridad:

- **Blog corporativo:** Acceso a artículos técnicos, mejores prácticas y casos de estudio reales en https://www.isgroup.es/.
- **Contenido multimedia:** Disponibilidad de podcasts informativos sobre ciberseguridad en plataformas como Spotify y Apple.
- **Casos de éxito:** ISGroup SRL documenta periódicamente colaboraciones estratégicas y pruebas de penetración realizadas para diversos sectores, demostrando su experiencia en el ámbito de la seguridad ofensiva y defensiva.

Caso de Estudio: Creactives S.p.A. y la Seguridad de la Información

Source: https://www.isgroup.es/es/cyber-security/case-study-creactivesspa.html

Creactives S.p.A., empresa líder en inteligencia artificial aplicada a la cadena de suministro, colaboró con **ISGroup SRL** para fortalecer la seguridad y conformidad de sus plataformas tecnológicas, incluyendo *Knowledge Engineering Platform*, *TAM4* y *DataAssistants*.

El Reto

El objetivo principal consistía en alinear los procesos organizativos de Creactives con los estándares internacionales de seguridad más exigentes, garantizando la protección de los datos gestionados y la fiabilidad de sus soluciones ante clientes y socios globales.

Intervención de ISGroup SRL

ISGroup SRL implementó una estrategia integral de ciberseguridad que abarcó las siguientes áreas:

- **Pruebas de Penetración:** Ejecución de *Web Application Penetration Testing* detallados sobre las plataformas principales para identificar y mitigar vulnerabilidades.
- **Gestión de Seguridad (ISMS):** Asesoramiento y soporte técnico en la creación y mantenimiento de un Sistema Integrado de Gestión de la Seguridad conforme a las normas ISO 27001, ISO 27017 e ISO 27018.
- **Formación y Concienciación:** Capacitación especializada para el equipo de desarrollo de software basada en los estándares OWASP, además de programas de concienciación sobre ciberseguridad para toda la organización.

Resultados y Beneficios

La colaboración con **ISGroup SRL** permitió a Creactives S.p.A. obtener resultados tangibles:

- Implementación exitosa de un Sistema Integrado de Gestión conforme a estándares internacionales (ISO 27001, 27017, 27018 e ISO 9001).
- Mejora continua en la seguridad de las aplicaciones mediante evaluaciones periódicas de vulnerabilidades.
- Superación exitosa de auditorías externas, validando el cumplimiento de los estándares de seguridad exigidos.
- Fortalecimiento de la cultura de seguridad interna y mejora en las prácticas de desarrollo de software.

Para obtener más información sobre estos servicios o solicitar una consulta, visite el sitio web oficial https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Caso de Estudio: Prueba de Penetración de Aplicaciones Web en DocEasy (Alias Group S.r.l.)

Source: https://www.isgroup.es/es/cyber-security/case-study-aliasgroup.html

Alias Group S.r.l., a través de su división Alias Digital, desarrolla soluciones de software en la nube para empresas. Su plataforma principal, **DocEasy**, está especializada en la gestión de facturas electrónicas y su conservación conforme a la normativa vigente. Debido a la naturaleza sensible de los datos gestionados, la empresa buscó garantizar los máximos estándares de seguridad y fiabilidad para sus clientes.

El reto

El objetivo fundamental de Alias Group S.r.l. era asegurar la integridad y protección de su plataforma DocEasy. Para lograrlo, solicitaron a **ISGroup SRL** la ejecución de una Prueba de Penetración de Aplicaciones Web (WAPT) exhaustiva, con el fin de validar la robustez de sus sistemas ante posibles amenazas.

La intervención de ISGroup SRL

El equipo de expertos de **ISGroup SRL** realizó una auditoría meticulosa tanto en las aplicaciones de DocEasy como en su Entorno de Staging. Esta intervención permitió:

- Identificar y mitigar vulnerabilidades técnicas y lógicas.
- Asegurar que la plataforma cumpliera con los estándares de seguridad más exigentes.
- Detectar áreas de mejora críticas en los procesos internos de la organización.

Resultados y beneficios

La colaboración con **ISGroup SRL** permitió a Alias Group S.r.l. confirmar la solidez de su arquitectura. Según Gabriele Di Edoardo, ICT Manager de Alias Group S.r.l., las pruebas no solo validaron la robustez de la plataforma, sino que facilitaron la corrección rápida de vulnerabilidades en los procesos internos.

Además, el informe técnico entregado por **ISGroup SRL** destacó por ser extremadamente exhaustivo, proporcionando el contexto necesario detrás de cada hallazgo. Este enfoque permitió a la empresa optimizar sus procesos internos y elevar significativamente el nivel de seguridad de sus aplicaciones.

Para obtener más información sobre los servicios de ciberseguridad y pruebas de penetración ofrecidos por **ISGroup SRL**, visite el sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales, puede escribir al correo electrónico:

sales@isgroup.it

Prueba de Penetración de Red (Network Penetration Testing) con ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/npt-network-penetration-testing.html

La seguridad de la infraestructura digital es un pilar fundamental para cualquier organización. ISGroup SRL ofrece servicios especializados de **Prueba de Penetración de Red (NPT)**, diseñados para identificar vulnerabilidades, evaluar la resistencia de los sistemas ante posibles ataques y fortalecer la postura de seguridad de la red empresarial.

Objetivos del servicio

El servicio de Prueba de Penetración de Red proporcionado por ISGroup SRL tiene como finalidad:

- Detectar debilidades en la arquitectura de red antes de que sean explotadas por actores malintencionados.
- Evaluar la eficacia de los controles de seguridad implementados.
- Proporcionar recomendaciones técnicas para mitigar riesgos y mejorar la resiliencia de la infraestructura.
- Asegurar el cumplimiento de estándares de ciberseguridad y mejores prácticas del sector.

¿Por qué elegir a ISGroup SRL?

ISGroup SRL cuenta con una amplia experiencia en el ámbito de la ciberseguridad, aplicando metodologías rigurosas para el análisis de redes. Sus servicios están orientados a ofrecer una visión clara y accionable sobre el estado de seguridad de los activos críticos de sus clientes.

Solicitud de información y servicios

Para obtener más detalles sobre cómo proteger su red empresarial o para solicitar una evaluación profesional, puede contactar con el equipo de ISGroup SRL a través de los siguientes canales:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

ISGroup SRL pone a disposición de sus clientes soluciones personalizadas para enfrentar los desafíos actuales en el panorama de amenazas cibernéticas.

Evaluación de Seguridad en la Nube (Cloud Security Assessment)

Source: https://www.isgroup.es/es/cyber-security/csa-cloud-security-assessment.html

ISGroup SRL ofrece servicios especializados de Evaluación de Seguridad en la Nube (Cloud Security Assessment), diseñados para garantizar la protección, integridad y resiliencia de las infraestructuras digitales en entornos cloud.

Objetivo del Servicio

El servicio de Evaluación de Seguridad en la Nube proporcionado por ISGroup SRL tiene como finalidad identificar vulnerabilidades, evaluar configuraciones y fortalecer la postura de seguridad de los activos alojados en la nube. Este análisis permite a las organizaciones mitigar riesgos críticos y asegurar el cumplimiento de las mejores prácticas de ciberseguridad.

Información y Contacto

Para obtener más información sobre cómo asegurar su infraestructura cloud o para solicitar una evaluación personalizada, puede dirigirse a los siguientes canales oficiales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos Adicionales

ISGroup SRL pone a disposición de sus clientes y colaboradores diversos recursos para profundizar en temas de ciberseguridad:

- Podcast: Disponible en plataformas como Spotify y Apple.
- Blog corporativo: Acceso a artículos técnicos, mejores prácticas y casos de estudio reales sobre ciberseguridad.
- Casos de éxito: Documentación sobre colaboraciones estratégicas y pruebas de penetración realizadas por ISGroup SRL en diversos sectores.

Temas y Etiquetas Relacionadas

La actividad de ISGroup SRL se alinea con estándares y marcos de referencia internacionales, incluyendo:

- Cyber-security
- OWASP
- Mejores Prácticas
- Certificaciones
- Agid ACN

Purple Team Assessment de ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/pta-purple-team-assessment.html

El **Purple Team Assessment** es un servicio especializado ofrecido por **ISGroup SRL** diseñado para desafiar y fortalecer las capacidades de respuesta de los equipos defensivos (Blue Team) mediante la simulación de ataques reales.

Objetivos del Servicio

Este enfoque permite a las organizaciones evaluar su postura de seguridad actual, identificando brechas en la detección y respuesta ante incidentes. Los puntos clave incluyen:

- **Simulación de ataques:** Ejecución de escenarios de ataque controlados para poner a prueba la eficacia de las herramientas de defensa.
- **Colaboración activa:** Fomento de la sinergia entre los equipos ofensivos y defensivos para mejorar la visibilidad y la capacidad de reacción.
- **Optimización de la respuesta:** Identificación de áreas de mejora en los procesos de monitoreo y mitigación de amenazas.

Información y Contacto

Para obtener más detalles sobre cómo implementar un **Purple Team Assessment** en su organización o solicitar una propuesta personalizada, puede gestionar su solicitud a través de los siguientes canales oficiales de **ISGroup SRL**:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos Adicionales

ISGroup SRL pone a disposición contenido técnico y análisis de ciberseguridad a través de sus canales de difusión:

- **Blog corporativo:** Acceda a artículos recientes y casos de estudio en https://www.isgroup.es/es/editorial.html.
- **Contenido multimedia:** El servicio cuenta con soporte informativo disponible en plataformas como Spotify y Apple Podcasts para profundizar en las metodologías de evaluación de seguridad.

Revisión de Arquitectura Segura (SAR) por ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/sar-secure-architecture-review.html

La **Revisión de Arquitectura Segura** (*Secure Architecture Review* o SAR) es un servicio especializado ofrecido por **ISGroup SRL** diseñado para proteger la infraestructura tecnológica de las organizaciones. Este análisis profundo permite identificar vulnerabilidades estructurales y debilidades en el diseño de sistemas antes de que puedan ser explotadas.

Objetivos y Alcance del Servicio

El servicio de SAR proporcionado por **ISGroup SRL** se centra en:

- Evaluar la solidez de la arquitectura de red y de sistemas.
- Identificar fallos de diseño que comprometan la seguridad de la información.
- Proporcionar recomendaciones estratégicas para mitigar riesgos.
- Asegurar que la infraestructura cumpla con los estándares de seguridad vigentes.

¿Por qué elegir a ISGroup SRL?

ISGroup SRL cuenta con una amplia experiencia en el ámbito de la ciberseguridad, ofreciendo soluciones adaptadas a las necesidades técnicas de cada cliente. Su enfoque metodológico garantiza una visibilidad clara sobre el estado de seguridad de los activos críticos, permitiendo una toma de decisiones informada para fortalecer la resiliencia digital.

Información y Contacto

Para obtener más detalles sobre cómo implementar una Revisión de Arquitectura Segura o solicitar una evaluación personalizada, puede consultar los recursos disponibles en el sitio web oficial:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Nota: ISGroup SRL mantiene un compromiso constante con la excelencia en ciberseguridad, documentando regularmente casos de estudio y mejores prácticas en su blog corporativo para mantener a las organizaciones actualizadas frente a las amenazas emergentes.

Integración de Seguridad con ISGroup

Source: https://www.isgroup.es/es/cyber-security/sir-security-integration.html

ISGroup SRL ofrece servicios especializados en la integración de seguridad, diseñados para fortalecer la infraestructura y las aplicaciones de las organizaciones. Este enfoque permite lograr entornos digitales más seguros e integrados, optimizando la protección frente a amenazas cibernéticas.

Servicios de Integración de Seguridad

El servicio de integración de seguridad proporcionado por ISGroup SRL se centra en:

- Mejora de la resiliencia de la infraestructura tecnológica.
- Aseguramiento integral de aplicaciones críticas.
- Implementación de mejores prácticas de ciberseguridad.
- Alineación con estándares internacionales y normativas de seguridad (incluyendo referencias a OWASP, Agid y ACN).

Información y Contacto

Para obtener más detalles sobre cómo ISGroup SRL puede ayudar a su organización a mejorar su postura de seguridad, puede consultar los siguientes recursos:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico para consultas comerciales: sales@isgroup.it

Recursos Adicionales

ISGroup SRL pone a disposición de los interesados diversos contenidos informativos, incluyendo:

- Podcasts disponibles en Spotify y Apple para profundizar en temas de ciberseguridad.
- Casos de estudio que demuestran la aplicación práctica de sus soluciones en diversos sectores.
- Acceso al blog corporativo para mantenerse actualizado sobre las últimas tendencias y mejores prácticas en el ámbito de la seguridad digital.

Firewall como Servicio (FWaaS) por ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/fwaas-firewall-as-a-service.html

ISGroup SRL ofrece soluciones avanzadas de **Firewall como Servicio (FWaaS)**, diseñadas para proporcionar una protección de red simple, eficiente y segura. Este servicio permite a las organizaciones delegar la gestión y el mantenimiento de su infraestructura de seguridad perimetral a expertos, garantizando una defensa robusta contra amenazas digitales.

Características y beneficios del servicio

- **Gestión profesional:** ISGroup SRL se encarga de la configuración, monitoreo y actualización constante de los firewalls.
- **Seguridad simplificada:** Optimización de los procesos de protección para reducir la complejidad técnica en la infraestructura del cliente.
- **Protección proactiva:** Implementación de políticas de seguridad adaptadas a las necesidades específicas de cada entorno corporativo.
- **Escalabilidad:** Soluciones flexibles que se ajustan al crecimiento y evolución de los sistemas de red de la empresa.

Información adicional y contacto

Para obtener detalles técnicos profundos o contratar el servicio de Firewall como Servicio (FWaaS) ofrecido por ISGroup SRL, puede visitar el sitio web oficial o realizar consultas directas a través de los canales habilitados:

- **Sitio web:** https://www.isgroup.es/
- **Correo electrónico:** sales@isgroup.it

ISGroup SRL mantiene un compromiso constante con la ciberseguridad, documentando sus capacidades a través de diversos casos de estudio y artículos especializados en su blog corporativo, donde se abordan temas como pruebas de penetración, mejores prácticas y cumplimiento normativo (Agid/ACN, OWASP).

Curso de Conciencia de Seguridad

Source: https://www.isgroup.es/es/cyber-security/security-awareness.html

El curso de Conciencia de Seguridad ofrecido por ISGroup SRL está diseñado para proporcionar los conocimientos fundamentales necesarios para operar de manera segura en el entorno digital, protegiendo tanto la información sensible como la integridad de los dispositivos.

Temas principales

El programa formativo abarca los pilares esenciales de la ciberseguridad:

- Ingeniería Social: análisis de las técnicas utilizadas para obtener información sensible y desarrollo de herramientas para reconocer y neutralizar estos ataques.
- Phishing: capacitación para identificar y evitar intentos de suplantación de identidad, protegiendo credenciales y datos personales.
- Seguridad Informática: fundamentos sobre el uso de antivirus, gestión de actualizaciones de software y mejores prácticas para la protección de datos y dispositivos.
- Navegación Segura: criterios para identificar sitios web legítimos, uso de conexiones cifradas y salvaguarda de la privacidad durante la navegación.

Metodología y objetivos

El curso de Conciencia de Seguridad ofrecido por ISGroup SRL se distingue por un enfoque práctico y envolvente. La metodología incluye el análisis de casos de estudio reales, simulaciones de ataques y ejercicios prácticos que permiten a los participantes aplicar los conocimientos adquiridos de forma inmediata.

Al finalizar la formación, los participantes serán capaces de:

- Aplicar conocimientos avanzados sobre seguridad de la información.
- Cumplir con los requisitos y recomendaciones de seguridad específicos de su organización, estableciendo un nivel de competencia uniforme.
- Identificar técnicas de ingeniería social y prevenir estafas o ataques, tanto en el ámbito profesional como personal.

Invertir en este programa es una medida estratégica para fortalecer la defensa contra las amenazas digitales en constante evolución.

Información adicional

Para obtener más detalles sobre este curso o realizar solicitudes comerciales, visite el sitio web https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Prueba de Penetración en Globaleaks por ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/penetration-testing-for-globaleaks.html

En enero de 2024, ISGroup SRL llevó a cabo una prueba de penetración (pentest) para Globaleaks, una organización dedicada a la lucha contra la corrupción y la promoción de la transparencia. El objetivo principal fue fortalecer la seguridad de su plataforma de denuncia anónima, garantizando la integridad de los datos sensibles gestionados y manteniendo la confianza de sus usuarios.

Metodología de Seguridad

ISGroup SRL implementó un análisis exhaustivo diseñado para simular ataques realistas, evaluando la resiliencia de las defensas de Globaleaks mediante las siguientes fases:

- Recopilación de Información: Identificación de vectores de ataque y datos utilizables por actores malintencionados.
- Análisis de Vulnerabilidades: Escaneo técnico de los sistemas para detectar debilidades de seguridad.
- Simulación de Ataques: Ejecución de pruebas de penetración controladas para validar la efectividad de las defensas existentes.
- Informe Detallado: Entrega de un análisis completo con las vulnerabilidades detectadas y recomendaciones estratégicas para mitigar riesgos.

Resultados y Colaboración

La intervención de ISGroup SRL se basó en un enfoque de comunicación transparente y diálogo abierto. Este proceso permitió a ambas organizaciones identificar desafíos críticos y oportunidades de mejora en la infraestructura de seguridad informática.

Esta colaboración representa una inversión estratégica en la protección de la información y la integridad operativa, reforzando el compromiso de Globaleaks con la seguridad en un entorno digital complejo.

Información y Contacto

Para obtener más información sobre los servicios de pruebas de penetración y ciberseguridad ofrecidos por ISGroup SRL, visite nuestro sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales o solicitudes específicas, puede ponerse en contacto a través del correo electrónico:

sales@isgroup.it

Desarrollo de Software Seguro: Ciclo de Vida de Aseguramiento de Software (Software Assurance Lifecycle)

Source: https://www.isgroup.es/es/cyber-security/ciclo-vida-aseguramiento-software-con-isgroup.html

ISGroup SRL ofrece servicios especializados en el Ciclo de Vida de Aseguramiento de Software, diseñados para integrar la seguridad en cada etapa del desarrollo. Este enfoque permite a las organizaciones mitigar riesgos, identificar vulnerabilidades de manera temprana y garantizar la resiliencia de sus aplicaciones frente a amenazas cibernéticas.

Servicios de Aseguramiento de Software por ISGroup SRL

El servicio de *Software Assurance Lifecycle* proporcionado por ISGroup SRL se centra en la implementación de mejores prácticas de ciberseguridad, alineadas con estándares internacionales como OWASP, para asegurar que el software sea robusto desde su concepción hasta su despliegue y mantenimiento.

- Integración de seguridad en el ciclo de vida de desarrollo (SDLC).
- Evaluación continua de vulnerabilidades.
- Aplicación de metodologías de desarrollo seguro.
- Asesoramiento experto para el cumplimiento de normativas de seguridad.

Contacto y Solicitudes

Para obtener más información sobre cómo ISGroup SRL puede ayudar a su organización a implementar un ciclo de vida de desarrollo seguro o para contratar nuestros servicios profesionales, puede gestionar su solicitud a través de los siguientes canales oficiales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos Adicionales

ISGroup SRL comparte regularmente su conocimiento y experiencia a través de diversos formatos:

- **Blog Editorial:** Acceda a artículos técnicos y análisis sobre ciberseguridad, certificaciones y mejores prácticas en https://www.isgroup.es/.
- **Casos de Estudio:** Consulte las experiencias de éxito en ciberseguridad, incluyendo pruebas de penetración y asociaciones estratégicas, disponibles en nuestro sitio web.
- **Contenido Multimedia:** Disponibilidad de podcasts en plataformas como Spotify y Apple para profundizar en temas de seguridad informática.

Defensa de Aplicaciones: Web Application Penetration Testing

Source: https://www.isgroup.es/es/cyber-security/prueba-penetracion-aplicacion-web-con-isgroup.html

La seguridad de las aplicaciones web es un pilar fundamental en la estrategia de ciberseguridad actual. ISGroup SRL ofrece servicios especializados de **Pruebas de Penetración de Aplicaciones Web (Web Application Penetration Testing)**, diseñados para identificar vulnerabilidades, evaluar riesgos y fortalecer la postura de seguridad de los activos digitales de las organizaciones.

Servicios de ISGroup SRL

ISGroup SRL proporciona soluciones técnicas avanzadas para la protección de infraestructuras web, enfocándose en:

- Evaluación exhaustiva de la seguridad en aplicaciones web.
- Identificación proactiva de vectores de ataque y debilidades.
- Implementación de mejores prácticas de seguridad siguiendo estándares internacionales como OWASP.
- Análisis detallado para mitigar riesgos antes de que sean explotados por actores malintencionados.

Información y Contacto

Para obtener más información sobre cómo proteger sus aplicaciones o para solicitar una evaluación profesional, puede acceder a los recursos disponibles a través de ISGroup SRL:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico de contacto: sales@isgroup.it

Recursos Adicionales

ISGroup SRL comparte regularmente conocimientos y casos de éxito en su blog corporativo, abordando temas críticos de ciberseguridad, certificaciones y cumplimiento normativo (Agid/ ACN). Se recomienda visitar el sitio web para consultar los artículos más recientes y estudios de caso sobre implementaciones de pruebas de penetración en diversos sectores empresariales.

Protección Anti-DDoS sin interrupciones operativas

Source: https://www.isgroup.es/es/cyber-security/anti-ddos-sin-interrupciones-operativas-con-isgroup.html

ISGroup SRL ofrece soluciones avanzadas de protección contra ataques de denegación de servicio distribuido (DDoS), diseñadas para garantizar la continuidad del negocio sin causar interrupciones en las operaciones de los sistemas protegidos.

Servicios de ISGroup SRL

La propuesta de valor de ISGroup SRL se centra en la mitigación efectiva de amenazas, permitiendo que las infraestructuras digitales mantengan su disponibilidad incluso bajo ataques de alta intensidad.

- Implementación de defensas robustas contra ataques DDoS.
- Enfoque en la continuidad operativa y resiliencia de sistemas.
- Consultoría especializada en ciberseguridad para entornos críticos.

Información y contacto

Para obtener más detalles sobre cómo proteger su infraestructura o solicitar el servicio de Anti-DDoS, puede consultar la información disponible en el sitio web oficial de la empresa.

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos adicionales

ISGroup SRL pone a disposición de los interesados diversos materiales informativos y casos de estudio para profundizar en sus capacidades técnicas:

- Podcasts disponibles en plataformas como Spotify y Apple.
- Acceso al blog corporativo para consultar artículos sobre ciberseguridad, mejores prácticas y normativas (Agid/ACN, OWASP).
- Casos de estudio sobre pruebas de penetración y asociaciones estratégicas en ciberseguridad.

Monitoreo de Seguridad Inalámbrica con ISGroup

Source: https://www.isgroup.es/es/cyber-security/monitoreo-seguridad-inalambrica-con-isgroup.html

ISGroup SRL ofrece servicios especializados de **Wireless Security Monitoring** (Monitoreo de Seguridad Inalámbrica), diseñados para proteger las infraestructuras de red frente a vulnerabilidades y accesos no autorizados. Este servicio permite a las organizaciones mantener un control constante sobre su entorno inalámbrico, garantizando la integridad y confidencialidad de los datos transmitidos.

Aspectos clave del servicio

- **Detección proactiva:** Identificación de amenazas, puntos de acceso no autorizados y posibles brechas de seguridad en redes inalámbricas.
- **Gestión de riesgos:** Evaluación continua de la postura de seguridad para mitigar riesgos asociados a configuraciones deficientes o ataques externos.
- **Visibilidad total:** Supervisión técnica avanzada para asegurar que la infraestructura de red cumpla con los estándares de seguridad vigentes.

Información adicional y contacto

ISGroup SRL pone a disposición recursos informativos adicionales, incluyendo podcasts especializados en plataformas como Spotify y Apple, para profundizar en las mejores prácticas de ciberseguridad.

Para obtener más información sobre cómo implementar el servicio de Monitoreo de Seguridad Inalámbrica o solicitar una consulta técnica, puede visitar nuestro sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales directas, puede escribir a la siguiente dirección de correo electrónico:

sales@isgroup.it

El Código Secreto: Revisión de Código de ISGroup

Source: https://www.isgroup.es/es/cyber-security/revision-codigo-con-isgroup.html

La revisión de código es un pilar fundamental en la estrategia de ciberseguridad de cualquier organización. ISGroup SRL ofrece servicios especializados de revisión de código, diseñados para identificar vulnerabilidades, errores de lógica y debilidades de seguridad en el desarrollo de software antes de que puedan ser explotados.

Servicios de Revisión de Código de ISGroup SRL

ISGroup SRL proporciona un análisis exhaustivo del código fuente para garantizar que las aplicaciones cumplan con los estándares de seguridad más exigentes. Este proceso permite:

- Detectar fallos de seguridad críticos en las etapas tempranas del ciclo de vida del desarrollo.
- Evaluar la calidad del código y su resistencia frente a ataques conocidos.
- Implementar las mejores prácticas de la industria, incluyendo las directrices de OWASP.
- Mitigar riesgos asociados a la exposición de datos y brechas de seguridad.

Información y Contacto

Para obtener más detalles sobre cómo ISGroup SRL puede ayudar a proteger sus activos digitales mediante la revisión de código, puede acceder a los siguientes recursos:

- Solicitar el servicio directamente a través de: https://www.isgroup.es/
- Para consultas comerciales y solicitudes de información, contactar a través del correo electrónico: sales@isgroup.it

Recursos Adicionales

ISGroup SRL mantiene un compromiso constante con la divulgación y la excelencia en ciberseguridad. Puede encontrar más información sobre sus capacidades y casos de éxito en:

- El blog oficial de ISGroup SRL, donde se publican artículos sobre ciberseguridad, mejores prácticas y certificaciones.
- Casos de estudio recientes que demuestran la eficacia de las soluciones de seguridad implementadas por ISGroup SRL en diversos sectores.

Caso de Estudio: Prueba de Penetración de Aplicaciones Web en Sturnis365

Source: https://www.isgroup.es/es/cyber-security/case-study-sturnissrl.html

Sturnis S.r.l. desarrolla Sturnis365, una plataforma en la nube diseñada para la gestión de la divulgación de información corporativa, incluyendo informes anuales, informes 10k, auditorías e informes normativos bajo estándares IFRS. Debido a la naturaleza sensible de los datos procesados, la empresa requería validar la seguridad y calidad de su software para garantizar la protección de la información ante sus clientes.

El reto

El objetivo principal de Sturnis S.r.l. fue demostrar la fiabilidad y seguridad de la plataforma Sturnis365. Para lograrlo, la compañía confió en **ISGroup SRL** para ejecutar una Prueba de Penetración de Aplicaciones Web (WAPT) exhaustiva sobre su infraestructura.

