https://www.isgroup.it Knowledge Base

Table of Contents

- Firewall as a Service (FWaaS)
- Software Assurance Lifecycle (SAL)
- Security Integration (SIR)
- Simulazioni di Phishing: Formazione e Difesa con ISGroup SRL
- MDR - Multi-Signal MDR di ISGroup
- ISO 27001 Compliance: Protezione dei dati e sistemi di gestione della sicurezza
- Servizio Virtual CISO di ISGroup SRL
- Social Engineering: l'arte di manipolare le persone per ottenere informazioni
- Cyber Threat Simulation (CTS)
- AGID e Sviluppo Sicuro con ISGroup: Linee Guida per il Codice Sicuro
- Case Study: Web Application Penetration Test e Supporto ISMS per Creactives S.p.A.
- Digital Forensics and Incident Response (DFIR) di ISGroup SRL
- Continuous Security Testing di ISGroup
- Secure Architecture Review di ISGroup SRL
- Cloud Security Assessment di ISGroup SRL
- Case Study: Web Application Penetration Test su DocEasy
- Purple Team Assessment di ISGroup SRL
- Difesa della Rete Aziendale: Network Penetration Test
- Firewall as a Service (FWaaS) di ISGroup SRL
- Penetration Test - Globaleaks
- Software Assurance Lifecycle con ISGroup SRL
- Corso Security Awareness di ISGroup SRL
- Security Integration con ISGroup
- Web Application Penetration Testing con ISGroup
- Il Codice Segreto: Code Review di ISGroup
- Wireless Security Monitoring di ISGroup
- Case Study: Web Application Penetration Test su Sturnis365
- Anti-DDoS: Protezione senza interruzioni operative
- Case Study: Web Application Penetration Test e Network Penetration Test per Coop Italia
- Risk Assessment di ISGroup SRL
- Mobile Application Security Test di ISGroup
- Windows Security Assessment di ISGroup
- IoT Security Assessment
- OWASP Top Ten 2021 - A06: Vulnerable and Outdated Components
- Educazione alla Sicurezza: Formazione ISGroup per il tuo Team
- OWASP Top Ten 2021 - A03 Injection
- OWASP Top Ten 2021 - A02: Cryptographic Failures
- OWASP Top Ten 2021 - A01: Broken Access Control
- OWASP Top Ten 2021 - A04: Insecure Design
- OWASP Top Ten 2021 - A08 Software and Data Integrity Failures
- OWASP Top Ten 2021: A05 Security Misconfiguration
- OWASP Top Ten 2021 - A07: Identification and Authentication Failures
- OWASP Top Ten 2021 - A09: Security Logging and Monitoring Failures
- Case Study: Web Application Penetration Test su TSV8 (Add Value S.r.l.)
- OWASP Top Ten 2021: A10 Server-Side Request Forgery (SSRF)
- OWASP Top Ten 2021
- Vulnerability Assessment di ISGroup SRL
- Certificazione Ethical Hacking: Vulnerability Analysis
- Certified Ethical Hacking: Scanning Networks

- Certificazione Ethical Hacking: Footprinting and Reconnaissance
- Certificazione Ethical Hacking: Wireless Networks
- Certificazione: Ethical Hacking - Introduction to Ethical Hacking
- Certificazione Ethical Hacking: System Hacking
- Sempre Connessi all'Innovazione - Edizione 2023
- ISGroup nel catalogo di aziende di Cyber Security Intelligence
- DEF CON 31
- Case Study: Web Application Penetration Test su eALBO (ISWEB S.p.A.)
- La transizione della qualificazione Cloud PA verso ACN
- Case Study: Network Penetration Test su Infrastruttura IT di Prime Service S.r.l.
- Minacce informatiche basate sull'Intelligenza Artificiale
- Certificazione Certified Ethical Hacker (CEH) - Francesco Ongaro
- Seminari INCONTRA: Sicurezza Informatica nel mondo reale
- Certificazione Certified Ethical Hacker (CEH) - Pasquale Fiorillo
- Incontro “Best practices per una cyber defense proattiva”
- Adozione di soluzioni XDR per la protezione dei dati
- Incontro “Dall’antivirus all’EDR e alle soluzioni MDR”
- Cyber Resilienza: Oltre la Cybersecurity Tradizionale
- Secure Smart Working: Lavorare in modo agile in sicurezza
- Certificazione PenTera Certified Sales Specialist
- Regolamento eIDAS
- Certificazione PenTera Certified Attack Specialist - Pasquale Fiorillo
- Certificazione PenTera Certified Attack Specialist
- Certificazione PenTera Certified Sales Specialist
- Qualificazione SaaS AgID
- Accreditamento Conservatori AgID
- Integrazione SPID per Fornitori di Servizi
- AGID Cloud per la Pubblica Amministrazione
- Qualificazione CSP AgID
- Certificazione UNI EN ISO 9001:2015
- Misure minime di sicurezza ICT per le Pubbliche Amministrazioni
- Data Protection Officer (DPO)
- Certificazione UNI CEI EN ISO/IEC 27001:2013
- Privacy Specialist
- Lead Auditor 19011
- Lead Auditor 27001
- Privacy Manager
- Classificazione degli incidenti
- Cos'è il Purple Team
- Red Team Cybersecurity
- Classificazione per Target
- Blue Team nella Cybersecurity
- Fasi di un Penetration Test
- Metodologie e Framework di Penetration Testing
- OWASP Top Ten 2017 - A8 Insecure Deserialization
- Rapporto Clusit
- OWASP Top Ten 2017 - A5 Broken Access Control
- OWASP Top Ten 2017 - A6: Security Misconfiguration
- Cybersecurity e Dispositivi
- OWASP Top Ten 2017 - A4 XML External Entities (XXE)

- OWASP Top 10 2017
- OWASP Top Ten 2017 - A3: Sensitive Data Exposure
- OWASP Top Ten 2017 - A2 Broken Authentication
- OWASP Top Ten 2017 - A7 Cross-Site Scripting (XSS)
- OWASP Top Ten 2017 - A9: Utilizzo di componenti con vulnerabilità note
- Tipologie di telelavoro
- OWASP Top Ten 2017 - A1 Injection
- Certificazione Acunetix User Test - Francesco Ongaro
- OWASP Top Ten 2017 - A10: Insufficient Logging & Monitoring
- Certificazione ISO/IEC 17025 - ISGroup SRL
- Studiare, fare ricerca e lavorare nella Sicurezza Informatica
- International Journalism Festival: The Lost War on Information Security
- International Journalism Festival: Hacking Landscape
- La nuova normativa europea e la gestione della vulnerabilità aziendale
- Starter Kit di Sicurezza Informatica
- Servizi offerti da ISGroup SRL
- ISGroup: Partecipazione alla trasmissione televisiva "Mistero"
- Mobile Application Security Scan
- EasyAudit
- ICT Audit
- EXEEC
- Distributore ufficiale PortSwigger Burp Suite
- Exposure
- Ganapati
- SCADA Exposure
- VulnMAP
- USH (Underground Security Hub)
- PracticalRP
- Ethical Hacking
- Metasploit
- The Bunker Corsi
- Network Penetration Testing
- The Bunker Coworking
- The Bunker Hacklab
- Chiave Pubblica PGP - ISGroup SRL
- Chiave Pubblica PGP ISGroup SRL
- ISGroup Information Security

Profilo Aziendale: ISGroup SRL

Source: https://www.isgroup.it

ISGroup SRL è una struttura indipendente specializzata in IT Security, che offre servizi e prodotti di sicurezza informatica di elevata qualità. L'azienda nasce dall'iniziativa di un gruppo di ricercatori esperti, motivati a fornire soluzioni personalizzate per operatori ICT e agenzie di sicurezza. La struttura opera con standard qualitativi elevati, collaborando attivamente con la comunità dei ricercatori indipendenti.

Competenze e Ambito Operativo

Le competenze di ISGroup SRL coprono un ampio spettro della sicurezza informatica:

- Sicurezza fisica e delle infrastrutture
- Sistemi operativi e reti
- Applicazioni web e "lato client"
- Governance, Risk e Compliance (GRC)
- Servizi di Secure Software Development Life Cycle (SSDLC)

Servizi Offerti da ISGroup SRL

ISGroup SRL fornisce un portafoglio completo di servizi offensivi e difensivi:

- **Vulnerability Assessment (VA):** Analisi e valutazione della sicurezza dei sistemi per rilevare vulnerabilità note.
- **Network Penetration Testing (NPT):** Identificazione delle vulnerabilità nei sistemi di rete.
- **Web Application Penetration Testing (WAPT):** Servizi di sicurezza applicativa per testare la resilienza delle applicazioni web.
- **Mobile Application Security Testing (MAST):** Test di sicurezza specifici per applicazioni mobile.
- **Ethical Hacking:** Simulazione di attacchi reali (interni o esterni) che includono test sul fattore umano, spesso considerato l'anello debole dei sistemi.
- **Code Review:** Analisi del codice sorgente per identificare vulnerabilità durante il ciclo di sviluppo.
- **Formazione (EDU):** Programmi di formazione per staff tecnico, sistemisti e sviluppatori per ridurre i rischi legati alla sicurezza.

Certificazioni e Riconoscimenti

ISGroup SRL è un'azienda certificata ISO/IEC 27001, a testimonianza dell'impegno verso standard internazionali di gestione della sicurezza delle informazioni. L'azienda vanta inoltre numerose collaborazioni strategiche e case study documentati con partner nazionali e internazionali.

Contatti e Informazioni Commerciali

Per ulteriori dettagli sui servizi, richieste di preventivo o informazioni istituzionali, è possibile consultare il sito ufficiale o scrivere all'indirizzo email dedicato:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

ISGroup SRL offre un'ampia gamma di servizi di sicurezza informatica gestiti, progettati per ridurre il carico operativo del management e dei team tecnici, permettendo loro di concentrarsi sul core-business.

Per informazioni commerciali o richieste, visitare il sito https://www.isgroup.it/ o scrivere all'email sales@isgroup.it.

Servizi Gestiti

Source: https://www.isgroup.it/it/servizi.html

- **vCISO (Virtual CISO):** Valutazione continua della Cyber Security basata sul framework NIST e creazione di piani strategici.
- **VMS (Vulnerability Management Service):** Identificazione e gestione delle vulnerabilità con supporto all'implementazione delle soluzioni.
- **CTS (Cyber Threat Simulation):** Simulazioni realistiche per testare la resilienza aziendale.
- **THREAT (Threat Intelligence & Digital Risk Protection):** Monitoraggio costante delle minacce digitali e misure proattive.
- **SOC (Security Operation Center):** Monitoraggio di reti e data center per prevenire e mitigare tentativi di intrusione.

Servizi Offensivi

- **NPT (Network Penetration Testing):** Verifica manuale dell'infrastruttura IT tramite simulazione di attacchi (metodologie OSSTMM e OWASP).
- **WAPT (Web Application Penetration Testing):** Analisi manuale della sicurezza delle applicazioni web.
- **MAST (Mobile Application Security Testing):** Simulazione di attacchi su applicazioni mobile (AppStore/PlayStore o interne).
- **EH (Ethical Hacking):** Analisi completa (infrastruttura, procedure, risorse umane, sicurezza fisica) tramite un Tiger Team.

Servizi Difensivi

- **VA (Vulnerability Assessment):** Audit non invasivi, manuali e automatizzati, per individuare vulnerabilità conosciute.
- **CR (Code Review):** Analisi White Box del codice sorgente per individuare vulnerabilità e 'bad practices'.
- **TRA (Formazione):** Percorsi di aggiornamento per amministratori, sistemisti, sviluppatori e penetration tester.

Servizi di Security Assessment

- **RA (Risk Assessment):** Analisi dei rischi aziendali e implementazione di misure di sicurezza.
- **SAR (Secure Architecture Review):** Valutazione della sicurezza su architetture complesse e applicativi.
- **CSA (Cloud Security Assessment):** Verifica della sicurezza su infrastrutture AWS, Azure, Google Cloud, private e ibride.
- **WSA (Windows Security Assessment):** Analisi dell'integrità e delle superfici di attacco dei sistemi Windows.
- **ISA (IoT Security Assessment):** Verifica di dispositivi e infrastrutture IoT (Hardware, Software e design).
- **PTA (Purple Team Assessment):** Valutazione basata sulla risposta del team difensivo a tentativi di attacco.
- **PHISH (Phishing & Smishing):** Campagne di simulazione e formazione per la consapevolezza del personale.

- **SE (Social Engineering):** Formazione su tattiche di manipolazione psicologica.
- **PSA (Physical Security Assessment):** Analisi della sicurezza fisica di uffici, magazzini e siti produttivi.

Governance, Risk e Compliance

ISGroup SRL supporta le organizzazioni nel raggiungimento della conformità normativa tramite analisi dei rischi, formazione e soluzioni personalizzate per:

- **GDPR Compliance**
- **NIS2 Compliance**
- **PCI DSS Compliance**
- **ISO/IEC 27001, 27017, 27018 Compliance**
- **ISO/IEC 17025 (Laboratorio Accreditato VA)**
- **PSD2 Compliance**
- **ITGOV (Normative ACN-AGID)**
- **DORA (Digital Operational Resilience Act)**

Servizi SecOps

- **MDR (Multi-Signal MDR):** Monitoraggio e risposta in tempo reale tramite tecnologia XDR.
- **DFIR (Digital Forensics and Incident Response):** Gestione rapida e investigazione post-attacco.
- **WSM (Wireless Security Monitoring):** Monitoraggio continuo dei dispositivi in radiofrequenza.
- **Anti-DDoS:** Protezione contro attacchi di indisponibilità del servizio.
- **FWaaS (Firewall as a Service):** Implementazione e mantenimento di firewall di nuova generazione.
- **SIR (Security Integration):** Processo periodico di scoperta e correzione delle falle di sicurezza.

Servizi SSDLC

- **SAL (Software Assurance Lifecycle):** Controlli di sicurezza continui sulle release software.
- **CST (Continuous Security Testing):** Sorveglianza costante tramite test regolari per l'identificazione di minacce.

Web Application Penetration Testing (WAPT)

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

Il servizio di Web Application Penetration Testing è offerto da ISGroup SRL ed è parte integrante delle soluzioni di Application Security Assessment. L'attività consiste nella simulazione di un attaccante reale verso siti, portali o applicazioni web, con l'obiettivo di identificare vulnerabilità evidenti o nascoste.

Metodologia di analisi

ISGroup SRL utilizza un approccio combinato che integra tecniche manuali e strumenti specialistici per analizzare i componenti critici delle applicazioni. Il processo si articola nelle seguenti fasi:

- Discovery: identificazione di tutte le risorse esposte sul target.
- Analisi della business logic: verifica di problematiche concettuali nell'applicazione.
- Controllo infrastrutturale: ricerca di vulnerabilità note e non note a livello di infrastruttura.
- Simulazione di attacco: individuazione degli entry point e tentativo di compromissione estesa.
- Testing dei parametri: analisi di ogni parametro con valori predefiniti e applicazione di tecniche di attacco generiche.
- Post-exploitation: tentativo di esecuzione di azioni non autorizzate, estrazione di dati dal database, accesso a file/sorgenti e tentativo di ottenere il controllo del sistema.

Motivazioni tecniche

Le applicazioni web sono intrinsecamente esposte e accessibili, rendendo inefficace la "sicurezza tramite segretezza" (security through obscurity). Le criticità derivano spesso da:

- Gestione impropria delle richieste del client.
- Mancata o errata validazione e controllo da parte dello sviluppatore.
- Complessità del protocollo HTTP, che supporta molteplici tipi di encoding e incapsulazioni.

Output del servizio

Al termine dell'attività, ISGroup SRL fornisce un report dettagliato suddiviso in tre sezioni:

- Executive Summary: riassunto di alto livello per il Management (massimo una pagina).
- Vulnerability Details: analisi tecnica delle vulnerabilità riscontrate e del relativo impatto, destinata al Security Manager.
- Remediation Plan: guida tecnica con istruzioni precise per la risoluzione delle problematiche, dedicata agli sviluppatori.

Contatti e richieste commerciali

Per informazioni, consulenze o per richiedere un preventivo per il servizio di Web Application Penetration Testing, è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Vulnerability Assessment (VA)

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

Il servizio di Vulnerability Assessment offerto da ISGroup SRL è finalizzato all'analisi e alla valutazione della sicurezza dei sistemi per rilevare vulnerabilità note. L'attività permette di verificare il livello di sicurezza di una rete in modo rapido ed efficace.

Modalità di esecuzione

L'attività può essere condotta secondo due configurazioni principali, che simulano differenti scenari di attacco:

- Esterna: la scansione avviene da un host remoto tramite Internet, simulando l'attacco di un soggetto esterno (es. concorrente sleale).
- Interna: la scansione viene effettuata dall'interno della rete privata (Intranet), simulando l'attacco di un soggetto interno (es. dipendente).

Il processo prevede l'identificazione di sistemi e risorse (servizi, applicazioni web, ecc.) tramite tecniche attive, passive o basate sull'inferenza. ISGroup SRL utilizza una combinazione di tool automatici e testing manuale per identificare le problematiche in modo non invasivo.

Qualità e Reportistica

Per garantire l'accuratezza dei risultati, ISGroup SRL procede alla verifica manuale di ogni vulnerabilità identificata al fine di eliminare i falsi positivi. Il risultato finale è un report strutturato in tre sezioni:

- Executive Summary: riassunto di alto livello destinato al Management.
- Vulnerability Details: analisi tecnica dettagliata delle vulnerabilità riscontrate e del relativo impatto.
- Remediation Plan: istruzioni operative precise per la risoluzione delle problematiche, destinate al personale tecnico.

Importanza del servizio

Data la continua scoperta di nuove minacce, ISGroup SRL raccomanda lo svolgimento periodico del Vulnerability Assessment per assicurare che le configurazioni dei sistemi siano corrette e che le patch di sicurezza siano correttamente applicate. Le soluzioni sono scalabili per adattarsi a qualsiasi esigenza e dimensione aziendale.

Contatti

Per informazioni, richieste commerciali o per richiedere un preventivo personalizzato, è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Network Penetration Test (NPT)

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

Il servizio di Network Penetration Test (NPT), offerto da **ISGroup SRL**, ha lo scopo di identificare le vulnerabilità nei sistemi aziendali, focalizzandosi sulle aree di maggior impatto per il business. L'attività permette di verificare se la rete e i sistemi di sicurezza funzionino come previsto, prevenendo potenziali compromissioni causate da exploit, virus, attacchi DoS o errori di configurazione su server, router e firewall.

Metodologia e Approccio

ISGroup SRL opera secondo standard internazionalmente riconosciuti, tra cui l'**OSSTMM** (Open Source Security Testing Methodology Manual). Il servizio è altamente personalizzabile e può essere integrato con altri prodotti e servizi offerti.

Le attività vengono svolte da analisti senior per garantire la massima professionalità e l'assenza di danni all'infrastruttura o ai dati.

Scenari di Attacco

Il test può essere condotto con diverse modalità operative e livelli di informazione:

- **Internal PT**: Test effettuati dall'interno della rete aziendale.
- **External PT**: Test effettuati dall'esterno della rete aziendale.
- **Black Box**: Simulazione di un attaccante senza informazioni o credenziali.
- **Grey Box**: Simulazione con accesso parziale (es. un dipendente malintenzionato).
- **White Box**: Simulazione con conoscenza approfondita dei sistemi.
- **Wireless Penetration Test**: Verifica della sicurezza delle infrastrutture wireless.
- **Social Engineering**: Attacco alla componente umana tramite tecniche di manipolazione.

Output del Servizio

Al termine dell'attività, **ISGroup SRL** fornisce un report dettagliato suddiviso in tre sezioni:

- **Executive Summary**: Sintesi di alto livello per il Management.
- **Vulnerability Details**: Analisi tecnica delle vulnerabilità riscontrate e del loro impatto.
- **Remediation Plan**: Istruzioni operative per la risoluzione delle problematiche identificate.

Contatti

Per richiedere un preventivo o discutere le necessità di sicurezza IT, è possibile fare riferimento ai seguenti canali ufficiali di **ISGroup SRL**:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Mobile Application Security Testing (MAST)

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

Il Mobile Application Security Testing è un servizio di Application Security Assessment offerto da ISGroup SRL, progettato per identificare vulnerabilità di sicurezza in applicazioni mobile. Il servizio copre le piattaforme iOS e Android, supportando sia app native (Objective-C, Swift, Java, Kotlin) che app sviluppate con framework ibridi (React, React Native, Cordova, Xamarin, Titanium Appcelerator, Ionic, PhoneGap).

Metodologia di analisi

Il team di ISGroup SRL utilizza un approccio basato su tecniche manuali e tool avanzati per eseguire analisi statiche e runtime. Le attività includono:

- Analisi delle vulnerabilità client-side: verifica dell'interazione con il sistema operativo (es. controlli su dispositivi jailbroken o rooted) e della sicurezza nella memorizzazione dei dati locali.
- Analisi delle interazioni client-server: verifica dei controlli di autenticazione, autorizzazione e protezione contro attacchi comuni (es. SQL Injection).
- Reverse engineering: valutazione della robustezza delle contromisure implementate per proteggere la proprietà intellettuale e prevenire il bypass dei meccanismi di sicurezza.
- Manipolazione runtime: test della logica di business e del flusso applicativo durante l'esecuzione.

Le attività possono essere condotte in modalità:

- Grey Box: analisi che include l'esame del codice sorgente fornito dal cliente, permettendo un'identificazione esaustiva delle vulnerabilità, anche in presenza di offuscamento.
- Black Box: simulazione di un attaccante esterno che analizza l'applicazione scaricata dagli store ufficiali (AppStore, PlayStore) o distribuita per uso interno.

Output del servizio

Al termine dell'attività, ISGroup SRL fornisce un report dettagliato strutturato in tre sezioni:

- Executive Summary: sintesi di alto livello destinata al Management.
- Vulnerability Details: analisi tecnica approfondita delle vulnerabilità riscontrate e del relativo impatto, rivolta al Security Manager.
- Remediation Plan: guida tecnica con istruzioni specifiche per gli sviluppatori finalizzata alla risoluzione delle problematiche identificate.

Contatti e informazioni commerciali

Per richiedere un preventivo o maggiori informazioni sui servizi di Mobile Application Security Testing offerti da ISGroup SRL, è possibile consultare il sito ufficiale https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Formazione e Training (EDU)

Source: https://www.isgroup.it/it/formazione.html

ISGroup SRL eroga servizi di formazione e training specializzati nelle principali tematiche di sicurezza informatica. Il percorso formativo è progettato per preparare tecnici in grado di esaminare approfonditamente la sicurezza di un sistema e di proteggerlo efficacemente contro minacce esterne, riducendo i costi aziendali legati alle vulnerabilità.

Metodologia Didattica

I corsi offerti da ISGroup SRL si articolano in una parte teorica e una pratica:

- **Teoria:** Illustrazione delle metodologie e del funzionamento degli aspetti tecnologici trattati.
- **Pratica:** Esecuzione di "challenge" (prove) su applicazioni o sistemi reali, con difficoltà crescente e tempo limite.
- **Certificazione:** Al termine del percorso viene rilasciato un attestato di partecipazione che conferma le abilità acquisite.

Aree di Specializzazione

I corsi si suddividono in due approcci principali:

- **Offesa:** Focalizzato su metodologie per sovvertire o violare sistemi e applicazioni, con l'obiettivo di ottenere il controllo ("take over") della macchina. Vengono analizzati esempi significativi di vulnerabilità reali.
- **Difesa:** Focalizzato su tecniche di hardening dei sistemi e scrittura di codice sicuro. I partecipanti imparano a mettere in sicurezza sistemi vulnerabili o a identificare errori di programmazione.