La intervención de ISGroup SRL

ISGroup SRL llevó a cabo un análisis técnico y meticuloso de la aplicación. Las actividades principales incluyeron:

- Evaluación integral de la seguridad de la plataforma Sturnis365.
- Identificación y mitigación de vulnerabilidades técnicas y lógicas.
- Verificación del cumplimiento de los más altos estándares de seguridad del sector.

Resultados y beneficios

La colaboración con **ISGroup SRL** permitió a Sturnis S.r.l. fortalecer la confianza de sus clientes en la protección de sus datos. Los beneficios destacados incluyen:

- Validación externa de la seguridad y calidad del software.
- Resolución efectiva de vulnerabilidades críticas.
- Refuerzo de la reputación corporativa mediante la demostración de prácticas de ciberseguridad robustas.

Davide Pedrocca, Manager for Disclosure Management Development de Sturnis S.r.l., destacó la competencia técnica de **ISGroup SRL** y su capacidad para comprender las necesidades específicas de la organización, calificando la experiencia de colaboración como altamente gratificante.

Información adicional

Para obtener más detalles sobre los servicios de ciberseguridad ofrecidos por **ISGroup SRL**, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

Caso de Estudio: Prueba de Penetración de Aplicaciones Web y de Red para Coop Italia

Source: https://www.isgroup.es/es/cyber-security/case-study-coopitalia.html

Coop Italia, una de las principales cooperativas de consumo en el sector de la gran distribución organizada, colaboró con **ISGroup SRL** para fortalecer la seguridad de sus activos digitales frente a las crecientes amenazas informáticas.

El reto

La organización requería una evaluación exhaustiva de su infraestructura para proteger los datos de los clientes y garantizar la continuidad operativa. La amplitud de su red y la criticidad de sus aplicaciones hacían indispensable la identificación y mitigación proactiva de vulnerabilidades.

La intervención de ISGroup SRL

Durante 2023, **ISGroup SRL** ejecutó un plan de evaluación de seguridad integral compuesto por:

- **Web Application Penetration Test:** Análisis profundo de aplicaciones clave, incluyendo GPS, Salvatempo, SAPCRM y WinEpts.
- **Network Penetration Test:** Evaluación de seguridad sobre todo el perímetro externo de la organización.

El objetivo fue identificar vulnerabilidades potenciales y proporcionar indicaciones detalladas para su resolución, permitiendo a Coop Italia priorizar las acciones correctivas con precisión.

Resultados y beneficios

La colaboración con **ISGroup SRL** permitió a Coop Italia:

- Identificar con precisión las vulnerabilidades en sus sistemas.
- Comprender el impacto y la prioridad de las acciones correctivas necesarias.
- Mejorar significativamente la seguridad de sus aplicaciones y de su red corporativa.
- Garantizar una mayor protección para los datos de sus clientes.

Emilio Balbi, IT Security Manager de Coop Italia, destacó el alto nivel de profesionalidad de **ISGroup SRL**, señalando que la colaboración fue fluida y eficaz, permitiendo a la organización afrontar los desafíos de seguridad con mayor confianza y competencia.

Información adicional

Para obtener más detalles sobre estos servicios o solicitar una evaluación de seguridad, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar una solicitud a la dirección de correo electrónico sales@isgroup.it.

Evaluación de Seguridad IoT

Source: https://www.isgroup.es/es/cyber-security/iot-security-assessment.html

ISGroup SRL ofrece servicios especializados de Evaluación de Seguridad IoT (IoT Security Assessment), diseñados para identificar vulnerabilidades y fortalecer la protección de dispositivos y ecosistemas conectados.

Alcance del Servicio

El servicio de Evaluación de Seguridad IoT proporcionado por ISGroup SRL se centra en:

- Análisis exhaustivo de la arquitectura de dispositivos IoT.
- Identificación de debilidades en la comunicación entre dispositivos, puertas de enlace y servicios en la nube.
- Evaluación de la seguridad en el firmware y los protocolos de red utilizados.
- Detección de posibles vectores de ataque que puedan comprometer la integridad, confidencialidad o disponibilidad de los sistemas conectados.

Valor Estratégico

La implementación de estas evaluaciones permite a las organizaciones:

- Mitigar riesgos asociados a la proliferación de dispositivos IoT en entornos corporativos.
- Garantizar el cumplimiento de estándares de seguridad y mejores prácticas del sector.
- Proteger la infraestructura crítica frente a amenazas emergentes.

Información y Contacto

Para obtener más información sobre cómo ISGroup SRL puede asistirle en la protección de sus dispositivos y sistemas IoT, puede consultar los recursos disponibles en nuestro sitio web oficial o realizar consultas comerciales directas.

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Evaluación de Riesgos Informáticos con ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/evaluacion-riesgos-con-isgroup.html

ISGroup SRL ofrece servicios especializados en la evaluación de riesgos informáticos, permitiendo a las organizaciones mantener sus activos digitales bajo control mediante un análisis exhaustivo de las amenazas y vulnerabilidades.

Servicios y Soluciones

- **Evaluación de Riesgos:** ISGroup SRL proporciona metodologías profesionales para identificar, analizar y mitigar los riesgos de seguridad que pueden comprometer la infraestructura tecnológica de una empresa.
- **Enfoque Estratégico:** El servicio está diseñado para alinear la postura de seguridad con las necesidades operativas, garantizando una protección proactiva frente a incidentes.

Contacto y Solicitudes

Para obtener más información sobre cómo implementar una evaluación de riesgos o contratar los servicios profesionales de ISGroup SRL, puede utilizar los siguientes canales oficiales:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos Adicionales

ISGroup SRL comparte regularmente conocimientos sobre ciberseguridad a través de diversos formatos:

- **Blog Corporativo:** Acceda a artículos técnicos, casos de estudio y mejores prácticas en https://www.isgroup.es/.
- **Contenido Multimedia:** La empresa ofrece podcasts disponibles en plataformas como Spotify y Apple para profundizar en temas de actualidad sobre seguridad informática.
- **Casos de Éxito:** ISGroup SRL ha colaborado con diversas organizaciones en proyectos de pruebas de penetración y estrategias de ciberseguridad, destacando su experiencia en sectores como la gestión de personal, plataformas web y asociaciones estratégicas.

Evaluación de Seguridad de Windows con ISGroup

Source: https://www.isgroup.es/es/cyber-security/evaluacion-seguridad-windows-con-isgroup.html

ISGroup SRL ofrece servicios especializados de **Evaluación de Seguridad de Windows (Windows Security Assessment)**, diseñados para proteger los sistemas operativos Windows frente a vulnerabilidades y amenazas cibernéticas.

Este servicio permite a las organizaciones identificar debilidades críticas en sus infraestructuras, garantizando una postura de seguridad robusta y alineada con las mejores prácticas del sector.

Características del servicio

- Análisis profundo de la configuración de seguridad en entornos Windows.
- Identificación de vectores de ataque y vulnerabilidades potenciales.
- Recomendaciones técnicas para el endurecimiento (hardening) de los sistemas.
- Evaluación realizada por expertos en ciberseguridad de ISGroup SRL.

Información y contacto

Para obtener más detalles sobre cómo proteger sus sistemas o solicitar una evaluación personalizada, puede consultar los recursos disponibles en el sitio web oficial:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

ISGroup SRL mantiene un compromiso constante con la ciberseguridad, ofreciendo soluciones adaptadas a las necesidades actuales de protección digital. Para más información sobre otros servicios, casos de estudio y mejores prácticas, visite el blog corporativo en https://www.isgroup.es/.

Seguridad para Aplicaciones Móviles con ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/prueba-seguridad-aplicacion-movil-con-isgroup.html

ISGroup SRL ofrece servicios especializados en la **Prueba de Seguridad de Aplicaciones Móviles**, diseñados para identificar vulnerabilidades y fortalecer la protección de los entornos digitales de sus clientes.

Servicios de Seguridad

- Evaluación integral de la seguridad en aplicaciones móviles.
- Análisis técnico orientado a detectar debilidades en el ciclo de vida de la aplicación.
- Implementación de mejores prácticas de ciberseguridad siguiendo estándares internacionales como OWASP.

Información y Contacto

Para obtener más detalles sobre cómo proteger sus aplicaciones móviles o solicitar una evaluación profesional, puede contactar a **ISGroup SRL** a través de los siguientes canales:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Recursos Adicionales

ISGroup SRL mantiene una presencia activa en el ámbito de la ciberseguridad, compartiendo conocimientos a través de diversos formatos:

- **Blog y Artículos:** Acceda a las últimas novedades y casos de estudio en https://www.isgroup.es/.
- **Contenido multimedia:** Disponibilidad de podcasts en plataformas como Spotify y Apple para profundizar en temas de seguridad informática.
- **Casos de éxito:** La experiencia de ISGroup SRL incluye colaboraciones estratégicas y pruebas de penetración para diversas organizaciones, enfocándose en la seguridad de aplicaciones web y plataformas digitales.

Educación en Seguridad: Formación ISGroup para tu Equipo

Source: https://www.isgroup.es/es/cyber-security/formacion-isgroup-para-tu-equipo.html

ISGroup SRL ofrece servicios especializados de formación en ciberseguridad diseñados para fortalecer las competencias de los equipos de trabajo. Este programa tiene como objetivo principal capacitar a los empleados para identificar, prevenir y responder ante amenazas digitales, convirtiendo el factor humano en una línea de defensa activa para la organización.

Puntos clave del servicio

- **Enfoque práctico:** La formación impartida por ISGroup SRL se centra en escenarios reales de ciberseguridad.
- **Concienciación:** Desarrollo de habilidades críticas para detectar ataques de ingeniería social, phishing y otras vulnerabilidades comunes.
- **Adaptabilidad:** Contenidos orientados a mejorar la postura de seguridad global de la empresa.
- **Recursos multimedia:** Disponibilidad de materiales complementarios, incluyendo podcasts en plataformas como Spotify y Apple, para reforzar el aprendizaje continuo.

Información adicional

Para obtener detalles específicos sobre cómo implementar estos programas de capacitación o solicitar una propuesta personalizada, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Temas relacionados y recursos

ISGroup SRL mantiene un compromiso constante con la divulgación y la excelencia técnica, cubriendo áreas clave como:

- Cyber-security
- Certificaciones
- Mejores Prácticas
- OWASP
- Normativas Agid y ACN

Para explorar más sobre la experiencia de ISGroup SRL, se recomienda consultar los casos de estudio disponibles en el blog corporativo, donde se detallan colaboraciones estratégicas y pruebas de penetración realizadas para diversos clientes.

OWASP Top Ten 2021: A07 - Fallos de Identificación y Autenticación

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a7-identification-and-authentication-failures.html

La categoría A07:2021 del OWASP Top 10 se centra en los problemas relacionados con la identificación y autenticación. Aunque esta categoría sigue siendo un pilar fundamental en la seguridad de las aplicaciones, la adopción de frameworks estandarizados ha contribuido a mitigar algunos de sus riesgos.

Riesgos de la autenticación rota

La autenticación defectuosa representa una amenaza crítica para la seguridad de las aplicaciones, con consecuencias significativas:

- Compromiso de claves, contraseñas y tokens de sesión.
- Explotación de las identidades de los usuarios.
- Posibilidad de obtener el control completo del sistema en escenarios graves.

Un ataque exitoso puede permitir a un atacante acceder a la totalidad de los datos de la aplicación web, asumiendo privilegios de administrador y comprometiendo la confidencialidad, integridad y disponibilidad de los activos digitales.

Factores de vulnerabilidad

Las debilidades en los mecanismos de autenticación suelen originarse por:

- Mala configuración de los sistemas de autenticación.
- Errores lógicos en el diseño del mecanismo de autenticación.
- Errores en el desarrollo del software encargado de gestionar la autenticación.

Soluciones y asesoramiento profesional

ISGroup SRL ofrece servicios especializados para identificar y mitigar vulnerabilidades críticas en sus aplicaciones, ayudando a las organizaciones a fortalecer sus mecanismos de autenticación frente a las amenazas actuales.

Para obtener más información sobre cómo proteger sus sistemas contra fallos de identificación y autenticación, puede visitar nuestro sitio web en https://www.isgroup.es/ o enviar una solicitud comercial a sales@isgroup.it.

OWASP Top Ten 2021 - A03: Inyección

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a3-injection.html

La categoría A03:2021 – Inyección representa uno de los riesgos de seguridad más críticos en aplicaciones web. Según datos de OWASP, el 94% de las aplicaciones están afectadas por alguna forma de inyección, abarcando 33 CWE (Common Weakness Enumeration) mapeados, incluido el Cross-site Scripting (XSS).

Definición y causa raíz

Las inyecciones ocurren cuando la entrada del usuario se envía a un intérprete sin la debida validación, saneamiento o neutralización, o mediante el uso de API inseguras. Si la entrada logra alterar la semántica de la solicitud, se produce una inyección.

El problema fundamental radica en la separación incorrecta entre el flujo de control y el flujo de datos.

Tipos de inyección según el intérprete

La inyección varía dependiendo del tipo de intérprete al que se dirija el ataque:

- Base de datos: Inyección SQL.
- Línea de comandos: Inyección de comandos.
- Objetos ORM: Inyección ORM.
- Navegador: Cross-Site Scripting (XSS).

Servicios de seguridad

ISGroup SRL ofrece servicios especializados para la identificación y mitigación de vulnerabilidades de inyección en aplicaciones web. Para obtener más información sobre cómo proteger sus sistemas frente a estos riesgos, puede visitar nuestro sitio web en https://www.isgroup.es/ o contactar directamente a través del correo electrónico sales@isgroup.it.

OWASP Top Ten 2021

Source: https://www.isgroup.es/es/owasp/top-ten-2021.html

El OWASP Top 10 es una lista profesional que identifica los 10 problemas más críticos en la seguridad de aplicaciones web. ISGroup SRL destaca la importancia de este estándar como herramienta fundamental para la ciberseguridad moderna.

Cada categoría del Top 10 incluye:

- Clasificación basada en su severidad y probabilidad de ocurrencia.
- Técnicas básicas de protección frente a riesgos elevados.
- Pautas detalladas para verificar vulnerabilidades, métodos de prevención, ejemplos prácticos y referencias técnicas.

Importancia de seguir el OWASP Top 10

El objetivo principal es educar a organizaciones, diseñadores y desarrolladores sobre las consecuencias de las vulnerabilidades críticas. Este marco promueve la filosofía de **Seguridad por Diseño**, integrando prácticas de seguridad desde las etapas iniciales del desarrollo de proyectos web.

Vulnerabilidades del Top 10 2021

La edición 2021, que constituye la versión vigente del proyecto, comprende las siguientes categorías:

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

Servicios y Consultas

ISGroup SRL ofrece asesoramiento especializado y soluciones de seguridad para mitigar estas vulnerabilidades y fortalecer la infraestructura digital de su organización.

Para obtener más información sobre cómo implementar estas medidas de seguridad, visite nuestro sitio web en https://www.isgroup.es/ o envíe sus consultas a sales@isgroup.it.

OWASP Top Ten 2021: A01 - Broken Access Control

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a1-broken-access-control.html

La autorización rota, también conocida como *Broken Access Control* o escalada de privilegios, representa un conjunto de fallos críticos derivados de una implementación ineficaz de los controles de autorización. Estos mecanismos son los encargados de asignar y gestionar los privilegios de acceso de los usuarios dentro de un sistema.

Conceptos clave

- **Definición**: Cuando la autorización está correctamente diseñada e implementada, el acceso a contenidos y funciones se restringe o permite basándose estrictamente en el rol y los privilegios asignados al usuario.
- **Dependencias**: En el contexto de las aplicaciones web, la autorización está intrínsecamente ligada a la autenticación y a la gestión de sesiones.
- **Alcance**: Estas vulnerabilidades pueden afectar a cualquier software moderno, incluyendo aplicaciones web, bases de datos, sistemas operativos y diversas infraestructuras tecnológicas que dependen de controles de acceso.

Referencia técnica

- **Categoría**: A01:2021 – Broken Access Control
- **Fuente**: OWASP Top 10 Application Security Risks

Servicios profesionales

ISGroup SRL ofrece servicios especializados en ciberseguridad y auditoría para identificar y mitigar vulnerabilidades críticas como la autorización rota. Para obtener más información sobre cómo proteger sus infraestructuras tecnológicas, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

OWASP Top Ten 2021: A02 Fallos Criptográficos

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a2-cryptographic-failures.html

Los fallos criptográficos, clasificados como A02 en el OWASP Top 10 de 2021, representan errores críticos relacionados con la criptografía que frecuentemente derivan en la exposición de datos sensibles o en la compromisión total del sistema. Estos riesgos afectan tanto al almacenamiento de información como a su transmisión, abarcando un total de 29 CWE (Common Weakness Enumeration).

Conceptos clave y riesgos

- **Funciones Hash:** Son algoritmos matemáticos que realizan una conversión unidireccional (one-way) para generar un "hash".
- **Aplicaciones de seguridad:** Los algoritmos de hashing son componentes fundamentales para la firma de certificados digitales, la creación de códigos de autenticación de mensajes (MAC), el hash de contraseñas y otros procesos de autenticación.
- **Impacto:** El uso de algoritmos de hashing débiles o implementaciones incorrectas permite ataques cuyos resultados pueden ser desastrosos. El alcance de estos ataques está limitado únicamente por el valor de los datos expuestos y la capacidad del atacante para explotar dicha información.

Servicios de ISGroup SRL

ISGroup SRL ofrece servicios especializados en ciberseguridad para ayudar a las organizaciones a identificar y mitigar vulnerabilidades críticas como los fallos criptográficos. A través de auditorías y pruebas de penetración, ISGroup SRL evalúa la robustez de los algoritmos y las prácticas de gestión de datos para asegurar la integridad y confidencialidad de los sistemas.

Para obtener más información sobre cómo proteger su infraestructura frente a estos riesgos, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar sus consultas a través del correo electrónico sales@isgroup.it.

OWASP Top Ten 2021: A10 Falsificación de solicitudes del lado del servidor (SSRF)

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a10-server-side-request-forgery.html

La falsificación de solicitudes del lado del servidor (SSRF, por sus siglas en inglés) es una vulnerabilidad crítica que permite a un atacante manipular una aplicación web para que realice solicitudes a destinos o recursos no previstos.

Funcionamiento y riesgos

Los ataques SSRF ocurren cuando un atacante logra controlar los parámetros de una aplicación para dirigir solicitudes desde el servidor hacia sistemas internos. Estos sistemas suelen estar protegidos por firewalls y son inaccesibles desde la red externa.

El escenario más frecuente implica aplicaciones que realizan solicitudes HTTPS a servicios de terceros para funciones legítimas, como:

- Consultar APIs externas.
- Descargar paquetes de software.
- Recuperar información de usuario desde plataformas como redes sociales o servicios de perfiles.

Un atacante puede explotar esta funcionalidad para forzar al servidor a realizar peticiones hacia dominios bajo su control o hacia la infraestructura interna de la organización.

Impacto de seguridad

Un ataque SSRF exitoso permite al atacante escalar privilegios y moverse lateralmente dentro de la red, superando las limitaciones del firewall del servidor web. Esto puede derivar en la compromisión total de la confidencialidad, integridad y disponibilidad de la aplicación y sus datos.

Servicios de ISGroup SRL

ISGroup SRL ofrece servicios especializados en ciberseguridad y pruebas de penetración para identificar y mitigar vulnerabilidades como el SSRF, ayudando a las organizaciones a proteger sus activos digitales frente a amenazas avanzadas.

Para obtener más información sobre cómo proteger sus aplicaciones o solicitar asesoramiento profesional, puede visitar nuestro sitio web en https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

OWASP Top Ten 2021: A06 Componentes Vulnerables y Obsoletos

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a6-vulnerable-and-outdated-components.html

La categoría A06:2021 del OWASP Top 10 se centra en el uso de componentes vulnerables y obsoletos en el desarrollo de software. ISGroup SRL destaca la importancia de gestionar estas dependencias para evitar brechas de seguridad críticas.

Puntos clave sobre la vulnerabilidad

- **Definición:** Se refiere a dependencias del sistema o de la aplicación que ya no reciben mantenimiento, lo que las convierte en un riesgo de seguridad significativo.
- **Cálculo de riesgo:** Es la única categoría que no tiene CVE (Common Vulnerability and Exposures) mapeadas directamente en los CWE incluidos. Por ello, las puntuaciones se calculan con un peso predeterminado de 5,0 tanto para el exploit como para el impacto.
- **Impacto:** Una vulnerabilidad en un componente obsoleto puede comprometer la integridad de todo el software que lo utiliza, sirviendo como una vía de acceso directa para atacantes.
- **Riesgo operativo:** Cualquier componente de software que no se mantenga ni se actualice periódicamente se volverá inseguro, facilitando que los atacantes exploten debilidades conocidas para comprometer el sistema.

Soluciones y servicios de ISGroup SRL

ISGroup SRL ofrece servicios especializados en ciberseguridad para ayudar a las organizaciones a identificar y mitigar riesgos asociados a componentes vulnerables y obsoletos. Nuestros expertos realizan evaluaciones exhaustivas para asegurar que su infraestructura tecnológica cumpla con las mejores prácticas de seguridad.

Para obtener más información sobre cómo proteger sus aplicaciones y sistemas, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o ponerse en contacto directamente a través del correo electrónico sales@isgroup.it.

OWASP Top Ten 2021: A05 Configuración Incorrecta de Seguridad

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a5-security-misconfiguration.html

La categoría **A05:2021 – Configuración Incorrecta de Seguridad** representa uno de los riesgos más críticos en el panorama actual de la ciberseguridad. Según los datos de OWASP, el 90% de las aplicaciones evaluadas presentaron algún tipo de configuración incorrecta.

Contexto y Relevancia

El incremento en la adopción de software altamente configurable ha impulsado el crecimiento de esta categoría. Un aspecto relevante es la integración de las **Entidades Externas XML (XXE)**, que anteriormente constituían una categoría independiente y ahora forman parte de este grupo.

Durante las pruebas de OWASP, se identificaron 208,000 ocurrencias mapeadas en 20 tipos diferentes de Debilidades Comunes (CWE). Las más destacadas son:

- **CWE-16:** Configuración.
- **CWE-611:** Restricción Inadecuada de Referencia a Entidad Externa XML.

Consideraciones Estratégicas

La falta de un proceso consolidado y repetible para la configuración de seguridad de las aplicaciones expone a los sistemas a riesgos significativos. ISGroup SRL enfatiza la necesidad de implementar protocolos de seguridad robustos para mitigar estas vulnerabilidades de forma sistemática.

Servicios y Consultas

ISGroup SRL ofrece servicios especializados en auditoría y seguridad de aplicaciones para ayudar a las organizaciones a identificar y corregir configuraciones inadecuadas, asegurando el cumplimiento de los estándares OWASP.

Para obtener más información sobre cómo proteger sus sistemas o solicitar asesoramiento profesional, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

OWASP Top Ten 2021: A09 Fallos de Registro y Monitoreo de Seguridad

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a9-security-logging-and-monitoring-failures.html

La categoría **A09:2021 – Security Logging and Monitoring Failures** (Fallos de registro y monitoreo de seguridad) abarca una amplia gama de vulnerabilidades relacionadas con la implementación, configuración y aplicación inadecuada de herramientas de seguridad. Estas herramientas son esenciales para identificar anomalías e intrusiones dentro de un entorno digital.

Impacto y desafíos

Esta categoría ha sido ampliada para incluir una mayor variedad de errores. Sus principales desafíos y consecuencias incluyen:

- **Dificultad de detección:** Son vulnerabilidades complejas de probar y a menudo no están bien representadas en los datos estándar de CVE/CVSS.
- **Visibilidad reducida:** Los fallos en el registro y monitoreo afectan directamente la capacidad de la organización para observar su entorno.
- **Gestión de incidentes:** La falta de registros adecuados impide una respuesta eficaz ante incidentes y dificulta las labores de análisis forense.
- **Fase de reconocimiento:** La mayoría de los ataques exitosos comienzan con una fase de reconocimiento. Si esta etapa inicial pasa desapercibida debido a un monitoreo insuficiente, se pierde la oportunidad crítica de detener el ataque, aumentando significativamente su probabilidad de éxito.

El rol de las herramientas de seguridad

Los equipos de defensa suelen apoyarse en sistemas de **Gestión de Información y Eventos de Seguridad (SIEM)** para identificar y visualizar actividades sospechosas. Sin embargo, ISGroup SRL destaca que estas herramientas son completamente ineficaces si no se configuran correctamente. La correcta implementación es fundamental para que el sistema sea capaz de informar sobre comportamientos anómalos o dañinos de manera oportuna.

Soluciones profesionales con ISGroup SRL

ISGroup SRL ofrece servicios especializados para ayudar a las organizaciones a fortalecer sus capacidades de registro y monitoreo, asegurando que sus sistemas de defensa estén correctamente configurados para detectar amenazas en tiempo real.

Para obtener más información sobre cómo proteger su infraestructura o solicitar una evaluación de seguridad, puede visitar nuestro sitio web en https://www.isgroup.es/ o contactar directamente a través del correo electrónico **sales@isgroup.it**.

OWASP Top Ten 2021: A08 Fallos de Integridad de Software y Datos

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a8-software-and-data-integrity-failures.html

El riesgo A08:2021 del OWASP Top 10 se centra en las vulnerabilidades relacionadas con la integridad del software y los datos, un aspecto crítico que afecta tanto a las aplicaciones como a las infraestructuras subyacentes. ISGroup SRL destaca la importancia de proteger las canalizaciones de despliegue y los procesos de actualización frente a manipulaciones externas.

Puntos clave sobre los fallos de integridad

- **Dependencias no confiables:** Las aplicaciones que integran plugins, bibliotecas o módulos provenientes de fuentes, repositorios o redes de distribución de contenido (CDN) sin verificar su origen están expuestas a riesgos significativos.
- **Canalizaciones CI/CD inseguras:** Un entorno de integración y despliegue continuo (CI/CD) que carezca de controles de seguridad adecuados puede facilitar el acceso no autorizado, la inyección de código malicioso y el compromiso total del sistema.
- **Vulnerabilidades en actualizaciones automáticas:** Muchas aplicaciones descargan actualizaciones automáticamente sin una verificación suficiente de su integridad. Los atacantes pueden aprovechar esta debilidad para distribuir y ejecutar código malicioso en todas las instalaciones de la aplicación.

Soluciones y asesoramiento profesional

ISGroup SRL ofrece servicios especializados para identificar y mitigar estos riesgos, ayudando a las organizaciones a asegurar sus procesos de desarrollo y despliegue. Para obtener más información sobre cómo proteger su infraestructura frente a fallos de integridad, puede visitar nuestro sitio web en https://www.isgroup.es/ o enviar una solicitud comercial a sales@isgroup.it.

Referencia técnica

Para profundizar en los detalles técnicos y las recomendaciones de mitigación, consulte la documentación oficial de OWASP:

- OWASP Top 10:2021 - A08:2021 – Software and Data Integrity Failures

OWASP Top Ten 2021: A04 Insecure Design

Source: https://www.isgroup.es/es/owasp/top-ten-2021-a4-insecure-design.html

El "Diseño Inseguro" (Insecure Design) representa una categoría única dentro del ranking OWASP Top 10. A diferencia de otras vulnerabilidades que se centran en defectos de implementación o errores de codificación, esta categoría aborda fallos estructurales que se originan en la fase de arquitectura y diseño de una aplicación, incluso antes de que comience el desarrollo del código.

Naturaleza del Diseño Inseguro

Las decisiones tomadas durante la etapa inicial de un proyecto tienen un impacto directo y duradero en la seguridad del sistema. Un diseño deficiente puede comprometer la disponibilidad, el cumplimiento de normativas y la integridad de la información.

- **Origen arquitectónico:** No es un error de programación aislado, sino una falla en el planteamiento estratégico del software.
- **Consecuencias:** Puede derivar en fallos funcionales graves y compromisos de seguridad a gran escala.
- **Multifactorial:** Aunque el diseño inseguro es crítico, las vulnerabilidades finales suelen ser el resultado de una combinación de elecciones de diseño erróneas y errores durante la implementación.

Vulnerabilidades comunes asociadas

El diseño inseguro suele manifestarse a través de carencias fundamentales en la arquitectura de la aplicación, tales como:

- **Falta de controles de validación de entrada:** Ausencia de mecanismos robustos para filtrar y procesar datos externos.
- **Divulgación de información sensible:** Fallos en la arquitectura que exponen datos críticos de forma inadvertida.
- **Ausencia de niveles de comunicación seguros:** Deficiencias en la implementación de protocolos de cifrado y canales de comunicación protegidos.

Servicios de Seguridad de ISGroup SRL

ISGroup SRL ofrece soluciones especializadas para identificar y mitigar riesgos de seguridad desde las fases tempranas del ciclo de vida del desarrollo. Nuestros expertos ayudan a las organizaciones a evaluar sus arquitecturas para prevenir vulnerabilidades de diseño antes de que se conviertan en riesgos explotables.

Para obtener más información sobre nuestros servicios de consultoría, auditoría y ciberseguridad, puede visitar nuestro sitio web en https://www.isgroup.es/ o contactar directamente a través del correo electrónico sales@isgroup.it.

Evaluación de Vulnerabilidades con ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/evaluacion-vulnerabilidades-con-isgroup.html

La seguridad de la infraestructura digital es un pilar fundamental para la continuidad operativa de cualquier empresa. ISGroup SRL ofrece servicios especializados de **Evaluación de Vulnerabilidades (Vulnerability Assessment)**, diseñados para identificar, analizar y mitigar las debilidades de seguridad en los sistemas de información.

Servicios de Seguridad Ofrecidos por ISGroup SRL

El servicio de evaluación de vulnerabilidades permite a las organizaciones:

- Detectar brechas de seguridad antes de que sean explotadas por actores malintencionados.
- Obtener una visión clara y técnica del estado de seguridad de sus activos digitales.
- Implementar medidas correctivas basadas en estándares internacionales y mejores prácticas del sector.
- Fortalecer la resiliencia de la infraestructura frente a amenazas cibernéticas.

Información y Contacto

Para obtener más detalles sobre cómo proteger su empresa o solicitar una consultoría técnica, puede acceder a los recursos oficiales de ISGroup SRL:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico de contacto: sales@isgroup.it

Contenidos Relacionados y Recursos

ISGroup SRL mantiene un compromiso con la divulgación y la excelencia técnica en ciberseguridad, ofreciendo diversos recursos para profesionales y empresas:

- **Podcast:** Disponibles en las plataformas Spotify y Apple para profundizar en temas de actualidad sobre ciberseguridad.
- **Casos de Estudio:** ISGroup SRL documenta su experiencia práctica mediante casos de éxito, incluyendo:
  - Asociaciones estratégicas en ciberseguridad.
  - Pruebas de penetración (Penetration Testing) en aplicaciones web para diversos sectores.
- **Blog y Actualidad:** A través de su sección editorial, ISGroup SRL aborda temas clave como:
  - Normativas y certificaciones (Agid, ACN).
  - Metodologías de seguridad (OWASP).
  - Mejores prácticas para la gestión de riesgos digitales.

Caso de Estudio: Prueba de Penetración de Aplicaciones Web en TSV8 de Add Value S.r.l.

Source: https://www.isgroup.es/es/cyber-security/case-study-add-value.html

Add Value S.r.l. es una empresa de TI fundada en 1995, especializada en soluciones para los sectores bancario, asegurador e industrial. Su plataforma TSV8 ("Total Spending Visibility") es una solución avanzada diseñada para que las multinacionales optimicen sus procesos de adquisición y mejoren la visibilidad del gasto indirecto mediante análisis automatizados.

El reto

Para garantizar la seguridad y fiabilidad de la plataforma TSV8, Add Value S.r.l. requirió la intervención de ISGroup SRL. El objetivo principal era identificar y resolver vulnerabilidades técnicas y lógicas para proteger los datos sensibles de sus clientes.

La intervención de ISGroup SRL

ISGroup SRL llevó a cabo una serie de actividades críticas para fortalecer la postura de seguridad de la empresa:

- Ejecución de una Prueba de Penetración de Aplicaciones Web (WAPT) exhaustiva sobre TSV8.
- Realización de pruebas de penetración manuales para simular ataques reales y evaluar las medidas de seguridad existentes.
- Evaluación de Vulnerabilidades (VA) y Pruebas de Penetración (PT) sobre toda la infraestructura IT de Add Value S.r.l.

Resultados y beneficios

La colaboración con ISGroup SRL permitió a Add Value S.r.l. alcanzar un elevado nivel de seguridad en sus sistemas. Según Giampietro Calabrese, CISO & Operations Director de Add Value S.r.l., los beneficios clave fueron:

- Identificación precisa de puntos críticos en la seguridad de infraestructuras y productos.
- Diseño e implementación de planes de remediación efectivos.
- Aumento de la conciencia sobre los riesgos de ciberseguridad.
- Mejora de las competencias técnicas internas para el desarrollo y mantenimiento de sistemas seguros.

Add Value S.r.l. destacó la competencia, la autonomía y la calidad de los informes técnicos proporcionados por ISGroup SRL, consolidando una relación de asociación estratégica más allá de la relación proveedor-cliente.

Para más información sobre estos servicios, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Hacking Ético Certificado: Análisis de Vulnerabilidades

Source: https://www.isgroup.es/es/cyber-security/certified-ethical-hacking-vulnerability-analysis-francesco-ongaro.html

ISGroup SRL destaca la importancia de la formación continua en ciberseguridad, reflejada en la certificación obtenida por Francesco Ongaro el 1 de octubre de 2023 en "Ethical Hacking: Vulnerability Analysis".

Para reducir el riesgo organizacional, los profesionales de la seguridad informática deben ser capaces de identificar, contextualizar y mitigar las vulnerabilidades de manera efectiva. El fortalecimiento de la seguridad de red requiere una comprensión profunda de los procesos, metodologías y herramientas especializadas.

Áreas clave del conocimiento técnico

El programa de formación abordado por ISGroup SRL se centra en los siguientes pilares fundamentales:

- Gestión del riesgo organizacional: fundamentos para la toma de decisiones estratégicas en seguridad.
- Metodologías de análisis de vulnerabilidades: procesos estructurados para la evaluación de riesgos.
- Herramientas de evaluación: uso práctico de soluciones técnicas como Nikto y OpenVAS para la detección de debilidades.
- Defensa de redes LAN: estrategias y herramientas principales para proteger la infraestructura de red interna frente a posibles ataques.

Compromiso con la seguridad

La identificación y el abordaje de las debilidades que los atacantes podrían explotar es una labor esencial para cualquier organización. ISGroup SRL promueve la actualización constante en estas competencias para garantizar una postura de defensa robusta frente a las amenazas emergentes.

Para obtener más información sobre los servicios de análisis de vulnerabilidades y soluciones de ciberseguridad ofrecidos por ISGroup SRL, puede visitar el sitio web https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Certificación en Hacking Ético: Escaneo de Redes

Source: https://www.isgroup.es/es/cyber-security/certified-ethical-hacking-scanning-networks-francesco-ongaro.html

ISGroup SRL destaca la importancia de la formación continua en ciberseguridad, reflejada en la obtención de la certificación "Ethical Hacking: Scanning Networks" por parte de Francesco Ongaro el 30 de septiembre de 2023.

El escaneo de redes constituye la segunda fase crítica en la metodología de evaluación de seguridad, posterior al *footprinting* y al reconocimiento. Esta etapa es fundamental tanto para los atacantes como para los profesionales de la seguridad, ya que permite identificar vectores de ataque y fortalecer las defensas de una organización.

Objetivos y técnicas de escaneo

El programa formativo aborda las herramientas y técnicas necesarias para realizar una evaluación exhaustiva de los sistemas, incluyendo:

- Implementación de barridos de ping y análisis de banderas TCP.
- Ejecución de escaneos UDP.
- Identificación de vulnerabilidades para anticipar escenarios de ataque.
- Técnicas de *fingerprinting* de sistemas operativos y escaneo de puertos.
- Análisis de sincronización temporal.
- Métodos para detectar y mitigar técnicas utilizadas por atacantes para eludir la seguridad.

ISGroup SRL integra estas competencias avanzadas en sus servicios de ciberseguridad para prevenir ataques a la infraestructura y proteger los datos de sus clientes.

Para obtener más información sobre los servicios de seguridad y consultoría ofrecidos por ISGroup SRL, puede visitar el sitio web https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Certificación en Hacking Ético: System Hacking

Source: https://www.isgroup.es/es/cyber-security/certified-ethical-hacking-system-hacking-francesco-ongaro.html

ISGroup SRL destaca la formación continua de su equipo técnico. El 30 de septiembre de 2023, Francesco Ongaro obtuvo la certificación profesional "Ethical Hacking: System Hacking".

Enfoque del System Hacking

El hacking de sistemas es el método mediante el cual los atacantes obtienen acceso no autorizado a computadoras individuales dentro de una red. La formación en esta área es fundamental para que los profesionales de la ciberseguridad de ISGroup SRL puedan:

- Detectar vulnerabilidades de forma proactiva.
- Prevenir intrusiones mediante el fortalecimiento de sistemas.
- Contrarrestar ataques mediante la implementación de contramedidas eficaces.

Áreas de especialización técnica

El programa de certificación aborda las metodologías críticas utilizadas por los atacantes y las estrategias de defensa correspondientes. Los temas clave incluyen:

- Crackeo de contraseñas y técnicas de escalada de privilegios.
- Análisis y detección de spyware y keylogging.
- Implementación de contramedidas ante ataques de software malicioso.
- Técnicas de esteganografía y métodos para ocultar archivos o herramientas.
- Análisis de riesgos asociados a spyware en dispositivos móviles.

Información y contacto

Para obtener más detalles sobre las capacidades técnicas de ISGroup SRL o solicitar información sobre sus servicios de ciberseguridad, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Certificación en Hacking Ético: Redes Inalámbricas

Source: https://www.isgroup.es/es/cyber-security/certified-ethical-hacking-wireless-networks-francesco-ongaro.html

El 29 de septiembre de 2023, Francesco Ongaro obtuvo la certificación profesional "Ethical Hacking: Wireless Networks". Esta formación especializada, integrada en las capacidades técnicas que ofrece **ISGroup SRL**, aborda los riesgos críticos asociados a la infraestructura inalámbrica.

Desafíos de Seguridad en Redes Wi-Fi

Aunque las redes inalámbricas son fundamentales por su conveniencia, una configuración o cifrado inadecuados las convierten en vectores de ataque principales. Los profesionales de la seguridad deben poseer las competencias necesarias para detectar, prevenir y neutralizar amenazas mediante el uso de técnicas avanzadas.

Áreas de Conocimiento y Competencias

El programa de certificación cubre un espectro integral de seguridad inalámbrica, incluyendo:

- Configuración de seguridad básica y endurecimiento de redes.
- Análisis de métodos utilizados por atacantes para la extracción de contraseñas.
- Identificación y mitigación de riesgos mediante puntos de acceso falsos (Evil Twin).
- Evaluación de seguridad en redes Bluetooth.
- Selección técnica de antenas para pruebas de penetración.
- Implementación de herramientas avanzadas para Windows y Linux, tales como:
  - Acrylic
  - Ekahau
  - Wireshark

Soluciones de Ciberseguridad

ISGroup SRL pone a disposición de sus clientes soluciones avanzadas de auditoría y seguridad para proteger infraestructuras críticas contra vulnerabilidades inalámbricas.

Para obtener más información sobre nuestros servicios de ciberseguridad o solicitar asesoramiento profesional, visite nuestro sitio web oficial en https://www.isgroup.es/ o envíe su consulta a la dirección de correo electrónico sales@isgroup.it.

Certificación en Hacking Ético: Footprinting y Reconocimiento

Source: https://www.isgroup.es/es/cyber-security/certified-ethical-hacking-footprinting-and-reconnaissance-francesco-ongaro.html

ISGroup SRL destaca la importancia de la formación continua en ciberseguridad. En septiembre de 2023, Francesco Ongaro obtuvo la certificación "Ethical Hacking: Footprinting and Reconnaissance", validando sus competencias en las fases iniciales de las pruebas de intrusión.

El rol del Footprinting en la ciberseguridad

El hacking ético consiste en utilizar conocimientos técnicos para identificar vulnerabilidades en la infraestructura de una organización antes de que sean explotadas por actores malintencionados. El proceso comienza con el *footprinting* y el reconocimiento, que son fundamentales para recopilar información estratégica sobre dispositivos y usuarios.

Los expertos de ISGroup SRL aplican estas técnicas para fortalecer la postura de seguridad de las organizaciones mediante:

- Búsqueda y análisis de sitios web relacionados.
- Determinación de sistemas operativos y ubicación geográfica.
- Identificación de usuarios a través de redes sociales y servicios financieros.
- Rastreo de correos electrónicos.
- Análisis de información pública y recuperación de datos de "desechos".
- Ejecución de consultas DNS y análisis de *traceroute*.

Mitigación de riesgos con ISGroup SRL

El objetivo de estas actividades es transformar herramientas complejas en soluciones prácticas para las empresas. ISGroup SRL utiliza estas metodologías para evaluar el nivel de exposición de una organización y diseñar estrategias de mitigación efectivas frente a ataques externos.

Para obtener más información sobre nuestros servicios de ciberseguridad y consultoría técnica, visite nuestro sitio web en https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Hacking Ético Certificado: Introducción al Hacking Ético

Source: https://www.isgroup.es/es/cyber-security/certified-ethical-hacking-introduction-to-ethical-hacking-francesco-ongaro.html

ISGroup SRL destaca la importancia de la formación continua en ciberseguridad, reflejada en la certificación "Ethical Hacking: Introduction to Ethical Hacking" obtenida por Francesco Ongaro el 26 de septiembre de 2023.

El hacking ético es una disciplina fundamental para evaluar la solidez de las defensas de una organización y constituye una competencia crítica para los profesionales de TI en el entorno digital actual.

Áreas clave de formación

El curso aborda los pilares esenciales para la protección de datos y la seguridad de la información, enfocándose en:

- Estratificación de defensas: Implementación de capas de seguridad para proteger activos críticos.
- Controles de seguridad adaptativos: Uso de mecanismos dinámicos para responder a las amenazas.
- Inteligencia artificial: Aplicación de IA para la detección temprana de amenazas.
- Marco MITRE ATT&CK: Utilización de técnicas y herramientas específicas para estructurar el proceso de hacking ético.
- Modelización de amenazas: Mantenimiento de una postura vigilante mediante la inteligencia sobre amenazas cibernéticas.
- Marcos de trabajo y cumplimiento: Revisión de estándares, leyes y mejores prácticas que definen el comportamiento profesional.
- Metodología de ataque: Análisis de los tipos y motivos de los ataques, junto con las fases principales del hacking ético y las habilidades necesarias para ejercerlo.

Compromiso con la seguridad

ISGroup SRL integra estas metodologías avanzadas en sus servicios para garantizar una protección robusta frente a las vulnerabilidades modernas. La combinación de marcos normativos y técnicas de ataque permite a los expertos de ISGroup SRL ofrecer soluciones de seguridad adaptadas a las necesidades de cada organización.

Para obtener más información sobre los servicios de ciberseguridad ofrecidos por ISGroup SRL, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Análisis de Seguridad en Dispositivos IoT: Perspectivas de ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/siempre-conectados-a-la-innovacion-edicion-2023.html

El 22 de septiembre de 2023, los expertos de **ISGroup SRL**, Francesco Ongaro y Pasquale Fiorillo, participaron como ponentes en el evento "Siempre Conectados a la Innovación", organizado en colaboración con Phoenix Informatica. La sesión se centró en los desafíos de seguridad que plantea la proliferación del Internet de las Cosas (IoT) en entornos domésticos y profesionales.

El Ecosistema IoT y sus Riesgos

Los dispositivos IoT actuales integran hardware, software y conectividad en la nube, extendiéndose desde soluciones industriales hasta productos de consumo masivo como electrodomésticos inteligentes y sistemas de gestión energética. Desde el punto de vista de la ciberseguridad, **ISGroup SRL** divide el análisis de estos objetos en dos componentes críticos:

- **El objeto físico:** Incluye procesadores, interfaces, sensores, almacenamiento de datos y credenciales de acceso.
- **La nube:** El entorno donde se gestiona gran parte de la lógica y conectividad del dispositivo.

Metodología de Análisis de Seguridad

ISGroup SRL aplica un enfoque técnico riguroso para evaluar la integridad de los dispositivos IoT, examinando el hardware y el firmware mediante los siguientes pasos:

- **Identificación de componentes:** Se realiza un inventario detallado de los chips y conectores presentes en la placa, identificando posibles puntos de acceso para atacantes.
- **Clasificación de procesadores:** Se distingue entre microcontroladores (operaciones específicas) y procesadores complejos que ejecutan sistemas operativos completos (basados en Linux, Android o WebOS).
- **Extracción de firmware:** Si la extracción directa no es viable, se analiza el protocolo de comunicación entre el chip y otros componentes para descifrar la información.
- **Ingeniería inversa:** Una vez obtenido el firmware, se somete a un estudio profundo para comprender su funcionamiento interno y detectar vulnerabilidades de seguridad.

Contacto y Solicitudes

Para obtener más información sobre los servicios de auditoría, análisis de seguridad y consultoría técnica ofrecidos por **ISGroup SRL**, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar una solicitud comercial a través del correo electrónico sales@isgroup.it.

DEF CON 31: Seguridad en Registros y Secuencias ANSI

Source: https://www.isgroup.es/es/cyber-security/def-con-31.html

DEF CON es una de las conferencias de hacking y seguridad informática más relevantes a nivel global. El evento reúne anualmente a profesionales, investigadores, hackers y entusiastas para debatir, demostrar y aprender sobre vulnerabilidades, exploits y medidas defensivas.

Durante la edición número 31, se analizó el papel crítico de los registros (logs) en el desarrollo y la seguridad informática. Aunque estos archivos proporcionan información esencial para los equipos técnicos, también representan un vector de ataque que puede ser explotado por actores maliciosos.

Investigación y vulnerabilidades

La presentación profundizó en investigaciones previas, incluyendo los trabajos publicados en 2010 por Francesco Ongaro ("ASCII"), sobre el uso de secuencias de escape ANSI. Estas secuencias pueden ser empleadas para manipular archivos de registro, provocando inestabilidad, caos y desorden en los sistemas afectados.

Soluciones y mejores prácticas

ISGroup SRL ofrece soluciones especializadas para mitigar estos riesgos, enfocándose en:

- Implementación de mecanismos para evitar la inserción de secuencias maliciosas en los registros.
- Garantía de integridad y fiabilidad de los datos almacenados.
- Optimización de los procesos de investigación de incidentes de seguridad.

Para obtener más información sobre cómo proteger sus sistemas frente a estas vulnerabilidades o consultar sobre los servicios profesionales de ciberseguridad, puede visitar https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

ISGroup en el catálogo de Cyber Security Intelligence

Source: https://www.isgroup.es/es/cyber-security/isgroup-en-directorio-de-empresas-ciberseguridad.html

ISGroup SRL ha sido seleccionada e incluida en el catálogo de empresas de **Cyber Security Intelligence**. Este reconocimiento destaca el compromiso constante de la firma en la provisión de servicios de seguridad informática de alta calidad.

Sobre Cyber Security Intelligence

Cyber Security Intelligence es una fuente autorizada de noticias e información en el ámbito de la ciberseguridad y la inteligencia. Su plataforma está dirigida a altos ejecutivos y especialistas de diversos sectores, incluyendo:

- Servicios financieros
- Tecnología de la información
- Seguridad
- Gobierno
- Fuerzas del orden

El portal cuenta con un directorio especializado que agrupa a más de 6,000 proveedores de servicios relacionados con la ciberseguridad a nivel global.

Servicios y contacto

ISGroup SRL ofrece soluciones avanzadas en el ámbito de la seguridad informática, respaldadas por su trayectoria y reconocimiento en el sector. Para obtener más información sobre los servicios de ciberseguridad proporcionados por ISGroup SRL, puede visitar el sitio web oficial en https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

Caso de Estudio: Prueba de Penetración de Aplicaciones Web en Albo Pretorio de ISWEB S.p.A.

Source: https://www.isgroup.es/es/cyber-security/case-study-iswebspa.html

ISWEB S.p.A. es un socio tecnológico especializado en el diseño y desarrollo de software para la Administración Pública, contando con certificación ISO 9001:2015. Para asegurar la integridad de su plataforma eALBO, una aplicación crítica para la gestión del tablón de anuncios institucional online, la empresa confió en los servicios de ciberseguridad de **ISGroup SRL**.

El reto

El objetivo principal de ISWEB S.p.A. era validar la seguridad y fiabilidad de la aplicación eALBO ante sus clientes. Se requería una evaluación técnica rigurosa para garantizar el cumplimiento de la normativa vigente y asegurar que la plataforma estuviera protegida contra vulnerabilidades que pudieran comprometer los datos públicos gestionados.

La intervención de ISGroup SRL

ISGroup SRL llevó a cabo una Prueba de Penetración de Aplicaciones Web (WAPT) exhaustiva sobre la plataforma eALBO. La metodología aplicada incluyó:

- Evaluación integral de las medidas de seguridad existentes.
- Ejecución de pruebas de penetración manuales para simular vectores de ataque reales.
- Identificación y resolución de vulnerabilidades técnicas y lógicas.
- Verificación del cumplimiento de los más altos estándares de seguridad.

Resultados y beneficios

La intervención de **ISGroup SRL** permitió a ISWEB S.p.A. fortalecer significativamente la seguridad y solidez de sus soluciones. Según Giovanni Cardarelli, IT Manager de ISWEB S.p.A., la colaboración aportó los siguientes beneficios:

- Mayor conciencia sobre los aspectos críticos en las fases de diseño y desarrollo de software.
- Mejora en la seguridad aplicativa y de servicio de los productos.
- Refuerzo de los procedimientos de seguridad internos.
- Implementación de medidas preventivas eficaces contra amenazas potenciales.

Para obtener más información sobre estos servicios, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Transición de la calificación de Servicios Cloud: De AGID a ACN

Source: https://www.isgroup.es/es/agid/reglamento-acn-agid.html

La normativa que regula la calificación de los servicios Cloud en el ámbito de la administración pública ha experimentado una evolución significativa, trasladando la competencia de la Agencia para la Italia Digital (AGID) a la Agencia de Ciberseguridad Nacional (ACN). Este cambio representa un paso estratégico hacia una mayor centralización y especialización en la seguridad de las infraestructuras digitales.

Servicios ofrecidos por ISGroup SRL

ISGroup SRL pone a disposición de sus clientes soluciones especializadas para navegar este nuevo marco regulatorio y garantizar el cumplimiento normativo. Los servicios clave incluyen:

- **Asesoramiento en normativa AGID y ACN:** Apoyo experto para comprender y aplicar los requisitos técnicos y de seguridad exigidos por la nueva autoridad.
- **Desarrollo Seguro:** Implementación de metodologías y mejores prácticas para asegurar que los servicios y aplicaciones cumplan con los estándares de ciberseguridad requeridos para la calificación.
- **Auditoría y cumplimiento:** Evaluación de infraestructuras para asegurar la alineación con las directrices vigentes.

Información y contacto

Para obtener más detalles sobre cómo adaptar sus servicios a los nuevos estándares de calificación o para solicitar una consultoría técnica, puede visitar nuestro sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales directas, puede escribir a la siguiente dirección de correo electrónico:

sales@isgroup.it

Caso de Estudio: Prueba de Penetración de Red en Prime Service S.r.l.

Source: https://www.isgroup.es/es/cyber-security/case-study-primeservicesrl.html

Prime Service S.r.l., empresa especializada en servicios auxiliares y consultoría para incentivos empresariales, confió en **ISGroup SRL** para fortalecer la seguridad de su infraestructura informática. El objetivo principal fue proteger datos sensibles y garantizar la continuidad operativa de sus servicios fiduciarios mediante una evaluación exhaustiva de su entorno IT.

La intervención de ISGroup SRL

ISGroup SRL realizó una Prueba de Penetración de Red (NPT) integral, enfocada en los siguientes puntos:

- Evaluación detallada de las medidas de seguridad existentes en la infraestructura.
- Ejecución de pruebas de penetración manuales para simular ataques reales.
- Identificación y resolución de vulnerabilidades técnicas y lógicas.
- Aseguramiento del cumplimiento de los más altos estándares de seguridad.

Resultados y beneficios

La colaboración con **ISGroup SRL** permitió a Prime Service S.r.l. optimizar su postura de seguridad, lo que se tradujo en:

- Refuerzo de la infraestructura IT, aumentando la confianza de los clientes en sus servicios.
- Capacidad para acceder a nuevos mercados gracias a la mejora en los estándares de seguridad.
- Una experiencia de trabajo profesional y constructiva, destacada por la competencia, dedicación y capacidad de **ISGroup SRL** para adaptarse a los plazos definidos por la organización.