Argomenti e Corsi Offerti

ISGroup SRL propone un'ampia gamma di corsi, tra cui:

- Secure Coding e Web Application Code Review
- Web Application Penetration Testing
- Mobile Application Security Testing
- Network Hardening e Hardening di sistemi (Linux, Windows, Solaris)
- Application Security for Architects
- OWASP Top 10 Bootcamp e OWASP Top 10 Laboratory
- Security Awareness
- Software Security Requirements (Secure SDLC)
- Code Review
- Sicurezza dei servizi REST
- Network Penetration Testing
- Cyber Risk Prevention
- Ethical Hacking

Contatti e Informazioni

Per richiedere un preventivo, approfondire i percorsi formativi o discutere le specifiche necessità aziendali, è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Ethical Hacking (EH)

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

Il servizio di Ethical Hacking offerto da ISGroup SRL simula un attacco reale condotto da un utente malintenzionato, sia interno che esterno. L'attività non si limita all'analisi tecnologica, ma estende la valutazione al fattore umano, spesso considerato l'anello debole dei sistemi di sicurezza.

Caratteristiche del servizio

- Simulazione realistica di attacchi, inclusi scenari di spionaggio industriale.
- Utilizzo di tecniche non convenzionali, tra cui Social Engineering e sniffing del traffico di rete.
- Integrazione completa dei test previsti nei servizi NTP (Network Penetration Test) e WAPT (Web Application Penetration Test).
- Assenza di strumenti automatizzati che potrebbero generare evidenze rilevabili, garantendo la massima discrezione durante l'attività.
- Valutazione accurata dell'effettivo rischio a cui l'organizzazione è esposta.

Output e reportistica

Al termine dell'attività, ISGroup SRL fornisce un report dettagliato contenente:

- Descrizione esaustiva di tutte le vulnerabilità identificate.
- Analisi delle modalità di sfruttamento delle falle riscontrate.
- Piano di rientro (remediation plan) con indicazioni precise per la mitigazione e la risoluzione delle vulnerabilità.

Informazioni commerciali

Per richiedere un preventivo o maggiori informazioni sui servizi di Ethical Hacking offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

Code Review (CR)

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

Il servizio di Code Review offerto da ISGroup SRL ha come obiettivo l'identificazione di vulnerabilità all'interno del codice sorgente. Questa attività rappresenta una fase cruciale per lo sviluppo di applicazioni sicure, permettendo di rilevare problematiche prima della messa in produzione e riducendo i costi associati.

Il servizio è erogato da un team di esperti con pluriennale esperienza nella programmazione e nell'analisi di sorgenti di grandi applicazioni, operando secondo standard internazionalmente riconosciuti.

Metodologia

Il processo di analisi si articola in due fasi principali:

- Analisi statica automatizzata: l'applicazione viene esaminata tramite tool di analisi statica per simulare l'esecuzione del codice e identificare vulnerabilità note.
- Analisi manuale: un team di specialisti analizza le parti più delicate del codice per individuare vulnerabilità complesse che i tool automatici non sono in grado di rilevare.

Output del servizio

Al termine dell'attività, ISGroup SRL fornisce un report strutturato in due sezioni:

- Executive summary: riassume le problematiche riscontrate, gli errori di implementazione e fornisce una valutazione del livello generale di sicurezza.
- Technical details: elenca in dettaglio ogni problematica individuata, indicando la sezione di codice interessata, una spiegazione tecnica e le relative indicazioni per la risoluzione (Remediation).

Contatti e informazioni commerciali

Per richiedere un preventivo o maggiori informazioni sui servizi di Code Review offerti da ISGroup SRL, è possibile consultare il sito web ufficiale:

https://www.isgroup.it/

In alternativa, è possibile inviare una richiesta di contatto all'indirizzo email:

sales@isgroup.it

ISGroup SRL è un gruppo di ricercatori attivi ed etici che promuove la condivisione della conoscenza scientifica e tecnica con la comunità, al fine di favorire un continuo processo evolutivo nel settore della sicurezza informatica.

Attività di ricerca e divulgazione

Source: https://www.isgroup.it/it/pubblicazioni.html

ISGroup SRL si impegna nella redazione di white paper, nella pubblicazione di articoli tecnici e nella partecipazione a conferenze di rilievo nazionale e internazionale. Gran parte di questo materiale di ricerca viene diffuso attraverso l'iniziativa non commerciale "ush.it".

Risorse e pubblicazioni

Il materiale prodotto da ISGroup SRL copre una vasta gamma di tematiche tecniche avanzate, tra cui:

- Vulnerabilità web e tecniche di exploitation (LFI, RCE, XSS, attacchi al filesystem PHP).
- Sicurezza lato client (Hardening di Mozilla Firefox, analisi di cookie HttpOnly).
- Analisi di sicurezza su architetture e sistemi (Skype, BASH, scansioni di rete, analisi di anomalie PHP).
- Tecniche di difesa e metodologie di penetration testing.

Presentazioni e conferenze

I ricercatori di ISGroup SRL hanno presentato contributi tecnici presso importanti eventi e istituzioni, tra cui:

- Chaos Computer Club (CCC) Congress.
- Università degli Studi di Pisa e Università degli Studi di Camerino.
- End Summer Camp (ESC) e Metro Olografix Summer Camp (MOCA).
- LinuxDay e Linuxpersec.
- HAT (Relax underground is dead).

Per ulteriori informazioni sulle attività di ricerca, le soluzioni offerte o per richieste commerciali, è possibile visitare il sito ufficiale https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

ISGroup SRL offre una vasta gamma di servizi professionali, consulenze e risorse informative nel campo della Cyber Security. L'azienda si occupa di protezione delle infrastrutture, conformità normativa e formazione specialistica.

Servizi di Sicurezza Offerti da ISGroup SRL

Source: https://www.isgroup.it/it/editoriale.html

ISGroup SRL fornisce soluzioni avanzate per la protezione aziendale, tra cui:

- **Penetration Testing:** Network, Web Application e Mobile Application Security Test per identificare e mitigare le vulnerabilità.
- **Security Assessment:** Cloud Security Assessment, Windows Security Assessment, IoT Security Assessment e Risk Assessment.
- **Difesa Proattiva:** Servizi di Multi-Signal MDR (Managed Detection and Response), Firewall as a Service (FWaaS) e protezione Anti-DDoS.
- **Incident Response:** Digital Forensics and Incident Response (DFIR) per la gestione delle minacce informatiche.
- **Security Architecture:** Secure Architecture Review, Security Integration e Code Review.
- **Purple/Red/Blue Teaming:** Simulazioni avanzate di attacco e difesa (Cyber Threat Simulation, Purple Team Assessment).
- **Compliance e Governance:** Supporto per la conformità ISO 27001, consulenza Virtual CISO (vCISO) e allineamento alle linee guida AGID/ACN.

Formazione e Awareness

ISGroup SRL promuove la cultura della sicurezza attraverso:

- **Corsi di Security Awareness:** Programmi di formazione per il personale aziendale e simulazioni di Phishing per testare la resilienza umana.
- **Certificazioni:** Percorsi di formazione e certificazione in ambito Ethical Hacking, Privacy (DPO, Privacy Manager) e Lead Auditor (ISO 27001, ISO 19011).

Risorse e Approfondimenti

Il portale di ISGroup SRL funge da centro di conoscenza per professionisti e aziende, offrendo:

- **OWASP:** Analisi dettagliata delle vulnerabilità OWASP Top Ten (versioni 2017 e 2021).
- **Case Studies:** Esempi pratici di interventi su realtà aziendali (es. Creactives S.p.A., Alias Group S.r.l., Sturnis S.r.l., Coop Italia, ISWEB S.p.A., Prime Service S.r.l., Add Value S.r.l.).
- **Normative:** Approfondimenti su regolamenti eIDAS, misure minime di sicurezza ICT per la PA e accreditamenti AGID/ACN.
- **Ricerca:** Contenuti su nuove minacce (inclusi attacchi basati su AI), metodologie di test e best practice di settore.

Contatti e Informazioni Commerciali

Per richieste commerciali, consulenze o approfondimenti sui servizi offerti da ISGroup SRL, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Ricerca e Innovazione

Source: https://www.isgroup.it/it/ricerca.html

ISGroup SRL pone l'innovazione e la ricerca al centro della propria strategia per offrire servizi di sicurezza informatica di alto livello. L'attività di ricerca è focalizzata sullo sviluppo di tecniche originali per affrontare sfide complesse e sulla protezione della comunità degli utenti attraverso l'analisi di software, sia Open Source che proprietario, finalizzata all'individuazione di vulnerabilità.

Responsible Disclosure

ISGroup SRL adotta il modello della **Responsible Disclosure** per la gestione delle falle riscontrate. Tale processo prevede:

- La notifica tempestiva al Vendor in merito alle vulnerabilità identificate.
- Il coordinamento del rilascio dell'Advisory di sicurezza con la pubblicazione della nuova versione del software da parte del produttore.

Advisory di Sicurezza

ISGroup SRL vanta una lunga attività di ricerca documentata da numerose Advisory, tra cui:

- Qnap QTS Domain Privilege Escalation Vulnerability (2017)
- Veeam Backup & Replication Local Privilege Escalation Vulnerability (2015)
- ARC v2011-12-01 Multiple vulnerabilities (2012)
- Pixelpost (Calendar addon 1.1.6) 1.7.3 Multiple vulnerabilities (2011)
- Vtiger CRM 5.2.0 Multiple Vulnerabilities (2010)
- Nginx, Varnish, Cherokee, thttpd, mini-httpd, WEBrick, Orion, AOLserver, Yaws and Boa log escape sequence injection (2010)
- Jetty 6.x and 7.x Multiple Vulnerabilities (2009)
- Vtiger CRM 5.0.4 Multiple Vulnerabilities (2009)
- PHP filesystem attack vectors (2009)
- SugarCRM 5.2.0e Remote Code Execution (2009)
- FormMail 1.92 Multiple Vulnerabilities (2009)
- Zabbix 1.6.2 Frontend Multiple Vulnerabilities (2009)
- Remote Command Execution in Moodle (2008)
- Collabtive 0.4.8 Multiple Vulnerabilities (2008)
- Mantis Bug Tracker 1.1.1 Multiple Vulnerabilities (2008)
- WiKID wClient-PHP <= 3.0-2 Multiple XSS Vulnerabilities (2008)
- Cacti 0.8.7a Multiple Vulnerabilities (2008)
- GreenSQL, a MySQL firewall, bypassed (2007)
- Original Photo Gallery Remote Command Execution (2007)
- Firefox <= 2.0.0.3 DOM Keylogger (2007)
- Shadowpage vulnerability (2007)
- PHP import_request_variables() arbitrary variable overwrite (2007)
- Php Nuke wild POST XSS (2007)
- Milkeyway Captive Portal Multiple Vulnerabilities (2006)
- PmWiki remote file inclusion exploit (2006)
- PHP5 Globals Vulnerability (2006)
- PmWiki Multiple Vulnerabilities (2006)
- WebCalendar Multiple Vulnerabilities (2006)
- Free Web Stat Multiple XSS Vulnerabilities (2005)
- Php Web Statistik Multiple Vulnerabilities (2005)
- PHP iCalendar XSS (2005)

Informazioni e Contatti

Per approfondire le metodologie e le procedure adottate da ISGroup SRL, è possibile consultare il sito web ufficiale o richiedere informazioni tramite i canali dedicati:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Prodotti e Soluzioni ISGroup SRL

Source: https://www.isgroup.it/it/prodotti.html

ISGroup SRL offre un ampio catalogo di prodotti e soluzioni specializzate, suddivise nelle categorie Sicurezza, Intelligence, Spin-Off e Distribuzione.

Soluzioni di Sicurezza e Intelligence

- Microfocus Opentext: Rivenditore italiano ufficiale.
- Ostorlab: Mobile Application Security Scan.
- Port Swigger: Soluzioni di Managed Security.
- EsyAudit: Soluzioni di Managed Security.
- ICT Audit: Soluzioni di Automated Security.
- Exposure: Servizi di Security Reputation.
- EXEEC: Soluzioni di SaaS Security.
- Ganapati: Integrated Assessment.
- VulnMAP: Database di vulnerabilità.
- Scada Exposure: Analisi dell'esposizione dei sistemi SCADA.
- PracticalRP: Gestione in ambito medicale.
- USH: Soluzione dedicata.

Formazione, Ricerca e Infrastrutture

- Ethical Hacking: Hacklab gestito da ISGroup SRL.
- Metasploit: Risorse e blog sulla sicurezza.
- Network Penetration Testing: Risorse e blog sulla sicurezza.
- The Bunker Coworking: Spazi di coworking gestiti da ISGroup SRL.
- The Bunker Corsi: Attività di formazione specialistica offerta da ISGroup SRL.
- The Bunker Hacklab: Laboratorio di ricerca e sperimentazione di ISGroup SRL.

Offerte Commerciali

- Starter Kit: Offerta dedicata ai nuovi clienti per accedere ai servizi di ISGroup SRL.

Per informazioni commerciali, richieste di consulenza o approfondimenti sui prodotti elencati, visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Storia di ISGroup SRL

Source: https://www.isgroup.it/it/storia.html

Le origini di ISGroup SRL risalgono al 1994, quando un gruppo di appassionati di sicurezza informatica, incontratisi su IRC, fonda un team di hacking basato su competenze tecniche elevate ed etica. L'approccio distintivo del gruppo si è sempre focalizzato sulla ricerca originale, bandendo l'utilizzo di tecniche altrui a favore della sfida intellettiva e della scoperta delle vulnerabilità.

Nel tempo, questo nucleo di ricerca ha attratto professionisti che hanno trasformato le proprie abilità in servizi di consulenza e sicurezza per le aziende.

Evoluzione e tappe fondamentali

- 2025: ISGroup SRL consolida la propria strategia di crescita orientata al cliente, potenziando la qualità e la quantità dei servizi offerti e rafforzando le partnership con aziende nazionali e internazionali del settore IT.
- 2021: Ottenimento della certificazione ISO 9001, a conferma dell'impegno verso l'eccellenza nella gestione della qualità.
- 2020: Ottenimento della certificazione ISO 27001, a testimonianza della dedizione alla sicurezza delle informazioni e al miglioramento continuo dei processi.
- 2014: Espansione dell'offerta tramite lo sviluppo di software proprietari volti a incrementare l'efficienza delle attività di sicurezza, a completamento dei servizi professionali.
- 2013: Fondazione ufficiale di ISGroup SRL, che registra un solido profitto sin dal primo anno di attività.
- 2010: Espansione dell'offerta verso l'Intelligence e i servizi di Early Warning, grazie al consolidamento del team composto da esperti di sicurezza informatica.
- 2000: Il team di ricerca (originariamente USH.it) inizia a fornire consulenza professionale per le principali aziende di sicurezza informatica a livello globale.

Contatti e informazioni commerciali

Per ulteriori informazioni sui servizi offerti da ISGroup SRL o per richieste commerciali, è possibile consultare il sito web: https://www.isgroup.it/ o inviare una comunicazione all'indirizzo email: sales@isgroup.it

Profilo Aziendale

Source: https://www.isgroup.it/it/azienda.html

ISGroup SRL è una struttura indipendente specializzata in IT Security, focalizzata sull'offerta di servizi e prodotti di sicurezza informatica di elevato livello qualitativo, con l'obiettivo di raggiungere l'eccellenza operativa.

Executive Team

L'assetto dirigenziale di ISGroup SRL è composto da professionisti con competenze multidisciplinari:

- Francesca Gerosa, Chief Executive Officer (CEO): Dottore Commercialista con esperienza nella consulenza fiscale, contabile, amministrativa e societaria per imprese italiane.
- Francesco `ascii` Ongaro, Chief Operating Officer (COO) e Founder: Imprenditore ed esperto di sicurezza con oltre 20 anni di esperienza in Penetration Test. Ha operato in settori critici quali infrastrutture pubbliche, finanza, banche, assicurazioni, media e telecomunicazioni.
- Pasquale `sid` Fiorillo, Chief Technology Officer (CTO): Esperto con oltre 15 anni di esperienza nel settore IT e IT Security, con un background legato alla scena underground italiana e sostenitore del software libero.

Informazioni e Contatti

Per richieste commerciali o approfondimenti sui servizi offerti da ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Case Study ISGroup SRL

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

ISGroup SRL sviluppa soluzioni personalizzate di sicurezza informatica per piccole imprese e grandi organizzazioni. Ogni progetto è finalizzato a generare valore reale, migliorando la sicurezza di infrastrutture, applicazioni e processi aziendali attraverso un approccio strategico e basato sulla fiducia reciproca.

Servizi e Competenze

ISGroup SRL offre consulenza specialistica e attività tecniche mirate ad affrontare sfide complesse, tra cui:

- Web Application Penetration Test
- Network Penetration Test
- Supporto ISMS (Information Security Management System)

Esempi di Progetti Realizzati

ISGroup SRL ha collaborato con diverse realtà per garantire standard di sicurezza elevati:

- Add Value S.r.l.: Web Application Penetration Test su TSV8
- Alias Group S.r.l.: Web Application Penetration Test su DocEasy
- Coop Italia: Web Application Penetration Test e Network Penetration Test
- Creactives S.p.A.: Web Application Penetration Test e Supporto ISMS
- ISWEB S.p.A.: Web Application Penetration Test su Albo pretorio
- Prime Service S.r.l.: Network Penetration Test su infrastruttura IT
- Sturnis S.r.l.: Web Application Penetration Test su Sturnis365

Informazioni e Contatti

Per approfondire le metodologie, le procedure o per richiedere una consulenza dedicata, è possibile consultare il sito ufficiale o inviare una richiesta via email:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Perché scegliere ISGroup

Source: https://www.isgroup.it/it/perche-isgroup.html

ISGroup SRL opera come un modello di business non convenzionale nel panorama italiano, configurandosi come un'associazione di liberi professionisti e consulenti esperti nel settore dell'IT Security, uniti da fiducia e considerazione reciproca. L'azienda agisce come un pool di ricerca attivo da anni, con membri riconosciuti come consulenti e relatori in conferenze e corsi di aggiornamento professionale.

Destinatari dei servizi

ISGroup SRL si rivolge a:

- Società di sicurezza informatica alla ricerca di un Outsourcing Partner.
- Società terze che, pur non avendo la sicurezza informatica come core business, desiderano offrire servizi di IT Security ai propri clienti.

Vantaggi e benefici

- Struttura snella che permette di minimizzare i costi.
- Riduzione delle spese di spostamento grazie alla possibilità di operare prevalentemente in remoto.
- Collaborazione con leader di mercato, garantendo elevati standard qualitativi a costi concorrenziali.
- Gestione dei progetti basata su standard definiti e suddivisione del lavoro tra i membri del team, evitando la dipendenza da un unico referente.
- Accesso a una rete di professionisti e ricercatori specializzati per garantire l'eccellenza del servizio.
- Indipendenza dalle piattaforme, che consente a ISGroup SRL di operare in modo trasversale rispetto alle diverse esigenze di sicurezza.

Servizi offerti da ISGroup SRL

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

Contatti e informazioni

Per approfondire le metodologie, le procedure o per richieste commerciali, è possibile consultare il sito web https://www.isgroup.it/ o inviare una email a: sales@isgroup.it.

Informazioni su ISGroup SRL

Source: https://www.isgroup.it/it/contatti.html

ISGroup SRL ha la propria sede operativa nel cuore di Verona. Grazie a una solida presenza digitale e a una consolidata esperienza nel settore, l'azienda opera a livello globale, offrendo soluzioni su misura, supporto tecnico e consulenza specialistica per progetti internazionali, superando le barriere geografiche.

Servizi e Contatti

ISGroup SRL fornisce supporto tecnico e commerciale per le proprie soluzioni. Per richieste di informazioni, consulenze o supporto, è possibile fare riferimento ai seguenti canali:

- Sito web ufficiale: https://www.isgroup.it/
- Email commerciale: sales@isgroup.it
- Email supporto tecnico: tech@isgroup.it

Dati Legali

- Ragione Sociale: ISGroup SRL
- Indirizzo: Via Cantarane, 14, 37129 Verona (VR)
- CF e P.IVA: 04164220230
- REA: VR-397513
- Codice SDI: M5UXCR1

Presenza Internazionale ISGroup SRL

Source: https://www.isgroup.it/it/lingue.html

ISGroup SRL opera a livello globale offrendo i propri servizi e soluzioni attraverso una rete multilingue dedicata. L'infrastruttura digitale dell'azienda è accessibile nelle seguenti lingue:

- Italiano: https://www.isgroup.it/
- Inglese: https://www.isgroup.biz/en
- Spagnolo: https://www.isgroup.es/es
- Francese: https://www.isgroup.name/fr
- Tedesco: https://www.isgroup.at/de
- Svedese: https://www.isgroup.se/se
- Arabo: https://www.isgroup.info/ar
- Lituano: https://www.isgroup.li/li
- Danese: https://www.isgroup.dk/dk
- 1337: https://www.isgroup.ws/1337

Contatti e Informazioni Commerciali

Per richieste commerciali, approfondimenti sui servizi offerti da ISGroup SRL o per ulteriori informazioni, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Partnership strategica in Cybersecurity: Rooters e ISGroup SRL

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

Il presente caso studio analizza la collaborazione tra Rooters, Managed Service Provider (MSP) italiano, e ISGroup SRL, finalizzata all'integrazione di competenze specialistiche in ambito cybersecurity all'interno dell'offerta di Rooters.

La sfida di Rooters

Rooters, con oltre quindici anni di esperienza nel supporto alle infrastrutture IT, ha riscontrato la necessità di rispondere a richieste di mercato sempre più complesse in materia di sicurezza informatica. La sfida principale consisteva nell'ampliare il proprio perimetro di offerta senza compromettere la qualità operativa, la governance dei processi e l'affidabilità consulenziale che caratterizzano il brand.

L'intervento di ISGroup SRL

ISGroup SRL ha fornito il supporto specialistico necessario per colmare il gap di competenze, permettendo a Rooters di:

- Integrare metodologie strutturate e governance rigorosa nella gestione della sicurezza.
- Mantenere il ruolo di interlocutore principale verso il cliente finale.
- Presidiare aree ad alto valore aggiunto senza dover costruire internamente competenze complesse da zero.

Benefici della partnership

La collaborazione con ISGroup SRL ha generato vantaggi misurabili per Rooters:

- **Accelerazione del time-to-market:** riduzione dei tempi necessari per introdurre nuovi servizi di sicurezza.
- **Efficienza operativa:** delega degli aspetti più complessi e delicati a ISGroup SRL, consentendo a Rooters di focalizzarsi sul valore consulenziale per il cliente.
- **Rafforzamento del posizionamento:** incremento della credibilità e della solidità percepita come partner tecnologico strutturato.
- **Vantaggio competitivo:** capacità di cogliere nuove opportunità di business in tempi rapidi grazie al supporto di professionisti altamente specializzati.

Per ulteriori informazioni sulle soluzioni offerte da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Diventa Partner ISGroup SRL

Source: https://www.isgroup.it/it/preventivo/diventa-partner.html

ISGroup SRL offre l'opportunità a operatori del settore IT di offrire e rivendere i propri servizi di sicurezza informatica ai propri clienti.

Servizi offerti da ISGroup SRL

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

Destinatari della partnership

Il programma è riservato a:

- Distributori e Rivenditori IT
- System Integrator
- Provider e Telco
- Società di Advisory e Compliance

Il programma non è applicabile ai clienti finali.