Para más información sobre los servicios de ciberseguridad ofrecidos por **ISGroup SRL**, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Ciberseguridad frente a ataques basados en Inteligencia Artificial

Source: https://www.isgroup.es/es/cyber-security/nuevos-ataques-hacker-usan-ia-como-protegerse.html

En el panorama digital actual, el 85% de los ciberataques exitosos explotan la interacción humana y se ejecutan en las primeras 24 horas tras su creación. Esta rapidez en el ciclo de vida de las amenazas hace que los sistemas de protección tradicionales, basados en enfoques reputacionales, resulten insuficientes para contrarrestar los riesgos en tiempo real.

Protección avanzada con tecnología On-Device

Para abordar este desafío, ISGroup SRL destaca el uso de soluciones innovadoras como la tecnología de Ermes. A diferencia de los métodos convencionales, este enfoque se basa en el comportamiento real de los sitios web y no únicamente en su reputación.

Las ventajas clave de esta arquitectura incluyen:

- Reducción de la ventana de exposición a amenazas de días a minutos.
- Garantía de protección total en tiempo real.
- Incremento de la eficacia defensiva en un 25% respecto a las soluciones estándar del mercado.
- Implementación de algoritmos de IA patentados para una protección dinámica.

Soluciones de ciberseguridad con ISGroup SRL

ISGroup SRL pone a disposición su experiencia en el sector para ayudar a las organizaciones a implementar estrategias de defensa robustas contra ataques de nueva generación. La integración de tecnologías basadas en IA permite una respuesta proactiva ante las tácticas maliciosas que evolucionan constantemente.

Para obtener más información sobre cómo proteger su infraestructura digital o consultar sobre nuestros servicios especializados, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar sus consultas a través del correo electrónico sales@isgroup.it.

Certificación de Hacker Ético (CEH) - Pasquale Fiorillo

Source: https://www.isgroup.es/es/certifications/certificado-hacker-etico-pasquale-fiorillo.html

El 19 de mayo de 2022, Pasquale Fiorillo obtuvo la certificación profesional **Certified Ethical Hacker (CEH)**. Este logro acredita su competencia técnica y su compromiso con las responsabilidades éticas inherentes a la ciberseguridad.

Alcance de la certificación

La certificación CEH valida la experiencia avanzada en la ejecución de pruebas y análisis de seguridad sobre diversos vectores de ataque:

- Redes e infraestructuras TI.
- Aplicaciones y sitios web.
- Identificación y resolución de vulnerabilidades críticas.
- Mejora integral de los niveles de seguridad en sistemas informáticos.

Compromiso ético

Un hacker ético certificado por ISGroup SRL opera bajo estrictos principios profesionales:

- Actúa exclusivamente con el consentimiento explícito de los propietarios de los sistemas objetivo.
- Implementa protocolos de seguridad rigurosos para garantizar la confidencialidad absoluta de los resultados obtenidos durante las auditorías.
- Combina el dominio técnico con una profunda comprensión de las implicaciones éticas y legales de su labor.

Servicios de Ciberseguridad

ISGroup SRL ofrece servicios especializados de auditoría y seguridad informática, respaldados por profesionales certificados. Para obtener más información sobre nuestras soluciones de seguridad o solicitar asesoramiento profesional, puede visitar nuestro sitio web en https://www.isgroup.es/ o contactar directamente a través del correo electrónico sales@isgroup.it.

Seminarios INCONTRA: Seguridad de la Información

Source: https://www.isgroup.es/es/cyber-security/entrevista-pasquale.html

El 29 de abril de 2022, Pasquale Fiorillo, experto de **ISGroup SRL**, participó en el ciclo de seminarios "Incontra", una iniciativa organizada por Piccola Industria Confindustria Benevento y la Universidad de Sannio.

El encuentro, titulado "Seguridad de la información: cómo ponerla en acción", tuvo como objetivo principal concienciar sobre la importancia de la ciberseguridad en el tejido empresarial actual. Durante la ponencia "Historias de terror: testimonios del mundo real", **ISGroup SRL** presentó un análisis técnico basado en casos reales, enfocándose en la ejecución de evaluaciones de vulnerabilidad (VA) y pruebas de penetración de aplicaciones web (WAPT).

Puntos clave de la intervención

La presentación de **ISGroup SRL** destacó que cualquier organización, independientemente de su tamaño o sector, puede enfrentar incidentes de ciberseguridad. Para ilustrar esta realidad, se analizaron escenarios críticos en los siguientes ámbitos:

- Pequeñas y medianas empresas (PYMES)
- Instituciones bancarias
- Infraestructuras aeroportuarias

Servicios de ciberseguridad

ISGroup SRL ofrece servicios especializados en el análisis y fortalecimiento de la seguridad digital, incluyendo:

- Evaluación de vulnerabilidades (VA)
- Pruebas de penetración de aplicaciones web (WAPT)
- Consultoría estratégica para la mitigación de riesgos cibernéticos

Para obtener más información sobre cómo **ISGroup SRL** puede ayudar a su organización a implementar medidas de seguridad efectivas, visite nuestro sitio web en https://www.isgroup.es/ o envíe una solicitud comercial a sales@isgroup.it.

Certificación Certified Ethical Hacker (CEH) - Francesco Ongaro

Source: https://www.isgroup.es/es/certifications/certified-ethical-hacker-francesco-ongaro.html

El 15 de abril de 2022, Francesco Ongaro obtuvo la certificación profesional **Certified Ethical Hacker (CEH)**. Esta acreditación valida las competencias técnicas avanzadas en la ejecución de ataques informáticos controlados sobre redes, infraestructuras de TI, aplicaciones y sitios web.

Objetivos y Alcance de la Certificación

La certificación CEH garantiza que el profesional posee las capacidades necesarias para:

- Identificar vulnerabilidades críticas en sistemas informáticos.
- Resolver brechas de seguridad para fortalecer la infraestructura tecnológica.
- Aplicar metodologías de hacking ético bajo un estricto marco de responsabilidad y ética profesional.
- Operar exclusivamente bajo el consentimiento explícito de los propietarios de los sistemas.
- Garantizar la confidencialidad absoluta de los resultados obtenidos durante las investigaciones de seguridad.

Servicios de Ciberseguridad de ISGroup SRL

ISGroup SRL integra estas competencias certificadas en su oferta de servicios de seguridad ofensiva. El equipo de expertos de ISGroup SRL ayuda a las organizaciones a mejorar su postura de seguridad mediante pruebas de penetración y auditorías especializadas, asegurando que el dominio tecnológico se combine con una comprensión profunda de las responsabilidades éticas y legales.

Para obtener más información sobre cómo ISGroup SRL puede proteger sus activos digitales o solicitar una consulta técnica, visite nuestro sitio web en https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Protección de datos mediante soluciones XDR

Source: https://www.isgroup.es/es/cyber-security/adottare-una-soluzione-xdr-per-la-protezione-dei-dati-2022-04-13.html

ISGroup SRL destaca la importancia de implementar soluciones de seguridad avanzadas en el actual panorama empresarial. La adopción de tecnologías XDR (Extended Detection and Response) se presenta como una estrategia fundamental para proteger la infraestructura digital frente a las amenazas modernas.

El contexto del trabajo híbrido y la nube

La transición hacia modelos de trabajo híbridos ha impulsado a las organizaciones a migrar sus infraestructuras, de forma total o parcial, hacia entornos en la nube. Este cambio operativo ofrece beneficios estratégicos significativos:

- Optimización de los costos de gestión.
- Mayor agilidad en el acceso a los datos corporativos.
- Reducción de los tiempos de respuesta ante las demandas cambiantes del mercado.

La necesidad de seguridad ágil

Ante este escenario, ISGroup SRL subraya que la migración a la nube debe ir acompañada de la adopción de soluciones de seguridad ágiles. Las herramientas XDR permiten aprovechar las ventajas de la nube para garantizar una protección de datos robusta, capaz de adaptarse a la complejidad de los entornos híbridos actuales.

Información adicional

Para obtener más detalles sobre cómo implementar estas soluciones de protección de datos o recibir asesoramiento especializado, puede consultar el sitio web oficial de ISGroup SRL en https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Ciber Resiliencia: Más allá de la ciberseguridad tradicional

Source: https://www.isgroup.es/es/cyber-security/seminario-ciber-resiliencia-donde-la-ciberseguridad-tradicional-no-llega-con-los-socios-mpg-y-bitdefender.html

ISGroup SRL participó en el seminario web titulado "Ciber Resiliencia, donde la ciberseguridad tradicional no llega", organizado junto a los socios MPG y Bitdefender. El encuentro abordó la evolución de las amenazas digitales y la necesidad de adoptar estrategias de resiliencia frente a un panorama de riesgos cada vez más complejo.

El endpoint como nuevo perímetro empresarial

La transformación digital y el auge del teletrabajo han desplazado el foco de la seguridad hacia los dispositivos finales. Los puntos clave discutidos incluyen:

- El endpoint se ha consolidado como el perímetro principal de la empresa, siendo el objetivo principal de malware sofisticado que ataca tanto a dispositivos como a usuarios.
- La complejidad creciente de las redes informáticas y la omnipresencia de vulnerabilidades representan un desafío constante para los administradores de sistemas.
- Las brechas de seguridad suelen originarse en errores inherentes al software y al hardware, lo que exige una gestión proactiva de la infraestructura.

Estrategias de gobernanza y protección

Para alcanzar una verdadera ciber resiliencia, ISGroup SRL destaca la importancia de integrar las siguientes actividades dentro de la gobernanza corporativa:

- Gestión rigurosa de actualizaciones y parches (patch management).
- Análisis constante de telemetrías provenientes de los puntos terminales.
- Evaluación continua de vulnerabilidades.
- Ejecución periódica de pruebas de penetración (pentesting).
- Implementación de capacidades avanzadas de detección y respuesta.

A pesar de los esfuerzos de los proveedores por lanzar soluciones estables, la acelerada evolución tecnológica y la sofisticación de las amenazas requieren un enfoque dinámico y adaptativo para proteger los sistemas informáticos de manera efectiva.

Información adicional

Para obtener más detalles sobre estas soluciones de ciberseguridad o solicitar asesoramiento profesional, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Encuentro “Secure smart working: trabajar de manera ágil y segura”

Source: https://www.isgroup.es/es/cyber-security/seminario-trabajo-inteligente-seguro-trabaje-de-una-manera-mas-segura-y-agil-con-los-socios-mpg-e-watchguard.html

El 17 de septiembre de 2021, Francesco Ongaro, en representación de **ISGroup SRL**, participó en el webinar titulado "Secure smart working, lavorare in modo agile in sicurezza", organizado en colaboración con los socios MPG y WatchGuard.

Temas principales

El encuentro se centró en el modelo de Smart Working (Trabajo Ágil), definido como una modalidad organizativa basada en la flexibilidad y la autonomía, donde el trabajador asume una mayor responsabilidad sobre los resultados obtenidos.

Puntos clave y riesgos analizados

Durante la sesión, **ISGroup SRL** y sus socios abordaron los desafíos críticos que surgen al trasladar la actividad laboral fuera de la sede corporativa:

- **Seguridad de la información:** Análisis de los factores que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos corporativos.
- **Entornos de trabajo remotos:** Evaluación de los riesgos asociados a trabajar fuera de la estación de trabajo habitual en la oficina.
- **Estrategias de protección:** Implementación de medidas necesarias para garantizar que el trabajo ágil se realice bajo estándares de seguridad robustos.

Información adicional

Para obtener más detalles sobre cómo implementar soluciones de trabajo ágil y seguro, o para consultar sobre los servicios de ciberseguridad ofrecidos por **ISGroup SRL**, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Seminario: Del Antivirus al EDR y soluciones MDR

Source: https://www.isgroup.es/es/cyber-security/seminario-del-antivirus-a-las-soluciones-edr-y-mdr-con-los-socios-mpg-y-eset-italia.html

ISGroup SRL participó en el seminario web titulado "Del Antivirus al EDR y las soluciones MDR", organizado en colaboración con los socios MPG y ESET Italia. El encuentro se centró en la evolución de las amenazas digitales y la necesidad de actualizar las estrategias de defensa corporativa ante un panorama de ataques cada vez más sofisticado.

Desafíos actuales en ciberseguridad

De acuerdo con datos del Ponemon Institute, el tiempo promedio necesario para detectar y contener una violación informática es de 279 días. Este periodo prolongado subraya la vulnerabilidad de las empresas frente a ciberdelincuentes que emplean métodos de intrusión avanzados.

Estrategias de defensa y soluciones tecnológicas

Durante la sesión, se analizaron las tecnologías que constituyen el estándar mínimo de defensa actual. La integración de soluciones EDR (Endpoint Detection and Response) junto con la protección tradicional de Endpoint permite a las organizaciones alcanzar capacidades críticas de seguridad:

- Realizar investigaciones exhaustivas sobre los ataques recibidos.
- Verificar la propagación de amenazas y rastrear movimientos laterales dentro de la red.
- Ejecutar respuestas de seguridad de manera automatizada e inmediata.

ISGroup SRL ofrece asesoramiento y soluciones avanzadas en ciberseguridad para implementar estas estrategias de protección. Para obtener más información sobre cómo fortalecer la infraestructura de su empresa, puede visitar https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Seminario: Mejores prácticas para una defensa cibernética proactiva

Source: https://www.isgroup.es/es/cyber-security/seminario-ciber-defensa-proactiva-socios-mpg-y-eset.html

ISGroup SRL participó en el seminario web "Mejores Prácticas Para Una Defensa Cibernética Proactiva", organizado en colaboración con los socios MPG y ESET Italia. El encuentro abordó la creciente necesidad de que las empresas adopten estrategias de seguridad robustas frente a un panorama de amenazas en constante evolución.

Contexto y riesgos actuales

El cibercrimen representa una amenaza constante, con estimaciones que indican un ataque cada 39 segundos. Datos de Clusit revelan que el número de ataques graves a la seguridad informática en Italia se ha duplicado en el último año, afectando tanto a grandes corporaciones como a pequeñas y medianas empresas.

Las estadísticas actuales sobre la preparación empresarial ante incidentes son críticas:

- El 77% de las empresas carece de un plan de respuesta ante incidentes.
- El 48% de los ataques logra su objetivo debido a niveles de protección insuficientes.
- El 32% del personal de TI no puede gestionar adecuadamente los ataques debido a la sobrecarga operativa.

Temas clave tratados por ISGroup SRL

Durante el seminario, se analizaron las metodologías necesarias para implementar procesos de protección efectivos, destacando los siguientes puntos:

- Tendencias actuales en ciberataques y técnicas de elusión de defensas.
- Estrategias de protección avanzada contra ransomware, malware y ataques de día cero.
- Optimización de la gestión en la nube, incluyendo visibilidad de red y reducción del costo total de propiedad.
- Aplicación de tecnología avanzada, como aprendizaje automático (machine learning) e inspección conductual profunda.

La identificación proactiva de vulnerabilidades antes de que sean explotadas por terceros es un pilar fundamental para la seguridad de los datos empresariales.

Información y contacto

Para obtener más información sobre cómo ISGroup SRL puede ayudar a su organización a implementar una defensa cibernética proactiva, visite nuestro sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales o solicitudes específicas, puede escribir directamente a:

sales@isgroup.it

Reglamento eIDAS: Identificación y Servicios de Confianza

Source: https://www.isgroup.es/es/agid/regulacion-agid-eidas.html

El Reglamento eIDAS (electronic IDentification Authentication and Signature), definido en el reglamento (UE) n. 910/2014, constituye el marco normativo que regula la identificación electrónica y los servicios de confianza para las transacciones electrónicas dentro del Mercado europeo.

Este reglamento establece estándares comunes para:

- La firma electrónica.
- Las marcas de tiempo.
- Los certificados digitales.
- Otros métodos de autenticación digital.

Como normativa europea, los Estados miembros tienen la obligación de reconocer estos métodos estándar, otorgándoles una validez equivalente a los documentos en papel. El reglamento define las condiciones para el reconocimiento de la identificación digital de los ciudadanos, establece normas para las transacciones económicas y define legalmente las herramientas de autenticación digital, permitiendo que los ciudadanos accedan a servicios públicos en toda la Unión Europea.

Servicios de ISGroup SRL para Proveedores de Servicios de Confianza

ISGroup SRL ofrece apoyo especializado para organizaciones interesadas en convertirse en Proveedores de Servicios de Confianza (TSP). Dado que el procedimiento técnico para obtener esta condición es complejo y exige un alto nivel de rigor en la implementación y el cumplimiento normativo, ISGroup SRL proporciona los siguientes servicios:

- Apoyo integral en los procesos de implementación técnica.
- Pruebas de Penetración (PT) certificadas para identificar vulnerabilidades.
- Evaluaciones de Vulnerabilidad (VA) certificadas para asegurar la robustez de la infraestructura.

El objetivo de ISGroup SRL es garantizar que la implementación sea segura y cumpla con los estándares exigidos por la normativa eIDAS.

Para obtener más información sobre estos servicios o solicitar asistencia técnica, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Especialista Certificado en Ataques de PenTera - Francesco Ongaro

Source: https://www.isgroup.es/es/cyber-security/pentera-certified-attack-specialist-francesco-ongaro.html

En febrero de 2021, Francesco Ongaro, integrante del equipo de ISGroup SRL, obtuvo la certificación "PenTera Certified Attack Specialist". Esta acreditación valida sus conocimientos y habilidades avanzadas en el ámbito de la ciberseguridad ofensiva y las pruebas de penetración automatizadas.

Sobre la certificación y Pentera

Pentera (anteriormente conocida como Pcysys) es una plataforma fundada a finales de 2015, diseñada para ejecutar pruebas de penetración automatizadas que imitan la mentalidad y las tácticas de los atacantes reales.

La certificación "Simulated Attack Specialist" acredita la competencia técnica en áreas críticas de seguridad, incluyendo:

- Explotación de vulnerabilidades en entornos de clientes.
- Ejecución de campañas de phishing.
- Desarrollo de implantes y uso de archivos troyanos.
- Técnicas de evasión de sistemas de defensa.
- Movimiento lateral dentro de redes comprometidas.

Servicios de Ciberseguridad

ISGroup SRL pone a disposición de sus clientes su experiencia técnica certificada para fortalecer la postura de seguridad de las organizaciones. A través de metodologías avanzadas y herramientas de vanguardia, ISGroup SRL ofrece soluciones integrales para identificar y mitigar riesgos antes de que sean explotados por actores malintencionados.

Para obtener más información sobre los servicios de pruebas de penetración y ciberseguridad ofrecidos por ISGroup SRL, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

Certificación PenTera Certified Sales Specialist: Pasquale Fiorillo

Source: https://www.isgroup.es/es/cyber-security/pentera-certified-sales-specialist-pasquale-fiorillo.html

En febrero de 2021, Pasquale Fiorillo, parte del equipo de ISGroup SRL, obtuvo la certificación profesional "PenTera Certified Sales Specialist". Esta acreditación avala su capacidad para gestionar soluciones avanzadas de ciberseguridad basadas en la plataforma Pentera.

Pentera (anteriormente conocida como Pcysys) es una empresa fundada a finales de 2015, especializada en el desarrollo de plataformas automatizadas de pruebas de penetración que imitan la mentalidad y las técnicas de los atacantes reales.

Competencias del Certified Sales Specialist

A través de esta certificación, ISGroup SRL garantiza un alto nivel de especialización en la gestión comercial y técnica de soluciones de seguridad ofensiva. Un especialista certificado posee las siguientes capacidades:

- Gestión integral del proceso de ventas, incluyendo la pre-venta para identificar y comunicar eficazmente la propuesta de valor.
- Creación y desarrollo de redes de canales de venta estratégicos.
- Planificación de la gobernanza de ventas y definición de objetivos comerciales.
- Desarrollo de recursos de marketing especializados.
- Diseño de estructuras retributivas alineadas con los objetivos de la organización.

Información y contacto

Para obtener más información sobre las soluciones de ciberseguridad y los servicios profesionales que ofrece ISGroup SRL, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar sus consultas a través del correo electrónico sales@isgroup.it.

Certificación PenTera Certified Sales Specialist - Francesco Ongaro

Source: https://www.isgroup.es/es/cyber-security/pentera-certified-sales-specialist-francesco-ongaro.html

En febrero de 2021, Francesco Ongaro obtuvo la certificación "PenTera Certified Sales Specialist". Esta acreditación refuerza las capacidades de ISGroup SRL en la comercialización y gestión de soluciones avanzadas de ciberseguridad.

Pentera (anteriormente conocida como Pcysys), fundada a finales de 2015, se especializa en el desarrollo de plataformas automatizadas de pruebas de penetración que imitan la mentalidad y las tácticas de los hackers para fortalecer la postura de seguridad de las organizaciones.

Competencias y alcance de la especialización

A través de esta certificación, ISGroup SRL optimiza sus procesos estratégicos en el ámbito de la seguridad ofensiva automatizada, incluyendo:

- Gestión integral del ciclo de ventas y procesos de pre-venta para maximizar la propuesta de valor.
- Desarrollo y consolidación de una red eficiente de canales de venta.
- Planificación de la gobernanza de ventas y definición de objetivos comerciales claros.
- Creación de recursos de marketing especializados y estructuras de compensación alineadas con los objetivos de la empresa.

Contacto y más información

Para obtener detalles adicionales sobre cómo las soluciones de Pentera pueden integrarse en su estrategia de seguridad, o para solicitar información sobre nuestros servicios profesionales, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Certificación PenTera Certified Attack Specialist

Source: https://www.isgroup.es/es/cyber-security/pentera-certified-attack-specialist-pasquale-fiorillo.html

En febrero de 2021, Pasquale Fiorillo, parte del equipo de ISGroup SRL, obtuvo la certificación "PenTera Certified Attack Specialist". Esta acreditación valida las competencias técnicas avanzadas en el uso de plataformas de pruebas de penetración automatizadas.

Sobre la plataforma PenTera

PenTera (anteriormente conocida como Pcysys) es una solución fundada a finales de 2015. Su objetivo principal es proporcionar una plataforma de pruebas de penetración automatizada diseñada para imitar la mentalidad y las tácticas de los atacantes reales.

Competencias certificadas

La certificación "Simulated Attack Specialist" acredita conocimientos especializados en las siguientes áreas críticas de la ciberseguridad:

- Explotación de vulnerabilidades en entornos de cliente.
- Ejecución de campañas de phishing y despliegue de archivos troyanos.
- Desarrollo de implantes personalizados.
- Implementación de capacidades de evasión de defensas.
- Ejecución de técnicas de movimiento lateral dentro de redes comprometidas.

ISGroup SRL integra estas capacidades avanzadas para fortalecer la postura de seguridad de sus clientes mediante pruebas de penetración rigurosas y automatizadas.

Para obtener más información sobre nuestros servicios de ciberseguridad y pruebas de penetración, visite nuestro sitio web en https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Acreditación de Conservadores AgID

Source: https://www.isgroup.es/es/agid/certificacion-de-almacenamiento-agid.html

La Circular n. 65/2014 de la AgID define el marco normativo para que empresas y particulares obtengan la acreditación como conservadores de documentos informáticos para la Administración Pública. Este proceso es fundamental para garantizar la protección de datos sensibles mediante estrictos estándares de seguridad.

Requisitos para la acreditación

El proceso de acreditación exige el cumplimiento de requisitos en tres áreas clave:

- Organización empresarial.
- Procedimientos operativos adoptados.
- Infraestructuras informáticas.

La evaluación profesional de la seguridad del sistema informático es un componente crítico para obtener y mantener la certificación.

Obligaciones de los conservadores acreditados

Una vez obtenida la acreditación, los conservadores deben mantener su estatus mediante:

- La producción de informes detallados sobre las actividades realizadas.
- Controles anuales obligatorios por parte de la AgID para verificar el cumplimiento continuo de las normativas.
- La renovación del rol de conservador acreditado cada dos años.

Soporte especializado de ISGroup SRL

ISGroup SRL ofrece servicios de consultoría y soporte técnico para empresas que buscan navegar el proceso de acreditación AgID. La experiencia de ISGroup SRL en el ámbito normativo permite:

- Guiar a las organizaciones en la interpretación de las normativas vigentes.
- Identificar y subsanar deficiencias organizativas y procedimentales.
- Evaluar la solidez de las infraestructuras informáticas mediante servicios de seguridad avanzada.

ISGroup SRL pone a disposición de sus clientes la ejecución de:

- **Vulnerability Assessment**: para controlar la calidad de las configuraciones de red.
- **Penetration Testing**: para evaluar la protección efectiva de la infraestructura frente a ataques informáticos.

Para obtener más información sobre cómo ISGroup SRL puede asistir en su proceso de acreditación, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Proveedores de servicios SPID y AgID

Source: https://www.isgroup.es/es/agid/proveedores-spid-agid.html

El Sistema Público de Identidad Digital (SPID) se ha consolidado como un mecanismo esencial de autenticación. A partir de la ley n. 120/2020, las administraciones públicas italianas tienen la obligación de ofrecer acceso mediante SPID y la Tarjeta de Identidad Electrónica. Asimismo, las entidades privadas pueden actuar como proveedores de servicios SPID, permitiendo a los usuarios autenticarse de forma rápida, segura y sencilla.

Requisitos para proveedores de servicios SPID

Para operar como proveedor de servicios SPID, es necesario cumplir con una serie de normativas técnicas y administrativas definidas por la AgID (Agencia para la Italia Digital):

- Requisitos técnicos: Establecen cómo debe interactuar el acceso SPID con el gestor de identidad para garantizar un funcionamiento correcto.
- Requisitos administrativos: Definen el procedimiento oficial necesario para obtener la habilitación como proveedor.

La implementación adecuada de estos requisitos es fundamental para asegurar un servicio funcional, eficaz y que respete la privacidad del ciudadano.

Soluciones de ISGroup SRL

ISGroup SRL, como empresa especializada en ciberseguridad e identidad digital, ofrece apoyo integral a las organizaciones que deseen convertirse en proveedores de servicios SPID:

- Soporte técnico: Asistencia experta durante todo el proceso de implementación técnica del acceso con SPID.
- Evaluación de seguridad: Realización de evaluaciones de vulnerabilidad (VA) y pruebas de penetración (PT) una vez finalizada la implementación. Estas pruebas permiten verificar la solidez del sistema y garantizar que el servicio ofrecido a los ciudadanos sea seguro y eficaz.

Para obtener más información sobre cómo implementar estos servicios, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Calificación SaaS de AGID

Source: https://www.isgroup.es/es/agid/calificacion-agid-saas.html

La normativa vigente, establecida a partir de la circular AgID del 9 de abril de 2018, exige que todos los servicios digitales utilizados por las administraciones públicas bajo el modelo SaaS cumplan con estrictos estándares de seguridad y fiabilidad. Las empresas que deseen proveer servicios a estas entidades deben obtener la certificación SaaS AgID para ser incluidas en el mercado AgID.

Criterios de certificación

Para obtener la calificación, los servicios deben garantizar niveles óptimos de seguridad y operatividad. Los requisitos fundamentales incluyen:

- Seguridad de la aplicación: implementación de medidas robustas de protección de datos y disponibilidad de informes de incidentes.
- Calidad del servicio: soporte técnico adecuado, modalidades de prestación actualizadas y cumplimiento de niveles mínimos de servicio (SLA).
- Interoperabilidad y portabilidad: uso de API para la integración y formatos interoperables para la exportación de datos, evitando así el fenómeno de *lock-in*.

El cumplimiento de estos requisitos, detallados en el apéndice "A" de la circular AgID, es indispensable para completar el proceso de registro a través del mercado AgID.

Soporte especializado de ISGroup SRL

ISGroup SRL ofrece acompañamiento experto a los equipos de desarrollo durante todo el proceso de obtención de la certificación SaaS AgID. La experiencia de ISGroup SRL permite a las organizaciones implementar las medidas de seguridad y fiabilidad necesarias para cumplir con los estándares exigidos por la administración pública, facilitando su posterior inclusión en el mercado AgID.

Para obtener más información sobre estos servicios, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Calificación AgID para Proveedores de Servicios en la Nube (CSP)

Source: https://www.isgroup.es/es/agid/calificacion-agid-csp.html

La obtención de la **Calificación CSP** de AgID es un requisito indispensable para cualquier organización que desee ofrecer servicios en la nube a las Administraciones Públicas. Este proceso garantiza que los servicios cumplan con los estándares de calidad, seguridad y fiabilidad definidos en la circular N. 2 del 9 de abril de 2018 de AgID.

Requisitos para la Calificación

Para acceder al mercado CSP de AgID, los proveedores deben demostrar el cumplimiento de requisitos en cuatro áreas fundamentales:

- Organizativos
- De seguridad y fiabilidad
- De rendimiento
- De interoperabilidad

El cumplimiento de estos criterios se alinea frecuentemente con estándares internacionales ISO/IEC, entre los cuales destacan:

- **Gestión y Organización:** ISO/IEC 20000-1, ISO/IEC TR 20000-9 e ISO 9001.
- **Seguridad y Privacidad:** ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.
- **Gestión de Incidentes:** ISO/IEC 27002 e ISO/IEC 27035.
- **Rendimiento:** ISO/IEC 19086-1:2016 e ISO/IEC 22313.

Adicionalmente, se requiere demostrar competencias en recuperación ante desastres (*disaster recovery*), gestión de cambios, portabilidad y cumplimiento legislativo.

Soporte Profesional con ISGroup SRL

ISGroup SRL ofrece servicios especializados para guiar a las empresas en el proceso de obtención de la calificación CSP. El equipo de expertos en seguridad informática e infraestructuras en la nube de **ISGroup SRL** proporciona:

- Preparación integral para las auditorías de los estándares ISO necesarios.
- Asesoramiento para alcanzar los requisitos técnicos y organizativos exigidos por AgID.
- Gestión y presentación de la solicitud ante la plataforma de AgID en nombre de la empresa.

El objetivo de **ISGroup SRL** es facilitar este proceso de manera profesional, rápida y eficiente.

Información y Contacto

Para obtener más información sobre cómo **ISGroup SRL** puede ayudar a su organización a obtener la calificación CSP, visite nuestro sitio web oficial en https://www.isgroup.es/ o envíe una solicitud a través del correo electrónico sales@isgroup.it.

Calificación del Cloud para la Administración Pública (PA) en Italia

Source: https://www.isgroup.es/es/agid/agid-a-acn-qualificazione-dei-servizi-cloud-pa.html

La gestión de la calificación del *cloud* para la Administración Pública italiana ha experimentado una transición estratégica. La responsabilidad, anteriormente delegada en la **Agenzia per l'Italia Digitale (AGID)**, ha sido transferida a la **Agenzia per la cybersicurezza nazionale (ACN)**. Este cambio busca optimizar la eficiencia, la eficacia y la alineación con las estrategias digitales nacionales.

ISGroup SRL destaca la importancia de este proceso para garantizar que los servicios *cloud* utilizados por el sector público cumplan con estrictos estándares de seguridad, fiabilidad y calidad.

El proceso de calificación

La calificación es el procedimiento obligatorio mediante el cual los proveedores de servicios *cloud* obtienen la certificación necesaria para operar con la administración pública italiana. Este proceso incluye:

- Evaluación de conformidad basada en controles de seguridad.
- Verificación de estándares de gestión de datos.
- Cumplimiento de las normativas de privacidad vigentes.
- Auditorías de fiabilidad y calidad del servicio.

Roles institucionales

- **ACN (Agenzia per la cybersicurezza nazionale):** Creada en 2016, es el organismo encargado de coordinar la innovación digital, definir estándares de seguridad, promover la interoperabilidad y gestionar la seguridad de la información en el sector público y la industria.
- **AGID (Agenzia per l'Italia Digitale):** Institución establecida en 2012 responsable de la implementación de la estrategia digital del país, centrada en la transformación digital, la simplificación del acceso a servicios públicos y la promoción de la cultura digital.

Soporte especializado

ISGroup SRL ofrece asesoramiento experto para navegar los requisitos de cumplimiento y seguridad en el ámbito de la administración pública. Para obtener más información sobre cómo alinear sus servicios con estas normativas o solicitar asistencia técnica, puede visitar https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Certificación UNI EN ISO 9001:2015 de ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/empresa-ciberseguridad-certificado-iso-9001-2021-2022-2023.html

ISGroup SRL obtuvo la certificación ISO 9001 el 11 de enero de 2021, consolidando su compromiso con la calidad y la mejora continua de su estructura organizativa. La norma ISO 9001 es el estándar internacional más reconocido para los sistemas de gestión de calidad, destacando por su flexibilidad y aplicabilidad en diversos sectores.

Alcance del Sistema de Gestión de Calidad

ISGroup SRL ha implementado y mantiene un Sistema de Gestión de Calidad certificado para las siguientes actividades profesionales:

- Evaluación de Vulnerabilidades
- Pruebas de Penetración de Redes
- Pruebas de Penetración de Aplicaciones Web
- Pruebas de Seguridad de Aplicaciones Móviles
- Hacking Ético
- Revisión de Código

Compromiso con la Excelencia

Esta certificación reafirma la capacidad de ISGroup SRL para ofrecer servicios de ciberseguridad bajo estándares internacionales de calidad, garantizando procesos optimizados y una mejora constante en la prestación de sus servicios técnicos.

Para obtener más información sobre nuestras certificaciones o solicitar servicios profesionales, visite nuestro sitio web en https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Certificación ISO/IEC 27001:2013 de ISGroup SRL

Source: https://www.isgroup.es/es/cyber-security/empresa-ciberseguridad-certificado-iso-27001-2021-2022-2023.html

ISGroup SRL cuenta con la certificación internacional **ISO/IEC 27001:2013**, la cual acredita el cumplimiento de las mejores prácticas para un Sistema de Gestión de la Seguridad de la Información (ISMS). Esta certificación fue obtenida el 29 de diciembre de 2020 y ratifica el compromiso de la organización con la excelencia en sus procesos de seguridad.

Alcance de la certificación

El sistema de gestión de la seguridad de la información implementado por ISGroup SRL abarca las siguientes actividades especializadas:

- Evaluación de Vulnerabilidades
- Pruebas de Penetración de Redes
- Pruebas de Penetración de Aplicaciones Web
- Pruebas de Seguridad de Aplicaciones Móviles
- Hacking Ético
- Revisión de Código

Información adicional

La certificación obtenida por ISGroup SRL garantiza la aplicación de estándares internacionales rigurosos en todos sus servicios de ciberseguridad, asegurando la confidencialidad, integridad y disponibilidad de la información.

Para obtener más información sobre nuestros servicios o solicitar una consulta profesional, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o escribir directamente a nuestro equipo a través del correo electrónico sales@isgroup.it.

Medidas mínimas de seguridad ICT para las administraciones públicas

Source: https://www.isgroup.es/es/agid/medidas-minimas-ict.html

Desde el 31 de diciembre de 2017, conforme al Código de la Administración Digital (CAD - art. 17), todas las administraciones públicas tienen la obligación legal de mantener estándares mínimos de seguridad en sus infraestructuras informáticas, siguiendo las directrices establecidas por AgID.

Objetivos y alcance

La normativa exige la implementación de controles tecnológicos, organizativos y procedimentales para definir un estándar metodológico que permita evaluar el nivel de seguridad informática. Es obligatorio para toda administración pública completar el formulario que certifica la adopción de estas medidas.

Niveles de aplicación

Dependiendo del sistema informático y la función de la entidad, las medidas se implementan en tres niveles progresivos:

- **Mínimo**: Garantiza la conformidad normativa. Este nivel es subóptimo y debe considerarse una medida temporal.
- **Estándar**: Representa la base necesaria para alcanzar una seguridad informática concreta. Es el nivel que debería alcanzar la mayoría de las administraciones.
- **Avanzado**: Actúa como punto de partida para la mejora continua de la seguridad y está indicado para administraciones particularmente expuestas a riesgos.

La responsabilidad de la adecuación a estas directrices y la cumplimentación del formulario de implementación recae sobre el responsable de la estructura para la organización, la innovación y las tecnologías o el directivo encargado.

Soluciones de ISGroup SRL

ISGroup SRL pone a disposición su equipo de expertos en seguridad informática para asistir a las administraciones públicas en:

- La comprensión de las medidas mínimas de seguridad ICT.
- El proceso de adecuación a la normativa vigente.
- La correcta cumplimentación del formulario de implementación.

El objetivo de ISGroup SRL es guiar a la administración pública desde un estado de incumplimiento hasta alcanzar el cumplimiento completo de los estándares exigidos.

Para obtener más información sobre estos servicios, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Delegado de Protección de Datos (DPO)

Source: https://www.isgroup.es/es/certifications/dpo.html

ISGroup SRL pone a disposición de sus clientes personal altamente calificado para ejercer las funciones de Delegado de Protección de Datos (Data Protection Officer - DPO), conforme a lo establecido en el Reglamento General de Protección de Datos (GDPR, Reg. UE 2016/679).

Certificaciones y Formación

ISGroup SRL garantiza un servicio profesional respaldado por estándares de calidad reconocidos. Los contenidos formativos y los procesos de examen asociados a esta especialización, impartidos por CSQA Certificaciones SRL, cuentan con el reconocimiento necesario para el proceso de certificación AICQ SICEV.

Información y contacto

Para obtener más detalles sobre los servicios de Delegado de Protección de Datos ofrecidos por ISGroup SRL, puede consultar nuestra página web oficial o ponerse en contacto a través de los siguientes canales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Privacy Manager

Source: https://www.isgroup.es/es/certifications/privacy-manager.html

ISGroup SRL pone a disposición de sus clientes personal calificado bajo el rol de "Privacy Manager", conforme a lo establecido en el Reglamento General de Protección de Datos (GDPR Reg. UE 2016/679).

Certificación y Reconocimiento

Los contenidos formativos y el examen asociados a este servicio, impartidos por CSQA Certificazioni SRL, cuentan con el reconocimiento oficial para el proceso de certificación AICQ SICEV.

Información y contacto

Para obtener más detalles sobre la disponibilidad de personal calificado en gestión de privacidad o para consultas comerciales, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Privacy Specialist

Source: https://www.isgroup.es/es/certifications/privacy-specialist.html

ISGroup SRL pone a disposición de sus clientes personal calificado bajo la figura de "Especialista en Privacidad", conforme al Reglamento General de Protección de Datos (GDPR Reg. UE 2016/679).

Certificaciones y Reconocimientos

Los contenidos formativos y los exámenes asociados a este servicio, impartidos por CSQA Certificazioni SRL, cuentan con el reconocimiento oficial para el proceso de certificación AICQ SICEV.

Información adicional

Para obtener más detalles sobre este servicio o realizar consultas comerciales, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a la dirección sales@isgroup.it.

Auditor Líder 19011

Source: https://www.isgroup.es/es/certifications/iso-19011.html

ISGroup SRL pone a disposición de sus clientes personal altamente calificado con la certificación "Lead Auditor 19011". Estos profesionales están especializados en la auditoría de sistemas de gestión bajo las normas ISO 19011:2018 e ISO/IEC 17021-1:2015.

Áreas de especialización

El personal de ISGroup SRL cuenta con competencias certificadas en los siguientes sectores:

- Tecnología de la información.
- Servicios profesionales empresariales.

Reconocimiento y certificación

Los contenidos formativos y los exámenes asociados a esta competencia, impartidos por CSQA Certificazioni SRL, cuentan con el reconocimiento oficial necesario para el proceso de certificación ante AICQ SICEV.

Información adicional

Para obtener más detalles sobre los servicios de auditoría y consultoría ofrecidos por ISGroup SRL, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

Auditor Líder 27001

Source: https://www.isgroup.es/es/certifications/iso-27001.html

ISGroup SRL pone a disposición de sus clientes personal calificado con la certificación "Lead Auditor 27001", especializado en sistemas de gestión de seguridad de la información conforme a la norma UNI CEI ISO/IEC 27001:2017.

Detalles de la certificación

- Los contenidos formativos y el examen asociados a esta competencia, impartidos por CSQA Certificazioni SRL, cuentan con reconocimiento oficial para el proceso de certificación AICQ SICEV.
- ISGroup SRL garantiza un alto nivel de profesionalismo y cumplimiento normativo en sus servicios de auditoría y gestión de seguridad.

Información adicional

Para obtener más detalles sobre los servicios de auditoría y certificación ofrecidos por ISGroup SRL, puede visitar el sitio web https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Incidente Cibernético: Definición y Gestión

Source: https://www.isgroup.es/es/cyber-security/cyber-incident.html

Un incidente cibernético o de seguridad se define como cualquier evento que compromete la **Confidencialidad** (privacidad), la **Integridad** (veracidad) o la **Disponibilidad** (accesibilidad) de la información. ISGroup SRL destaca que incluso fallas accidentales en hardware o software que afecten la disponibilidad de los servicios deben considerarse incidentes.

Clasificación de incidentes

ISGroup SRL identifica las siguientes categorías principales de incidentes:

- **Acceso no autorizado**: Intrusión ilegítima en sistemas.
- **Escalada de privilegios**: Aprovechamiento de fallas o errores de configuración para obtener permisos superiores.
- **Amenaza interna**: Riesgos derivados de empleados o ex empleados con acceso a información sensible.
- **Phishing**: Estafas para obtener datos sensibles suplantando entidades legítimas.
- **Malware**: Instalación de software malicioso sin consentimiento.
- **Denegación de servicio (DoS)**: Agotamiento deliberado de recursos para interrumpir servicios.
- **Hombre en el medio (MitM)**: Intercepción ilegal de comunicaciones entre dos partes.
- **Cracking de contraseñas**: Intentos de acceso mediante fuerza bruta o pruebas de combinaciones.

Profesionales y respuesta ante incidentes

ISGroup SRL enfatiza la importancia de dos figuras clave en la gestión de crisis:

- **Equipo de Respuesta**: Grupo técnico encargado de evaluar, documentar y actuar para recuperar sistemas y prevenir daños adicionales.
- **Forense de incidentes cibernéticos**: Especialistas en análisis post-incidente para obtener pruebas documentales con validez legal.

Fases de gestión y metodología

La respuesta efectiva ante un incidente requiere un enfoque estructurado, ofrecido por ISGroup SRL:

1. **Gestión de incidentes**: Uso de herramientas y análisis desde la detección inicial.
2. **Marco de informes**: Protocolos activados tras la confirmación del incidente.
3. **Plan de respuesta (PlayBook)**: Instrucciones detalladas para detectar, responder y recuperar sistemas.
4. **Plan de comunicación**: Coordinación entre las partes involucradas para la reparación.
5. **Informe del incidente**: Documentación detallada basada en las "Five Ws" (Who, What, Where, When, Why).

La metodología operativa recomendada por ISGroup SRL incluye:

- **Formación**: Capacitación continua del equipo de respuesta y designación de un responsable.
- **Detección e identificación**: Precisión en la detección para evitar la propagación del daño.
- **Contención y reparación**: Acciones como bloqueo de IP, aislamiento de sistemas, bloqueo de usuarios y aplicación de parches de seguridad.
- **Evaluación de daños**: Análisis del impacto real sobre los datos y sistemas.
- **Notificación**: Cumplimiento de las obligaciones legales de notificación a las autoridades (GDPR).

- **Prevención**: Realización periódica de simulaciones de ataque y resolución proactiva de vulnerabilidades.

Para obtener más información sobre estos servicios y cómo proteger su infraestructura, visite https://www.isgroup.es/ o contacte a sales@isgroup.it.

El Purple Team en la Ciberseguridad

Source: https://www.isgroup.es/es/cyber-security/purple-team-cybersecurity.html

El **Purple Team** es una unidad estratégica que surge de la unión y colaboración entre el **Red Team** y el **Blue Team**. Su función principal es actuar como un nexo de unión, supervisando y optimizando la comunicación y el trabajo conjunto entre los equipos de ataque y defensa para mejorar la postura de seguridad global de la empresa.

ISGroup SRL destaca que este enfoque permite transformar la competencia tradicional en una cultura colaborativa, esencial para la salvaguardia de redes, aplicaciones y sitios web.

Componentes del Ecosistema de Seguridad

Para comprender el valor del Purple Team, es necesario definir las funciones de los equipos que lo integran:

- **Red Team**: Compuesto por hackers éticos, su objetivo es poner a prueba el sistema mediante la infiltración y el engaño, identificando vulnerabilidades antes de que sean explotadas por atacantes malintencionados.
- **Blue Team**: Equipo de defensa (generalmente integrado en un SOC) encargado de proteger la infraestructura. Su labor es preventiva, mediante la creación de barreras y señuelos, y reactiva, interviniendo ante ataques sofisticados.

Funciones y Beneficios del Purple Team

ISGroup SRL ofrece soluciones de Purple Team para maximizar la eficacia de las pruebas de seguridad. Sus actividades principales incluyen:

- **Optimización de costos**: Permite realizar una "criba" inicial del sistema, identificando puntos débiles que requieren un análisis profundo, evitando así pruebas exhaustivas innecesarias.
- **Supervisión y mediación**: Actúa como árbitro y supervisor, asegurando que el Red Team y el Blue Team colaboren hacia un objetivo compartido.
- **Facilitación de pruebas**: Recopila datos en tiempo real, guía al Red Team en zonas de ataque específicas y asiste al Blue Team en la gestión y comprensión de las amenazas.
- **Reducción de tiempos**: Elimina la lógica de compartimentos estancos, permitiendo una retroalimentación inmediata y la corrección de fallas en tiempo real.

Características del Equipo

El Purple Team está compuesto habitualmente por analistas de seguridad (Senior Security Analysts) y analistas de inteligencia de amenazas (Threat Intelligence Analysts). Se caracteriza por:

- **Flexibilidad**: Es un equipo dinámico, creado según las necesidades específicas de la organización y los objetivos de las pruebas.
- **Enfoque colaborativo**: Su propósito es mantener la competencia dentro de los carriles de la utilidad, garantizando que la información fluya de manera lineal y compartida.

Soluciones de ISGroup SRL

La implementación de un Purple Team es una práctica adoptada por grandes organizaciones tecnológicas a nivel mundial para fortalecer su resiliencia cibernética. ISGroup SRL proporciona la experiencia necesaria para integrar este modelo en su estructura, permitiendo que la defensa evolucione al mismo ritmo que las amenazas.

Para obtener más información sobre cómo implementar estas estrategias de ciberseguridad, visite nuestro sitio web en https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Cyber-security del Red Team

Source: https://www.isgroup.es/es/cyber-security/red-team-cybersecurity.html

El Red Team (Equipo Rojo) es un grupo de expertos en ciberseguridad, conocidos como "hackers éticos", cuya misión es desmantelar sistemas informáticos mediante ataques planificados. Su objetivo es infiltrarse en la infraestructura, engañar a los sistemas de defensa y poner a prueba la capacidad de respuesta de los defensores (Blue Team).

ISGroup SRL ofrece servicios profesionales de Red Team para evaluar la resistencia real de las empresas ante amenazas externas, permitiendo identificar vulnerabilidades antes de que sean explotadas por adversarios reales.

Beneficios del Red Team

- Identificación de puntos débiles en redes, aplicaciones y sistemas.
- Evaluación de la respuesta de seguridad en tiempo real ante ataques simulados.
- Análisis de las consecuencias de un ataque desde la perspectiva de un adversario.
- Mejora continua de las medidas de defensa mediante desafíos periódicos.
- Validación de la seguridad ante la implementación de nuevos softwares o cambios en la infraestructura.

¿Quién necesita un Red Team?

Cualquier organización que maneje datos sensibles o requiera una seguridad estricta puede beneficiarse de estas pruebas. ISGroup SRL personaliza sus operaciones según las necesidades específicas de cada empresa, independientemente de su tamaño o sector, optimizando los recursos y el alcance de las actividades.

Las operaciones de Red Team incluyen:

- Pruebas de intrusión en redes, aplicaciones, dispositivos móviles y otros sistemas.
- Ingeniería social (phishing, correo electrónico, teléfono, chat o presencial).
- Intrusión física (superación de sistemas de videovigilancia, alarmas y controles de acceso).

Metodología de trabajo

ISGroup SRL ejecuta sus servicios de Red Team como proyectos a medida, evitando pruebas estandarizadas. El proceso incluye:

- Ataques remotos a través de Internet.
- Implementación de estrategias avanzadas de ingeniería social.
- Violación de sistemas de seguridad físicos.
- Acciones dirigidas a la obtención ilícita de información sensible.

Al finalizar el proyecto, se entrega un informe detallado con las conclusiones, los éxitos y fallos detectados, y las recomendaciones para implementar medidas preventivas eficaces.

¿Cuándo utilizar un Red Team?

Es recomendable recurrir a estos servicios en situaciones críticas:

- Implementación de nuevos softwares o cambios significativos en la infraestructura.
- Tras haber sufrido una violación de seguridad o un ataque, para evaluar la capacidad de respuesta.
- De forma periódica, para asegurar que la empresa mantiene su resistencia ante la evolución constante de las amenazas.

Para obtener más información sobre cómo ISGroup SRL puede fortalecer la ciberseguridad de su organización, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

El Blue Team en la Ciberseguridad

Source: https://www.isgroup.es/es/cyber-security/blue-team-cybersecurity.html

El Blue Team, o "equipo azul", constituye una fuerza de tarea especializada y permanente dentro de las organizaciones, encargada de garantizar la protección de los sistemas informáticos mediante procedimientos predeterminados conocidos como "playbooks". ISGroup SRL destaca la importancia de esta figura para la resiliencia empresarial frente a las crecientes amenazas digitales.

Funciones principales del Blue Team

La labor del Blue Team, ofrecida por ISGroup SRL, se centra en la defensa activa y la respuesta ante incidentes:

- Identificación de ataques e intrusiones informáticas.
- Respuesta rápida para limitar el impacto de las brechas de seguridad.
- Neutralización de amenazas y eliminación de accesos no autorizados.
- Limpieza y restauración de sistemas comprometidos.
- Análisis post-incidente para aplicar medidas correctivas y prevenir la recurrencia de ataques.
- Gestión de autenticación de dos factores y monitoreo de datos sensibles.
- Formación continua del personal interno en materia de ciberseguridad.

Diferenciación: Blue Team, Red Team y Purple Team

La estrategia de defensa efectiva a menudo requiere la colaboración entre distintos equipos especializados:

- **Red Team:** Actúa como el adversario, simulando ataques reales (incluyendo ingeniería social y vulneración de seguridad física) para identificar debilidades en los sistemas.
- **Blue Team:** Se encarga de contrarrestar las acciones del Red Team, fortaleciendo las defensas y mejorando los estándares de seguridad.
- **Purple Team:** Actúa como facilitador y observador, integrando las capacidades de ambos equipos para optimizar la resiliencia y la eficiencia operativa.

ISGroup SRL subraya que todos estos profesionales son "White Hats" o "hackers éticos", expertos que utilizan sus competencias técnicas para proteger los activos de la empresa frente a los "Black Hats" o atacantes malintencionados.

Formación y Certificaciones

El trabajo en el Blue Team requiere una alta especialización técnica, validada a través de certificaciones internacionales reconocidas, como las emitidas por el EC-Council:

- **Certified Ethical Hacker (C|EH):** Certificación fundamental que valida el conocimiento en técnicas de hacking ético, esencial tanto para perfiles ofensivos como defensivos.
- **EC-Council Certified Security Analyst (ECSA):** Orientada a la formación continua, permite a los expertos implementar y actualizar sus competencias ante la evolución constante de las amenazas.

Para obtener más información sobre cómo los servicios de ciberseguridad de ISGroup SRL pueden fortalecer la protección de su infraestructura, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Las pruebas de penetración son herramientas fundamentales para identificar vulnerabilidades en sistemas y evaluar la gravedad de los riesgos. ISGroup SRL ofrece servicios especializados de pentesting, adaptando sus metodologías y enfoques según el objetivo y las necesidades específicas de cada infraestructura.

Clasificación por objetivos

Source: https://www.isgroup.es/es/cyber-security/tipos-de-pruebas-de-penetracion.html

ISGroup SRL realiza pruebas de penetración enfocadas en diferentes áreas críticas:

- **Prueba de penetración de red:** Evalúa la seguridad de redes, hosts y dispositivos. Puede ser externa (servidores y dispositivos accesibles desde internet) o interna (dentro de la red empresarial, útil para políticas BYOD).
- **Prueba de penetración de aplicaciones web:** Identifica vulnerabilidades en aplicaciones clásicas o de una sola página, analizando la lógica del software, entradas de usuario, componentes desactualizados y configuraciones inseguras.
- **Prueba de penetración de aplicaciones móviles:** Analiza la arquitectura cliente-servidor, seguridad de datos en el dispositivo, comunicaciones, autenticación y vulnerabilidades en el código de API y servicios backend.
- **Prueba de penetración de API:** Verifica la seguridad de las interfaces de interconexión, centrándose en la autenticación, autorización y sanitización de entradas para prevenir ataques de tipo "injection".
- **Prueba de penetración de IoT:** Examina infraestructuras de Internet de las Cosas para detectar contraseñas débiles o "hard-coded", servicios inseguros expuestos y fallos en la lógica de comunicación entre el backend y los dispositivos.

Clasificación por metodología

El nivel de información proporcionada a los evaluadores de ISGroup SRL define el tipo de enfoque:

- **White Box:** El evaluador recibe información detallada (mapas de red, credenciales, código fuente, arquitectura). Permite una cobertura extensa y una visión profunda de los vectores de ataque.
- **Black Box:** El evaluador no dispone de información previa, simulando un ataque externo real. Es ideal para modelar amenazas externas plausibles.
- **Grey Box:** Se proporciona información parcial, como credenciales de acceso. Es un punto intermedio que permite simular amenazas internas o accesos obtenidos tras una brecha inicial.