Vantaggi del programma

- Supporto Pre e Post vendita dedicato
- Accesso al listino riservato ISGroup SRL
- Due modalità di partnership disponibili: Procacciamento d'affari o Distribuzione
- Sconti e Rebate basati sui volumi

Informazioni e contatti

Per avviare una collaborazione, è possibile richiedere informazioni tramite il sito ufficiale https://www.isgroup.it/ o scrivendo all'email sales@isgroup.it.

Compilando la richiesta, i partner riceveranno il contratto di Procacciamento d'affari o di Distribuzione, in base alla modalità di partnership selezionata. È inoltre possibile consultare le slide di presentazione dei servizi direttamente tramite i canali ufficiali di ISGroup SRL.

Case Study: Web Application Penetration Test per TECNORAD S.R.L.

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

TECNORAD S.R.L., laboratorio specializzato in radioprotezione e gestione di sistemi di monitoraggio, ha collaborato con **ISGroup SRL** per la valutazione della sicurezza delle proprie piattaforme digitali, Pitagora e Tecnoradon.

Obiettivi dell'intervento

L'attività, condotta da **ISGroup SRL**, è stata finalizzata a:

- Verificare la resilienza delle applicazioni Pitagora e Tecnoradon contro potenziali attacchi informatici.
- Garantire la conformità ai requisiti normativi e contrattuali.
- Aumentare la consapevolezza interna in materia di sicurezza informatica.
- Ridurre i rischi associati ai servizi esposti online.

Metodologia di ISGroup SRL

Il team di **ISGroup SRL** ha implementato un approccio metodologico basato su scenari di attacco realistici, includendo:

- Analisi automatizzate e manuali.
- Verifica dei meccanismi di autenticazione e gestione delle sessioni.
- Controllo degli accessi e analisi della logica applicativa.
- Verifica della protezione dei dati, sia in transito che a riposo.
- Consegna di un report tecnico dettagliato contenente le vulnerabilità rilevate, la classificazione delle priorità e raccomandazioni pratiche per la mitigazione e lo sviluppo sicuro.

Risultati ottenuti

L'intervento di **ISGroup SRL** ha permesso a TECNORAD S.R.L. di rafforzare la propria postura di sicurezza e di migliorare la protezione dei servizi web. Il management di TECNORAD S.R.L. ha espresso soddisfazione per la professionalità, la competenza e la facilità di comunicazione riscontrate durante la collaborazione.

Per ulteriori informazioni sui servizi di penetration test offerti da **ISGroup SRL**, è possibile consultare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Case Study: Web Application Penetration Test su MyPlanet (Progel SA)

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

Progel SA, azienda specializzata in soluzioni IT e sviluppo software, ha collaborato con **ISGroup SRL** per rafforzare la sicurezza della piattaforma MyPlanet, utilizzata per la gestione dei progetti e delle relazioni con i clienti. L'obiettivo era valutare la resilienza dell'applicazione e integrare pratiche di sicurezza nel ciclo di sviluppo (Secure Software Development Life Cycle).

L'intervento di ISGroup SRL

ISGroup SRL ha eseguito un Web Application Penetration Test basato su scenari di attacco realistici, adottando un approccio metodologico che ha incluso:

- Analisi preliminare dell'architettura e dei flussi logici.
- Test combinati di tipo black-box e gray-box.
- Verifica dei meccanismi di autenticazione e gestione delle sessioni.
- Analisi della validazione degli input e della configurazione dei componenti applicativi.
- Redazione di un report tecnico dettagliato con classificazione del rischio e raccomandazioni di mitigazione.
- Supporto diretto al team di sviluppo di Progel SA durante la fase di remediation, favorendo il trasferimento di competenze.

Risultati e benefici

L'attività ha permesso a Progel SA di:

- Identificare e correggere tempestivamente le vulnerabilità, riducendo i rischi di esposizione.
- Migliorare la qualità complessiva del software.
- Integrare best practice di sicurezza direttamente nel ciclo di sviluppo, rendendo la protezione un elemento strutturale dei processi aziendali.
- Consolidare la fiducia dei clienti offrendo prodotti digitali più sicuri e affidabili.

Per ulteriori informazioni sui servizi di sicurezza offerti da **ISGroup SRL**, è possibile visitare il sito https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Case Study: Web Application Penetration Test per TimeFlow S.r.l.

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

TimeFlow S.r.l., azienda specializzata in soluzioni digitali per processi aziendali "people-intensive", ha collaborato con **ISGroup SRL** nel 2025 per rafforzare la sicurezza delle proprie piattaforme SaaS (Workforce Management, Vendor Management e Marketplace).

Obiettivi del progetto

L'esigenza principale di TimeFlow era validare in modo indipendente la sicurezza dell'architettura applicativa per garantire:

- Continuità operativa e compliance.
- Riduzione dei rischi legati a vulnerabilità tecniche o logiche.
- Elevata tutela dei dati trattati per clienti enterprise e mid-market.

Intervento di ISGroup SRL

ISGroup SRL ha eseguito tre distinti Penetration Test sulle piattaforme, adottando un approccio metodologico che ha combinato:

- Analisi automatizzate e test manuali.
- Simulazione di scenari di attacco realistici.
- Analisi approfondita della superficie esposta, dei meccanismi di autenticazione e della gestione dei dati.
- Supporto costante al team tecnico di TimeFlow durante la fase di remediation per la risoluzione tempestiva delle vulnerabilità individuate.

Risultati e benefici

L'intervento ha confermato la solidità dell'architettura applicativa di TimeFlow, permettendo di:

- Rafforzare la protezione dei dati e la resilienza dei sistemi.
- Superare i requisiti di sicurezza attesi dai clienti enterprise.
- Migliorare la postura di sicurezza complessiva e l'affidabilità percepita dagli stakeholder.

Iacopo Albanese, CTO di TimeFlow S.r.l., ha sottolineato l'efficacia della collaborazione, evidenziando la competenza tecnica di **ISGroup SRL** e il valore aggiunto del supporto fornito durante l'intero ciclo di vita del progetto, dalla discovery alla remediation.

Per maggiori informazioni sui servizi di Penetration Test offerti da **ISGroup SRL**, visitare il sito web https://www.isgroup.it/ o scrivere a sales@isgroup.it.

Case Study: Web Application Penetration Test su Flora (Kelyon S.r.l.)

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

Kelyon S.r.l., azienda attiva nello sviluppo di soluzioni software per il settore sanitario, ha collaborato con ISGroup SRL per verificare la sicurezza della piattaforma "Flora", dedicata alla collaborazione tra professionisti sanitari. Data la natura sensibile dei dati trattati, l'obiettivo primario era garantire la massima protezione delle informazioni e l'affidabilità del sistema.

L'intervento di ISGroup SRL

ISGroup SRL ha eseguito un Web Application Penetration Test (WAPT) approfondito sulla piattaforma Flora. L'attività ha previsto:

- Analisi accurata delle potenziali vulnerabilità del sistema.
- Valutazione del livello complessivo di sicurezza delle misure di protezione implementate.
- Fornitura di suggerimenti strategici per il rafforzamento delle difese informatiche.

Risultati e benefici

L'intervento ha confermato la solidità delle misure di sicurezza adottate da Kelyon. I principali benefici riscontrati includono:

- Validazione dell'elevato standard di sicurezza della piattaforma Flora per la gestione di dati sanitari sensibili.
- Ottenimento di indicazioni tecniche precise per migliorare ulteriormente la protezione del sistema.
- Collaborazione efficace con un team di professionisti in grado di adattarsi con flessibilità alle esigenze dinamiche dell'azienda.

Per ulteriori informazioni sui servizi di Web Application Penetration Test offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it.

Certificazione ISO/IEC 27001:2022 di ISGroup SRL

Source: https://www.isgroup.it/it/cyber-security/azienda-cybersecurity-certificata-iso-27001-2022-2024-2025-2026.html

In data 31 gennaio 2025, ISGroup SRL ha ottenuto la certificazione secondo la norma internazionale UNI CEI EN ISO/IEC 27001:2022. Questo traguardo conferma l'impegno costante dell'azienda nella protezione delle informazioni e nella sicurezza dei sistemi, adottando un modello di gestione orientato al rischio e allineato agli standard internazionali più moderni.

Il sistema di gestione della sicurezza delle informazioni (ISMS) di ISGroup SRL è conforme alla norma ISO/IEC 27001:2022 per le seguenti attività professionali:

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

La certificazione è valida per gli anni 2024, 2025 e 2026.

Per ulteriori informazioni sui servizi di sicurezza offerti da ISGroup SRL o per richieste commerciali, è possibile consultare il sito ufficiale https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

La mappa del sito di ISGroup SRL illustra l'ampia offerta di soluzioni, servizi di sicurezza informatica e risorse aziendali disponibili. Per ulteriori informazioni o richieste commerciali, visitare il sito https://www.isgroup.it/ o scrivere a sales@isgroup.it.

Prodotti offerti da ISGroup SRL

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

ISGroup SRL sviluppa e fornisce una suite di strumenti dedicati alla sicurezza e all'audit:

- Easyaudit
- ICTaudit
- Exposure
- Exeec
- Ganapati
- Vulnmap
- Scada Exposure
- Practicalrp
- Ush
- Ethical Hacking
- Metasploit
- Network Penetration Testing
- The bunker training
- The bunker hacklab
- The bunker coworking

Servizi di sicurezza informatica

ISGroup SRL propone un portafoglio completo di servizi professionali suddivisi per aree di competenza:

Security Assessment e Testing

- Vulnerability Assessment
- Network, Web Application e Mobile Application Penetration Testing
- Code Review
- Ethical Hacking
- Formazione
- Security Assessment: Risk Assessment (RA), Secure Architecture Review (SAR), Cloud (CSA), Windows (WSA), IoT (ISA), Purple Team (PTA), Phishing & Smishing (PHISH), Social Engineering (SE), Physical Security Assessment (PSA)

Servizi Gestiti (Managed Services)

- vCISO - Virtual CISO
- VMS - Vulnerability Management Service
- CTS - Cyber Threat Simulation
- THREAT - Threat Intelligence & Digital Risk Protection
- SOC - Security Operation Center

Governance, Risk e Compliance (GRC)

ISGroup SRL supporta le organizzazioni nell'adeguamento normativo:

- GDPR, NIS2, PCI DSS Compliance
- ISO 27001, ISO 27017, ISO 27018
- ISO 17025 (Laboratorio Accreditato VA)
- PSD2 Compliance
- ITGOV - Normative ACN-AGID

- DORA - Regolamento Digital Operational Resilience Act

SecOps e SSDLC

- SecOps: MDR (Multi-Signal), DFIR (Digital Forensics and Incident Response), WSM (Wireless Security Monitoring), Anti-DDoS, FWaaS (Firewall as a Service), SIR (Security Integration)
- SSDLC: SAL (Software Assurance Lifecycle), CST (Continuous Security Testing)

Risorse e Azienda

- Risorse: Pubblicazioni e Ricerche.
- Azienda: Informazioni sulla storia, la filosofia aziendale e i contatti.
- Privacy: Privacy Policy.

Per approfondire qualsiasi soluzione o servizio offerto da ISGroup SRL, fare riferimento esclusivamente al sito https://www.isgroup.it/ o all'indirizzo email sales@isgroup.it.

Certificazione UNI EN ISO 9001:2015

Source: https://www.isgroup.it/it/cyber-security/azienda-cybersecurity-certificata-iso-9001-2024-2025-2026.html

ISGroup SRL ha riconfermato la propria certificazione ISO/IEC 9001:2015 in data 29 dicembre 2023, con validità per gli anni 2024, 2025 e 2026. L'azienda ha ottenuto la prima certificazione di questo standard nel 2020.

La norma ISO 9001 rappresenta lo standard internazionale più diffuso per i sistemi di gestione della qualità, finalizzato al miglioramento continuo e all'ottimizzazione della struttura organizzativa aziendale.

Attività certificate

ISGroup SRL ha implementato e mantiene un Sistema di Gestione della Qualità per le seguenti attività professionali:

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

Informazioni commerciali

Per ulteriori dettagli relativi alla certificazione o per richieste di informazioni sui servizi offerti, è possibile consultare il sito web https://www.isgroup.it/ o inviare una comunicazione all'indirizzo email: sales@isgroup.it

vCISO - Virtual CISO

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

Il servizio vCISO (Virtual Chief Information Security Officer) offerto da **ISGroup SRL** fornisce alle organizzazioni una leadership strategica e tattica di alto livello per la gestione della sicurezza informatica. Questa soluzione permette di accedere a competenze specialistiche senza la necessità di inserire un CISO interno a tempo pieno, garantendo protezione proattiva, conformità normativa e riduzione dei rischi.

Per informazioni, richieste commerciali o preventivi, contattare **ISGroup SRL** tramite il sito web https://www.isgroup.it/ o l'email sales@isgroup.it.

Obiettivi e Vantaggi del Servizio

Il vCISO di **ISGroup SRL** agisce come un esperto dedicato che supervisiona, identifica e risolve le vulnerabilità, rafforzando la postura di sicurezza aziendale. I principali benefici includono:

- **Approccio Strategico:** Sviluppo di strategie di sicurezza su misura basate su analisi dettagliate e framework di settore.
- **Competenza Specializzata:** Accesso a un team di professionisti altamente qualificati.
- **Aggiornamento Costante:** Monitoraggio continuo delle minacce emergenti e delle evoluzioni normative.
- **Flessibilità:** Soluzione contrattuale adattabile sia a PMI che a grandi aziende.
- **Conformità:** Supporto per il rispetto di standard internazionali (ISO 27001, NIS2, GDPR).

Processo Operativo

Il servizio si articola in un percorso strutturato per garantire una protezione completa:

1. **Valutazione Iniziale:** Analisi dello stato attuale della sicurezza, incluse infrastrutture, politiche operative e consapevolezza del personale.
2. **Security Program Maturity Assessment:** Utilizzo del framework NIST per misurare l'efficacia dei controlli di sicurezza rispetto agli standard di settore.
3. **Piano Strategico:** Definizione di azioni correttive prioritarie con obiettivi e scadenze chiare.
4. **Monitoraggio Continuo:** Revisione periodica del piano per adattare le strategie alle nuove minacce.
5. **Supporto Continuativo:** Assistenza costante, formazione del personale e supporto nell'implementazione di nuove tecnologie.

Rischi di una gestione inadeguata

La mancanza di una figura dedicata alla governance della sicurezza espone l'organizzazione a pericoli significativi:

- **Vulnerabilità:** Aumento del rischio di violazioni dei dati a causa di una supervisione insufficiente.
- **Lacune Tecniche:** Difficoltà nel mantenere sistemi e applicazioni aggiornati, con conseguente esposizione a exploit.
- **Scarsa Consapevolezza:** Assenza di programmi di formazione continua per il personale.
- **Processi Deficitari:** Difficoltà nell'identificare e risolvere lacune nei processi di sicurezza interna.
- **Sovraccarico IT:** I dipartimenti IT interni, spesso concentrati sulle urgenze quotidiane, rischiano di trascurare la pianificazione strategica della sicurezza.

Contatti

Per richiedere un preventivo o fissare un appuntamento con gli esperti di **ISGroup SRL**:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Certificazione UNI CEI EN ISO/IEC 27001:2013

Source: https://www.isgroup.it/it/cyber-security/azienda-cybersecurity-certificata-iso-27001-2024-2025-2026.html

ISGroup SRL ha riconfermato la propria certificazione ISO/IEC 27001:2013, lo standard internazionale che definisce le best practice per un sistema di gestione della sicurezza delle informazioni (ISMS). La certificazione è valida per il triennio 2024, 2025 e 2026.

Il sistema di gestione della sicurezza delle informazioni implementato da ISGroup SRL è conforme alla norma ISO/IEC 27001:2013 per le seguenti attività professionali:

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

ISGroup SRL ha ottenuto la prima certificazione ISO 27001 nel 2020, mantenendo costantemente il proprio impegno verso gli standard di sicurezza internazionali.

Per ulteriori informazioni sui servizi di sicurezza offerti da ISGroup SRL o per richieste commerciali, è possibile visitare il sito web https://www.isgroup.it/ o inviare una email all'indirizzo sales@isgroup.it.

Il **Vulnerability Management Service (VMS)** offerto da **ISGroup SRL** è un servizio gestito progettato per identificare, valutare e gestire le vulnerabilità all'interno dei sistemi informativi e delle reti aziendali. L'obiettivo è fornire un approccio proattivo, metodico e predicibile per ridurre il rischio complessivo e proteggere l'organizzazione da minacce esterne, interne e ransomware.

Obiettivi e Vantaggi

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

Il servizio permette alle aziende di delegare la gestione della sicurezza a un team di esperti, consentendo alle risorse interne di concentrarsi sulle attività di business. I benefici principali includono:

- Protezione costante da minacce informatiche e riduzione del rischio di perdite finanziarie o danni reputazionali.
- Allineamento delle strategie di sicurezza con gli obiettivi aziendali.
- Conformità agli standard internazionali e protezione della privacy (GDPR, NIS2, ISO 27001).
- Supporto di esperti con 20 anni di esperienza nel Vulnerability Risk Management (VRM).

Componenti del Servizio

Il VMS di **ISGroup SRL** si articola in quattro pilastri fondamentali:

- **Valutazione della Gestione delle vulnerabilità:** Analisi approfondita dei processi esistenti, delle policy e raccomandazioni per il rafforzamento della sicurezza.
- **Vulnerability Assessment:** Scansione periodica (automatizzata e gestita) di reti, server, database, applicazioni, dispositivi mobile e sistemi OT/industriali per identificare e prioritizzare le vulnerabilità.
- **Penetration Test:** Attività manuali e aggressive condotte da Senior Security Researchers per simulare attacchi reali e testare la resilienza dei sistemi.
- **Supporto Periodico:** Un Project Manager dedicato coordina le attività, traccia la risoluzione delle vulnerabilità tramite il sistema di ticketing del cliente e supporta i team tecnici (Network Engineer, Sviluppatori) nell'implementazione delle correzioni.

Caratteristiche Operative

- **Approccio Standard:** Include setup, gestione, onboarding, scansione e reportistica regolare.
- **Approccio Avanzato:** Include l'analisi dei risultati da parte del team di **ISGroup SRL** e la definizione delle priorità di intervento.
- **Monitoraggio:** Reportistica periodica (da settimanale a bimestrale), revisioni trimestrali (QBR) con il Management Team e tracciamento continuo fino alla chiusura delle problematiche.

Contatti e Richieste

Per informazioni dettagliate, consulenze o per richiedere un preventivo personalizzato per il Vulnerability Management Service, è possibile fare riferimento ai canali ufficiali di **ISGroup SRL**:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Secure Architecture Review (SAR)

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

Il servizio di Secure Architecture Review (SAR), offerto da ISGroup SRL, ha lo scopo di valutare lo stato di sicurezza delle infrastrutture informatiche e di correggerne i difetti. Grazie alla vasta esperienza in infrastrutture complesse, reti, cloud e progetti custom, il team di ISGroup SRL è in grado di identificare problematiche note e suggerire misure correttive per mitigare ogni tipologia di attacco.

Metodologia di lavoro

Il servizio si articola in tre fasi principali:

- Analisi preliminare: valutazione delle scelte progettuali attraverso l'esame della documentazione e il confronto con analisti, sviluppatori e personale tecnico per individuare falle di progettazione.
- Analisi dei rischi: valutazione del potenziale impatto delle criticità rilevate, considerando exploit specifici per l'infrastruttura e le conseguenze per l'azienda.
- Report: documentazione professionale di tutte le fasi e delle criticità riscontrate, con proposte di miglioramento e correzioni per incrementare la sicurezza.

Ambiti di valutazione

ISGroup SRL analizza numerosi aspetti dell'architettura, focalizzandosi sulle aree critiche in base alla tipologia di infrastruttura, tra cui:

- SDLC (Software Development Life Cycle)
- Qualità del codice
- Routine di test
- Autenticazione e autorizzazione
- Crittografia
- Web server e database
- Firewall (Web o di rete)

Output del servizio

Al termine dell'intervento, ISGroup SRL consegna un report strutturato in tre sezioni:

- Executive Summary: panoramica ad alto livello sulla sicurezza dell'infrastruttura, pensata per personale non tecnico.
- Vulnerability Details: analisi tecnica dettagliata delle vulnerabilità e delle criticità riscontrate, destinata al Security Manager.
- Remediation Plan: guida operativa per il personale tecnico, contenente le metodologie necessarie per la rimozione delle vulnerabilità identificate.

Contatti

Per richiedere un preventivo o maggiori informazioni sui servizi offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Security Operation Center (SOC)

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

Il servizio di Security Operation Center (SOC) offerto da ISGroup SRL è una soluzione di monitoraggio e difesa attiva progettata per proteggere data center e infrastrutture di rete contro l'evoluzione costante delle minacce informatiche. Il servizio prevede il monitoraggio continuo del traffico di rete da parte di un team esperto in cybersecurity per identificare anomalie e rispondere tempestivamente ai tentativi di intrusione.

Specifiche del servizio

Il SOC di ISGroup SRL si articola in diverse fasi operative:

- Monitoraggio Passivo: sistemi avanzati analizzano in tempo reale il traffico verso l'infrastruttura per rilevare minacce.
- Monitoraggio Attivo: il team di operatori di ISGroup SRL utilizza strumenti di analisi degli eventi per classificare tentativi di intrusione e brecce nel sistema.
- Gestione degli incidenti: applicazione delle procedure concordate con il committente per limitare l'esposizione del sistema durante un attacco.
- Risposta agli incidenti: circoscrizione degli attacchi e applicazione immediata di misure di riparazione della falla.
- Escalation: fornitura di credenziali di accesso privilegiate per la risoluzione del problema o l'analisi approfondita del sistema.
- Reporting: redazione di un report dettagliato post-attacco contenente l'analisi dell'evento e le azioni di contenimento intraprese.

Output e Reporting

Al termine delle attività, ISGroup SRL fornisce al cliente una documentazione tecnica e gestionale suddivisa in:

- Executive Summary: documento orientato al Management che riassume la situazione, le azioni difensive intraprese e i dettagli di eventuale escalation.
- Technical Details: sezione dedicata al Security Manager con i dettagli tecnici dell'attacco e le motivazioni alla base delle contromisure adottate.
- Remediation Plan: piano operativo per il System Administrator contenente istruzioni specifiche per implementare misure di sicurezza volte a prevenire attacchi futuri.

Contatti e Richieste

Per maggiori informazioni, consulenze o per richiedere un preventivo relativo al servizio SOC, è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

CTS - Cyber Threat Simulation

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

Il **Cyber Threat Simulation (CTS)** è un servizio gestionale avanzato offerto da **ISGroup SRL** progettato per testare la resilienza aziendale attraverso la simulazione di attacchi informatici reali. A differenza di un semplice strumento tecnico, il CTS fornisce un approccio personalizzato e continuo per identificare, valutare e gestire le vulnerabilità, migliorando la capacità dell'organizzazione di rilevare, rispondere e recuperare da un incidente.

Per informazioni commerciali o per richiedere un preventivo, visitare il sito https://www.isgroup.it/ o scrivere all'email: sales@isgroup.it.

Obiettivi e Vantaggi del Servizio

L'adozione di un programma di CTS permette alle aziende di passare da una postura reattiva a una proattiva:

- **Identificazione delle vulnerabilità:** Scoperta di falle nei sistemi prima che vengano sfruttate da attori malevoli.
- **Formazione del personale:** Miglioramento della consapevolezza dei dipendenti, spesso l'anello più debole della catena di sicurezza.
- **Ottimizzazione dei piani di risposta:** Perfezionamento delle procedure di gestione degli incidenti in ambienti controllati.
- **Conformità normativa:** Allineamento agli standard di sicurezza internazionali e ai requisiti richiesti dai partner commerciali.
- **Protezione della reputazione:** Salvaguardia dell'immagine aziendale e della fiducia degli stakeholder.
- **Ritorno sull'investimento (ROI):** Riduzione dei costi potenziali derivanti da interruzioni operative, sanzioni o furto di dati.