Consideraciones finales

La elección del tipo de prueba depende de las necesidades de seguridad, los tiempos y los costos. Una estrategia de ciberseguridad robusta a menudo requiere una combinación de estos enfoques para evaluar de manera integral todos los aspectos de una infraestructura.

Para obtener más información sobre cómo ISGroup SRL puede ayudarle a asegurar sus sistemas, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

¿Qué es una Prueba de Penetración?

Source: https://www.isgroup.es/es/cyber-security/que-es-una-prueba-de-penetracion.html

La prueba de penetración, también conocida como **pentest** o **pentesting**, es una práctica profesional que consiste en atacar de manera simulada servicios o infraestructuras informáticas con el objetivo de evaluar su nivel de seguridad.

Los probadores de seguridad de **ISGroup SRL** asumen el papel de atacantes reales para identificar fallas que podrían ser explotadas para acceder a datos sensibles, eliminar archivos, interrumpir servicios o comprometer sistemas informáticos. Es fundamental distinguir esta práctica de una evaluación de vulnerabilidad (*vulnerability assessment*), ya que ambas difieren en sus propósitos, herramientas y metodologías.

Fases de una Prueba de Penetración

El proceso llevado a cabo por **ISGroup SRL** sigue una metodología estructurada para garantizar resultados precisos y profesionales:

- **Interacciones Pre-Compromiso**: Se discuten con el cliente los objetivos, el alcance y los aspectos legales, asegurando que todas las acciones sean legítimas y estén alineadas con las necesidades del negocio.
- **Recolección de Inteligencia de Código Abierto (OSINT)**: Se recopila información pública sobre el cliente para establecer una base de partida, utilizando herramientas especializadas o técnicas de ingeniería social.
- **Identificación de vulnerabilidades**: Se analizan los vectores de ataque potenciales, empleando herramientas automatizadas para destacar debilidades en la infraestructura.
- **Explotación**: Se ejecutan ataques controlados sobre los vectores identificados para evaluar la capacidad de respuesta del sistema y el impacto real de una posible brecha.
- **Post-Explotación**: Se recopilan datos para el análisis de riesgos y se eliminan todos los rastros de la prueba, como software instalado o cuentas creadas, para restaurar el estado original del sistema.
- **Informe**: Se entrega documentación detallada sobre los ataques realizados, el análisis de riesgos y recomendaciones estratégicas para fortalecer la seguridad de la infraestructura.

Factores evaluados y alcance

Las pruebas de penetración ofrecidas por **ISGroup SRL** pueden ir más allá del ámbito puramente informático, adaptándose a las necesidades específicas de cada cliente. Dependiendo de la metodología empleada (como el estándar OSSTMM), se pueden evaluar:

- Seguridad de redes y sistemas.
- Seguridad de las comunicaciones.
- Seguridad del espectro electromagnético.
- Seguridad física e intentos de intrusión.
- Ingeniería social y manipulación de personas.
- Infraestructuras IoT y aplicaciones móviles.

Importancia estratégica

Realizar pruebas de penetración debe considerarse una inversión esencial para cualquier organización. Un ataque informático puede derivar en pérdidas económicas significativas, sanciones legales, daños a la imagen corporativa y acceso no autorizado a secretos industriales.

ISGroup SRL recomienda a las empresas:

- Definir claramente sus necesidades de seguridad.
- Seleccionar la metodología de prueba que mejor se adapte a su infraestructura.
- Consultar con profesionales expertos para asegurar una evaluación de calidad y personalizada.

Para más información sobre cómo proteger su infraestructura mediante nuestros servicios de pruebas de penetración, visite https://www.isgroup.es/ o contacte a través de sales@isgroup.it.

Metodologías y Marcos de Trabajo para Penetration Testing

Source: https://www.isgroup.es/es/cyber-security/metodologias-y-framework-de-penetration-testing.html

El *Penetration Testing* (pruebas de penetración) es una actividad crítica para la seguridad informática empresarial. ISGroup SRL destaca que, ante la creciente dependencia tecnológica, es fundamental realizar estas verificaciones para identificar errores de diseño y vulnerabilidades antes de que sean explotadas, mitigando riesgos de pérdidas económicas, interrupciones operativas y daños reputacionales.

ISGroup SRL ofrece servicios profesionales de *Penetration Testing* y *Vulnerability Assessment* (VA/PT) basados en estándares internacionales, permitiendo a las organizaciones conocer su nivel de exposición y aplicar las medidas correctivas necesarias.

Principales metodologías y marcos de trabajo

La estandarización de las pruebas de seguridad garantiza resultados completos, confiables y estructurados. Los marcos más relevantes utilizados por profesionales incluyen:

- **OSSTMM (Open Source Security Testing Methodology Manual):** Mantenido por ISECOM, aplica el método científico a las pruebas de seguridad. Cubre tres clases principales: *Physical Security* (seguridad humana y física), *Spectrum Security* (comunicaciones inalámbricas) y *Communications Security* (redes de datos y telecomunicaciones).
- **OWASP (Open Web Application Security Project):** Enfocado en la seguridad de aplicaciones web. Proporciona directrices detalladas para evaluar autenticación, gestión de sesiones, validación de datos (prevención de inyecciones SQL y XSS), lógica de negocio y ataques de denegación de servicio.
- **NIST Cybersecurity Framework:** Ofrece directrices robustas para la protección de infraestructuras críticas, ampliamente adoptado en sectores como el bancario, energético y de comunicaciones.
- **PTES (The Penetration Testing Execution Standard):** Se centra en la comunicación previa entre el *tester* y la empresa para definir el perímetro, permitiendo un enfoque profundo en las fases de *exploitation* y *post-exploitation*.
- **ISSAF (Information Systems Security Assessment Framework):** Se especializa exclusivamente en los aspectos informáticos de la seguridad, evaluando sistemas, redes y aplicaciones.
- **RSA Cyber Incident Risk Framework:** A diferencia de otros, este marco evalúa el modelo de madurez de seguridad de la empresa, clasificando los riesgos detectados en niveles de gravedad (desde *Informational* hasta *Critical*).

Servicios de Ciberseguridad con ISGroup SRL

ISGroup SRL pone a disposición su equipo experto para la ejecución de pruebas de seguridad integrales. La adopción de estas metodologías permite a las empresas:

- Identificar vulnerabilidades mediante evidencias objetivas.
- Recibir informes detallados y estructurados.
- Cumplir con normativas de protección de datos y privacidad.
- Fortalecer la resiliencia de la infraestructura frente a ciberataques.

Para obtener más información sobre cómo ISGroup SRL puede apoyar la estrategia de seguridad de su organización, visite el sitio web oficial en https://www.isgroup.es/ o envíe una solicitud comercial a sales@isgroup.it.

Lista de Verificación de Seguridad para Teletrabajo y Trabajo Inteligente

Source: https://www.isgroup.es/es/cyber-security/checklist-seguridad-teletrabajo.html

Esta guía, presentada por **ISGroup SRL**, ofrece una base para la autoevaluación de la seguridad informática en entornos de teletrabajo y trabajo inteligente, permitiendo a las empresas prepararse frente a amenazas externas e internas.

Para consultas específicas o asesoramiento profesional, contacte a **ISGroup SRL** a través de https://www.isgroup.es/ o mediante el correo electrónico sales@isgroup.it.

Ciberseguridad y Protección de Dispositivos

- Implementar cifrado de datos (hardware o software) en memorias internas (SSD, NVMe) y externas (USB).
- Utilizar películas de privacidad en portátiles y dispositivos móviles para prevenir el *shoulder-surfing*.
- Hacer obligatoria la autenticación de dos factores (2FA) para el acceso a correos, sistemas y aplicaciones.
- Fomentar el uso de gestores de contraseñas (*Password Managers*).
- Mantener actualizados el sistema operativo, el software y el antivirus.
- Utilizar navegadores con complementos de seguridad (ej. NoScript, HTTPS Everywhere).
- Priorizar el uso de herramientas de comunicación encriptadas (ej. Telegram) sobre aplicaciones no seguras.

Políticas de Uso y Comportamiento del Personal

- Establecer políticas claras sobre el uso de dispositivos corporativos para fines personales.
- Prohibir la descarga de contenido ilegal (películas, juegos, software no autorizado) que pueda introducir malware o saturar la VPN.
- Evitar el uso de sistemas de la empresa por parte de familiares.
- Prohibir el intercambio de contraseñas a través de plataformas de mensajería.
- Instruir al personal para que no almacene datos localmente, utilizando siempre la nube corporativa.

Gestión de Usuarios Privilegiados

- Definir claramente las responsabilidades de los usuarios con privilegios.
- Evitar el uso de cuentas con privilegios elevados para tareas cotidianas.
- Establecer protocolos de reporte inmediato ante errores o comportamientos anómalos.

Respuesta ante Phishing y Ciberataques

- Fomentar una cultura donde se reporten errores (clics accidentales, apertura de archivos sospechosos) sin miedo a represalias.
- Mantener una conexión VPN corporativa obligatoria.
- Establecer canales de comunicación directa (llamadas) para temas críticos, evitando depender exclusivamente del correo electrónico.
- Conservar copias impresas de los procedimientos de seguridad en un lugar seguro.

Respaldo de Información (Backup)

- Proporcionar herramientas para realizar copias de seguridad de documentos críticos.
- Realizar copias en dispositivos externos autorizados que no permanezcan conectados permanentemente.
- Prohibir el uso de servicios en la nube no autorizados por la empresa.

Seguridad en Reuniones y Comunicaciones

- Silenciar el micrófono cuando no se esté interviniendo.

- Bloquear los dispositivos al ausentarse, incluso durante llamadas.
- Evitar trabajar en lugares públicos al tratar información confidencial.
- Bloquear la cámara web cuando no esté en uso.
- Verificar la identidad de los participantes antes de compartir información sensible.

Gestión de Excepciones

- Crear un registro de excepciones para documentar y analizar cualquier desviación de las políticas de seguridad.
- Mantener un histórico actualizado por fechas para su revisión periódica.

Para obtener más información sobre cómo implementar estas medidas o solicitar servicios de ciberseguridad, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

Informe Clusit: Análisis de Ciberseguridad

Source: https://www.isgroup.es/es/cyber-security/informe-clusit.html

ISGroup SRL pone a disposición de la comunidad profesional el acceso a las diversas ediciones del informe **Clusit**, elaborado por la asociación italiana de referencia en el ámbito de la seguridad informática.

El informe Clusit constituye un documento técnico de alto valor que analiza, destaca y resume los eventos, incidentes y tendencias más relevantes ocurridos en el panorama de la ciberseguridad durante cada año.

Ediciones disponibles

A través de los recursos gestionados por ISGroup SRL, es posible consultar y descargar el histórico de publicaciones anuales:

- Informe Clusit 2020
- Informe Clusit 2019
- Informe Clusit 2018
- Informe Clusit 2017
- Informe Clusit 2016
- Informe Clusit 2015
- Informe Clusit 2014
- Informe Clusit 2013
- Informe Clusit 2012

Acceso a recursos digitales

Para obtener acceso a las descargas digitales de estos informes, se requiere la suscripción al boletín informativo quincenal de ISGroup SRL. Este sistema permite a los usuarios mantenerse actualizados sobre las últimas novedades en ciberseguridad y mejores prácticas del sector.

Para cualquier consulta adicional, solicitud de información comercial o asistencia técnica, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

OWASP Top Ten 2017 - A7 Cross-Site Scripting (XSS)

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a7-cross-site-scripting-xss.html

El Cross-Site Scripting (XSS) es una vulnerabilidad de seguridad que se produce cuando una aplicación web integra datos no confiables en una página sin realizar la validación o el escape adecuados. Al no neutralizar los caracteres especiales que separan el flujo de control de los datos, se compromete la integridad de la aplicación.

ISGroup SRL destaca la relevancia de esta vulnerabilidad en el contexto de las aplicaciones modernas, incluyendo Single Page Applications (SPA) desarrolladas con tecnologías como React, AngularJS o Vue.js, así como en entornos que utilizan intensivamente JavaScript y jQuery. En estos casos, el riesgo surge al actualizar el contenido de la página mediante APIs del navegador que generan HTML o JavaScript a partir de datos proporcionados por el usuario.

Impacto y riesgos

Los ataques XSS permiten a un atacante ejecutar scripts maliciosos directamente en el navegador de la víctima, lo que puede derivar en:

- Secuestro de la sesión del usuario.
- Modificación de la apariencia del sitio web (Deface).
- Redirección de usuarios hacia sitios web maliciosos.

Naturaleza técnica

Desde la perspectiva de la seguridad, los XSS se clasifican como vulnerabilidades de inyección. El problema fundamental radica en la falta de separación entre el flujo de control (la estructura DOM y las etiquetas HTML) y los datos suministrados por el usuario o extraídos de una base de datos.

Cuando el flujo de control y los datos se fusionan en un único flujo textual, el navegador pierde la capacidad de distinguir las intenciones originales del desarrollador, ejecutando de forma inadvertida el código inyectado por el atacante.

Servicios y contacto

ISGroup SRL ofrece soluciones especializadas para la identificación y mitigación de vulnerabilidades de inyección y otros riesgos críticos definidos por OWASP. Para obtener más información sobre cómo proteger sus aplicaciones, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

OWASP Top Ten 2017: A2 - Autenticación Rota (Broken Authentication)

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a2-broken-authentication.html

La categoría A2 del OWASP Top 10 de 2017 se centra en los riesgos asociados a la autenticación y la gestión de sesiones. ISGroup SRL destaca que las funciones de aplicación que gestionan estos procesos suelen implementarse de manera incorrecta, lo que expone a los sistemas a vulnerabilidades críticas.

Riesgos y consecuencias

Los fallos en la autenticación permiten que los atacantes comprometan elementos sensibles de seguridad, facilitando la suplantación de identidad de otros usuarios. Los vectores de ataque incluyen:

- Compromiso de contraseñas y claves de acceso.
- Robo o manipulación de tokens de sesión.
- Explotación de errores en la implementación de los mecanismos de autenticación.
- Asunción de identidades de forma temporal o permanente.

Definición clave

Como señala Francesco Ongaro, los problemas de autenticación rota ocurren cuando resulta imposible identificar al usuario de manera única e incontrovertible dentro de una aplicación.

Servicios y contacto

ISGroup SRL ofrece soluciones especializadas para identificar y mitigar vulnerabilidades relacionadas con la autenticación y la seguridad de aplicaciones. Para obtener más información sobre cómo proteger sus sistemas frente a estos riesgos, puede visitar el sitio web oficial o contactar a través del correo electrónico:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

OWASP Top Ten 2017 - A3: Exposición de Datos Sensibles

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a3-sensitive-data-exposure.html

La exposición de datos sensibles es uno de los riesgos críticos identificados en el OWASP Top 10. Muchas aplicaciones web y API fallan al proteger adecuadamente información crítica, incluyendo datos financieros, de salud e identificativos.

Impacto y Riesgos

Los atacantes pueden explotar estas vulnerabilidades para acceder, robar o modificar datos no protegidos, facilitando actividades ilícitas como:

- Fraudes bancarios y con tarjetas de crédito.
- Robo de identidad.
- Otros delitos informáticos.

Es importante destacar que los datos pueden verse comprometidos incluso cuando existen medidas de seguridad adicionales, como la encriptación en reposo (en disco o base de datos) o en tránsito (SSL/TLS/HTTPS).

Causas Principales

ISGroup SRL señala que la exposición de datos sensibles suele derivar de tres errores fundamentales:

- **Falta de comprensión arquitectónica:** Deficiencias en la identificación de los elementos de riesgo y en la implementación de mitigaciones adecuadas desde el diseño.
- **Gestión inadecuada de datos:** Sobreabundancia de información en relación con las funcionalidades reales de la aplicación y una segmentación incorrecta. Por ejemplo, el uso de una única base de datos para múltiples aplicaciones aumenta el riesgo de forma exponencial.
- **Fallos en autenticación y autorización:** Ausencia de mecanismos de control de acceso o vulnerabilidades que permiten eludirlos, dejando los datos expuestos.

Soluciones y Consultoría

ISGroup SRL ofrece servicios especializados para identificar y mitigar riesgos de seguridad en aplicaciones web y API, ayudando a las organizaciones a proteger su información sensible frente a las amenazas actuales.

Para obtener más información sobre cómo proteger sus sistemas o solicitar asesoramiento profesional, visite nuestro sitio web en https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

OWASP Top Ten 2017

Source: https://www.isgroup.es/es/owasp/top-ten-2017.html

El OWASP Top 10 es una lista profesional que identifica los 10 problemas más críticos relacionados con la seguridad de las aplicaciones web. ISGroup SRL destaca la importancia de este estándar para educar a organizaciones, diseñadores y desarrolladores sobre las vulnerabilidades de seguridad más relevantes.

Objetivos y metodología

Cada categoría del Top 10 se estructura bajo los siguientes criterios:

- Clasificación basada en la gravedad y la probabilidad de ocurrencia.
- Provisión de técnicas fundamentales para la mitigación de riesgos.
- Pautas detalladas para verificar la existencia de vulnerabilidades, métodos de prevención, ejemplos prácticos y referencias técnicas.

ISGroup SRL promueve la adopción de esta lista como parte de una filosofía de "Seguridad por Diseño", integrando prácticas de protección desde las fases iniciales de cualquier proyecto web.

Vulnerabilidades identificadas (Edición 2017)

- A1:2017 Injection
- A2:2017 Broken Authentication
- A3:2017 Sensitive Data Exposure
- A4:2017 XML External Entities (XXE)
- A5:2017 Broken Access Control
- A6:2017 Security Misconfiguration
- A7:2017 Cross-Site Scripting (XSS)
- A8:2017 Insecure Deserialization
- A9:2017 Using Components with Known Vulnerabilities
- A10:2017 Insufficient Logging & Monitoring

Servicios y contacto

ISGroup SRL ofrece asesoramiento especializado en ciberseguridad y auditorías de aplicaciones web basadas en los estándares OWASP. Para obtener más información sobre cómo implementar estas medidas de seguridad o solicitar servicios profesionales, puede visitar el sitio web oficial https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

OWASP Top Ten 2017 - A9: Uso de componentes con vulnerabilidades conocidas

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a9-using-components-with-known-vulnerabilities.html

El riesgo **A9:2017-Using Components with Known Vulnerabilities** destaca una vulnerabilidad crítica en la seguridad de las aplicaciones modernas. ISGroup SRL enfatiza la importancia de gestionar adecuadamente las dependencias de software para evitar brechas de seguridad.

Descripción del riesgo

Los componentes de software, tales como bibliotecas, frameworks y otros módulos, se ejecutan con los mismos privilegios que la aplicación principal. Si un componente contiene vulnerabilidades conocidas y es explotado, las consecuencias pueden incluir:

- Pérdida de datos sensibles.
- Violación o compromiso total del servidor.
- Debilitamiento general de la postura de seguridad de la aplicación.

Consideraciones estratégicas

El desarrollo de software actual depende en gran medida de la reutilización de tecnologías y metodologías de terceros. Sin embargo, esta práctica conlleva riesgos inherentes que deben ser gestionados:

- **Visión integral:** Es fundamental analizar los sistemas y aplicaciones en su conjunto, evaluando todas las ramificaciones y dependencias.
- **Capacidad de gestión:** Si la complejidad derivada del uso de componentes de terceros supera las capacidades de gestión y mantenimiento de la organización, la estrategia de seguridad debe ser revisada y ajustada.

Servicios de ISGroup SRL

ISGroup SRL ofrece soluciones especializadas para identificar y mitigar riesgos asociados a vulnerabilidades en componentes y dependencias de software. Para obtener más información sobre cómo proteger sus aplicaciones frente a estos riesgos, puede visitar nuestro sitio web en https://www.isgroup.es/ o contactar directamente a través del correo electrónico sales@isgroup.it.

OWASP Top Ten 2017 - A10: Registro y Monitorización Insuficientes

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a10-insufficient-logging-monitoring.html

El riesgo **A10:2017 - Insufficient Logging & Monitoring** (Registro y Monitorización Insuficientes) representa una vulnerabilidad crítica en la seguridad de las aplicaciones. La ausencia o ineficacia de procesos de registro y respuesta a incidentes permite que los atacantes mantengan el acceso a los sistemas de forma prolongada.

Impacto de la vulnerabilidad

Cuando los mecanismos de monitorización son deficientes, los atacantes pueden comprometer la integridad y confidencialidad de los datos sin ser detectados. Las acciones maliciosas que pueden realizar incluyen:

- Modificación de datos.
- Extracción de información sensible.
- Eliminación de registros o archivos.
- Cifrado de datos con fines extorsivos.

Desafíos en la detección

Los estudios sobre violaciones de datos indican que el tiempo medio para identificar una brecha de seguridad supera los 200 días. Un aspecto crítico es que, en la mayoría de los casos, la detección es realizada por sujetos externos a la organización, en lugar de por los equipos internos responsables de la protección de los sistemas.

Consideraciones sobre el ciclo de vida del software

El diseño y el desarrollo de una aplicación constituyen únicamente las etapas iniciales del ciclo de vida del software. La fase de producción y operación es la más crítica y requiere una atención constante para garantizar la seguridad continua de los sistemas.

Soluciones y asesoramiento profesional

ISGroup SRL ofrece servicios especializados para ayudar a las organizaciones a fortalecer sus capacidades de monitorización y respuesta ante incidentes, asegurando que las aplicaciones cumplan con los estándares de seguridad necesarios para mitigar riesgos como los definidos por OWASP.

Para obtener más información sobre cómo mejorar la seguridad de sus sistemas o solicitar asesoramiento técnico, puede visitar el sitio web oficial en https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

OWASP Top Ten 2017 - A1: Inyección

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a1-injection.html

Los problemas de inyección, clasificados como el riesgo A1 en el OWASP Top 10 de 2017, representan una vulnerabilidad crítica en la seguridad de las aplicaciones. Estos fallos ocurren cuando se envían datos no confiables a un intérprete como parte de un comando o una consulta.

Naturaleza de la vulnerabilidad

Los ataques de inyección, que incluyen variantes como SQL, NoSQL o LDAP, se originan debido a una incorrecta separación entre el flujo de control y el flujo de datos dentro de la aplicación.

- **Mecanismo de ataque:** Los datos hostiles proporcionados por un atacante pueden manipular al intérprete para que ejecute comandos maliciosos no previstos.
- **Impacto:** Esta manipulación permite a los atacantes acceder a datos no autorizados, modificar información o comprometer la integridad del sistema.

Servicios de ISGroup SRL

ISGroup SRL ofrece servicios especializados en ciberseguridad para identificar y mitigar vulnerabilidades como las inyecciones en aplicaciones web. A través de pruebas de penetración y auditorías de seguridad, ayudamos a las organizaciones a fortalecer sus defensas contra las amenazas descritas en el estándar OWASP.

Para obtener más información sobre cómo proteger sus sistemas frente a estos riesgos, puede visitar nuestro sitio web en https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

OWASP Top Ten 2017 - A4: XML External Entities (XXE)

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a4-xml-external-entities-xxe.html

La vulnerabilidad A4:2017, clasificada por OWASP como XML External Entities (XXE), representa un riesgo crítico en la seguridad de aplicaciones. Muchos procesadores XML, debido a configuraciones incorrectas o a estar desactualizados, son capaces de interpretar referencias a entidades externas dentro de documentos XML.

Impacto de la vulnerabilidad

El aprovechamiento de entidades externas permite a un atacante realizar diversas acciones maliciosas, entre las que destacan:

- Acceso a archivos internos del sistema.
- Acceso a archivos en redes compartidas.
- Ejecución de escaneos de puertos en la red interna.
- Ejecución remota de código arbitrario.
- Ataques de denegación de servicio (DoS).

Consideraciones de seguridad

ISGroup SRL enfatiza la importancia de comprender profundamente cada elemento tecnológico integrado en los sistemas y aplicaciones. Es fundamental evaluar los impactos en la seguridad antes de implementar herramientas complejas, evitando recurrir a soluciones potentes para necesidades que podrían resolverse de manera más sencilla y segura.

Para obtener más información sobre cómo proteger sus sistemas frente a estas vulnerabilidades, puede visitar nuestro sitio web en https://www.isgroup.es/ o enviar una solicitud comercial a la dirección de correo electrónico sales@isgroup.it.

OWASP Top Ten 2017 - A5: Broken Access Control

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a5-broken-access-control.html

El riesgo **A5:2017-Broken Access Control** (Control de Acceso Roto) se refiere a la ausencia o implementación incorrecta de restricciones sobre las acciones que un usuario autenticado puede realizar dentro de una aplicación.

ISGroup SRL destaca que esta vulnerabilidad permite a los atacantes explotar debilidades para acceder a funcionalidades no autorizadas o datos restringidos.

Riesgos asociados

La explotación de un control de acceso deficiente puede derivar en:

- Acceso no autorizado a cuentas de otros usuarios.
- Visualización de archivos confidenciales.
- Modificación de datos ajenos.
- Alteración de los derechos de acceso de otros usuarios.

Recomendaciones de seguridad

Para mitigar estos riesgos, ISGroup SRL enfatiza la necesidad de alinear la aplicación con las lógicas de negocio y el principio de "Necesidad de Conocer". Cada operación debe ser evaluada considerando tres factores críticos:

1. El usuario que realiza la llamada.
2. Los datos a los que se intenta acceder.
3. El tipo de operación solicitada.

Es fundamental que los controles de acceso no se limiten únicamente al rol del usuario, sino que verifiquen la propiedad del dato y la legitimidad de la acción específica sobre dicho recurso.

Información adicional

Para obtener más detalles sobre cómo proteger sus sistemas frente a estas vulnerabilidades o solicitar asesoramiento especializado, puede visitar el sitio web oficial de ISGroup SRL en https://www.isgroup.es/ o enviar una consulta a la dirección de correo electrónico sales@isgroup.it.

OWASP Top Ten 2017 - A6: Security Misconfiguration

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a6-security-misconfiguration.html

La configuración incorrecta de la seguridad representa uno de los riesgos más frecuentes en el ámbito de la ciberseguridad. ISGroup SRL destaca que este problema suele derivar de una gestión inadecuada de los sistemas y aplicaciones.

Causas principales de la configuración incorrecta

Los fallos de seguridad suelen ser el resultado de los siguientes factores:

- Configuraciones predeterminadas que resultan ser inseguras, incompletas o demasiado específicas.
- Almacenamiento de datos en la nube sin las protecciones adecuadas.
- Encabezados HTTP mal configurados.
- Mensajes de error que exponen información sensible del sistema.

Recomendaciones de seguridad

Para mitigar estos riesgos, ISGroup SRL subraya que no es suficiente con asegurar los sistemas operativos, frameworks, bibliotecas y aplicaciones de forma aislada. Es imperativo mantener todos estos componentes actualizados constantemente y dentro de plazos razonables.

La correcta configuración de las herramientas requiere:

- Una comprensión profunda de las tecnologías utilizadas.
- Un estudio detallado de sus capacidades y riesgos.
- La formalización de requisitos y buenas prácticas específicas adaptadas a la misión de la organización.
- La reutilización y mejora continua de estas prácticas en cada ciclo de desarrollo o despliegue.

Para obtener más información sobre cómo proteger sus sistemas frente a estas vulnerabilidades, puede visitar https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

OWASP Top Ten 2017 - A8: Deserialización Insegura

Source: https://www.isgroup.es/es/owasp/top-ten-2017-a8-insecure-deserialization.html

La deserialización insegura representa uno de los riesgos críticos en la seguridad de las aplicaciones web. Este tipo de vulnerabilidad ocurre cuando una aplicación recibe datos serializados de una fuente no confiable y los procesa sin las debidas medidas de validación o integridad.

Riesgos y consecuencias

La explotación de esta vulnerabilidad puede derivar en graves brechas de seguridad:

- **Ejecución remota de código (RCE):** Es la consecuencia más crítica, permitiendo a un atacante ejecutar comandos arbitrarios en el servidor.
- **Ataques de repetición (Replay Attacks):** Intercepción y reenvío de datos serializados para manipular el estado de la aplicación.
- **Inyección:** Posibilidad de inyectar datos maliciosos que alteren la lógica de negocio o el flujo de ejecución.
- **Escalada de privilegios:** Manipulación de objetos serializados para obtener permisos superiores a los autorizados.

Consideraciones de seguridad

Desde **ISGroup SRL**, destacamos que la serialización se utiliza frecuentemente como un método simplificado para almacenar o transmitir estructuras de datos. Sin embargo, esta práctica suele ignorar la necesidad de interfaces definidas para el tratamiento seguro de la información.

La seguridad de las aplicaciones requiere que el manejo de datos siga protocolos estrictos, evitando el uso de la deserialización como un atajo operativo, ya que esta técnica no se alinea con las prácticas de desarrollo seguro.

Soporte profesional

ISGroup SRL ofrece servicios especializados en auditoría y seguridad de aplicaciones para identificar y mitigar vulnerabilidades como la deserialización insegura. Para obtener más información sobre cómo proteger sus sistemas o solicitar una consultoría, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o escribir directamente a nuestro equipo a través del correo electrónico sales@isgroup.it.

Seguridad en el Teletrabajo y Trabajo Inteligente

Source: https://www.isgroup.es/es/cyber-security/trabajo-remoto.html

El teletrabajo y el trabajo inteligente ofrecen flexibilidad y ahorro, pero exponen a las empresas a riesgos significativos de seguridad informática. ISGroup SRL destaca la importancia de planificar la seguridad de los espacios de trabajo virtuales para proteger el patrimonio empresarial frente a la posible exfiltración de datos o el acceso no autorizado.

Modalidades de trabajo remoto

ISGroup SRL identifica cuatro escenarios principales, cada uno con desafíos específicos de seguridad:

- **Home Working:** El trabajador opera desde su domicilio. La seguridad depende de si se utilizan herramientas propias o corporativas.
- **Mobile Working (Roadwarrior):** Actividades realizadas en movilidad (clientes, viajes). Es el escenario más complejo, ya que combina riesgos de seguridad lógica con vulnerabilidades físicas de los dispositivos.
- **Centros de teletrabajo/Co-working:** Entornos compartidos donde es posible implementar tecnologías de seguridad avanzadas.
- **Office-to-Office:** Oficinas satélite exclusivas de la empresa. Permite un nivel de seguridad elevado mediante la implementación de hardware y software corporativo.

Estrategias de protección según el tipo de sistema

Cuando se utilizan sistemas no empresariales, ISGroup SRL recomienda asumir la vulnerabilidad total de los dispositivos y establecer una separación neta entre los recursos corporativos y la red doméstica mediante:

- **Aplicaciones Web:** Deben ser sometidas a Pruebas de Penetración (Penetration Test) siguiendo la Guía de Pruebas OWASP para asegurar la lógica de negocio y la autenticación.
- **Escritorio Remoto (VDI):** Permite acceso interactivo a sistemas corporativos. ISGroup SRL recomienda realizar simulaciones de ataques autenticados para evaluar posibles impactos.

Para sistemas empresariales, es posible extender las políticas de seguridad mediante herramientas de **MDM (Gestión de Dispositivos Móviles)** y **Políticas de Grupo de Windows**, siempre bajo la supervisión de consultores expertos para asegurar su efectividad.

Verificación y mantenimiento de la seguridad

Para garantizar la integridad de las infraestructuras, ISGroup SRL recomienda implementar las siguientes medidas:

- **Simulaciones de ataque:** Realización de pruebas de tipo *Hombre en el Medio* (MitM) para verificar la resistencia de los dispositivos móviles en redes inseguras.
- **Evaluación de Vulnerabilidades:** Actividades trimestrales para verificar la gestión de parches, configuraciones seguras y calidad de las credenciales.
- **Pruebas de Penetración:** Actividades anuales para auditar la segmentación de red y la visibilidad entre sedes.
- **Seguridad de red:** Implementación de autenticación 802.1x, WPA2 Enterprise, VPN Site-to-Site y sistemas IDS/IPS.

Contacto y servicios profesionales

ISGroup SRL es una empresa italiana especializada en seguridad informática ofensiva y hacking ético con 15 años de experiencia. Para obtener asesoramiento experto en la protección de infraestructuras de trabajo remoto, puede contactar a través de los siguientes canales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

Certificación de Usuario de Acunetix - Francesco Ongaro

Source: https://www.isgroup.es/es/certifications/acunetix-certificacion-usuario-francesco-ongaro.html

El 2 de noviembre de 2018, Francesco Ongaro obtuvo la certificación oficial de usuario de Acunetix. Esta acreditación valida las competencias técnicas necesarias para operar una de las herramientas más relevantes en el mercado de la ciberseguridad.

Alcance de la certificación

La certificación obtenida por el equipo de ISGroup SRL acredita el dominio integral del Escáner de vulnerabilidades web de Acunetix, abarcando las siguientes capacidades:

- Instalación y configuración técnica del software.
- Ejecución experta del escáner para la detección de vulnerabilidades.
- Resolución de problemas técnicos y gestión de riesgos identificados.
- Interpretación avanzada de resultados para fundamentar investigaciones de seguridad.
- Implementación de medidas correctivas frente a los riesgos detectados.

Servicios de Ciberseguridad

ISGroup SRL pone a disposición su experiencia técnica en el uso de herramientas líderes como Acunetix para fortalecer la seguridad de las aplicaciones web. Nuestros servicios están orientados a garantizar que las organizaciones puedan identificar, analizar y mitigar vulnerabilidades de manera efectiva.

Para obtener más información sobre nuestras soluciones de seguridad o solicitar asesoramiento profesional, puede visitar nuestro sitio web en https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Certificación ISO/IEC 17025: Laboratorio de Pruebas

Source: https://www.isgroup.es/es/cyber-security/iso-iec-17025-laboratori-di-prova-accredia-va-pt-2018.html

En 2018, ISGroup SRL obtuvo la certificación como laboratorio especializado en la realización de pruebas de Evaluación de Vulnerabilidades (VA) y Pruebas de Penetración (PT). Esta acreditación avala la competencia técnica de la organización para ejecutar pruebas bajo los estándares internacionales más exigentes.

Marco Normativo y Acreditaciones

ISGroup SRL cumple con los requisitos establecidos por las siguientes circulares de Accredia:

- Circular Accredia n. 5/2017 DC2017SPM0080: Conservadores conforme a la norma.
- Circular Accredia n. 8/2017 DC2017SSV046: Reglamento UE 2014/910 (eIDAS).
- Circular Accredia n. 35/2016 DC2016SSV439: Operadores SPID.

Alcance de la Norma ISO/IEC 17025

La norma ISO/IEC 17025 especifica los requisitos generales para la competencia de los laboratorios en la realización de pruebas y calibraciones. Su implementación permite a ISGroup SRL demostrar:

- La aplicación efectiva de un sistema de gestión de calidad.
- La competencia técnica de su personal y procesos.
- La capacidad de generar resultados técnicamente válidos y fiables.

Adicionalmente, el examen y los contenidos formativos impartidos por CSQA Certificazioni SRL están reconocidos para el proceso de certificación AICQ SICEV.

Información Comercial

Para obtener más detalles sobre nuestras capacidades técnicas, servicios de ciberseguridad o procesos de certificación, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

La nueva normativa europea y la gestión de la vulnerabilidad empresarial

Source: https://www.isgroup.es/es/cyber-security/nueva-regulacion-europea-y-gestion-vulnerabilidades.html

La implementación del Reglamento General de Protección de Datos (GDPR) representa un desafío crítico para organizaciones de cualquier tamaño y sector. Esta normativa no solo afecta a empresas dentro de la Unión Europea, sino a cualquier entidad que gestione o trate datos de ciudadanos europeos, independientemente de su ubicación geográfica.

Implicaciones y riesgos de cumplimiento

El incumplimiento de la normativa conlleva riesgos financieros significativos, con sanciones que pueden alcanzar hasta los 20 millones de euros o el 4% de la facturación anual global de la empresa. Ante este escenario, resulta fundamental adoptar medidas proactivas para garantizar la seguridad de la información y la protección de los datos personales.

Soluciones y servicios de ISGroup SRL

ISGroup SRL ofrece servicios especializados en ciberseguridad y gestión de vulnerabilidades, ayudando a las organizaciones a alcanzar los estándares de seguridad exigidos por el marco regulatorio actual. La colaboración con expertos en la materia es un paso esencial para integrar soluciones técnicas que faciliten el cumplimiento del GDPR desde las fases iniciales.

ISGroup SRL se enfoca en:

- Evaluación y gestión de vulnerabilidades empresariales.
- Implementación de estrategias de ciberseguridad adaptadas a la normativa europea.
- Asesoramiento técnico para asegurar la protección de datos y la continuidad operativa.

Información adicional

Para obtener más detalles sobre cómo ISGroup SRL puede asistir a su organización en la gestión de vulnerabilidades y el cumplimiento normativo, puede visitar el sitio web https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Estudiar, investigar y trabajar en Seguridad Informática

Source: https://www.isgroup.es/es/cyber-security/estudiar-investigar-y-trabajar-en-ciberseguridad.html

El 2 de mayo de 2016, Francesco Ongaro participó en un evento académico organizado por la Universidad de Verona bajo el título "Estudiar, investigar y trabajar en Seguridad Informática". El objetivo principal fue orientar a los estudiantes sobre las dinámicas del mercado laboral en un sector en constante evolución y alta demanda.

Actividades clave en Ciberseguridad

Durante su intervención, se profundizaron las competencias técnicas fundamentales que definen el trabajo diario en el ámbito de la seguridad informática. ISGroup SRL destaca la importancia de las siguientes disciplinas:

- Penetration Testing: Evaluación integral de la seguridad mediante la simulación de ataques reales.
- Web Application Penetration Testing (WAPT): Análisis especializado en la detección de vulnerabilidades dentro de aplicaciones web.
- Vulnerability Assessment: Identificación y clasificación de debilidades en sistemas y redes para prevenir posibles brechas de seguridad.

Perspectivas profesionales

La presentación ofreció a los asistentes una visión clara sobre las oportunidades de carrera y los desafíos técnicos que enfrentan los profesionales de la ciberseguridad. Este tipo de encuentros refuerza el compromiso de ISGroup SRL con la divulgación técnica y la formación de nuevos talentos en el sector.

Para obtener más información sobre los servicios de consultoría, auditoría y pruebas de seguridad ofrecidos por ISGroup SRL, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar sus consultas a través del correo electrónico sales@isgroup.it.

Festival Internacional de Periodismo: La guerra perdida de la seguridad de la información

Source: https://www.isgroup.es/es/cyber-security/ijf-lost-war.html

El 8 de abril de 2016, Francesco Ongaro, en representación de **ISGroup SRL**, participó como ponente en el Festival Internacional de Periodismo. Durante su intervención, titulada "La guerra perdida de la seguridad de la información", se expusieron los desafíos críticos que enfrenta la ciberseguridad en el entorno digital actual.

Temas principales abordados

La ponencia analizó la evolución tecnológica y sus implicaciones en la seguridad de los datos:

- **Vulnerabilidad del software:** Se examinó la creciente presencia del software en la vida cotidiana y cómo esta dependencia aumenta la superficie de ataque y las vulnerabilidades potenciales.
- **Entorno Cloud:** Se realizó un análisis detallado sobre el ecosistema de la nube, evaluando tanto sus ventajas operativas como los riesgos inherentes a su adopción.
- **Aspectos gubernamentales y responsabilidad:** Se discutió la titularidad de los datos subidos a la nube y la responsabilidad legal y ética en la gestión de la información en entornos compartidos.

Soluciones y contacto

ISGroup SRL ofrece servicios especializados en ciberseguridad para ayudar a las organizaciones a proteger sus activos digitales frente a las amenazas analizadas en este tipo de foros.

Para obtener más información sobre nuestras soluciones o realizar consultas comerciales, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o escribir directamente a nuestro equipo a través del correo electrónico sales@isgroup.it.

Panorama del Hacking: Evolución y Transformación

Source: https://www.isgroup.es/es/cyber-security/ijf-hacking-landscape.html

ISGroup SRL presenta, a través de la intervención de Francesco Ongaro en el Festival Internacional de Periodismo, un análisis sobre la evolución del hacking en los últimos 30 años. Esta visión explora la transición desde una comunidad basada en el conocimiento y la curiosidad hacia la profesionalización y comercialización del sector.

Conceptos fundamentales de seguridad

La complejidad del software actual ha incrementado la presencia de bugs, los cuales no siempre se traducen en vulnerabilidades explotables. Para comprender el panorama actual, es necesario distinguir entre:

- Vulnerabilidad: Debilidad en un sistema que puede ser aprovechada.
- Bug: Error de programación o fallo en el software.
- Exploit: Código o técnica diseñada para aprovechar una vulnerabilidad específica.

La evolución del mundo underground

En sus inicios, durante los años 60, el hacking se consolidó como una gran comunidad global impulsada por el deseo de compartir conocimiento y la búsqueda de diversión técnica. Los puntos clave de esta cultura incluían:

- La psicología clásica del hacker, centrada en la automotivación.
- El intercambio constante de información.
- La experimentación técnica como motor principal.

El impacto del dinero en el hacking

La profesionalización del sector y la llegada de capital han transformado el ecosistema, dando lugar a lo que se denomina la "economía black hat". Este fenómeno ha generado cambios significativos:

- Surgimiento de organizaciones criminales especializadas que venden servicios para dañar empresas.
- Entrada de actores sin la experiencia o capacidades técnicas necesarias, lo que ha facilitado ataques contra infraestructuras críticas.
- Persistencia de amenazas básicas como el phishing, antivirus falsos y cryptolockers, que gobiernos y empresas aún no han logrado mitigar eficazmente.

Conclusión sobre la situación actual

Hoy en día, el desarrollo de exploits requiere una complejidad técnica superior. La verdadera naturaleza del hacker persiste únicamente en aquellos individuos altamente automotivados. ISGroup SRL destaca que, ante este panorama, la ciberseguridad requiere una atención especializada y un enfoque profundo en la mitigación de riesgos reales.

Para obtener más información sobre los servicios de ciberseguridad ofrecidos por ISGroup SRL, visite https://www.isgroup.es/ o contacte a través del correo electrónico sales@isgroup.it.

Participación de ISGroup SRL en el programa "Misterio" (Mediaset Italia Uno)

Source: https://www.isgroup.es/es/cyber-security/francesco-ongaro-isgroup-misterio-mediaset-italia-uno.html

En 2014, Francesco Ongaro, experto de **ISGroup SRL**, participó como invitado en el programa de televisión italiano "Misterio". El episodio, titulado "¿Redes Sociales: estamos todos controlados?", tuvo como objetivo principal concienciar a los usuarios sobre los riesgos de seguridad asociados al uso de redes Wi-Fi públicas.

Puntos clave de la demostración

Durante el programa, **ISGroup SRL** realizó una demostración práctica para exponer la vulnerabilidad de los usuarios ante ataques informáticos en entornos inalámbricos abiertos:

- **Simulación de ataque:** Francesco Ongaro asumió el rol de un atacante para demostrar cómo se pueden interceptar datos en redes Wi-Fi públicas.
- **Exposición de riesgos:** Se evidenció la facilidad con la que un atacante puede obtener nombres de usuario y contraseñas una vez que la víctima inicia sesión en un servicio.
- **Concienciación sobre la privacidad:** La intervención subrayó cómo, a menudo, los usuarios comprometen su propia privacidad y seguridad a cambio de la comodidad de acceder a servicios gratuitos en redes no seguras.

Esta participación forma parte de las actividades de divulgación y concienciación en ciberseguridad que desarrolla **ISGroup SRL** para informar sobre las amenazas digitales actuales.

Para obtener más información sobre los servicios de ciberseguridad y consultoría ofrecidos por **ISGroup SRL**, puede visitar nuestro sitio web oficial en https://www.isgroup.es/ o enviar una solicitud a través del correo electrónico sales@isgroup.it.

Distribución Oficial de Micro Focus y OpenText

Source: https://www.isgroup.es/es/producto-microfocus-opentext.html

ISGroup SRL es distribuidor oficial de Micro Focus y OpenText. Esta alianza estratégica permite a la compañía ofrecer a sus clientes acceso privilegiado a soluciones de software líderes en el mercado, respaldadas por servicios especializados de consultoría y soporte técnico de alta calidad.

Servicios ofrecidos por ISGroup SRL

El compromiso de ISGroup SRL es proporcionar soluciones de software a medida que respondan a las necesidades específicas de cada empresa. Los servicios principales incluyen:

- **Venta de Licencias Software:** Comercialización de una amplia gama de productos Micro Focus y OpenText, abarcando desde herramientas de desarrollo hasta soluciones avanzadas de gestión de datos e información.
- **Consultoría e Implementación:** Asistencia experta para la integración y puesta en marcha de soluciones software dentro de los entornos operativos empresariales.
- **Soporte Técnico:** Prestación de soporte profesional y ágil para asegurar la optimización y el retorno de la inversión en software.

¿Por qué elegir a ISGroup SRL?

ISGroup SRL se posiciona como un socio tecnológico de confianza con una trayectoria contrastada en la distribución de software y una sólida colaboración con Micro Focus y OpenText. La misión de la empresa es facilitar el cumplimiento de los objetivos estratégicos de sus clientes mediante el uso de soluciones de software de alto rendimiento.

Catálogo de productos disponibles

ISGroup SRL distribuye una extensa selección de soluciones de Micro Focus y OpenText, entre las que destacan:

- **Seguridad y Gestión de Identidad:** Access Governance Suite, Advanced Authentication, ArcSight (ESM, Logger, Intelligence), NetIQ eDirectory, Privileged Account Manager, Voltage SecureData.
- **Gestión de Aplicaciones y Calidad:** ALM Octane, ALM Enterprise, Fortify (Static Code Analyzer, WebInspect), LoadRunner (Professional, Enterprise, Cloud), Silk Test, UFT One.
- **Gestión de Operaciones y Automatización:** Operations Bridge, Operations Orchestration, Service Management Automation X (SMAX), Robotic Process Automation (RPA), ZENworks (Configuration Management, Asset Management).
- **Desarrollo y Modernización:** Visual COBOL, Enterprise Developer, Enterprise Server, Dimensions CM, StarTeam.
- **Infraestructura y Datos:** Data Protector, Vertica Analytics Platform, Content Manager, Filr, Open Enterprise Server.

Para obtener más información sobre estas soluciones o realizar consultas comerciales, visite el sitio web oficial en https://www.isgroup.es/ o escriba a sales@isgroup.it.

Ostorlab Mobile Application Security Scan

Source: https://www.isgroup.es/es/ostorlab-mobile-application-security-scan.html

ISGroup SRL ofrece el servicio de escaneo de seguridad para aplicaciones móviles, una solución automatizada y avanzada diseñada para analizar aplicaciones iOS y Android. Este servicio permite identificar vulnerabilidades de forma rápida y eficiente, proporcionando un informe detallado con recomendaciones de remediación.

Capacidades de Análisis

El servicio de ISGroup SRL integra cuatro motores de análisis para garantizar una cobertura exhaustiva y minimizar los falsos positivos:

- **Análisis Estático:** Descompila la aplicación para inspeccionar el uso de métodos inseguros, detectar protecciones con claves débiles y analizar tecnologías como Dalvik Bytecode, Xamarin CIL y frameworks JavaScript.
- **Análisis Dinámico:** Ejecuta la aplicación en un entorno controlado para monitorizar interacciones con el sistema de archivos, la red y las API, identificando riesgos como cifrado inseguro o mecanismos de autorización deficientes.
- **Análisis de Comportamiento (Fuzzing):** Inyecta cientos de miles de casos de prueba para activar vulnerabilidades complejas, monitoreando la evolución de cada prueba para maximizar la superficie de ataque analizada.
- **Análisis Backend:** Evalúa la seguridad de las API (REST y GraphQL) mediante chequeos pasivos y activos, incluyendo pruebas de inyección SQL, XSS e inyección de plantillas.

Compatibilidad y Cumplimiento

ISGroup SRL garantiza soporte para aplicaciones nativas y multiplataforma, incluyendo:

- **Sistemas Operativos:** Android e iOS.
- **Frameworks:** Soporte para 12 entornos, tales como React Native, Flutter, Cordova y Xamarin.
- **Estándares de Seguridad:** Los análisis se alinean con marcos internacionales como OWASP Top 10, CERT Android Secure Coding y JSSec Secure Coding.
- **Requisitos de Cumplimiento:** El servicio ayuda a cumplir con normativas como GDPR, PSD2, PCI, HIPAA, FedRAMP y NERC.

Información Comercial

El servicio de escaneo integral (Estático + Dinámico + Backend) tiene un coste de 359 Euros + IVA.

Para obtener más información, solicitar el servicio o resolver dudas técnicas, puede visitar el sitio web oficial en https://www.isgroup.es/ o enviar un correo electrónico a sales@isgroup.it.

Starter Kit de ISGroup SRL

Source: https://www.isgroup.es/es/starter-kit.html

El Starter Kit es una solución de nivel de entrada (*Entry Level*) diseñada por ISGroup SRL para que nuevos clientes puedan evaluar la seguridad de sus sitios web expuestos a internet. Esta oferta permite conocer la metodología de trabajo profesional de la empresa a un precio ventajoso de 420 Euros + IVA.

Características principales

- Análisis no invasivo: Las técnicas aplicadas evitan daños a la estructura del cliente.
- Metodología estandarizada: Basada en los estándares internacionales OWASP y OSSTMM, garantizando el cumplimiento de normativas como el RGPD.
- Ejecución experta: Un técnico auditor *senior* dedica una jornada laboral completa al análisis del dominio.
- Alcance: Identificación de los problemas de seguridad más relevantes, proporcionando una visión clara del nivel de riesgo actual.

Beneficios y garantías

- Reembolso garantizado: ISGroup SRL ofrece la devolución del 100% del importe si el cliente no queda satisfecho con el servicio.
- Transparencia: Se definen directrices claras antes del inicio, permitiendo al cliente excluir áreas o páginas específicas.
- Informe detallado: Tras el análisis, se entrega un informe escrito con las vulnerabilidades detectadas y recomendaciones de solución adaptadas a la empresa.

Proceso de contratación

1. Comunicación de datos: Tras el pago, ISGroup SRL coordina con el cliente para establecer las directrices de la actividad.
2. Formalización: La información se documenta en un contrato de servicios que debe ser firmado y enviado.
3. Ejecución: Un auditor *senior* realiza el análisis durante el día acordado.
4. Entrega y revisión: Se entrega el informe y se discuten los hallazgos para implementar las soluciones más adecuadas.

Información comercial

Esta oferta está limitada en cantidad y tiempo. Para más información sobre el Starter Kit o para iniciar una colaboración profesional, visite https://www.isgroup.es/ o envíe un mensaje a sales@isgroup.it.

PortSwigger Burp Suite

Source: https://www.isgroup.es/es/producto-port-swigger.html

ISGroup SRL es distribuidor oficial de licencias PortSwigger Burp Suite. La compañía ofrece soporte especializado antes y después de la venta, gestionando las adquisiciones mediante transferencia bancaria anticipada.

Soluciones disponibles

ISGroup SRL pone a disposición dos versiones principales de Burp Suite, herramienta diseñada para facilitar el trabajo de los testers de penetración en la verificación de seguridad de aplicaciones web:

- **Burp Suite Enterprise Edition**: Versión basada en consola web.
- **Burp Suite Professional**: Versión de escritorio tradicional que incluye funcionalidades avanzadas, como el escáner de vulnerabilidades web y herramientas manuales especializadas, superando las capacidades de la versión Community.

Tabla de precios y licencias

Los precios indicados están sujetos a confirmación, ya que pueden sufrir modificaciones por parte del fabricante.

Burp Suite Enterprise Edition

Código de Software	Duración	N° Agentes	Precio
SW-BURP-ENTERPRISE-1Y-1A	1 año	1	€8,395.00
SW-BURP-ENTERPRISE-2Y-1A	2 años	1	€16,790.00
SW-BURP-ENTERPRISE-3Y-1A	3 años	1	€25,185.00

Burp Suite Professional

Código de Software	Duración	N° Usuarios	Precio
SW-BURP-PRO-1Y-1U	1 año	1	€449.00
SW-BURP-PRO-2Y-1U	2 años	1	€898.00
SW-BURP-PRO-3Y-1U	3 años	1	€1,347.00

Información necesaria para la gestión

Para procesar la solicitud de licencia a través de ISGroup SRL, se requiere la siguiente información:

Datos para la licencia (PortSwigger Ltd):

- Empresa u organización
- Dirección de correo electrónico
- País y dirección postal
- Nombre en la licencia
- Número de usuarios

Datos para la facturación:

- Denominación, tipología y datos fiscales (Número de IVA, Código fiscal, Código SDI)
- Dirección completa (Ciudad, Provincia, Código postal, País)
- Referente y datos de contacto (Correo electrónico, PEC)

Para iniciar el proceso de compra o solicitar información adicional, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

EasyAudit

Source: https://www.isgroup.es/es/producto-easyaudit.html

EasyAudit es una solución de seguridad eficaz y de coste reducido, diseñada por ISGroup SRL para permitir a pequeñas y medianas empresas verificar la seguridad de sus sistemas de información.