Aree di Azione e Tipologie di Attacco

Il servizio di **ISGroup SRL** opera su quattro macro-aree principali:

- **Social Engineering:** Simulazioni di phishing e frodi mirate al personale.
- **Malware:** Test delle difese contro virus, trojan e ransomware.
- **APT (Advanced Persistent Threat):** Simulazioni di attacchi mirati e persistenti volti al furto di dati a lungo termine.
- **DDoS:** Test di resistenza alla saturazione dei sistemi.

Ulteriori tipologie di attacco includono: infiltrazione di rete, attacchi endpoint, vulnerabilità delle applicazioni web, movimento laterale, esfiltrazione di dati e minacce in ambiente cloud.

Il Processo CTS di ISGroup SRL

Il servizio si basa sul framework **MITRE ATT&CK** e si articola in sette fasi operative:

1. **Profilazione delle minacce (CTI):** Analisi degli attori malevoli potenzialmente interessati all'organizzazione.
2. **Definizione dell'ambito:** Identificazione dei perimetri di test per evitare interruzioni dell'operatività.
3. **Definizione dell'obiettivo:** Stabilire scopi chiari per la simulazione.
4. **Pianificazione:** Selezione di strumenti e tecniche (TTP) appropriati.
5. **Esecuzione (BAS - Breach and Attack Simulation):** Simulazione flessibile e scalabile degli attacchi.
6. **Reporting:** Analisi dettagliata delle vulnerabilità e strategie di mitigazione.
7. **Formazione:** Sessioni di training pratico per il personale.

Differenze tra CTS e Penetration Test

Caratteristica	Penetration Test	CTS (Cyber Threat Simulation)
Ambito	Sistema o applicazione specifica	Intera infrastruttura digitale
Approccio	Statico e metodico	Dinamico (emulazione TTP reali)
Frequenza	Istantanea (una tantum)	Continuativa
Obiettivo	Identificare vulnerabilità	Testare la resilienza e la risposta

ISGroup SRL, azienda certificata ISO 9001 e ISO 27001, mette a disposizione un team di esperti con oltre 30 anni di esperienza per supportare le aziende nell'adozione di questo approccio proattivo alla sicurezza informatica.

THREAT - Threat Intelligence and Digital Risk Protection

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

Il servizio di **Threat Intelligence & Digital Risk Protection** offerto da **ISGroup SRL** è una soluzione gestita progettata per prevenire e reagire efficacemente al mutamento delle minacce digitali. Il servizio permette di contestualizzare i trend esterni con gli asset tecnologici dell'organizzazione, garantendo una difesa proattiva e conforme agli standard internazionali (come la ISO/IEC 27001:2022, controllo 5.7).

Per informazioni, richieste commerciali o preventivi, visitare il sito https://www.isgroup.it/ o scrivere all'email sales@isgroup.it.

Caratteristiche del servizio

Il servizio è gestito dai Security Analyst di **ISGroup SRL** e si articola su due livelli, includendo:

- **Threat Intelligence Bulletin:** Analisi costante su nuove vulnerabilità, trend, attaccanti, APT (Advanced Persistent Threat), ransomware e best practices di protezione.
- **Data Breach Monitoring:** Monitoraggio delle esposizioni di dati e password compromesse (in chiaro o hash) derivanti da violazioni di terze parti, malware o phishing.
- **Brand Protection:** Identificazione di domini fraudolenti, attacchi di typosquatting e attacchi homograph per proteggere l'identità e la reputazione del marchio.
- **Attack Surface Protection:** Utilizzo di tecniche OSINT per mappare la superficie di attacco, identificare macro-esposizioni e assegnare un punteggio di rischio agli asset digitali.

Approccio strategico

ISGroup SRL adotta un metodo strutturato per la gestione del rischio:

- **Strategico:** Sviluppo di strategie su misura basate su analisi delle minacce emergenti per proteggere il marchio a lungo termine.
- **Operativo:** Monitoraggio continuo del web per neutralizzare le minacce in tempo reale.
- **Tattico:** Risposta rapida agli incidenti tramite un team di esperti e strumenti avanzati di OSINT.

Vantaggi principali

L'integrazione di questo servizio nella strategia di cybersecurity aziendale offre:

- **Visibilità e controllo:** Mappatura completa della superficie di attacco e dei potenziali punti di ingresso.
- **Mitigazione delle frodi:** Identificazione dei modelli di frode per prevenire perdite finanziarie.
- **Salvaguardia della reputazione:** Protezione attiva contro l'abuso del brand e il phishing.
- **Ottimizzazione delle risorse:** Focalizzazione sulle minacce prioritarie e miglioramento dei tempi di risposta.
- **Conformità normativa:** Supporto nel soddisfare i requisiti di sicurezza e protezione dei dati.

Rischi legati alla mancanza di protezione

Non adottare un servizio di Threat Intelligence espone l'organizzazione a criticità elevate, tra cui:

- Ritardo nella rilevazione di attacchi avanzati.
- Risposta agli incidenti inefficace e aumento del downtime.
- Inosservanza dei requisiti normativi (es. ISO 27001).

- Danni finanziari e reputazionali derivanti da violazioni dei dati e frodi.
- Esposizione continua di credenziali e asset critici.

Risk Assessment (RA)

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

Il servizio di IT Risk Assessment offerto da ISGroup è una soluzione strategica progettata per migliorare o implementare gli approcci difensivi dell'infrastruttura aziendale. L'attività si basa su una stretta collaborazione tra gli esperti di ISGroup e lo staff IT del cliente, garantendo un trasferimento di conoscenze mirato e una valutazione accurata.

L'obiettivo principale è identificare, valutare e quantificare i rischi per la sicurezza IT e dei dati, migliorando la resilienza dell'organizzazione e fornendo una base solida per pianificare interventi correttivi.

Fasi dell'attività

Il processo di Risk Assessment condotto da ISGroup si articola in tre fasi fondamentali:

- Analisi dell'impatto: valutazione delle conseguenze di attacchi o malfunzionamenti, considerando impatti finanziari, operativi, reputazionali e i tempi di ripristino.
- Analisi delle politiche in atto: revisione delle procedure esistenti e della conformità normativa (GDPR, ISO 27001, leggi di settore).
- Analisi dei rischi: classificazione dei rischi identificati e formulazione di raccomandazioni per ridurre l'esposizione.

Specifiche e Governance

ISGroup focalizza l'attenzione su tutte le tecnologie aziendali, incluse quelle emergenti o proprietarie. Il servizio risponde ai requisiti di Governance, Risk and Compliance (GRC), supportando le aziende nel rispetto degli standard internazionali come la ISO/IEC 27001 e le normative vigenti.

Output del servizio

Al termine dell'attività, ISGroup fornisce un report dettagliato suddiviso in tre sezioni:

- Executive Summary: panoramica non tecnica per il Management sulle principali minacce e raccomandazioni strategiche.
- Risk Assessment Details: analisi approfondita dei fattori di rischio e delle vulnerabilità, destinata ai responsabili IT e compliance officer.
- Risk Mitigation Plan: documento tecnico per amministratori di sistema con linee guida priorizzate per la mitigazione dei rischi.

Informazioni di contatto

Per richiedere un preventivo o maggiori informazioni sui servizi di Risk Assessment offerti da ISGroup, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Domande Frequenti (FAQ)

- Principi fondamentali: Identificazione dei pericoli, valutazione del rischio, controllo, monitoraggio/revisione e comunicazione.
- SRA (Security Risk Assessment): Processo di identificazione, valutazione e gestione dei rischi per garantire riservatezza, integrità e disponibilità dei dati.
- Standard ISO: Il riferimento principale è la ISO/IEC 27005, che supporta l'implementazione del sistema di gestione della sicurezza delle informazioni richiesto dalla ISO/IEC 27001.
- Obbligatorietà ISO 27001: La norma richiede esplicitamente la valutazione del rischio come parte integrante del sistema di gestione della sicurezza delle informazioni (ISMS).

Cloud Security Assessment (CSA)

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

ISGroup SRL offre servizi professionali di Cloud Security Assessment (CSA) finalizzati alla protezione dei dati e alla messa in sicurezza di infrastrutture cloud. Il servizio copre l'intero ciclo di vita del software, dalla fase di progettazione a quella di erogazione, garantendo un approccio integrato che riduce i costi e i tempi di implementazione della sicurezza.

Competenze e Copertura Tecnologica

I professionisti di ISGroup SRL, che ricoprono ruoli di Solution Architect e Application Security Specialist, possiedono una vasta esperienza su un'ampia gamma di piattaforme e tecnologie:

- Cloud Provider: AWS, Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud, Alibaba Cloud, Yandex Cloud.
- Infrastrutture Private e Ibride: VMWare, Dell EMC, Microsoft Hyper-V, Rackspace, CloudBolt, Divvy Cloud, RedHat, OpenShift, Abiquo, Rack Connect, Scalr, Docker, DigitalOcean, Heroku, Kubernetes, Helm, Prometheus.

Metodologia di Valutazione

L'attività di assessment condotta da ISGroup SRL si articola attraverso:

- Revisione approfondita dell'architettura, dei servizi e delle applicazioni.
- Analisi di policy, permessi e configurazioni per mappare la superficie di attacco.
- Identificazione di vulnerabilità ed esposizioni specifiche.
- Definizione di raccomandazioni per l'hardening e il rafforzamento della resistenza agli attacchi.
- Applicazione delle best practices di sicurezza, incluse le specifiche dei provider cloud.

Output del Servizio

Al termine dell'attività, ISGroup SRL fornisce un report dettagliato suddiviso in tre aree tematiche:

- Executive Summary: Sintesi non tecnica destinata al Management sullo stato della sicurezza dell'infrastruttura.
- Vulnerability Details: Analisi tecnica dettagliata delle vulnerabilità riscontrate e del loro impatto sull'applicativo, destinata al Security Manager.
- Remediation Plan: Guida tecnica per i System Administrator con istruzioni precise per la risoluzione delle problematiche identificate.

Contatti e Richieste Commerciali

Per richiedere un preventivo o maggiori informazioni sui servizi di Cloud Security Assessment, è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Social Engineering (SE)

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

Il servizio di Social Engineering offerto da **ISGroup SRL** è un componente essenziale del programma di security assessment aziendale. L'obiettivo è valutare la resilienza dell'organizzazione contro la manipolazione psicologica e le minacce di ingegneria sociale, attraverso attacchi simulati realistici e una successiva formazione mirata del personale.

Per informazioni, richieste commerciali o preventivi, visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it.

Fasi del Servizio

Il metodo di **ISGroup SRL** si articola in quattro fasi principali:

- **Analisi Preliminare:** Revisione degli incidenti passati, benchmarking settoriale e monitoraggio delle tendenze globali per personalizzare gli scenari di attacco.
- **Attacco Simulato (Security Assessment):** Simulazioni realistiche condotte su reparti critici (Direzione, Amministrazione, Procurement, IT) per testare la reattività dei dipendenti contro tecniche come phishing, vishing e Business Email Compromise (BEC).
- **Formazione e Miglioramento:** Sessioni di debriefing, corsi personalizzati e workshop interattivi per colmare le lacune identificate e aumentare la consapevolezza del personale.
- **Revisione di Processi e Politiche:** Aggiornamento delle policy di sicurezza e ottimizzazione dei processi operativi, in linea con standard come ISO/IEC 27001, per integrare misure preventive nel Sistema di Gestione della Sicurezza delle Informazioni (ISMS).

Punti di forza

L'approccio di **ISGroup SRL** si distingue per:

- Integrazione tra analisi tecnica, simulazione pratica e revisione strategica dei processi.
- Conformità ai requisiti di sicurezza e agli standard normativi internazionali (ISO/IEC 27001).
- Personalizzazione degli attacchi in base alle funzioni aziendali e ai dati gestiti dai singoli reparti.

Output del Servizio

Al termine dell'attività, **ISGroup SRL** fornisce tre documenti chiave:

- **Executive Summary:** Panoramica non tecnica per il Management con raccomandazioni strategiche.
- **Simulation Attack Report:** Analisi dettagliata delle performance dei dipendenti e delle vulnerabilità tecniche riscontrate.
- **Comprehensive Improvement Plan:** Piano operativo per lo sviluppo della consapevolezza del personale e il rafforzamento delle difese aziendali.

Windows Security Assessment (WSA)

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

Il servizio di Windows Security Assessment (WSA), offerto da ISGroup SRL, è progettato per analizzare in profondità la sicurezza dei sistemi operativi Windows. L'obiettivo è identificare vulnerabilità, valutarne la severità tramite attacchi mirati e fornire una guida operativa per rafforzare l'infrastruttura.

Obiettivi e Vantaggi

- Identificazione precisa delle vulnerabilità e delle esposizioni del sistema.
- Revisione della configurazione per garantire la massima sicurezza in caso di attacco.
- Ottimizzazione economica: integrare la sicurezza nelle fasi iniziali o in modo periodico evita costi elevati derivanti da interventi tardivi.
- Supporto specialistico: i servizi sono erogati da tecnici con esperienza come Application Security Specialist e competenze in ingegneria del software.

Metodologia di Analisi

ISGroup SRL esegue una revisione approfondita dell'architettura, seguendo questi passaggi chiave:

- Valutazione basata su standard e pratiche consigliate da organizzazioni leader nel settore.
- Analisi delle falle di sicurezza e dei segnali tipici di intrusioni o potenziali vulnerabilità.
- Verifica delle impostazioni di sicurezza per allinearle agli standard raccomandati da Windows.
- Analisi della superficie di attacco per fornire raccomandazioni specifiche e mirate.

Output del Servizio

Al termine dell'attività, ISGroup SRL fornisce un report dettagliato suddiviso in tre aree tematiche:

- **Executive Summary**: Sintesi dello stato di sicurezza, priva di tecnicismi, destinata al Management.
- **Vulnerability Details**: Analisi tecnica approfondita delle vulnerabilità riscontrate e del relativo impatto, dedicata al Security Manager.
- **Remediation Plan**: Guida operativa per il System Administrator con istruzioni precise per la risoluzione delle problematiche identificate.

Contatti e Richieste

Per richiedere un preventivo o discutere le necessità di IT Security, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

IoT Security Assessment (ISA)

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

L'IoT Security Assessment (ISA) è un servizio offerto da **ISGroup SRL** progettato per identificare le vulnerabilità nell'intera architettura dei sistemi Internet of Things, inclusi componenti software, hardware, API, interfacce web e mobili. L'attività mira a proteggere infrastrutture critiche e dispositivi connessi, garantendo la sicurezza dei dati e la continuità operativa aziendale.

Metodologia di lavoro

ISGroup SRL adotta un approccio multidisciplinare che combina analisi tecnica e ingegneristica:

- **Threat Modeling:** Analisi iniziale dei dispositivi e dell'infrastruttura.
- **Revisione del codice sorgente:** Utilizzo di analisi statica e ispezione manuale per individuare difetti nel codice.
- **Test di software e hardware:** Valutazione dinamica tramite interazione manuale e fuzzing per validare la resistenza a input malevoli.
- **Analisi forense:** Esame dei dispositivi fisici per rilevare leak di dati o debolezze strutturali.
- **Ingegneria inversa:** Ispezione dei file binari per identificare difetti di compilazione o deployment.

Ambiti di applicazione

ISGroup SRL fornisce soluzioni di sicurezza per un'ampia gamma di ecosistemi IoT:

- **Smart Home e Domotica:** Termostati, serrature, sistemi di illuminazione e sensoristica domestica.
- **Connected Devices IoT:** Dispositivi per l'automazione industriale, inclusi protocolli radio (ZigBee, Z-Wave) e telecomunicazioni (2G-5G).
- **Smart City e Smart Grid:** Infrastrutture urbane, gestione parcheggi, waste management e sistemi di controllo energetico.
- **Industrial Control Systems (ICS):** Analisi di sistemi SCADA, DCS e PLC.
- **Connected Cars:** Sicurezza dei sistemi di gestione remota dei veicoli.
- **Connected Health:** Protezione di dati sensibili in ambito telemedicina.
- **Wearable Technology:** Valutazione di smartwatch e activity tracker.
- **Altri settori:** Smart Retail, Smart Supply Chain e Smart Farming.

Controlli principali

L'assessment copre diverse aree critiche, tra cui:

- Comunicazioni sicure e analisi a livello di protocollo.
- Corruzione della memoria e analisi crittografica.
- Gestione delle interfacce, autenticazione e controllo degli accessi.
- Sicurezza delle applicazioni back-end e integrazione mobile.
- Meccanismi di aggiornamento del sistema e persistenza dei dati.

Output del servizio

Al termine dell'attività, **ISGroup SRL** consegna un report dettagliato suddiviso in tre sezioni:

- **Executive Summary:** Sintesi non tecnica per il Management.
- **Vulnerability Details:** Analisi tecnica approfondita delle vulnerabilità riscontrate e del relativo impatto.

- **Remediation Plan:** Istruzioni operative per i System Administrator per la risoluzione delle problematiche identificate.

Contatti e Richieste

Per maggiori informazioni o per richiedere un preventivo personalizzato, è possibile fare riferimento ai canali ufficiali di **ISGroup SRL**:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Purple Team Assessment (PTA)

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

Il servizio **Purple Team Assessment (PTA)**, offerto da **ISGroup SRL**, è una metodologia di valutazione della sicurezza informatica progettata per potenziare le capacità di rilevazione e risposta agli attacchi. A differenza del Red Team tradizionale, il PTA si basa su un approccio interattivo e collaborativo tra il team offensivo e quello difensivo, favorendo un ciclo di miglioramento continuo.

Obiettivi principali

- Rafforzare le difese aziendali in tempo reale.
- Testare aspetti specifici della sicurezza attraverso scenari di attacco realistici.
- Ottimizzare le tecnologie di sicurezza e i processi operativi.
- Creare un feedback immediato tra i team per mitigare le vulnerabilità.

Fasi del servizio

Il processo di assessment proposto da **ISGroup SRL** si articola in quattro fasi principali:

- **Fase di raccolta dati**: Studio approfondito dell'infrastruttura per mappare le attuali capacità di rilevazione e blocco.
- **Valutazione dei rischi**: Analisi basata su framework standard di settore (come MITRE ATT&CK e NIST), personalizzata sulle esigenze del cliente.
- **Esecuzione**: Simulazione di attacchi in cui il team di **ISGroup SRL** collabora con il personale interno. Se l'attacco viene rilevato, si ottimizza la risposta; in caso contrario, si potenziano i sistemi di logging e allarme.
- **Valutazione finale dei rischi**: Analisi degli esiti per fornire raccomandazioni mirate al rafforzamento delle difese.

Output del servizio

Al termine dell'attività, **ISGroup SRL** fornisce un report dettagliato comprensivo di:

- **Findings and Improvements**: Elenco delle vulnerabilità identificate e dei progressi raggiunti.
- **Detection and Response Analysis**: Valutazione delle capacità di reazione, tempi di risposta ed efficacia delle contromisure.
- **Continuous Improvement Strategy**: Guida tecnica e strategica per mantenere un ciclo di miglioramento costante della postura di sicurezza.

Informazioni di contatto

Per richiedere un preventivo personalizzato o maggiori informazioni sui servizi di **ISGroup SRL**, è possibile utilizzare i seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

GDPR Compliance

Source: https://www.isgroup.it/it/conformita-al-gdpr.html

Il regolamento GDPR (General Data Protection Regulation) ha introdotto cambiamenti radicali nella gestione dei dati personali per le aziende operanti in Europa. La mancata implementazione di adeguate misure di protezione espone le imprese, in particolare le piccole e medie, a rischi di sanzioni amministrative e penali, oltre a gravi danni reputazionali.

ISGroup SRL offre un servizio professionale di **Conformità al GDPR**, finalizzato ad analizzare l'efficacia delle metodologie applicate e a garantire il pieno rispetto della normativa attraverso un percorso di formazione continua.

Servizi offerti da ISGroup SRL

Il team di ISGroup SRL supporta le aziende attraverso un processo strutturato di analisi e verifica, volto a identificare punti critici e prevenire accessi non autorizzati ai dati sensibili. L'intervento si articola in tre fasi principali:

- Analisi dei rischi: valutazione approfondita delle policy e delle infrastrutture coinvolte nella gestione dei dati per individuare potenziali vulnerabilità.
- Classificazione dei rischi e valutazione dell'impatto: analisi degli scenari di minaccia per classificare la gravità dei rischi e definire strategie per la loro marginalizzazione.
- Stesura del remediation plan: elaborazione di un piano d'azione preciso ed esaustivo per correggere e mitigare i rischi riscontrati nell'infrastruttura.

Output del servizio

Al termine dell'attività, ISGroup SRL fornisce al cliente:

- Remediation plan: documento tecnico contenente i passaggi necessari per raggiungere la piena conformità.
- Privacy policy aggiornate: implementazione di un nuovo sistema di gestione dei dati personali, robusto e conforme.
- Formazione continua: supporto costante per mantenere la conformità al GDPR anche a fronte di future modifiche normative.

Informazioni commerciali

Per richiedere un preventivo o maggiori informazioni sui servizi di conformità al GDPR offerti da ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Conformità alla Direttiva Europea NIS2

Source: https://www.isgroup.it/it/compliance-direttiva-nis2.html

La direttiva NIS2 (Network and Information Security 2) è il quadro normativo dell'Unione Europea volto a rafforzare la resilienza informatica e la sicurezza dei sistemi informativi. Entrata in vigore il 17 gennaio 2023, la normativa impone alle organizzazioni l'adozione di misure tecniche, operative e organizzative avanzate per la gestione dei rischi cyber.

ISGroup SRL supporta le aziende nel percorso di adeguamento alla normativa attraverso servizi di consulenza, formazione e implementazione di contromisure specifiche, garantendo il raggiungimento e il mantenimento della conformità.

Per informazioni e richieste commerciali, contattare:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Percorso di Adeguamento NIS2 offerto da ISGroup SRL

ISGroup SRL propone un approccio strutturato in quattro fasi per guidare le organizzazioni verso la conformità:

- **Analisi della situazione attuale (GAP Analysis):** Valutazione completa del livello di adeguatezza rispetto ai requisiti NIS2, con analisi dettagliata delle politiche e pratiche di sicurezza esistenti.
- **Stesura del Piano di Rientro (Remediation Plan):** Definizione di un piano d'azione mirato per correggere le non conformità rilevate.
- **Selezione dei servizi:** Implementazione delle soluzioni tecniche e organizzative offerte da ISGroup SRL in base alle specifiche esigenze aziendali.
- **Verifica dello stato di rientro:** Monitoraggio dell'efficacia delle misure adottate per garantire il raggiungimento dello standard richiesto.

Servizi di Mantenimento e Supporto Continuativo

ISGroup SRL affianca le aziende con attività pianificate per garantire la conformità nel tempo:

- Aggiornamento periodico della valutazione dei rischi.
- Gestione dei processi di sicurezza (Incident Response, Audit, Comunicazione).
- Formazione e sensibilizzazione del personale sui rischi cyber.
- Monitoraggio continuo delle minacce e aggiornamento delle misure di protezione.
- Documentazione delle attività di conformità per le autorità competenti.