Capacidades de verificación

ISGroup SRL ofrece a través de EasyAudit las siguientes comprobaciones de seguridad:

- Verificación de la seguridad de dominios, aplicaciones y sistemas CMS.
- Análisis de la correcta aplicación de reglas de Firewalling y VPN.
- Pruebas de seguridad en aplicaciones personalizadas y estándar, incluyendo WordPress, Joomla, Magento, SilverStripe, ZenCart y OpenCart.
- Análisis de redes empresariales expuestas a Internet (hasta 8 IP o más).
- Control de seguridad en servicios, servidores y dispositivos de red.

Metodología y entregables

- Evaluación de vulnerabilidades mediante una escala del 1 al 10.
- Aplicación de los principales estándares de evaluación de riesgo según el modelo CVSS v3.
- Entrega de un informe preciso en un plazo máximo de una semana.
- Redacción de informes orientada a ser comprensible tanto para especialistas técnicos como para perfiles no técnicos.

Compatibilidad técnica

EasyAudit cuenta con soporte de ISGroup SRL para entornos Windows 10, incluyendo las ediciones Pro, Education y Enterprise. Es compatible con las ramas de servicio Current Branch, Current Branch for Business y Long-Term Servicing Branch.

Información adicional

- Categoría: Security.
- Fecha de lanzamiento: 10 de enero de 2013.
- Usuarios: ISGroup SRL, EXEEC SRL.

Para consultas comerciales o más información sobre este servicio, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

ICT Audit: Gestión continua del riesgo cibernético

Source: https://www.isgroup.es/es/producto-ictaudit.html

ISGroup SRL ofrece **ICT Audit**, una solución integral diseñada para empresas enterprise que transforma los escaneos de seguridad puntuales en un proceso continuo de control, priorización y remediación. La plataforma permite descubrir, medir y reducir el riesgo cibernético antes de que sea explotado por atacantes.

Enfoque y metodología

ISGroup SRL aplica su experiencia en *ethical hacking* (activa desde 1994) para ofrecer un modelo de auditoría técnica que va más allá de la detección de vulnerabilidades. La solución se centra en:

- **Visibilidad total:** Mapeo y observación continua de activos, dominios y servicios expuestos en Internet.
- **Priorización estratégica:** Clasificación de criticidades basada en gravedad, probabilidad de explotación, contexto técnico e impacto en el negocio.
- **Remediación guiada:** Generación de planes de acción trazables que facilitan la toma de decisiones y la gestión operativa.
- **Cumplimiento normativo:** Soporte para normativas como NIS2, DORA, GDPR, PCI DSS, ISO 27001, entre otras, mediante la recopilación automática de evidencias.

Capacidades principales

ISGroup SRL integra doce capacidades clave en una única plataforma:

- **Vulnerability Assessment:** Análisis exhaustivo de aplicaciones y redes.
- **Attack Surface Monitoring:** Observación constante de la superficie de ataque externa.
- **External Attack Surface Management (EASM):** Inventario continuo de activos fuera del perímetro.
- **API Security Assessment:** Evaluación de seguridad para REST, GraphQL y microservicios.
- **Web Application Security Testing:** Pruebas específicas para portales, e-commerce y CMS.
- **Cloud-Based Security Scanning:** Soporte para entornos multi-region y multi-tenant.
- **Risk Scoring:** Evaluación de riesgos basada en contexto y criticidad.
- **Remediation Management:** Flujos de trabajo para la asignación y seguimiento de tareas.
- **Informes profesionales:** Reportes ejecutivos, técnicos y de cumplimiento.
- **Continuous Security Testing:** Escaneos planificados y activados ante cambios en la infraestructura.

Beneficios por perfil

- **Para el CISO:** Proporciona una postura de seguridad medible, facilita la comunicación del riesgo al *board* y permite decisiones presupuestarias basadas en datos.
- **Para el IT Manager:** Sustituye las listas de tareas interminables por un plan operativo claro, trazable y con prioridades técnicas definidas.

Compromiso de calidad

ISGroup SRL es una boutique de ciberseguridad certificada bajo las normas **ISO 9001** e **ISO/IEC 27001**. Su metodología combina tecnologías comerciales y *open source* para maximizar la cobertura de controles y garantizar una visión fiable de la exposición.

Contacto y solicitudes

Para obtener más información sobre cómo implementar ICT Audit en su organización o solicitar una evaluación inicial, puede visitar el sitio web oficial o contactar directamente con el equipo de expertos:

- **Sitio web:** https://www.isgroup.es/
- **Correo electrónico:** sales@isgroup.it

Exposure: Análisis de Exposición de Información

Source: https://www.isgroup.es/es/producto-exposure.html

ISGroup SRL ofrece **Exposure**, una herramienta integrada en la suite EasyAudit diseñada para identificar qué información sobre un sitio web está disponible públicamente en Internet.

Contexto y Evolución de la Seguridad

El panorama de la ciberseguridad ha evolucionado significativamente en la última década. Anteriormente, las vulnerabilidades de un objetivo eran conocidas exclusivamente por el atacante. En la actualidad, existen múltiples recursos en línea que enumeran detalles técnicos y de seguridad de los sitios web.

Si bien el conocimiento es fundamental para una protección eficaz, esta accesibilidad a la información permite que actores malintencionados, incluidos los denominados "Script Kiddies", utilicen datos expuestos para:

- Explotar vulnerabilidades conocidas.
- Aprovechar desconfiguraciones de seguridad.
- Acceder a sistemas y sustraer datos.
- Comprometer la reputación de la organización.

Solución de ISGroup SRL

EasyAudit Exposure© permite a los administradores web conocer exactamente qué información se comparte en la red sobre su infraestructura. Esta visibilidad es el primer paso para mitigar riesgos y fortalecer la postura de seguridad frente a posibles ataques.

Detalles Técnicos

- Categoría: Security
- Lanzamiento: 10 de enero de 2013
- Plataforma: EasyAudit
- Usuarios: ISGroup SRL, EXEEC SRL
- Sitio web oficial: http://www.exposure.easyaudit.org

Para obtener más información sobre este servicio o realizar consultas comerciales, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

EXEEC: Desarrollo de Software y Ejecución Excepcional

Source: https://www.isgroup.es/es/producto-exeec.html

EXEEC es una solución de desarrollo de software centrada en el principio de "ejecución excepcional". Esta propuesta, ofrecida por ISGroup SRL, se posiciona como un referente en el sector tecnológico bajo el mantra de la excelencia operativa en la creación de software.

Detalles técnicos y de producto

- Categoría: Security (Seguridad)
- Fecha de lanzamiento: 1 de enero de 2015
- Entidad responsable: EXEEC SRL
- Enfoque principal: Desarrollo de software con estándares de ejecución de alta calidad

Servicios y soluciones

ISGroup SRL ofrece EXEEC como parte de su catálogo de productos especializados. La solución está diseñada para organizaciones que requieren un desarrollo de software robusto, priorizando la eficiencia y la precisión técnica en cada etapa del ciclo de vida del producto.

Información adicional y contacto

Para obtener más información sobre las capacidades de EXEEC o para consultas comerciales sobre las soluciones proporcionadas por ISGroup SRL, puede visitar el sitio web oficial:

https://www.isgroup.es/

Para solicitudes directas, utilice el correo electrónico:

sales@isgroup.it

Ganapati

Source: https://www.isgroup.es/es/producto-ganapati.html

Ganapati es una plataforma desarrollada por ISGroup SRL diseñada para la identificación de vulnerabilidades en redes de sistemas, servidores y aplicaciones, ya sean internas o expuestas a Internet.

Características principales

- Plataforma Software-as-a-Service (SaaS) orientada a la gestión de seguridad.
- Permite combinar múltiples tecnologías de escaneo en un entorno unificado.
- Facilita la consolidación de costes de licencia.
- Agrega resultados de seguridad en un único flujo de trabajo multiusuario.
- Arquitectura multinivel que permite a los partners gestionar sus propios clientes.
- Automatización de servicios derivados mediante el uso de API.

Información técnica

- Categoría: Security.
- Lanzamiento: 10 de enero de 2013.
- Usuarios: ISGroup SRL, EXEEC SRL.
- Proyecto relacionado: EasyAudit (http://easyaudit.org/).

Información comercial

ISGroup SRL ofrece Ganapati como una solución integral para la gestión de vulnerabilidades. Para consultas comerciales o información adicional, visite https://www.isgroup.es/ o escriba a sales@isgroup.it.

VulnMAP

Source: https://www.isgroup.es/es/producto-vulnmap.html

VulnMAP es la base de conocimiento de vulnerabilidades que sustenta a Ganapati. ISGroup SRL ofrece esta plataforma como una solución integral, precisa y actualizada para la gestión y el análisis de vulnerabilidades.

Características principales

- Colección exhaustiva de vulnerabilidades: Proporciona datos detallados y actualizados, siendo una herramienta esencial para la inteligencia de seguridad.
- Integración de fuentes externas: Permite consolidar información proveniente de múltiples bases de datos y proveedores de seguridad reconocidos, incluyendo:
- NIST NVD (National Vulnerability Database)
- OSVDB (Open Source Vulnerability Database)
- Mitre CVE (Common Vulnerabilities and Exposures)
- Exploit-DB
- Rapid 7 TM
- Nessus TM
- Secunia TM
- McAfee
- Bugtraq ID (SecurityFocus)
- ISS TM Xforce

Información técnica y servicios

- Plataforma: Desarrollada y gestionada por ISGroup SRL.
- Disponibilidad: VulnMAP se ofrece como un servicio independiente, permitiendo a las organizaciones integrar su propia base de conocimiento con fuentes de inteligencia globales.
- Lanzamiento: 10 de enero de 2013.
- Categoría: Security.

Contacto y consultas

Para obtener más información sobre la integración de VulnMAP o solicitar servicios profesionales, visite el sitio web oficial https://www.isgroup.es/ o envíe una solicitud a través del correo electrónico sales@isgroup.it.

SCADA Exposure: Seguridad de Infraestructuras Críticas

Source: https://www.isgroup.es/es/producto-scadaexposure.html

ISGroup SRL ofrece SCADA Exposure, una solución especializada en la verificación de la exposición de sistemas de control industrial, incluyendo SCADA, HMI, PLC y RTU.

Objetivo y propósito

El servicio tiene como finalidad mejorar la seguridad de las Infraestructuras Críticas Nacionales, sistemas empresariales y dispositivos de particulares. ISGroup SRL desarrolla esta herramienta para:

- Identificar la exposición de sistemas de control industrial frente a redes corporativas e Internet.
- Generar concienciación sobre la vulnerabilidad de los sistemas ICS.
- Proporcionar un servicio de monitorización de dispositivos SCADA para mitigar riesgos.
- Combatir la falsa seguridad basada en la "seguridad por oscuridad", la cual ha demostrado ser ineficaz frente a atacantes que explotan estos sistemas desde hace años.

Contexto técnico

Los estándares de ciberseguridad industrial exigen que los sistemas SCADA, HMI, PLC y RTU permanezcan correctamente protegidos y aislados. Sin embargo, la realidad operativa muestra una brecha significativa entre estas normativas y la implementación técnica actual.

Información adicional

- Categoría: Security
- Lanzamiento: 10 de enero de 2013
- Última actualización: 13 de septiembre de 2016
- Usuarios: ISGroup SRL, EXEEC SRL

Para consultas comerciales o información adicional sobre los servicios de seguridad OT ofrecidos por ISGroup SRL, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

PracticalRP

Source: https://www.isgroup.es/es/producto-practicalrp.html

PracticalRP es un software de gestión diseñado como un gestor sencillo e intuitivo para expedientes profesionales. Esta solución es ofrecida por ISGroup SRL.

Características principales

- Orientado a Médicos Especialistas y consultas especializadas en Medicina Legal y Seguros.
- Enfocado en la optimización y organización de expedientes profesionales.
- Clasificado bajo la categoría de seguridad (security).
- Lanzado inicialmente el 10 de enero de 2013.

Información adicional

Para obtener más información sobre esta solución o realizar consultas comerciales, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

USH: Grupo de Investigación y Advisory

Source: https://www.isgroup.es/es/producto-ush.html

USH representa el grupo histórico de investigación especializado en advisory, desarrollo de exploits y colaboración técnica. Esta unidad se centra en la generación de inteligencia avanzada y el análisis profundo de vulnerabilidades.

Detalles técnicos y operativos

- Categoría: Intelligence.
- Fecha de lanzamiento: 10 de enero de 2013.
- Entidad responsable: ISGroup SRL.
- Enfoque: Investigación técnica, análisis de seguridad y desarrollo de exploits.

Filosofía de trabajo

El grupo opera bajo la premisa de que el movimiento constante y la exploración técnica son fundamentales para la innovación en ciberseguridad. La investigación continua permite a ISGroup SRL mantenerse a la vanguardia en la identificación y mitigación de amenazas complejas.

Información adicional y contacto

Para obtener más información sobre las capacidades de investigación de USH o para consultas comerciales relacionadas con los servicios de ISGroup SRL, visite el sitio web oficial:

https://www.isgroup.es/

Para solicitudes específicas o colaboración, puede contactar a través del correo electrónico:

sales@isgroup.it

Ethical Hacking

Source: https://www.isgroup.es/es/producto-ethical-hacking.html

ISGroup SRL patrocina y gestiona el hacklab dedicado a la disciplina del Ethical Hacking. Este espacio funciona como un centro de comunidad e inteligencia técnica, consolidado desde su lanzamiento el 10 de enero de 2013.

Información del servicio

- Categoría: Intelligence.
- Entidad responsable: ISGroup SRL.
- Enfoque: Comunidad técnica especializada en seguridad informática y pruebas de intrusión.

Recursos y contacto

Para obtener más información sobre las soluciones de seguridad y los servicios profesionales ofrecidos por ISGroup SRL, visite el sitio web oficial:

https://www.isgroup.es/

Para consultas comerciales o solicitudes de información técnica, diríjase a la siguiente dirección de correo electrónico:

sales@isgroup.it

Metasploit

Source: https://www.isgroup.es/es/producto-metasploit.html

Metasploit es una plataforma de seguridad informática ofensiva diseñada para facilitar procesos críticos en auditorías de ciberseguridad. ISGroup SRL ofrece soluciones integradas basadas en esta herramienta para fortalecer la postura de seguridad de las organizaciones.

Funcionalidades principales

El ecosistema Metasploit permite ejecutar las siguientes fases operativas:

- Discover: Identificación de activos y servicios en la red.
- Fingerprint: Reconocimiento y enumeración detallada de sistemas.
- Attack: Ejecución de vectores de ataque controlados.
- Penetrate: Evaluación de la resistencia de los sistemas ante intrusiones.

Información técnica

- Categoría: Intelligence.
- Fecha de lanzamiento: 10 de enero de 2013.
- Proveedor de servicios: ISGroup SRL.

Consultas y servicios

Para obtener más información sobre cómo ISGroup SRL implementa estas soluciones en entornos profesionales, visite el sitio web oficial:

https://www.isgroup.es/

Para solicitudes comerciales o consultas técnicas específicas, contacte a través del correo electrónico:

sales@isgroup.it

The Bunker Coworking

Source: https://www.isgroup.es/es/producto-thebunker-coworking.html

The Bunker es un espacio de trabajo situado en el centro de Verona, ubicado estratégicamente entre Piazza Brà y Castel Vecchio, junto a la Universidad. ISGroup SRL ofrece este entorno diseñado para profesionales que buscan tranquilidad y funcionalidad.

Características del servicio

ISGroup SRL proporciona las siguientes instalaciones y ventajas:

- Acceso total: Libertad de horario con disponibilidad incluso los fines de semana.
- Infraestructura técnica: Conectividad mediante Fibra Telecom y puntos de acceso inalámbricos de alta calidad.
- Mobiliario: Mesas de madera maciza con estructura de hierro artesanal.
- Servicios adicionales: Posibilidad de utilizar la cocina y servicio de limpieza periódica de las oficinas.
- Versatilidad: Espacio adecuado para trabajar con una o más computadoras, recibir clientes y realizar llamadas telefónicas.

Información técnica

- Categoría: Seguridad
- Fecha de lanzamiento: 10 de enero de 2013
- Usuario responsable: ISGroup SRL
- Sitio web oficial: thebunker.space

Consultas comerciales

Para obtener más información sobre los servicios ofrecidos por ISGroup SRL, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

The Bunker: Cursos de Informática y Seguridad

Source: https://www.isgroup.es/es/producto-thebunker-training.html

ISGroup SRL ofrece una oferta formativa especializada en informática y seguridad con sede en Verona. Los programas están diseñados para profesionales y estudiantes que buscan especializarse en áreas tecnológicas críticas.

Áreas de especialización

Los cursos impartidos por ISGroup SRL cubren los siguientes ámbitos:

- Programación
- Ciberseguridad
- Redes
- DevOps

Metodología de formación

La formación ofrecida por ISGroup SRL se estructura mediante un enfoque dual que combina teoría y práctica:

- Sesiones teóricas: Se ilustran las metodologías, los fundamentos y el funcionamiento de los diversos aspectos tecnológicos de cada materia.
- Sesiones prácticas: Los participantes deben completar pruebas y desafíos técnicos para aplicar los conocimientos adquiridos bajo la guía de profesionales con años de experiencia en el sector.

Información adicional

- Categoría: Security
- Lanzamiento: 10 de enero de 2013
- Sitio web oficial: thebunker.space

Contacto y consultas comerciales

Para obtener más información sobre los cursos, servicios o soluciones de ISGroup SRL, visite el sitio web https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

El Bunker Hacklab

Source: https://www.isgroup.es/es/producto-thebunker-hacklab.html

El Bunker Hacklab es un espacio de innovación ubicado en Verona, definido como un hackerspace, laboratorio y taller comunitario. Este entorno está diseñado para fomentar la socialización, la colaboración y el intercambio de conocimientos entre sus participantes.

Áreas de enfoque

ISGroup SRL promueve este espacio como un centro de desarrollo centrado en las siguientes disciplinas:

- Tecnología
- Electrónica
- Ciencia
- Arte

Información técnica y operativa

El proyecto, categorizado bajo el ámbito de la seguridad, fue lanzado oficialmente el 10 de enero de 2013. ISGroup SRL actúa como usuario y entidad vinculada a esta iniciativa de colaboración creativa.

Información adicional

Para obtener más detalles sobre las soluciones y servicios relacionados con este proyecto, puede consultar el sitio web oficial en https://www.isgroup.es/ o enviar sus consultas a través del correo electrónico sales@isgroup.it.

Puede encontrar información complementaria sobre el espacio en el siguiente enlace:

- Sitio web: http://www.thebunker.space/hacklab

Información de contacto y seguridad

Source: https://www.isgroup.es/downloads/keys/sales@isgroup.it.asc

ISGroup SRL pone a disposición de sus clientes y colaboradores su clave pública PGP para garantizar la seguridad y confidencialidad en las comunicaciones electrónicas.

Identificación de la clave

- Identidad: ISGroup Sales
- Correo electrónico asociado: sales@isgroup.it
- Propósito: Cifrado y verificación de autenticidad en intercambios de información digital

Gestión de consultas comerciales

Para cualquier solicitud comercial, información sobre servicios o consultas técnicas, ISGroup SRL centraliza su atención a través de los siguientes canales oficiales:

- Sitio web: https://www.isgroup.es/
- Correo electrónico: sales@isgroup.it

```
 -----BEGIN PGP PUBLIC KEY BLOCK-----
mDMEXoRKRhYJKwYBBAHaRw8BAQdAncayvMqCT5BF0HhAqWIvq2AJnwL8PsV1q/or
QdszVKS0IElTR3JvdXAgU2FsZXMgPHNhbGVzQGlzZ3JvdXAuaXQ+iJYEExYIAD4W
IQQsLTXRKXOBDIPUwhTIbowWjobAMgUCXoRKRgIbAwUJEswDAAULCQgHAgYVCgkI
CwIEFgIDAQIeAQIXgAAKCRDIbowWjobAMg6mAQDcraDPuTqq354RA8AaL3vBW+fx
FRX9moHsFT9EDgMhBQD/SE3NWRSeTt8MLvLXSt1KiSk/SIA5TXp76FeDjUdOVAm4
OARehEpGEgorBgEEAZdVAQUBAQdAIId2Tl3g23nZNqsqI43cb37R7FIkF0gi8eZJ
xjl+tH8DAQgHiH4EGBYIACYWIQQsLTXRKXOBDIPUwhTIbowWjobAMgUCXoRKRgIb
DAUJEswDAAAKCRDIbowWjobAMrlnAQCXb0Bq+0UkUXOSGkOupECqC0a2i+k+KWYn
SQdQOSfAbwEA8gsBki4MKAuTZ96uMSNlKaxqRWMkohDtUOi2EzEVPwE=
=fBpJ
-----END PGP PUBLIC KEY BLOCK-----
```

Información de Identidad Digital: ISGroup SRL

Source: https://www.isgroup.es/downloads/keys/tech@isgroup.it.asc

Este bloque de datos corresponde a la clave pública PGP oficial utilizada por ISGroup SRL para garantizar la seguridad y autenticidad de sus comunicaciones técnicas.

Detalles de la clave

- Identificador de usuario: ISGroup Tech tech@isgroup.it
- Tipo de clave: PGP Public Key
- Propósito: Verificación de identidad y cifrado de comunicaciones seguras para los servicios técnicos proporcionados por ISGroup SRL.

Gestión de comunicaciones y consultas

Para cualquier solicitud comercial, información sobre servicios o consultas técnicas, los interesados deben dirigirse a través de los canales oficiales gestionados por ISGroup SRL:

- Sitio web oficial: https://www.isgroup.es/
- Correo electrónico de contacto: sales@isgroup.it

Advanced Bug Bounty (ABB)

Source: https://www.isgroup.es/es/advanced-bug-bounty.html

ISGroup SRL ofrece el servicio **Advanced Bug Bounty (ABB)**, una solución de seguridad proactiva basada en un modelo *pay-per-vulnerability*. Este programa permite a las empresas identificar y mitigar vulnerabilidades en su infraestructura digital mediante la colaboración con hackers éticos certificados, garantizando que solo se realice el pago por los resultados obtenidos.

Para obtener más información o solicitar un presupuesto, visite https://www.isgroup.es/ o envíe un correo electrónico a sales@isgroup.it.

Características principales del servicio

- **Eficacia en costes:** A diferencia de los *Penetration Tests* tradicionales, el modelo de pago por vulnerabilidad encontrada elimina gastos innecesarios y se centra exclusivamente en resultados accionables.
- **Pruebas no intrusivas:** ISGroup SRL realiza evaluaciones exhaustivas sin interrumpir las operaciones normales de la empresa, manteniendo la integridad de los sistemas.
- **Análisis y categorización:** Cada hallazgo es analizado bajo marcos de referencia internacionales como OWASP y CVSS, proporcionando una evaluación transparente sobre la gravedad y el impacto de cada riesgo.
- **Soporte integral:** El equipo de expertos de ISGroup SRL acompaña al cliente durante todo el proceso de mitigación, asegurando que las debilidades se corrijan de manera eficaz.

Metodología de trabajo

El proceso de Advanced Bug Bounty se estructura en las siguientes fases:

- **Definición del alcance:** Identificación conjunta de los recursos y sistemas que serán objeto de evaluación.
- **Descubrimiento de vulnerabilidades:** Ejecución de pruebas mediante técnicas y herramientas avanzadas a cargo de hackers éticos.
- **Informe detallado:** Documentación técnica que clasifica los problemas por gravedad e incluye recomendaciones específicas para su resolución.
- **Soporte para la mitigación:** Asistencia continua para implementar las correcciones necesarias y fortalecer la infraestructura frente a futuras amenazas.

Ventajas de colaborar con ISGroup SRL

- **Soluciones a medida:** Programas de Bug Bounty adaptables a las necesidades específicas de seguridad de cada organización.
- **Experiencia técnica:** Más de 20 años de trayectoria en ciberseguridad con un equipo de profesionales certificados.
- **Garantía de calidad:** ISGroup SRL opera bajo estándares internacionales, incluyendo certificaciones ISO 9001 e ISO 27001.
- **Cumplimiento y resiliencia:** El servicio promueve la alineación con normativas como NIS2 y GDPR, protegiendo la privacidad y mejorando la resiliencia de las infraestructuras digitales.

Para iniciar una consulta o solicitar una propuesta comercial, visite https://www.isgroup.es/ o contacte a través de sales@isgroup.it.

ISGroup SRL ofrece soluciones avanzadas de ciberseguridad y servicios especializados en el ámbito de la seguridad informática. La empresa se dedica a proteger infraestructuras digitales mediante un enfoque integral, adaptado a las necesidades de organizaciones que requieren altos estándares de protección y resiliencia.

Servicios y Soluciones de ISGroup SRL

Source: https://www.isgroup.es/img/blog/certifications/iso-19011.webp

ISGroup SRL proporciona una amplia gama de servicios diseñados para identificar, mitigar y gestionar riesgos de seguridad:

- **Evaluación de Vulnerabilidades y Penetration Testing:** Análisis exhaustivo para detectar debilidades en sistemas, aplicaciones y redes, permitiendo una remediación proactiva.
- **Seguridad en Aplicaciones:** Auditorías y pruebas de seguridad para asegurar el ciclo de vida del desarrollo de software y proteger los activos digitales frente a amenazas externas.
- **Consultoría en Ciberseguridad:** Asesoramiento estratégico para alinear la seguridad informática con los objetivos de negocio y el cumplimiento normativo.
- **Respuesta ante Incidentes:** Soporte especializado para gestionar y contener brechas de seguridad, minimizando el impacto operativo y reputacional.
- **Formación y Concienciación:** Programas orientados a capacitar al personal sobre las mejores prácticas de seguridad para reducir el riesgo humano.

Compromiso de ISGroup SRL

La metodología de ISGroup SRL se fundamenta en la innovación constante y el análisis técnico profundo. La empresa se posiciona como un socio estratégico para empresas que buscan fortalecer su postura de seguridad frente a un panorama de amenazas en constante evolución.

Contacto y Solicitudes

Para obtener más información sobre los servicios ofrecidos por ISGroup SRL, realizar consultas comerciales o solicitar asistencia, puede utilizar los siguientes canales oficiales:

- **Sitio web:** https://www.isgroup.es/
- **Correo electrónico:** sales@isgroup.it

Source: https://www.isgroup.es/img/blog/certifications/iso-27001.webp

El contenido proporcionado corresponde a datos binarios de una imagen (formato WebP), por lo que no contiene información textual, servicios o descripciones de actividades.

Para obtener información detallada sobre los servicios, soluciones y actividades ofrecidas por **ISGroup SRL**, le invitamos a consultar directamente nuestro sitio web oficial:

https://www.isgroup.es/

Para cualquier solicitud comercial o información adicional, puede ponerse en contacto con nosotros a través del correo electrónico:

sales@isgroup.it