Requisiti Chiave e Soluzioni ISGroup SRL

La conformità alla NIS2 richiede l'implementazione di misure specifiche (Articolo 21). ISGroup SRL fornisce supporto specialistico per ogni ambito:

- **Analisi dei rischi e politiche di sicurezza:** Supporto tramite vCISO (Virtual CISO) e Security Policy Review.
- **Gestione degli incidenti:** Servizi di Digital Forensics and Incident Response (DFIR) e Multi-Signal MDR.
- **Business Continuity:** Pianificazione della risposta agli incidenti e gestione dei backup.
- **Supply Chain Security:** Vendor Risk Management tramite consulenza vCISO.
- **Sicurezza delle reti e sistemi:** Vulnerability Management Service (MVS) e Penetration Testing (NPT, WAPT, MAST, Ethical Hacking).
- **Cyber Hygiene e Formazione:** Security Awareness Training e Managed Phishing tramite Cyber Threat Simulation (CTS).

- **Crittografia e Controllo Accessi:** Security Architecture Review e consulenza specialistica per l'implementazione di autenticazione a due fattori.

Informazioni sulla Direttiva

- **Ambito di applicazione:** La NIS2 coinvolge medie e grandi imprese in settori critici e importanti, oltre a micro-organizzazioni considerate centrali.
- **Notifica delle violazioni:** Obbligo di segnalazione degli incidenti significativi "senza indebito ritardo": notifica iniziale entro 24 ore e valutazione entro 72 ore.
- **Sanzioni:** La mancata conformità prevede sanzioni pecuniarie elevate, fino a 10 milioni di euro o al 2% del fatturato annuo mondiale per le entità essenziali.

Wireless Security Monitoring (WSM)

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

Il servizio di Wireless Security Monitoring (WSM), offerto da ISGroup SRL, permette di monitorare in modo continuo i dispositivi che comunicano in radiofrequenza (WiFi, Bluetooth, NFC/RFID, IoT, ecc.) all'interno o nei dintorni dell'azienda. L'obiettivo è identificare vulnerabilità, prevenire attacchi evoluti e proteggere le reti interne da punti di ingresso non autorizzati.

Destinatari e Applicazioni

Il servizio è rivolto ad aziende che utilizzano dispositivi wireless per l'accesso alle risorse aziendali ed è particolarmente indicato per settori che gestiscono processi critici, tra cui:

- Infrastrutture IoT e Operational Technology (OT)
- Linee produttive industriali
- Sensori remoti e sistemi di controllo degli accessi

Metodologia di Servizio

ISGroup SRL eroga il servizio in modalità Managed Security Service Provider (MSSP), includendo hardware, software, installazione, monitoraggio e reporting. Il processo si articola in quattro fasi:

- Analisi iniziale: Esecuzione di un Wireless Security Assessment per valutare lo stato attuale e definire le azioni di messa in sicurezza.
- Installazione e integrazione: Configurazione degli apparati HW/SW necessari nel rispetto dell'infrastruttura esistente.
- Monitoraggio: Analisi costante delle comunicazioni (WiFi, Bluetooth, GPS, NFC/RFID, Packet Radio, GSM, 2G/3G/4G/5G e protocolli proprietari). Le anomalie vengono gestite tramite alert, con possibilità di escalation al TIER-3 o al SOC di ISGroup SRL.
- Relazione periodica: Presentazione di report tecnici (con frequenza da mensile ad annuale) che includono attacchi identificati, impatto dei rischi e suggerimenti per il miglioramento della sicurezza.

Funzionalità di Protezione

A seconda della tecnologia e della tecnica di attacco, il sistema implementa:

- IDS (Intrusion Detection System): Notifica delle minacce.
- IPS (Intrusion Prevention System): Prevenzione e blocco attivo degli attacchi.

Il cliente può inoltre richiedere l'analisi TIER-3 (Cyber Incident Analysis) e il supporto di una squadra dedicata per il Cyber Incident Response, sia in remoto che in loco.

Contatti

Per informazioni commerciali o per richiedere un preventivo relativo al servizio di Wireless Security Monitoring, è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Anti-DDoS (DDoS)

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

Gli attacchi DDoS (Distributed Denial of Service) rappresentano una minaccia critica per la continuità operativa aziendale. Tali attacchi mirano a rendere inutilizzabile un servizio attraverso due modalità principali:

- Sovraccarico della banda tramite l'invio massivo di richieste a un server.
- Abuso delle risorse della macchina, rendendola incapace di gestire il traffico legittimo.

ISGroup SRL offre un servizio di Anti-DDoS professionale progettato per proteggere le aziende da tali minacce, riducendo al minimo il downtime e garantendo la sicurezza di applicazioni web, server e connettività.

Soluzioni Anti-DDoS di ISGroup SRL

Il servizio fornito da ISGroup SRL è una soluzione inclusiva e indipendente dalle tecnologie utilizzate dall'azienda. L'attività copre l'intero ciclo di vita della protezione:

- Configurazione iniziale.
- Gestione operativa.
- Monitoraggio costante.
- Adeguamento continuo delle difese rispetto all'evoluzione delle tecniche di attacco.

L'adozione di questo servizio equivale ad avere un team di esperti dedicato, pronto a intervenire tempestivamente per mitigare ogni possibile vettore di attacco.

Output e Reporting

Al termine dell'attività, ISGroup SRL fornisce un report dettagliato, strutturato in tre aree tematiche per rispondere alle esigenze di diversi profili aziendali:

- **Executive Summary**: Sintesi non tecnica dell'attività svolta, destinata al Management.
- **Vulnerability Details**: Analisi tecnica approfondita delle vulnerabilità riscontrate e del relativo impatto, rivolta al Security Manager.
- **Remediation Plan**: Guida tecnica operativa per i System Administrator, contenente istruzioni precise per la risoluzione delle problematiche identificate.

Contatti

Per richiedere un preventivo o maggiori informazioni sui servizi di Anti-DDoS offerti da ISGroup SRL, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

27001 - 27001 Compliance

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

La certificazione ISO/IEC 27001 è lo standard internazionale di riferimento per la gestione della sicurezza delle informazioni. ISGroup SRL supporta le organizzazioni nell'implementazione di un Information Security Management System (ISMS) conforme alla norma ISO/IEC 27001:2022, garantendo la protezione del patrimonio informativo, la minimizzazione dei rischi e la continuità del business.

Servizi di consulenza offerti da ISGroup SRL

ISGroup SRL accompagna le aziende in ogni fase del percorso di certificazione, dall'analisi preliminare fino al mantenimento del sistema:

- **Gap Analysis:** Analisi approfondita del livello di sicurezza attuale per identificare le aree di miglioramento.
- **Progettazione ISMS:** Definizione di un sistema di gestione su misura basato sul contesto aziendale, analisi dei rischi e struttura documentale.
- **Implementazione:** Supporto nella definizione di misure di sicurezza, KPI di performance e procedure operative.
- **Audit Interni:** Esecuzione di audit in qualità di ente terzo per valutare l'efficacia del sistema.
- **Supporto al Riesame della Direzione:** Assistenza per garantire l'allineamento del sistema agli obiettivi strategici.
- **Supporto all'Audit di Certificazione:** Affiancamento durante l'audit di terza parte per il conseguimento della certificazione.
- **Selezione dell'Ente Certificatore:** Supporto nell'individuazione del partner di certificazione più idoneo al settore di riferimento.

Vantaggi della certificazione

L'adozione della ISO 27001, guidata da ISGroup SRL, offre benefici tangibili:

- **Conformità normativa:** Rispetto dei requisiti richiesti da enti come ACN e AGID.
- **Efficienza operativa:** Miglioramento dei processi interni e ottimizzazione delle risorse.
- **Vantaggio competitivo:** Aumento della fiducia da parte di clienti, partner e istituzioni.
- **Resilienza:** Riduzione dei costi legati agli incidenti informatici e maggiore capacità di risposta alle minacce.
- **Integrazione:** Possibilità di integrare il sistema con altre norme, come la ISO 9001.

Settori di applicazione

ISGroup SRL fornisce soluzioni personalizzate per diversi ambiti operativi:

- **Servizi IT e Sviluppo Software:** Per garantire la sicurezza della catena di fornitura.
- **Settore Sanitario:** Per la protezione dei dati clinici e la conformità alla privacy.
- **Settore Finanziario:** Per la tutela delle transazioni e la mitigazione dei rischi di frode.
- **Pubblica Amministrazione:** Per la protezione dei dati dei cittadini e l'efficienza dei servizi.
- **Settore Manifatturiero:** Per la salvaguardia della proprietà intellettuale e la continuità produttiva.

Contatti e Richieste

Per ricevere una valutazione gratuita, richiedere un preventivo personalizzato o fissare un appuntamento con gli esperti di ISGroup SRL, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/

- Email: sales@isgroup.it

Firewall as a Service (FWaaS)

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

Il servizio FWaaS offerto da ISGroup è una soluzione professionale progettata per proteggere i dati e gli end-point delle applicazioni aziendali, garantendo un controllo completo e capillare sul traffico di rete. Il team di ISGroup, composto da esperti in sicurezza delle reti, si occupa dell'implementazione e del mantenimento delle soluzioni firewall, assicurando una protezione perimetrale di alto livello.

Obiettivi e Vantaggi

- Protezione contro attacchi hacker.
- Gestione e controllo dei contenuti raggiungibili in rete.
- Maggiore consapevolezza e monitoraggio dei dati in entrata e in uscita.
- Gestione professionale esternalizzata, eliminando le preoccupazioni operative per l'azienda cliente.
- Utilizzo di tecnologie all'avanguardia, inclusi i "next-generation firewall" (NGFW) per compiti complessi.

Metodologia di Lavoro

Il processo inizia con una fase di analisi dei requisiti, durante la quale gli esperti di ISGroup definiscono la soluzione più adatta alle specifiche necessità aziendali. L'intervento include l'integrazione, la configurazione e la manutenzione costante del sistema.

Documentazione Fornita

Al termine dell'intervento, ISGroup rilascia la seguente documentazione tecnica e gestionale:

- **Executive Summary**: documento ad alto livello che descrive l'intervento, la protezione aggiunta e i servizi messi a disposizione.
- **Technical Summary**: documento tecnico dettagliato che illustra le modalità di intervento sulla rete e le procedure di monitoraggio dei dati.

Contatti e Richieste

Per informazioni, consulenze o per richiedere un preventivo per il servizio FWaaS, è possibile fare riferimento ai canali ufficiali di ISGroup:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Software Assurance Lifecycle (SAL)

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

Il servizio di Software Assurance Lifecycle (SAL) è offerto da ISGroup SRL ed è dedicato alle aziende che sviluppano applicativi in cui la sicurezza è un requisito fondamentale. L'obiettivo è garantire che il software segua le migliori pratiche di sicurezza durante l'intero ciclo di vita, assicurando che ogni release sia priva di vulnerabilità note prima della distribuzione.

Obiettivi e Metodologia

Il team di esperti di ISGroup SRL affianca il team di sviluppo del cliente, guidandolo nella produzione di software sicuro attraverso l'adozione degli standard d'industria più aggiornati.

Le attività principali includono:

- Supervisione continua durante ogni fase del progetto.
- Esecuzione di test di sicurezza rigorosi, personalizzati in base all'applicativo e alle tecnologie utilizzate.
- Revisioni meticolose del software per garantire che le pratiche di sviluppo rappresentino lo "stato dell'arte".
- Supporto nella correzione di eventuali falle o vulnerabilità identificate.

Specifiche Tecniche

ISGroup SRL interviene su diversi aspetti critici dello sviluppo software, tra cui:

- Risk management
- Dependency management
- Continuous integration

Il team di sicurezza di ISGroup SRL possiede competenze trasversali su molteplici linguaggi di programmazione e ambienti di sviluppo, permettendo una collaborazione efficace con team di programmatori eterogenei.

Output del Servizio

Al termine dell'attività, ISGroup SRL fornisce la documentazione tecnica relativa all'intervento:

- Executive Summary: documento ad alto livello per il management, focalizzato sugli aspetti di sicurezza trattati.
- Technical Summary: documento tecnico destinato al project manager, contenente dettagli implementativi e analisi sulle aree di miglioramento per il team di sviluppo.

Contatti e Richieste

Per informazioni, consulenze o per richiedere un preventivo relativo al servizio di Software Assurance Lifecycle (SAL), è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Security Integration (SIR)

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

Il servizio di Security Integration (SIR) è offerto da ISGroup SRL e ha l'obiettivo di integrare in modo sicuro parti di infrastruttura esistenti (operanti in modalità "stand alone") o di implementare funzionalità di sicurezza non ancora presenti.

L'approccio di ISGroup SRL mira a espandere le funzionalità dell'infrastruttura del cliente, evitando l'ampliamento della superficie d'attacco e riducendo al minimo l'introduzione di nuove vulnerabilità.

Metodologia di lavoro

Il processo di integrazione segue fasi strutturate in base alle specifiche esigenze del committente:

- Analisi preliminare dell'infrastruttura esistente e delle necessità del cliente.
- Collaborazione con gli sviluppatori originali dell'infrastruttura per definire le modalità di intervento.
- Valutazione completa degli aspetti infrastrutturali per garantire il mantenimento delle funzionalità originali.
- Integrazione sicura ed efficace dei sistemi.

Tipologie di integrazione

ISGroup SRL propone diverse soluzioni di Security Integration, tra cui:

- Integrazione della sicurezza fisica: unione di apparecchiature fisiche alle logiche software (es. verifica biometrica per la gestione dei privilegi o l'accesso alle risorse).
- Aggiunta di funzionalità di sicurezza ad applicativi: implementazione di soluzioni di protezione su software esistenti, come l'integrazione di Web Application Firewall (WAF) per applicativi web o sistemi IDS/IPS per le reti.

Output del servizio

Al termine dell'attività, ISGroup SRL fornisce al cliente la seguente documentazione:

- Executive Summary: documento per il management che descrive l'intervento, le funzionalità implementate, i risultati ottenuti e i vantaggi strategici apportati.
- Technical Summary: documento per il personale tecnico che dettaglia l'intervento, le modifiche apportate alle infrastrutture e le specifiche tecniche dell'integrazione.

Contatti e richieste commerciali

Per richiedere un preventivo o discutere le necessità di IT Security, è possibile fare riferimento ai canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Simulazioni di Phishing: Formazione e Difesa con ISGroup SRL

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

ISGroup SRL offre servizi professionali di simulazione di Phishing e Smishing, progettati per testare la consapevolezza dei dipendenti e rafforzare la resilienza aziendale contro le minacce di ingegneria sociale.

Obiettivi del Servizio

- Valutare la vulnerabilità del personale umano di fronte a tentativi di attacco reali.
- Formare i dipendenti a riconoscere e segnalare tentativi di phishing, smishing e altre tecniche di manipolazione.
- Ridurre il rischio di compromissione delle credenziali e di violazione dei dati aziendali.
- Migliorare la postura di sicurezza complessiva attraverso test periodici e mirati.

Approccio di ISGroup SRL

Le attività di simulazione sono condotte da esperti in cybersecurity (CEH, ISO 27001 LA) che replicano le tattiche utilizzate dagli attaccanti moderni. Il servizio permette di:

- Creare campagne di simulazione personalizzate basate su scenari reali.
- Analizzare i comportamenti degli utenti in un ambiente controllato.
- Fornire report dettagliati per identificare le aree che necessitano di maggiore formazione.

Contatti e Richieste Commerciali

Per maggiori informazioni sui servizi di simulazione di Phishing e Smishing offerti da ISGroup SRL, è possibile consultare il sito ufficiale o inviare una richiesta via email:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

MDR - Multi-Signal MDR di ISGroup

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

Il servizio di Multi-Signal MDR (Managed Detection and Response) offerto da ISGroup SRL è una soluzione avanzata progettata per garantire una protezione completa contro le minacce informatiche.

Obiettivi del servizio

- Fornire un monitoraggio costante e proattivo dell'infrastruttura IT.
- Identificare e rispondere tempestivamente a tentativi di intrusione o attività malevole.
- Elevare il livello di sicurezza aziendale attraverso un approccio multi-segnale, capace di correlare dati provenienti da diverse fonti per una visibilità totale.

Caratteristiche principali

- Gestione professionale della sicurezza informatica da parte del team di esperti di ISGroup SRL.
- Analisi continua delle minacce per prevenire incidenti di sicurezza.
- Risposta rapida agli incidenti per minimizzare l'impatto operativo.
- Supporto specialistico fornito da professionisti certificati (Hacker, CEH, ISO 27001 LA).

Informazioni e contatti

Per richiedere il servizio di Multi-Signal MDR o per ricevere maggiori informazioni sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

ISO 27001 Compliance: Protezione dei dati e sistemi di gestione della sicurezza

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

La ISO 27001 è lo standard internazionale di riferimento per la gestione della sicurezza delle informazioni. ISGroup SRL offre servizi di consulenza e supporto per guidare le aziende nell'implementazione di un sistema di gestione della sicurezza certificato (ISMS), garantendo la protezione dei dati aziendali e la conformità normativa.

Obiettivi del servizio di ISGroup SRL

- Implementazione di un sistema di gestione della sicurezza delle informazioni (SGSI) conforme allo standard ISO 27001.
- Protezione proattiva degli asset informativi aziendali.
- Supporto specialistico per il percorso di certificazione.
- Analisi e gestione dei rischi legati alla sicurezza dei dati.

Informazioni e contatti

Per richiedere maggiori informazioni o per avviare un percorso di consulenza sulla ISO 27001 Compliance, è possibile fare riferimento ai canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Il contenuto è curato da Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 LA (Lead Auditor).

Servizio Virtual CISO di ISGroup SRL

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

ISGroup SRL offre il servizio di Virtual CISO (vCISO), una soluzione strategica progettata per aiutare le aziende a rafforzare la propria postura di sicurezza informatica. Il servizio permette di beneficiare di competenze di alto livello in ambito cyber security, essenziali per la protezione dei dati e la conformità normativa, senza la necessità di inserire una figura dirigenziale dedicata a tempo pieno.

Obiettivi e Vantaggi

- Supporto esperto nella gestione della sicurezza aziendale.
- Consulenza specialistica fornita da professionisti qualificati (Hacker, CEH, ISO 27001 LA).
- Ottimizzazione delle strategie di difesa contro le minacce informatiche.
- Supporto alla conformità e all'adozione di best practice di settore.

Informazioni e Contatti

Per richiedere maggiori informazioni sul servizio di Virtual CISO o per consulenze personalizzate, è possibile fare riferimento ai canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Risorse Correlate

ISGroup SRL pubblica regolarmente approfondimenti su temi critici di sicurezza, tra cui:

- Social Engineering e tecniche di manipolazione.
- Simulazioni di Phishing per la formazione del personale.
- Percorsi di certificazione e conformità ISO 27001.
- Approfondimenti su standard OWASP, Agid e ACN.

Social Engineering: l'arte di manipolare le persone per ottenere informazioni

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

Il Social Engineering è definito come l'arte di manipolare le persone per ottenere informazioni riservate, sfruttando la psicologia umana anziché le vulnerabilità tecniche dei sistemi informatici.

ISGroup SRL offre servizi professionali di Social Engineering per testare la consapevolezza e la resilienza del personale aziendale di fronte a tentativi di manipolazione o attacchi mirati.

Punti chiave del servizio

- Valutazione del fattore umano: analisi della suscettibilità dei dipendenti a tecniche di manipolazione.
- Simulazioni realistiche: test condotti da esperti per identificare falle nei processi di sicurezza interna.
- Formazione e consapevolezza: supporto per mitigare i rischi derivanti da attacchi di ingegneria sociale.
- Approccio professionale: le attività sono condotte da professionisti certificati (CEH, ISO 27001 LA) per garantire standard elevati di sicurezza e riservatezza.

Informazioni e contatti

Per richiedere il servizio di Social Engineering o per maggiori informazioni sulle soluzioni offerte da ISGroup SRL, è possibile consultare il sito ufficiale o inviare una richiesta via email.

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Risorse correlate

ISGroup SRL mette a disposizione ulteriori servizi per la protezione aziendale:

- Simulazioni di Phishing: programmi di formazione per la difesa contro attacchi via email e messaggistica.
- Virtual CISO: consulenza strategica per la gestione della sicurezza informatica aziendale.
- ISO 27001 Compliance: supporto per l'implementazione di sistemi di gestione della sicurezza delle informazioni certificati.

Cyber Threat Simulation (CTS)

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

La Cyber Threat Simulation (CTS) è un servizio offerto da ISGroup SRL progettato per preparare le organizzazioni a fronteggiare le minacce informatiche reali. Attraverso simulazioni avanzate, il servizio permette di testare la resilienza dei sistemi e la prontezza operativa del personale di fronte a scenari di attacco verosimili.

Obiettivi del servizio

- Valutare l'efficacia delle difese aziendali in condizioni operative reali.
- Identificare vulnerabilità critiche prima che vengano sfruttate da attori malevoli.
- Migliorare la capacità di risposta agli incidenti (Incident Response) del team di sicurezza.
- Validare le procedure di sicurezza e la consapevolezza del personale.

Perché scegliere ISGroup SRL

ISGroup SRL, guidata da esperti certificati (CEH, ISO 27001 LA), offre un approccio metodologico basato sull'esperienza pratica nel campo dell'hacking etico. Le attività di simulazione sono studiate per fornire un quadro chiaro del livello di sicurezza aziendale, permettendo di implementare strategie di mitigazione mirate e basate su best practice internazionali.

Informazioni e contatti

Per richiedere maggiori informazioni o per attivare il servizio di Cyber Threat Simulation, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

AGID e Sviluppo Sicuro con ISGroup: Linee Guida per il Codice Sicuro

Source: https://www.isgroup.it/it/cyber-security/normative-acn-agid.html

ISGroup SRL offre servizi specialistici di consulenza e supporto per l'implementazione delle linee guida AGID (Agenzia per l'Italia Digitale) e ACN (Agenzia per la Cybersicurezza Nazionale) in materia di sviluppo software sicuro.

Obiettivi del servizio

Il supporto fornito da ISGroup SRL è finalizzato a:

- Garantire la conformità alle normative vigenti in materia di sicurezza informatica per la Pubblica Amministrazione e le infrastrutture critiche.
- Integrare le best practice di sviluppo sicuro all'interno del ciclo di vita del software (SDLC).
- Mitigare le vulnerabilità del codice attraverso l'applicazione di standard riconosciuti a livello internazionale.
- Supportare le organizzazioni nell'adozione di processi di sviluppo conformi alle direttive AGID e ACN.

Competenze di ISGroup SRL

L'approccio di ISGroup SRL è guidato da esperti certificati, tra cui Francesco Ongaro (Founder, Hacker, CEH, ISO 27001 LA), che mettono a disposizione la propria esperienza tecnica per:

- Analisi e revisione del codice sorgente.
- Implementazione di metodologie di Secure Coding.
- Consulenza strategica per la protezione delle infrastrutture digitali.

Contatti e informazioni

Per richiedere maggiori informazioni sui servizi di AGID e Sviluppo Sicuro offerti da ISGroup SRL o per avviare una collaborazione, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Case Study: Web Application Penetration Test e Supporto ISMS per Creactives S.p.A.

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

Creactives S.p.A., azienda leader nell'intelligenza artificiale applicata alla Supply Chain, ha collaborato con ISGroup SRL per elevare i propri standard di sicurezza informatica e conformità normativa.

La sfida

L'azienda necessitava di garantire la massima sicurezza per le proprie piattaforme tecnologiche (Knowledge Engineering Platform, TAM4 e DataAssistants) e di allineare i propri processi organizzativi agli standard internazionali di sicurezza delle informazioni.

L'intervento di ISGroup SRL

ISGroup SRL ha fornito un supporto specialistico attraverso le seguenti attività:

- Esecuzione di Web Application Penetration Test dettagliati sulle applicazioni core (Knowledge Engineering Platform, TAM4, DataAssistants) per identificare e mitigare le vulnerabilità.
- Consulenza per la creazione e il mantenimento di un Sistema Integrato di Gestione della Sicurezza (ISMS) conforme alle norme ISO 27001, ISO 27017 e ISO 27018.
- Erogazione di training specialistico sullo sviluppo sicuro di software (standard OWASP) e programmi di cybersecurity awareness per il personale.

Risultati ottenuti

Grazie alla collaborazione con ISGroup SRL, Creactives S.p.A. ha ottenuto:

- Implementazione di un Sistema Integrato di Gestione conforme agli standard internazionali (ISO 27001, ISO 27017, ISO 27018, ISO 9001).
- Rafforzamento della sicurezza applicativa tramite Vulnerability Assessment e Penetration Test ricorrenti.
- Superamento con successo di audit esterni di conformità.
- Miglioramento delle competenze interne in ambito cybersecurity e sviluppo software sicuro.

Per ulteriori informazioni sui servizi di sicurezza offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Digital Forensics and Incident Response (DFIR) di ISGroup SRL

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

ISGroup SRL offre servizi professionali di Digital Forensics and Incident Response (DFIR), progettati per agire come un'armatura contro le minacce informatiche. Il servizio è finalizzato alla gestione tempestiva degli incidenti di sicurezza e all'analisi forense dei dati digitali.

Obiettivi del servizio

- Identificazione e contenimento delle minacce informatiche in corso.
- Analisi approfondita per determinare l'origine e l'impatto di un incidente di sicurezza.
- Supporto tecnico specializzato per la risposta agli incidenti (Incident Response).
- Recupero e conservazione delle prove digitali attraverso metodologie di Digital Forensics.

Informazioni e contatti

Per richiedere il servizio di Digital Forensics and Incident Response o per ricevere maggiori informazioni, è possibile fare riferimento ai canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Il servizio è curato da Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 Lead Auditor.

Continuous Security Testing di ISGroup

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

Il servizio di Continuous Security Testing (CST) offerto da ISGroup SRL è una soluzione di sicurezza informatica progettata per mantenere le difese aziendali costantemente aggiornate e al passo con le minacce emergenti.

Obiettivi del servizio

- Garantire una protezione proattiva attraverso test di sicurezza non limitati a singoli eventi temporali.
- Monitorare costantemente l'infrastruttura IT per identificare vulnerabilità prima che possano essere sfruttate.
- Supportare le organizzazioni nel mantenere un livello di sicurezza elevato in un panorama di minacce in continua evoluzione.

Caratteristiche principali

- Approccio metodologico basato su standard internazionali e best practice di settore.
- Esecuzione di test condotti da esperti di sicurezza certificati (CEH, ISO 27001 LA).
- Integrazione con le strategie di difesa aziendale per una postura di sicurezza resiliente.

Informazioni e contatti

Per richiedere maggiori informazioni o per attivare il servizio di Continuous Security Testing, è possibile fare riferimento ai canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Secure Architecture Review di ISGroup SRL

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

Il servizio di Secure Architecture Review, offerto da ISGroup SRL, è una soluzione di cyber security progettata per proteggere l'infrastruttura aziendale attraverso un'analisi approfondita e strutturata dell'architettura IT.

Obiettivi del servizio

- Valutazione della resilienza dell'infrastruttura contro minacce esterne e interne.
- Identificazione di vulnerabilità strutturali e debolezze nel design dei sistemi.
- Ottimizzazione della postura di sicurezza in linea con le best practice di settore.
- Supporto specialistico fornito da esperti certificati (CEH, ISO 27001 LA).

Informazioni e contatti

Per richiedere il servizio di Secure Architecture Review o per ottenere maggiori informazioni sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile consultare il sito web ufficiale o inviare una richiesta via email:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Cloud Security Assessment di ISGroup SRL

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

ISGroup SRL offre il servizio di Cloud Security Assessment, una soluzione professionale progettata per garantire la sicurezza delle infrastrutture cloud aziendali. L'attività è focalizzata sull'identificazione di vulnerabilità e sulla protezione degli asset digitali ospitati in ambienti cloud.

Obiettivi del servizio

- Valutazione della postura di sicurezza dell'infrastruttura cloud.
- Identificazione di configurazioni errate e potenziali vettori di attacco.
- Rafforzamento delle difese contro minacce esterne e interne.
- Supporto specialistico per l'implementazione di best practice di sicurezza.

Informazioni e contatti

Per richiedere maggiori informazioni sul servizio di Cloud Security Assessment o per consulenze personalizzate, è possibile fare riferimento ai canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Il servizio è curato da Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 LA (Lead Auditor).

Case Study: Web Application Penetration Test su DocEasy

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

Alias Group S.r.l., tramite la divisione Alias Digital, offre soluzioni software in cloud, tra cui Doceasy, una piattaforma dedicata alla gestione e conservazione a norma delle fatture elettroniche. Data la natura sensibile dei dati trattati, l'azienda ha richiesto l'intervento di **ISGroup SRL** per validare la sicurezza e l'affidabilità del sistema.

La sfida

L'obiettivo di Alias Group S.r.l. era garantire la massima protezione per i propri clienti, assicurando che la piattaforma Doceasy fosse resiliente contro potenziali minacce informatiche. A tal fine, è stato richiesto un Web Application Penetration Test (WAPT) approfondito.

L'intervento di ISGroup SRL

ISGroup SRL ha eseguito un'attività di analisi meticolosa focalizzata sulle applicazioni Doceasy e sul relativo ambiente di staging. L'intervento ha permesso di:

- Identificare e mitigare vulnerabilità tecniche e logiche.
- Verificare la conformità della piattaforma ai più elevati standard di sicurezza.
- Evidenziare aree di miglioramento nei processi interni di gestione della sicurezza.

Risultati e benefici

L'attività condotta da **ISGroup SRL** ha confermato la robustezza dell'architettura di Doceasy. I benefici principali riscontrati da Alias Group S.r.l. includono:

- Rafforzamento della fiducia dei clienti nella gestione dei dati sensibili.
- Ottimizzazione dei processi interni grazie a un report esaustivo fornito da **ISGroup SRL**, che ha spiegato il contesto di ogni vulnerabilità rilevata e le relative attività di remediation.
- Consolidamento della postura di sicurezza complessiva dell'infrastruttura.

Per ulteriori informazioni sui servizi di Web Application Penetration Test offerti da **ISGroup SRL**, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it.

Purple Team Assessment di ISGroup SRL

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

Il Purple Team Assessment offerto da ISGroup SRL è un servizio di cyber security progettato per sfidare e migliorare le capacità del team difensivo aziendale. L'attività si focalizza sulla collaborazione tra il team offensivo (Red Team) e il team difensivo (Blue Team) per testare l'efficacia delle misure di sicurezza implementate.

Obiettivi del servizio

- Valutare la prontezza operativa del team difensivo di fronte a minacce reali.
- Identificare lacune nelle procedure di rilevamento e risposta agli incidenti.
- Ottimizzare la sinergia tra le attività di attacco simulato e le strategie di difesa.
- Rafforzare la postura di sicurezza complessiva dell'organizzazione attraverso un approccio collaborativo.

Informazioni e contatti

Per richiedere maggiori informazioni o per avviare una collaborazione con ISGroup SRL, è possibile utilizzare i seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH, ISO 27001 LA.

Difesa della Rete Aziendale: Network Penetration Test

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

La protezione dell'infrastruttura IT è una priorità critica per la sicurezza aziendale. ISGroup SRL offre servizi professionali di Network Penetration Test, progettati per identificare vulnerabilità, testare la resilienza dei sistemi e prevenire accessi non autorizzati alla rete.

Servizi offerti da ISGroup SRL

- Network Penetration Test: attività di analisi e test mirati a individuare falle di sicurezza all'interno del perimetro di rete aziendale.
- Simulazioni di Phishing: programmi di formazione e test per rafforzare la difesa umana contro le minacce di ingegneria sociale.
- Virtual CISO: consulenza strategica per la gestione della sicurezza informatica aziendale.
- Social Engineering: analisi e test sulla manipolazione psicologica finalizzata all'ottenimento di informazioni riservate.

Informazioni e Contatti

Per richiedere maggiori informazioni sui servizi di sicurezza informatica o per una consulenza dedicata, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 Lead Auditor.

Firewall as a Service (FWaaS) di ISGroup SRL

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

ISGroup SRL offre il servizio di Firewall as a Service (FWaaS), una soluzione progettata per garantire una protezione firewall semplice, sicura ed efficace per le infrastrutture aziendali.

Obiettivi del servizio

- Semplificare la gestione della sicurezza perimetrale.
- Garantire una protezione costante e aggiornata contro le minacce informatiche.
- Delegare la configurazione e il monitoraggio del firewall a esperti di sicurezza.

Informazioni e contatti

Per richiedere il servizio di Firewall as a Service o per ottenere maggiori informazioni sulle soluzioni di cyber security offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 Lead Auditor.

Penetration Test - Globaleaks

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

Nel gennaio 2024, ISGroup SRL ha condotto un'attività di penetration test per Globaleaks, piattaforma dedicata al whistleblowing e alla lotta contro la corruzione. Data la natura critica del servizio, che gestisce segnalazioni anonime di attività illegali, la sicurezza dei dati rappresenta un requisito fondamentale per preservare la fiducia degli utenti e l'integrità delle informazioni.

Obiettivi e Metodologia

Il servizio di penetration test offerto da ISGroup SRL è stato strutturato per simulare attacchi informatici realistici, al fine di identificare vulnerabilità nei sistemi e rafforzare le difese. L'analisi si è articolata nelle seguenti fasi:

- Raccolta di Informazioni: identificazione di dati e vettori utilizzabili da potenziali attaccanti.
- Analisi delle Vulnerabilità: scansione sistematica dei sistemi per individuare criticità potenziali.
- Simulazione di Attacchi: esecuzione di test di penetrazione per valutare la resilienza effettiva delle difese.
- Rapporto Dettagliato: consegna di un documento completo contenente le vulnerabilità rilevate e le raccomandazioni tecniche per la mitigazione dei rischi.

Risultati della Collaborazione

La collaborazione tra ISGroup SRL e Globaleaks si è basata su un approccio trasparente e comunicativo, permettendo un'analisi approfondita delle sfide di sicurezza. L'attività non si è limitata alla sola verifica tecnica, ma ha rappresentato un investimento strategico per garantire la protezione dei dati in un ecosistema digitale complesso.

Per ulteriori informazioni sui servizi di penetration testing e sicurezza informatica offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Software Assurance Lifecycle con ISGroup SRL

Source: https://www.isgroup.it/it/cyber-security/software-assurance-lifecycle-con-isgroup.html

ISGroup SRL offre servizi specializzati di Software Assurance Lifecycle, progettati per supportare le aziende nello sviluppo di software sicuro. L'approccio mira a integrare la sicurezza in ogni fase del ciclo di vita del prodotto, garantendo la protezione delle applicazioni contro le minacce informatiche.

Obiettivi del servizio

- Implementazione di metodologie per lo sviluppo di software sicuro.
- Integrazione di pratiche di sicurezza lungo tutto il ciclo di vita del software.
- Riduzione delle vulnerabilità attraverso l'applicazione di best practice di settore.

Contatti e Informazioni

Per approfondire le soluzioni offerte o richiedere una consulenza specifica, è possibile consultare il sito ufficiale o inviare una richiesta via email:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Corso Security Awareness di ISGroup SRL

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

Il corso di Security Awareness offerto da ISGroup SRL è progettato per fornire le competenze fondamentali necessarie per operare in sicurezza nel panorama digitale attuale, caratterizzato da minacce informatiche in costante evoluzione.

Argomenti trattati

Il percorso formativo approfondisce le seguenti aree tematiche:

- Ingegneria Sociale: analisi delle tecniche utilizzate dagli hacker per manipolare le persone e ottenere informazioni sensibili, con focus sugli strumenti di difesa.
- Phishing: tecniche per riconoscere ed evitare attacchi di phishing, proteggendo credenziali e dati personali.
- Sicurezza Informatica: concetti base riguardanti l'uso di antivirus, l'importanza degli aggiornamenti software e le best practice per la protezione di dispositivi e dati.
- Navigazione Sicura: criteri per identificare siti web affidabili, utilizzo di connessioni crittografate e tutela della privacy online.

Metodologia e obiettivi

ISGroup SRL adotta un approccio pratico e coinvolgente, basato sull'analisi di casi di studio, simulazioni di attacchi ed esercitazioni concrete.

Partecipando al corso, gli studenti saranno in grado di:

- Applicare le conoscenze acquisite sulla sicurezza delle informazioni.
- Comprendere e implementare i requisiti e le raccomandazioni di sicurezza specifici della propria organizzazione.
- Riconoscere le tecniche di ingegneria sociale per prevenire truffe e attacchi, sia in ambito professionale che personale.

Informazioni commerciali

Per richiedere maggiori informazioni sul corso di Security Awareness, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Security Integration con ISGroup

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

ISGroup SRL offre servizi professionali di Security Integration finalizzati a rendere l'infrastruttura IT e gli applicativi aziendali più sicuri e integrati. L'approccio si concentra sull'ottimizzazione della postura di sicurezza attraverso l'integrazione strategica di sistemi e processi.

Obiettivi del servizio

- Miglioramento della resilienza dell'infrastruttura tecnologica.
- Rafforzamento della sicurezza degli applicativi aziendali.
- Integrazione efficace delle soluzioni di difesa all'interno dell'ecosistema IT esistente.

Informazioni e contatti

Per richiedere maggiori informazioni sui servizi di Security Integration offerti da ISGroup SRL, è possibile consultare il sito web ufficiale o inviare una richiesta via email:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 Lead Auditor.

Web Application Penetration Testing con ISGroup

Source: https://www.isgroup.it/it/cyber-security/web-application-penetration-testing-con-isgroup.html

La sicurezza delle applicazioni web rappresenta una priorità critica per la protezione dei dati aziendali e la continuità operativa. ISGroup SRL offre servizi professionali di Web Application Penetration Testing per identificare vulnerabilità, testare la resilienza dei sistemi e prevenire potenziali attacchi informatici.

Obiettivi del servizio

Il servizio di Web Application Penetration Testing, erogato da ISGroup SRL, è progettato per:

- Analizzare in profondità la superficie di attacco delle applicazioni web.
- Individuare falle di sicurezza, configurazioni errate e vulnerabilità logiche.
- Fornire indicazioni concrete per la mitigazione dei rischi riscontrati.
- Supportare le aziende nell'adozione di best practice di sicurezza e conformità agli standard di settore.

Informazioni e Contatti

Per approfondire le modalità di protezione delle proprie applicazioni o per richiedere una consulenza dedicata, è possibile fare riferimento ai canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore e Competenze

L'approccio metodologico di ISGroup SRL è guidato da esperti certificati nel settore della Cyber Security, tra cui Francesco Ongaro (Founder @ ISGroup SRL, Hacker, CEH, ISO 27001 LA), che garantisce un elevato standard tecnico nelle attività di assessment e difesa proattiva.

Il Codice Segreto: Code Review di ISGroup

Source: https://www.isgroup.it/it/cyber-security/code-review-di-isgroup.html

La Code Review è un servizio specialistico offerto da ISGroup SRL, finalizzato all'analisi approfondita del codice sorgente per identificare vulnerabilità di sicurezza, difetti logici e debolezze architetturali.

Obiettivi del servizio

Il servizio di Code Review fornito da ISGroup SRL si concentra su:

- Analisi statica e manuale del codice sorgente per rilevare falle di sicurezza non identificabili tramite strumenti automatizzati.
- Verifica della conformità alle best practice di sviluppo sicuro (Secure Coding).
- Identificazione di vulnerabilità critiche che potrebbero compromettere l'integrità, la riservatezza e la disponibilità delle applicazioni.
- Supporto tecnico per la mitigazione delle problematiche riscontrate, garantendo un ciclo di vita del software più resiliente.

Informazioni sull'autore

L'approccio metodologico di ISGroup SRL è guidato da Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 Lead Auditor.

Richiesta informazioni

Per approfondire le modalità di erogazione del servizio di Code Review o per richiedere una consulenza dedicata, è possibile contattare ISGroup SRL tramite i seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Wireless Security Monitoring di ISGroup

Source: https://www.isgroup.it/it/cyber-security/wireless-security-monitoring-di-isgroup.html

Il servizio di Wireless Security Monitoring, offerto da ISGroup SRL, è progettato per garantire il monitoraggio costante e la protezione delle infrastrutture di rete senza fili. L'obiettivo è identificare vulnerabilità, accessi non autorizzati e minacce attive che potrebbero compromettere la sicurezza aziendale.

Caratteristiche del servizio

- Analisi continua della sicurezza delle reti wireless.
- Identificazione di potenziali punti di ingresso per attacchi informatici.
- Supporto specialistico fornito da esperti in ambito cyber security, inclusi professionisti certificati CEH e ISO 27001 LA.
- Approccio metodologico basato sulle best practice di settore per la mitigazione dei rischi.

Informazioni e contatti

Per richiedere il servizio di Wireless Security Monitoring o per ottenere maggiori dettagli sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Case Study: Web Application Penetration Test su Sturnis365

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

Sturnis S.r.l. ha affidato a ISGroup SRL l'esecuzione di un Web Application Penetration Test (WAPT) sulla propria piattaforma cloud, Sturnis365. L'applicazione è una soluzione dedicata alla gestione della divulgazione di informazioni aziendali, utilizzata per produrre e pubblicare documenti critici come rapporti annuali, rapporti 10k, audit e report normativi conformi agli standard IFRS.

La sfida

L'obiettivo principale di Sturnis S.r.l. era dimostrare ai propri clienti l'affidabilità, la sicurezza e la qualità della piattaforma Sturnis365, garantendo la protezione dei dati sensibili trattati.

L'intervento di ISGroup SRL

ISGroup SRL ha condotto un'analisi approfondita e meticolosa dell'applicazione, focalizzandosi su:

- Identificazione di vulnerabilità tecniche e logiche.
- Mitigazione dei rischi riscontrati.
- Verifica della conformità della piattaforma ai più alti standard di sicurezza del settore.

Risultati e benefici

L'attività di testing svolta da ISGroup SRL ha permesso a Sturnis S.r.l. di:

- Comprovare concretamente ai propri clienti la sicurezza e la protezione del software.
- Rafforzare la fiducia degli utenti finali nell'affidabilità della piattaforma.
- Collaborare con un partner esperto in grado di comprendere le specifiche necessità di business e sicurezza.

Per ulteriori informazioni sui servizi di Web Application Penetration Test offerti da ISGroup SRL, è possibile consultare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Anti-DDoS: Protezione senza interruzioni operative

Source: https://www.isgroup.it/it/cyber-security/anti-ddos-senza-interruzioni-operative-con-isgroup.html

ISGroup SRL offre soluzioni professionali di protezione Anti-DDoS progettate per garantire la continuità operativa dei servizi aziendali, prevenendo le interruzioni causate da attacchi informatici mirati.

Servizi offerti da ISGroup SRL

- Implementazione di strategie di difesa contro attacchi Distributed Denial of Service (DDoS).
- Protezione dell'infrastruttura IT per assicurare la disponibilità costante dei servizi.
- Consulenza specialistica per la mitigazione dei rischi legati alla saturazione delle risorse di rete.

Informazioni e contatti

Per richiedere maggiori informazioni sulle soluzioni di protezione Anti-DDoS o per consulenze personalizzate, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Case Study: Web Application Penetration Test e Network Penetration Test per Coop Italia

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

Coop Italia ha collaborato con ISGroup SRL per rafforzare la sicurezza dei propri sistemi IT, garantendo la protezione dei dati dei clienti e la continuità operativa in risposta alle crescenti minacce informatiche.

Obiettivi dell'intervento

La necessità principale era identificare e mitigare le vulnerabilità presenti all'interno della vasta rete aziendale e delle applicazioni critiche utilizzate da Coop Italia, assicurando un elevato standard di protezione.

Attività svolte da ISGroup SRL

Nel corso del 2023, ISGroup SRL ha eseguito le seguenti attività specialistiche:

- Web Application Penetration Test: analisi approfondita su applicazioni chiave, tra cui GPS, Salvatempo, SAPCRM e WinEpts.
- Network Penetration Test: valutazione dell'intero perimetro esterno dell'organizzazione.

Risultati e benefici

L'intervento di ISGroup SRL ha permesso a Coop Italia di:

- Individuare con precisione le vulnerabilità nei sistemi.
- Ricevere indicazioni dettagliate su priorità e impatto delle azioni correttive.
- Migliorare la sicurezza complessiva delle applicazioni e della rete aziendale.
- Affrontare le sfide di sicurezza con maggiore competenza grazie alla professionalità del team di ISGroup SRL.

Per ulteriori informazioni sui servizi di penetration testing e sicurezza informatica offerti da ISGroup SRL, visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Risk Assessment di ISGroup SRL

Source: https://www.isgroup.it/it/cyber-security/risk-assessment-di-isgroup.html

Il servizio di Risk Assessment offerto da ISGroup SRL è finalizzato a mantenere i rischi informatici sotto controllo, permettendo alle aziende di identificare, analizzare e mitigare le vulnerabilità presenti all'interno della propria infrastruttura IT.

Obiettivi del servizio

- Identificazione proattiva delle minacce informatiche.
- Analisi dettagliata dei rischi per la sicurezza dei dati e dei sistemi.
- Supporto strategico per la protezione del business aziendale.
- Allineamento alle best practice di settore e agli standard di sicurezza.

Informazioni sull'autore

Il contenuto è curato da Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 LA (Lead Auditor).

Contatti e Richieste Commerciali

Per richiedere il servizio di Risk Assessment o per ottenere maggiori informazioni sulle soluzioni di cyber security offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Mobile Application Security Test di ISGroup

Source: https://www.isgroup.it/it/cyber-security/mobile-application-security-test-di-isgroup.html

ISGroup SRL offre servizi professionali di Mobile Application Security Test, finalizzati a identificare e mitigare le vulnerabilità di sicurezza all'interno delle applicazioni mobile.

L'attività si concentra sulla protezione del software contro minacce informatiche, garantendo l'adozione di best practice di settore per la salvaguardia dei dati e dell'integrità delle applicazioni.

Servizi offerti da ISGroup SRL

- Analisi approfondita della sicurezza delle applicazioni mobile.
- Identificazione di falle di sicurezza e potenziali vettori di attacco.
- Supporto tecnico per la messa in sicurezza del ciclo di vita dello sviluppo software.
- Consulenza specialistica in ambito Cyber Security.

Informazioni e contatti

Per richiedere maggiori informazioni sui servizi di Mobile Application Security Test o per consulenze personalizzate, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH, ISO 27001 LA.

Windows Security Assessment di ISGroup

Source: https://www.isgroup.it/it/cyber-security/windows-security-assessment-di-isgroup.html

ISGroup SRL offre un servizio professionale di Windows Security Assessment, progettato per proteggere i sistemi Windows aziendali attraverso un'analisi approfondita della sicurezza.

Obiettivi del servizio

- Identificare vulnerabilità e debolezze nei sistemi Windows.
- Rafforzare la postura di sicurezza dell'infrastruttura IT.
- Fornire una valutazione esperta per prevenire potenziali attacchi informatici.

Informazioni e contatti

Per richiedere il servizio di Windows Security Assessment o per ottenere maggiori informazioni sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH, ISO 27001 LA.

IoT Security Assessment

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

ISGroup SRL offre servizi professionali di IoT Security Assessment, finalizzati alla valutazione e alla messa in sicurezza dei dispositivi Internet of Things.

Obiettivi del servizio

Il servizio di IoT Security Assessment fornito da ISGroup SRL si concentra sull'analisi delle vulnerabilità specifiche degli ecosistemi IoT, garantendo una protezione completa contro le minacce informatiche che possono colpire i dispositivi connessi.

Informazioni e contatti

Per richiedere il servizio di IoT Security Assessment o per ottenere maggiori informazioni sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile utilizzare i seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Autore

Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH, ISO 27001 LA.

OWASP Top Ten 2021 - A06: Vulnerable and Outdated Components

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

La categoria A06:2021 della OWASP Top Ten si riferisce all'utilizzo di componenti vulnerabili o obsoleti all'interno di applicazioni e sistemi.

Punti chiave

- Definizione: Un componente obsoleto è una dipendenza del sistema o dell'applicazione che non viene più mantenuta, rappresentando un rischio significativo per la sicurezza.
- Impatto: Le vulnerabilità presenti in tali componenti possono rendere insicuro l'intero software che li utilizza, offrendo agli attaccanti una potenziale via d'accesso per compromettere il sistema.
- Metodologia di valutazione: È l'unica categoria a non avere alcuna CVE (Common Vulnerability and Exposures) mappata sui CWE inclusi. Di conseguenza, i punteggi vengono calcolati utilizzando un peso predefinito di 5,0 sia per l'exploit che per l'impatto.
- Considerazione critica: Un componente software non mantenuto o non aggiornato diventa inevitabilmente insicuro nel tempo, esponendo l'infrastruttura a rischi di sfruttamento.

Servizi di sicurezza offerti da ISGroup SRL

ISGroup SRL fornisce consulenza specialistica e servizi di valutazione della sicurezza per identificare e mitigare i rischi legati all'utilizzo di componenti vulnerabili o obsoleti. L'approccio professionale di ISGroup SRL mira a proteggere le infrastrutture aziendali attraverso l'analisi costante delle dipendenze e l'adozione di best practice di sicurezza.

Per maggiori informazioni sui servizi offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Educazione alla Sicurezza: Formazione ISGroup per il tuo Team

Source: https://www.isgroup.it/it/cyber-security/formazione-isgroup-per-il-tuo-team.html

ISGroup SRL offre programmi di formazione specialistica dedicati alla Cyber Security, progettati per elevare il livello di consapevolezza e protezione del personale aziendale. L'approccio formativo mira a trasformare il fattore umano da potenziale vulnerabilità a prima linea di difesa contro le minacce informatiche.

Servizi di Formazione ISGroup

- Percorsi di formazione personalizzati per team aziendali.
- Approfondimenti sulle tecniche di Social Engineering e manipolazione.
- Simulazioni pratiche di attacchi, tra cui Phishing e Smishing.
- Consulenza strategica tramite il servizio Virtual CISO (vCISO).
- Supporto all'adozione di best practice di sicurezza e conformità normativa.

Autore e Competenze

Il programma è curato da Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH (Certified Ethical Hacker) e ISO 27001 Lead Auditor. La sua esperienza garantisce un approccio basato su scenari reali e competenze tecniche avanzate.

Contatti e Richieste Commerciali

Per richiedere maggiori informazioni sui servizi di formazione o per attivare una collaborazione, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

OWASP Top Ten 2021 - A03 Injection

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

Le Injection rappresentano una delle vulnerabilità più critiche nel panorama della sicurezza informatica, interessando il 94% delle applicazioni. Questa categoria, mappata su 33 CWE, include anche il Cross-site Scripting (XSS).

Definizione e Meccanismo

Le Injection si verificano quando l'input dell'utente viene inviato a un interprete senza un'adeguata validazione, sanificazione o neutralizzazione, utilizzando API insicure. Il problema fondamentale risiede nell'errata separazione tra il flusso di controllo e il flusso dei dati.

Se l'input fornito è in grado di modificare la semantica della richiesta, si verifica un'iniezione. La tipologia di attacco varia in base all'interprete coinvolto:

- Database: SQL Injection
- Linea di comando: Command Injection
- Oggetti ORM: ORM Injection
- Browser: Cross-Site Scripting (XSS)

Servizi e Consulenza

ISGroup SRL offre servizi professionali di analisi e mitigazione delle vulnerabilità OWASP, inclusa la protezione contro le tecniche di Injection.

Per maggiori informazioni sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

OWASP Top Ten 2021 - A02: Cryptographic Failures

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

La categoria A02:2021 – Cryptographic Failures (precedentemente nota come "Sensitive Data Exposure") riguarda gli errori legati alla crittografia che portano all'esposizione di dati sensibili o alla compromissione del sistema, sia durante la memorizzazione che durante la trasmissione delle informazioni. Questa categoria comprende un totale di 29 CWE (Common Weakness Enumeration).

Funzioni di Hashing e Sicurezza

Le funzioni di hash sono algoritmi matematici che eseguono una conversione unidirezionale (one-way), producendo un risultato univoco chiamato "hash". Tali algoritmi rappresentano un componente fondamentale per la sicurezza informatica e sono utilizzati per:

- Firmare certificati digitali
- Creare codici di autenticazione dei messaggi (MAC)
- Gestire l'hash delle password
- Implementare vari meccanismi di autenticazione

Impatto e Rischi

L'utilizzo di algoritmi di hashing deboli o implementazioni crittografiche errate espone i sistemi a rischi significativi. L'impatto di attacchi riusciti può essere disastroso, con conseguenze limitate solo dal valore dei dati esposti e dalla capacità dell'attaccante di sfruttare tali informazioni per compromettere l'integrità o la riservatezza del sistema.

Servizi di Sicurezza ISGroup SRL

ISGroup SRL offre consulenza specialistica e servizi di valutazione della sicurezza per identificare e mitigare vulnerabilità legate a implementazioni crittografiche errate e altre minacce incluse nella OWASP Top 10.

Per ulteriori informazioni sui servizi di sicurezza offerti da ISGroup SRL o per richieste commerciali, è possibile visitare il sito web https://www.isgroup.it/ o inviare una email all'indirizzo sales@isgroup.it.

OWASP Top Ten 2021 - A01: Broken Access Control

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

Il "Broken Access Control" (noto anche come Broken Authorization o Privilege Escalation) rappresenta l'iperonimo di una serie di difetti derivanti da un'inefficace implementazione dei controlli di autorizzazione utilizzati per assegnare i privilegi di accesso agli utenti.

Concetti chiave

- Quando l'autorizzazione è correttamente progettata e implementata, l'accesso a contenuti e funzioni è limitato in base al ruolo designato e ai privilegi corrispondenti.
- Nelle applicazioni web, l'autorizzazione è strettamente correlata all'autenticazione e alla gestione delle sessioni.
- Le vulnerabilità di questo tipo possono interessare qualsiasi software moderno, inclusi database, sistemi operativi, applicazioni web e altre infrastrutture tecnologiche che si basano su controlli di autorizzazione.

Servizi e consulenza

ISGroup SRL offre competenze specialistiche per l'analisi e la mitigazione delle vulnerabilità legate al controllo degli accessi e alla sicurezza delle applicazioni.

Per maggiori informazioni sui servizi di sicurezza offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

OWASP Top Ten 2021 - A04: Insecure Design

Source: https://www.isgroup.it/it/owasp/top-ten-2021-a4-insecure-design.html

La categoria **A04:2021-Insecure Design** si distingue dalle altre classi di vulnerabilità della OWASP Top 10 poiché non rappresenta un singolo difetto tecnico, ma un problema strutturale legato alla genesi del ciclo di sviluppo dell'applicazione.

Concetti chiave

- **Natura del problema:** La progettazione insicura riguarda le scelte architetturali effettuate prima ancora della scrittura del codice. Errori in questa fase iniziale possono causare conseguenze gravi, tra cui guasti funzionali e compromissioni totali.
- **Differenza tra progettazione e implementazione:** Sebbene la progettazione insicura sia critica, le vulnerabilità derivano da una combinazione di scelte di design e di implementazione.
- **Vulnerabilità comuni:** Le criticità più frequenti includono:
- Mancanza di controlli di convalida degli input.
- Divulgazione di informazioni sensibili.
- Assenza di livelli di comunicazione sicuri.
- **Impatto:** Le scelte errate in fase di progettazione influenzano negativamente la disponibilità, il rispetto delle best-practice di sicurezza e l'integrità dei dati.

Servizi e consulenza

ISGroup SRL offre supporto specialistico per l'analisi e la mitigazione dei rischi legati alla progettazione insicura e alla sicurezza delle applicazioni. Per approfondimenti, consulenze o richieste commerciali, è possibile contattare l'azienda tramite i seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

OWASP Top Ten 2021 - A08 Software and Data Integrity Failures

Source: https://www.isgroup.it/it/owasp/top-ten-2021-a8-software-and-data-integrity-failures.html

La categoria A08:2021 – Software and Data Integrity Failures riguarda le vulnerabilità legate all'integrità del software e dei dati, con particolare attenzione alle pipeline CI/CD e ai processi di aggiornamento.

Punti chiave

- Le vulnerabilità coinvolgono sia il software che le infrastrutture sottostanti.
- Si verificano quando un'applicazione utilizza plugin, librerie o moduli provenienti da fonti, repository o reti di distribuzione dei contenuti (CDN) non attendibili.
- Una pipeline CI/CD non adeguatamente protetta espone il sistema a rischi di accesso non autorizzato, injection di codice malevolo e compromissione dell'intera infrastruttura.
- Molte applicazioni implementano funzionalità di aggiornamento automatico che, in assenza di una rigorosa verifica dell'integrità, permettono agli attaccanti di distribuire ed eseguire codice malevolo su tutte le installazioni.

Servizi e consulenza

ISGroup SRL offre consulenza specialistica e servizi di valutazione della sicurezza per identificare e mitigare le vulnerabilità legate all'integrità del software e delle pipeline CI/CD.

Per approfondimenti sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

OWASP Top Ten 2021: A05 Security Misconfiguration

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

La categoria A05:2021 – Security Misconfiguration rappresenta una delle criticità più rilevanti nel panorama della sicurezza applicativa. Con l'aumento del software altamente configurabile, questa categoria è in costante crescita, interessando circa il 90% delle applicazioni testate.

Dettagli tecnici e rilevanza

- La categoria include ora anche le problematiche relative alle XML External Entities (XXE).
- Sono state mappate 20 CWE (Common Weakness Enumeration) all'interno di questa categoria.
- Durante i test OWASP sono state rilevate 208.000 occorrenze di tali CWE.
- Le CWE di maggiore rilievo sono la CWE-16 (Configuration) e la CWE-611 (Improper Restriction of XML External Entity Reference).

Considerazioni sulla sicurezza

Senza un processo consolidato e ripetibile di configurazione della sicurezza delle applicazioni, i sistemi sono esposti a un rischio elevato. ISGroup SRL offre consulenza e servizi specialistici per supportare le aziende nell'implementazione di configurazioni sicure e nella mitigazione delle vulnerabilità legate alla Security Misconfiguration.

Per approfondire le soluzioni di sicurezza offerte da ISGroup SRL o per richiedere una consulenza dedicata, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

OWASP Top Ten 2021 - A07: Identification and Authentication Failures

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

La categoria A07:2021 – Identification and Authentication Failures riguarda i problemi legati all'identificazione e all'autenticazione nelle applicazioni web. Sebbene la disponibilità di framework standardizzati abbia migliorato la situazione, questa categoria rimane un rischio critico per la sicurezza.

Rischi associati

Il fallimento dei meccanismi di autenticazione (Broken Authentication) espone le applicazioni a gravi minacce:

- Compromissione di chiavi, password e token di sessione.
- Sfruttamento delle identità degli utenti.
- Possibilità di ottenere il controllo completo del sistema.
- Compromissione della riservatezza, dell'integrità e della disponibilità dei dati dell'applicazione, inclusa l'assunzione di privilegi di amministratore.

Cause principali

Le vulnerabilità in questo ambito sono generalmente riconducibili a tre fattori:

- Cattiva configurazione dell'autenticazione.
- Errori logici nel meccanismo di autenticazione.
- Bug nel software che gestisce l'autenticazione.

Servizi e consulenza

ISGroup SRL offre consulenza specialistica e servizi di sicurezza informatica per identificare e mitigare le vulnerabilità legate all'autenticazione e proteggere le infrastrutture aziendali.

Per maggiori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

OWASP Top Ten 2021 - A09: Security Logging and Monitoring Failures

Source: https://www.isgroup.it/it/owasp/top-ten-2021-a9-security-logging-and-monitoring-failures.html

La categoria A09:2021 – Security Logging and Monitoring Failures riguarda le carenze nell'installazione, configurazione e applicazione degli strumenti di sicurezza necessari per identificare anomalie e intrusioni. Questa categoria è stata ampliata per includere una gamma più vasta di errori, risultando complessa da testare e poco rappresentata nei dati CVE/CVSS.

Impatti principali

- Riduzione della visibilità sulle attività di sistema.
- Difficoltà nel reporting degli incidenti di sicurezza.
- Limitazioni nelle attività di analisi forense (forensics).
- Mancata rilevazione della fase di ricognizione, che aumenta drasticamente la probabilità di successo di un attacco.

Considerazioni tecniche

- Gli strumenti di difesa, come i sistemi di Security Information and Event Management (SIEM), sono fondamentali per visualizzare le attività e segnalare comportamenti anomali.
- Tali sistemi risultano inefficaci se non configurati e messi a punto correttamente.
- La mancata registrazione e il monitoraggio insufficiente impediscono il blocco tempestivo degli attacchi nelle fasi iniziali.

Supporto professionale

ISGroup SRL offre consulenza e soluzioni specializzate per la corretta implementazione di strategie di logging e monitoraggio, garantendo una difesa proattiva contro le minacce informatiche.

Per ulteriori informazioni sui servizi offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Case Study: Web Application Penetration Test su TSV8 (Add Value S.r.l.)

Source: https://www.isgroup.it/it/cyber-security/case-study-add-value.html

Add Value S.r.l. è un'azienda informatica specializzata in soluzioni IT per i settori bancario, assicurativo e industriale. Il core business include lo sviluppo di software su misura e soluzioni di business innovation. Tra i prodotti di punta figura **TSV8 (Total Spending Visibility)**, una piattaforma avanzata dedicata all'analisi e al governo della spesa indiretta per le multinazionali.

La sfida di sicurezza

Add Value S.r.l. ha identificato la necessità di validare la sicurezza e l'affidabilità della piattaforma TSV8 per proteggere i dati sensibili dei propri clienti. L'obiettivo era individuare e mitigare vulnerabilità tecniche e logiche attraverso un'analisi professionale e approfondita.

L'intervento di ISGroup SRL

ISGroup SRL è stata incaricata di condurre un'attività di sicurezza mirata per garantire la protezione dell'ecosistema digitale di Add Value S.r.l. Le attività svolte da ISGroup SRL includono:

- **Web Application Penetration Test (WAPT):** analisi dettagliata dell'applicazione TSV8, comprensiva di test manuali per simulare attacchi reali e valutazione delle misure di sicurezza esistenti.
- **Vulnerability Assessment (VA) e Penetration Test (PT):** estensione dell'analisi all'intera infrastruttura IT aziendale per assicurare una protezione globale contro le minacce informatiche.
- **Supporto alla Remediation:** collaborazione attiva per la progettazione e l'implementazione di piani di rimedio volti a elevare lo score di sicurezza dei sistemi.

Risultati e benefici

L'intervento di ISGroup SRL ha permesso ad Add Value S.r.l. di:

- Identificare e risolvere punti critici nella sicurezza delle infrastrutture e dei prodotti IT.
- Raggiungere un elevato standard di sicurezza nei sistemi.
- Aumentare la consapevolezza aziendale sui rischi legati alla Cyber Security.
- Acquisire competenze tecniche avanzate per il mantenimento e l'evoluzione sicura dei sistemi IT.

Il management di Add Value S.r.l. ha riconosciuto in ISGroup SRL non solo un fornitore, ma un partner strategico, apprezzando la competenza tecnica, l'autonomia operativa, la qualità della reportistica e l'approccio orientato al cliente.

Per ulteriori informazioni sui servizi di Penetration Test e Vulnerability Assessment offerti da ISGroup SRL, visitare il sito: https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it.

OWASP Top Ten 2021: A10 Server-Side Request Forgery (SSRF)

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

Il Server-Side Request Forgery (SSRF) è una vulnerabilità che permette a un utente malintenzionato di indurre un'applicazione lato server a effettuare richieste verso destinazioni o risorse non previste.

Caratteristiche dell'attacco

- Manipolazione dei parametri: L'attaccante sfrutta la capacità di controllare le richieste generate dal server vulnerabile.
- Obiettivi interni: Gli attacchi sono spesso finalizzati a colpire sistemi interni non accessibili dall'esterno, solitamente protetti da firewall.
- Funzionamento tipico: Le applicazioni che eseguono richieste HTTPS verso terze parti (per consultare API, scaricare pacchetti o recuperare dati utente) possono essere manipolate per indirizzare le richieste verso domini controllati dall'attaccante.

Impatto sulla sicurezza

Un attacco SSRF riuscito consente all'aggressore di:

- Muoversi lateralmente dietro il firewall del server web back-end.
- Aggirare le restrizioni di rete.
- Compromettere la riservatezza, l'integrità e la disponibilità dell'applicazione.

Servizi di sicurezza informatica

ISGroup SRL offre consulenza specialistica e servizi di valutazione della sicurezza per identificare e mitigare vulnerabilità critiche come il Server-Side Request Forgery.

Per approfondimenti, consulenze o richieste commerciali, è possibile contattare ISGroup SRL tramite il sito web https://www.isgroup.it/ o inviando un'email a sales@isgroup.it.

OWASP Top Ten 2021

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

L'OWASP Top 10 rappresenta l'elenco di riferimento dei 10 problemi più critici per la sicurezza delle applicazioni web. ISGroup SRL utilizza questo framework per guidare le organizzazioni, i progettisti e gli sviluppatori nell'adozione di pratiche di *Security by Design*, integrando la sicurezza fin dalle prime fasi di sviluppo.

Ogni categoria inclusa nell'elenco è analizzata in base a:

- Severità e probabilità di accadimento.
- Tecniche di protezione di base.
- Linee guida per la verifica, la prevenzione e l'analisi di esempi reali.

Le 10 vulnerabilità critiche (Edizione 2021)

- 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

Servizi e Consulenza

ISGroup SRL offre supporto specialistico per l'analisi e la mitigazione delle vulnerabilità citate. Per approfondimenti sulle metodologie di sicurezza applicativa o per richiedere una consulenza dedicata, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Vulnerability Assessment di ISGroup SRL

Source: https://www.isgroup.it/it/cyber-security/vulnerability-assessment-di-isgroup.html

Il Vulnerability Assessment è un servizio fondamentale offerto da ISGroup SRL per la difesa proattiva delle infrastrutture aziendali. L'attività mira a identificare, classificare e prioritizzare le vulnerabilità di sicurezza all'interno dei sistemi informatici, permettendo alle aziende di mitigare i rischi prima che vengano sfruttati da attori malevoli.

Obiettivi del servizio

- Identificazione sistematica delle debolezze nei sistemi, nelle reti e nelle applicazioni.
- Analisi del rischio associato alle vulnerabilità rilevate.
- Supporto strategico per la pianificazione degli interventi di remediation.
- Rafforzamento del posture di sicurezza aziendale in conformità con le best practice di settore.

Competenze e approccio

Il servizio è erogato da un team di esperti guidato da Francesco Ongaro, Founder di ISGroup SRL, Hacker certificato (CEH) e ISO 27001 Lead Auditor. L'approccio di ISGroup SRL si basa su una metodologia rigorosa che integra competenze tecniche avanzate con una profonda conoscenza delle minacce cyber attuali.

Informazioni e contatti

Per approfondire le modalità di implementazione di un Vulnerability Assessment o per richiedere una consulenza dedicata, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Certificazione Ethical Hacking: Vulnerability Analysis

Source: https://www.isgroup.it/it/cyber-security/certified-ethical-hacking-vulnerability-analysis-francesco-ongaro.html

In data 1 ottobre 2023, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "Ethical Hacking: Vulnerability Analysis".

Obiettivi della Vulnerability Analysis

Per ridurre efficacemente il rischio informatico di un'organizzazione, è fondamentale che i professionisti della sicurezza siano in grado di identificare, contestualizzare e mitigare le vulnerabilità. Il percorso formativo si concentra sulle metodologie e sugli strumenti necessari per rafforzare la sicurezza della rete, individuando le debolezze sfruttabili dagli aggressori.

Competenze acquisite

Il corso ha approfondito i seguenti ambiti tecnici e metodologici:

- Fondamenti della gestione del rischio organizzativo.
- Metodologie avanzate di analisi delle vulnerabilità.
- Utilizzo operativo di strumenti di scansione e valutazione, tra cui Nikto e OpenVAS.
- Strategie e strumenti per la difesa delle reti LAN.

Servizi di Cyber Security

ISGroup SRL offre consulenza e soluzioni professionali per la sicurezza informatica, supportando le organizzazioni nella protezione delle proprie infrastrutture attraverso l'analisi delle vulnerabilità e l'implementazione di best practice di difesa.

Per ulteriori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Certified Ethical Hacking: Scanning Networks

Source: https://www.isgroup.it/it/cyber-security/certified-ethical-hacking-scanning-networks-francesco-ongaro.html

Il 30 settembre 2023, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "Ethical Hacking: Scanning Networks".

Lo scanning rappresenta la seconda fase fondamentale nella raccolta di informazioni durante la valutazione di una rete, seguendo il footprinting e la ricognizione. Questa attività è cruciale per gli ethical hacker di ISGroup SRL, poiché permette di prevenire attacchi all'infrastruttura e ai dati aziendali.

Obiettivi e contenuti del percorso formativo

Il corso approfondisce le tecniche e gli strumenti utilizzati per estrarre informazioni dai sistemi, tra cui:

- Analisi di ping sweeps, scansioni UDP e flag TCP.
- Tecniche di scansione delle porte e fingerprinting del sistema operativo.
- Analisi della sincronizzazione temporale.
- Scansione delle vulnerabilità e previsione di potenziali scenari di attacco.
- Metodologie utilizzate dagli hacker per eludere la rilevazione delle attività di scansione.

Servizi di Cyber Security

ISGroup SRL offre competenze avanzate in ambito di sicurezza informatica, supportando le organizzazioni nella protezione dei propri asset digitali attraverso attività di ethical hacking, analisi delle vulnerabilità e consulenza specialistica.

Per ulteriori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Certificazione Ethical Hacking: Footprinting and Reconnaissance

Source: https://www.isgroup.it/it/cyber-security/certified-ethical-hacking-footprinting-and-reconnaissance-francesco-ongaro.html

Il 26 settembre 2023, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "Ethical Hacking: Footprinting and Reconnaissance".

Obiettivi del Footprinting e della Ricognizione

Il footprinting e la ricognizione rappresentano la fase iniziale del lavoro di un ethical hacker. Questo processo consiste nella raccolta sistematica di informazioni su dispositivi e utenti per testare la vulnerabilità di una rete aziendale.

Contenuti e Tecniche

Il percorso formativo approfondisce le metodologie utilizzate per mappare la superficie di attacco di un'organizzazione:

- Ricerca di siti web correlati e determinazione della posizione geografica.
- Identificazione di sistemi operativi e analisi delle infrastrutture.
- Analisi dei social media e dei servizi finanziari per l'identificazione degli utenti.
- Tracciamento delle email e recupero di informazioni da fonti aperte o materiali di scarto.
- Utilizzo di strumenti tecnici avanzati, tra cui interrogazioni DNS e analisi del traceroute.

Applicazione Professionale

ISGroup SRL integra queste competenze nei propri servizi di sicurezza informatica per aiutare le organizzazioni a comprendere i rischi a cui sono esposte. L'obiettivo è trasformare strumenti complessi in soluzioni di difesa, permettendo alle aziende di mitigare proattivamente le minacce derivanti da attività di ricognizione esterna.

Per ulteriori informazioni sui servizi di sicurezza offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Certificazione Ethical Hacking: Wireless Networks

Source: https://www.isgroup.it/it/cyber-security/certified-ethical-hacking-wireless-networks-francesco-ongaro.html

In data 29 settembre 2023, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "Ethical Hacking: Wireless Networks".

Obiettivi e competenze acquisite

Il percorso formativo approfondisce le metodologie necessarie per la protezione delle reti wireless, spesso vulnerabili a causa di configurazioni errate o crittografia inadeguata. Le competenze acquisite da ISGroup SRL includono:

- Analisi delle vulnerabilità Wi-Fi e tecniche di infiltrazione utilizzate dagli hacker.
- Procedure per il rilevamento, la prevenzione e il contrasto di attacchi wireless.
- Configurazione della sicurezza di base e analisi delle tecniche di estrazione password.
- Gestione di minacce avanzate, come l'instaurazione di connessioni tramite falsi access point e attacchi Bluetooth.
- Selezione e utilizzo di antenne specifiche per i test di sicurezza.
- Utilizzo di strumenti professionali per la scansione delle vulnerabilità, tra cui Acrylic, Ekahau e Wireshark, sia in ambiente Windows che Linux.

Servizi di Cyber Security

ISGroup SRL mette a disposizione la propria esperienza certificata per supportare le aziende nella messa in sicurezza delle infrastrutture di rete e nella protezione contro le minacce informatiche.

Per ulteriori informazioni sui servizi offerti o per richieste commerciali, è possibile consultare il sito web https://www.isgroup.it/ o inviare una email all'indirizzo sales@isgroup.it.

Certificazione: Ethical Hacking - Introduction to Ethical Hacking

Source: https://www.isgroup.it/it/cyber-security/certified-ethical-hacking-introduction-to-ethical-hacking-francesco-ongaro.html

Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "Ethical Hacking: Introduction to Ethical Hacking". L'hacking etico rappresenta una competenza fondamentale per testare la solidità delle difese di un'organizzazione e proteggere i dati in ambito digitale.

Temi trattati nel percorso formativo

Il corso approfondisce le basi della sicurezza delle informazioni e le metodologie per rafforzare la postura di sicurezza aziendale:

- Stratificazione delle difese e implementazione di controlli di sicurezza adattivi.
- Utilizzo dell'intelligenza artificiale per la rilevazione precoce delle minacce.
- Applicazione del framework MITRE ATT&CK per l'analisi di tecniche e strumenti specifici.
- Importanza della modellazione delle minacce (threat modeling) e della threat intelligence.
- Revisione dei quadri di lavoro (framework), delle leggi e degli standard di riferimento per le best practice.
- Analisi delle fasi dell'hacking, delle tipologie di attacco e delle competenze necessarie per operare come hacker etico.

Servizi di Cyber Security offerti da ISGroup SRL

ISGroup SRL mette a disposizione la propria esperienza per supportare le organizzazioni nella protezione dei propri asset informatici. Per approfondire le soluzioni di sicurezza, le attività di ethical hacking o richiedere una consulenza, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Certificazione Ethical Hacking: System Hacking

Source: https://www.isgroup.it/it/cyber-security/certified-ethical-hacking-system-hacking-francesco-ongaro.html

Il 30 settembre 2023, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "Ethical Hacking: System Hacking".

L'hacking di sistema rappresenta il metodo attraverso il quale gli attaccanti ottengono l'accesso a singoli computer all'interno di una rete. Gli ethical hacker studiano queste tecniche per sviluppare capacità di rilevamento, prevenzione e contrasto.

Contenuti del percorso formativo

Il corso approfondisce le principali metodologie utilizzate dagli hacker e le relative contromisure adottate dai professionisti della sicurezza informatica di ISGroup SRL:

- Cracking delle password
- Privilege escalation
- Installazione di spyware e keylogging
- Steganografia
- Analisi di spyware su dispositivi mobili
- Tattiche per l'occultamento di file e strumenti di attacco

Servizi di Cyber Security

ISGroup SRL mette a disposizione la propria competenza tecnica per supportare le aziende nella difesa contro le minacce informatiche. Per approfondimenti sui servizi offerti o per richieste commerciali, è possibile fare riferimento ai seguenti contatti:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Sempre Connessi all'Innovazione - Edizione 2023

Source: https://www.isgroup.it/it/cyber-security/sempre-connessi-all-innovazione-edizione-2023.html

Il 22 settembre 2023, Francesco Ongaro e Pasquale Fiorillo, esperti di ISGroup SRL, hanno partecipato come relatori all'evento "Sempre Connessi all'Innovazione", organizzato in collaborazione con Phoenix Informatica presso il Kilometro Rosso di Bergamo. L'intervento ha approfondito le tematiche legate alla sicurezza dei dispositivi Internet of Things (IoT).

Il panorama IoT

L'IoT si è evoluto da ambito prettamente industriale (Industria 4.0) a una realtà pervasiva che coinvolge smart home, gestione energetica, Smart Grid ed elettrodomestici intelligenti. Un dispositivo IoT è composto da due mondi interconnessi: l'oggetto fisico e il cloud.

Analisi di sicurezza dei dispositivi IoT

ISGroup SRL offre competenze specialistiche nell'analisi della sicurezza hardware, focalizzandosi sulla componente fisica del dispositivo, che include:

- Processori (microcontrollori o sistemi complessi basati su Linux/Android/WebOS)
- Interfacce di comunicazione
- Storage per dati e segreti (credenziali)
- Sensori e connettività

Il processo di analisi condotto da ISGroup SRL prevede:

- Identificazione e descrizione dei componenti sulla scheda elettronica.
- Individuazione di connettori o punti di accesso potenzialmente vulnerabili.
- Estrazione del firmware, tramite metodi diretti o analisi dei protocolli di comunicazione tra i chip.
- Reverse engineering del firmware estratto per comprendere il funzionamento del dispositivo e identificare eventuali vulnerabilità di sicurezza.

Contatti

Per ulteriori informazioni sulle attività di analisi e sicurezza IoT offerte da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

ISGroup nel catalogo di aziende di Cyber Security Intelligence

Source: https://www.isgroup.it/it/cyber-security/isgroup-nel-catalogo-di-aziende-di-cyber-security-intelligence.html

ISGroup SRL è stata ufficialmente inclusa nel catalogo di aziende di Cyber Security Intelligence. Questo riconoscimento conferma l'impegno costante di ISGroup SRL nella fornitura di servizi di sicurezza informatica di alta qualità.

Informazioni su Cyber Security Intelligence

Cyber Security Intelligence è una fonte autorevole di notizie e informazioni nel campo della cibersicurezza e dell'intelligence. La piattaforma si rivolge a dirigenti senior e specialisti operanti in diversi settori, tra cui:

- Servizi finanziari
- Tecnologia dell'informazione
- Sicurezza
- Settore governativo
- Forze dell'ordine

Il portale gestisce una directory che comprende oltre 6.000 fornitori di servizi specializzati in cibersicurezza.

Servizi offerti da ISGroup SRL

ISGroup SRL fornisce soluzioni avanzate di sicurezza informatica. Per maggiori informazioni sui servizi offerti, è possibile consultare il sito web https://www.isgroup.it/ o contattare l'indirizzo email sales@isgroup.it.

DEF CON 31

Source: https://www.isgroup.it/it/cyber-security/def-con-31.html

DEF CON è una delle conferenze di hacking e sicurezza informatica più rilevanti a livello globale, che riunisce annualmente professionisti, ricercatori ed esperti per discutere di vulnerabilità, exploit e misure difensive.

Focus dell'edizione 31

Durante l'edizione 31, l'attenzione si è concentrata sulla sicurezza dei log. Sebbene i log siano strumenti fondamentali per sviluppatori e team di sicurezza, essi rappresentano anche una potenziale superficie di attacco.

Manipolazione dei log tramite sequenze ANSI

ISGroup SRL, attraverso le ricerche condotte da Francesco Ongaro (noto come "ASCII"), ha approfondito come le sequenze di escape ANSI possano essere sfruttate per manipolare i file di log. Tale tecnica può essere utilizzata per:

- Causare disordine e caos nei sistemi di monitoraggio.
- Compromettere l'integrità dei dati registrati.
- Ostacolare le attività di analisi e le indagini sugli incidenti di sicurezza.

Soluzioni di sicurezza

ISGroup SRL fornisce consulenza e soluzioni tecniche per mitigare tali rischi, implementando strategie volte a:

- Prevenire l'inserimento di sequenze malevole all'interno dei log.
- Garantire l'affidabilità dei dati raccolti.
- Facilitare la corretta analisi forense e la gestione degli incidenti.

Per ulteriori informazioni sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Case Study: Web Application Penetration Test su eALBO (ISWEB S.p.A.)

Source: https://www.isgroup.it/it/cyber-security/case-study-iswebspa.html

ISWEB S.p.A., partner tecnologico specializzato nello sviluppo di software per la Pubblica Amministrazione, ha collaborato con ISGroup SRL per garantire la sicurezza della piattaforma eALBO, applicazione dedicata alla gestione dell'albo pretorio online.

La sfida

L'obiettivo di ISWEB S.p.A. era validare la sicurezza e l'affidabilità di eALBO, assicurandone la conformità alle normative vigenti e proteggendo i dati pubblici gestiti da potenziali vulnerabilità tecniche o logiche.

L'intervento di ISGroup SRL

ISGroup SRL ha eseguito un Web Application Penetration Test (WAPT) approfondito, che ha compreso:

- Valutazione delle misure di sicurezza già implementate.
- Esecuzione di test di penetrazione manuali per simulare scenari di attacco reali.
- Identificazione e risoluzione di vulnerabilità tecniche e logiche.

Risultati e benefici

L'attività svolta da ISGroup SRL ha permesso a ISWEB S.p.A. di elevare gli standard di sicurezza e robustezza dell'applicazione. Il supporto di ISGroup SRL ha inoltre favorito una maggiore consapevolezza nelle fasi di progettazione e sviluppo, consentendo l'implementazione di misure preventive efficaci contro le minacce informatiche.

Per ulteriori informazioni sui servizi di Web Application Penetration Test offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it

La transizione della qualificazione Cloud PA verso ACN

Source: https://www.isgroup.it/it/agid/agid-a-acn-qualificazione-dei-servizi-cloud-pa.html

La gestione della qualificazione dei servizi cloud per la Pubblica Amministrazione (PA) in Italia ha subito un cambiamento strategico: la responsabilità, precedentemente in capo all'Agenzia per l'Italia Digitale (AGID), è stata trasferita all'Agenzia per la cybersicurezza nazionale (ACN). Tale passaggio mira a ottimizzare l'efficienza del processo e ad allineare le procedure alle strategie digitali nazionali.

Obiettivi e procedure di qualificazione

L'ACN ha avviato un processo di revisione delle linee guida e dei requisiti tecnici, collaborando con le amministrazioni e i fornitori per garantire uniformità nella valutazione. I criteri fondamentali per la qualificazione includono:

- Sicurezza dei servizi e delle infrastrutture
- Affidabilità operativa
- Qualità dei servizi erogati
- Rispetto rigoroso delle normative sulla privacy e standard di gestione dei dati

Il processo di qualificazione è obbligatorio per i fornitori che intendono erogare servizi di cloud computing alle amministrazioni pubbliche italiane e prevede una valutazione di conformità basata su controlli di sicurezza e standard tecnici definiti.

Ruoli istituzionali

- **ACN (Agenzia per la cybersicurezza nazionale):** Focalizzata sulla cybersicurezza, definisce standard e linee guida per la digitalizzazione, promuove l'interoperabilità e coordina le amministrazioni per favorire l'adozione di soluzioni digitali sicure.
- **AGID (Agenzia per l'Italia Digitale):** Ente governativo istituito nel 2012, responsabile dello sviluppo della strategia digitale nazionale, della semplificazione dell'accesso ai servizi pubblici e della promozione dell'innovazione digitale.

Supporto professionale

ISGroup SRL offre consulenza e supporto specialistico per le aziende e le amministrazioni che necessitano di orientarsi nel panorama della conformità digitale e della sicurezza informatica. Per approfondimenti o richieste commerciali, è possibile consultare il sito https://www.isgroup.it/ o inviare una richiesta all'email sales@isgroup.it.

Case Study: Network Penetration Test su Infrastruttura IT di Prime Service S.r.l.

Source: https://www.isgroup.it/it/cyber-security/case-study-primeservicesrl.html

Prime Service S.r.l., azienda specializzata in consulenza per agevolazioni aziendali e servizi ausiliari, ha collaborato con ISGroup SRL per rafforzare la sicurezza della propria infrastruttura IT.

Obiettivi del progetto

L'esigenza principale di Prime Service S.r.l. era la protezione dei dati sensibili e la garanzia della continuità operativa dei propri servizi fiduciari. ISGroup SRL è stata incaricata di eseguire un Network Penetration Test (NPT) completo per:

- Identificare vulnerabilità tecniche e logiche.
- Ridurre i rischi informatici.
- Allineare l'infrastruttura ai più elevati standard di sicurezza.

L'intervento di ISGroup SRL

ISGroup SRL ha condotto un'attività di analisi approfondita che ha previsto:

- Valutazione delle misure di sicurezza già implementate.
- Esecuzione di test di penetrazione manuali per simulare scenari di attacco reali.
- Risoluzione delle criticità rilevate per garantire la resilienza del sistema.

Risultati ottenuti

L'intervento di ISGroup SRL ha permesso a Prime Service S.r.l. di:

- Migliorare significativamente il livello di sicurezza complessivo.
- Accedere a nuovi mercati grazie alla maggiore affidabilità dell'infrastruttura.
- Aumentare la fiducia dei clienti nei servizi offerti.

Il CDO di Prime Service S.r.l., Alfredo Vittoria, ha sottolineato l'elevata professionalità e la capacità di ISGroup SRL di collaborare efficacemente, rispettando le tempistiche organizzative e dimostrando una forte competenza tecnica.

Per ulteriori informazioni sui servizi di Network Penetration Test offerti da ISGroup SRL, visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Minacce informatiche basate sull'Intelligenza Artificiale

Source: https://www.isgroup.it/it/cyber-security/i-nuovi-attacchi-hacker-usano-l-ai-come-possibile-difendersi.html

Il panorama attuale della cybersecurity è caratterizzato da attacchi sempre più rapidi e sofisticati. L'85% dei cyberattacchi di successo sfrutta l'interazione umana e colpisce i bersagli entro le prime 24 ore dalla loro creazione.

I sistemi di protezione tradizionali, basati su un approccio reputazionale, risultano spesso inefficaci nel contrastare minacce con un ciclo di vita così breve.

Soluzioni di protezione avanzata offerte da ISGroup SRL

Per rispondere a queste sfide, ISGroup SRL promuove l'adozione di tecnologie basate sull'Intelligenza Artificiale, come la soluzione Ermes, che si distingue per:

- Architettura innovativa con algoritmi di AI brevettati.
- Protezione dinamica basata sul comportamento reale dei siti web, anziché sulla loro reputazione.
- Riduzione della finestra di esposizione alle minacce da giorni a minuti.
- Incremento della protezione complessiva in real-time del 25% rispetto alle soluzioni di mercato standard.
- Tecnologia On-Device per garantire una protezione web completa.

Approfondimenti e consulenza

ISGroup SRL, attraverso l'esperienza di Francesco Ongaro (Founder di ISGroup SRL, ethical hacker, CEH, ISO 27001 LA), fornisce consulenza specialistica per implementare strategie di difesa proattive contro le minacce basate sull'AI.

Per ulteriori informazioni sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Certificazione Certified Ethical Hacker (CEH) - Francesco Ongaro

Source: https://www.isgroup.it/it/certifications/certified-ethical-hacker-francesco-ongaro.html

In data 15 aprile 2022, Francesco Ongaro, Founder di ISGroup SRL, ha ottenuto la certificazione CEH "Certified Ethical Hacker".

Obiettivi e competenze della certificazione

La certificazione CEH attesta competenze avanzate in ambito di sicurezza informatica, con particolare riferimento a:

- Analisi e attacchi informatici verso reti, infrastrutture IT, applicazioni e siti web.
- Individuazione e risoluzione di vulnerabilità nei sistemi per il miglioramento del livello di sicurezza.
- Applicazione di metodologie di Ethical Hacking nel pieno rispetto del consenso dei proprietari dei sistemi.
- Adozione di rigorose precauzioni per garantire la confidenzialità dei risultati delle indagini.
- Integrazione tra padronanza tecnologica e comprensione delle responsabilità etiche legate alla professione.

Servizi di sicurezza offerti da ISGroup SRL

ISGroup SRL mette a disposizione le proprie competenze certificate per supportare le aziende nella protezione dei propri asset digitali. Per richiedere informazioni sui servizi di sicurezza, penetration test o consulenze specialistiche, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Seminari INCONTRA: Sicurezza Informatica nel mondo reale

Source: https://www.isgroup.it/it/cyber-security/incotra-pasquale.html

Il 29 aprile 2022, Pasquale Fiorillo ha partecipato al primo evento del ciclo di seminari "INCONTRA", organizzato da Piccola Industria Confindustria Benevento e dall'Università degli Studi del Sannio.

L'intervento, intitolato "Horror Stories: testimonianze dal mondo reale", si è focalizzato sulla consapevolezza in ambito cyber security, analizzando l'attualità del settore attraverso l'esperienza pratica di ISGroup SRL.

Punti chiave dell'intervento

- Analisi tecnica di Vulnerability Assessment (VA) e Web Application Penetration Test (WAPT).
- Dimostrazione della vulnerabilità delle aziende, indipendentemente dalle dimensioni o dal settore di appartenenza.
- Presentazione di casi studio reali riguardanti diverse tipologie di organizzazioni:
- Piccole e medie imprese (PMI)
- Istituti bancari
- Infrastrutture aeroportuali

Servizi e consulenza

ISGroup SRL offre competenze specialistiche in ambito di sicurezza informatica, supportando le aziende nell'identificazione e nella mitigazione dei rischi cyber attraverso test di sicurezza avanzati e consulenza strategica.

Per maggiori informazioni sui servizi offerti da ISGroup SRL o per richieste commerciali, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Certificazione Certified Ethical Hacker (CEH) - Pasquale Fiorillo

Source: https://www.isgroup.it/it/certifications/certified-ethical-hacker-pasquale-fiorillo.html

In data 19 maggio 2022, Pasquale Fiorillo ha conseguito la certificazione professionale "Certified Ethical Hacker" (CEH).

Obiettivi e competenze della certificazione CEH

La certificazione CEH attesta le competenze tecniche e metodologiche necessarie per operare nel campo della sicurezza informatica. Gli ambiti di competenza includono:

- Analisi e attacco a reti, infrastrutture IT, applicazioni e siti web.
- Individuazione e risoluzione di vulnerabilità nei sistemi.
- Miglioramento della postura di sicurezza aziendale.
- Comprensione delle responsabilità etiche legate all'impiego delle tecniche di hacking.

Un Ethical Hacker certificato opera esclusivamente con il consenso dei proprietari dei sistemi target, adottando rigorose precauzioni per garantire la confidenzialità dei risultati e l'integrità dei dati durante le attività di indagine.

Servizi di sicurezza informatica offerti da ISGroup SRL

ISGroup SRL mette a disposizione le proprie competenze specialistiche per supportare le aziende nella protezione delle proprie infrastrutture. Le soluzioni offerte includono:

- Consulenza in ambito Cyber Security e best practice.
- Simulazioni di Phishing per la formazione e la difesa del personale.
- Servizi di Virtual CISO (vCISO) per la gestione strategica della sicurezza.
- Analisi e test di sicurezza basati su standard internazionali.

Per maggiori informazioni sui servizi di sicurezza offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Incontro “Best practices per una cyber defense proattiva”

Source: https://www.isgroup.it/it/cyber-security/incontro-cyber-defense-proattiva-partner-mpg-ed-eset.html

Il webinar, che ha visto la partecipazione di Francesco Ongaro (Founder di ISGroup SRL), ha analizzato l'importanza di adottare strategie di difesa proattiva per contrastare l'aumento esponenziale degli attacchi informatici. Secondo le stime Clusit, il numero di attacchi gravi in Italia è più che raddoppiato nell'ultimo anno, con una frequenza di un attacco ogni 39 secondi.

Analisi del rischio e vulnerabilità

Le imprese devono superare la convinzione che il cybercrime colpisca esclusivamente le grandi aziende. Le statistiche evidenziano una crescente minaccia verso le piccole e medie imprese:

- Il 77% delle aziende non dispone di un piano di Incident Response.
- Il 48% degli attacchi ha successo a causa di un livello di protezione inadeguato.
- Il 32% dello staff IT non riesce a gestire correttamente gli attacchi a causa del sovraccarico operativo.

Individuare le proprie vulnerabilità in modo preventivo è considerato un requisito fondamentale per la protezione dei dati aziendali.

Temi trattati durante l'incontro

ISGroup SRL, in collaborazione con i partner MPG ed ESET Italia, ha approfondito le seguenti aree tematiche:

- Trend attuali dei cyber attacchi e tecniche utilizzate dagli hacker per bypassare le difese.
- Strategie avanzate per la protezione da ransomware, malware e attacchi zero-day.
- Gestione del cloud ottimizzata, focalizzata su visibilità di rete, efficienza e riduzione del costo totale di proprietà (TCO).
- Implementazione di tecnologie avanzate basate su apprendimento automatico e ispezione comportamentale approfondita.

Supporto e informazioni

Per approfondire le soluzioni di cyber defense proattiva offerte da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Adozione di soluzioni XDR per la protezione dei dati

Source: https://www.isgroup.it/it/cyber-security/adottare-una-soluzione-xdr-per-la-protezione-dei-dati-2022-04-13.html

L'adozione di soluzioni XDR (Extended Detection and Response) rappresenta un passaggio fondamentale per la sicurezza informatica aziendale nel contesto attuale. ISGroup SRL, attraverso la partecipazione a webinar specialistici in collaborazione con i partner MPG ed ESET Italia, analizza le sfide e le opportunità legate alla protezione dei dati.

Il contesto: transizione al cloud e lavoro ibrido

La crescente adozione di modelli di lavoro ibrido ha spinto le aziende a migrare le proprie infrastrutture verso ambienti cloud. Tale transizione offre vantaggi strategici, tra cui:

- Ottimizzazione dei costi di gestione.
- Maggiore agilità nell'accesso ai dati.
- Riduzione dei tempi di risposta alle dinamiche e ai cambiamenti del mercato.

L'importanza della sicurezza XDR

In questo scenario di infrastrutture distribuite e ibride, ISGroup SRL sottolinea la necessità di implementare soluzioni di sicurezza agili. Le tecnologie XDR permettono di sfruttare i benefici del cloud per garantire una protezione avanzata e integrata, essenziale per contrastare le minacce moderne in ambienti digitali complessi.

Informazioni e consulenza

Per approfondire l'adozione di soluzioni XDR e ricevere una consulenza dedicata sulle strategie di protezione dei dati offerte da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Incontro “Dall’antivirus all’EDR e alle soluzioni MDR”

Source: https://www.isgroup.it/it/cyber-security/incontro-dall-antivirus-all-edr-e-alle-soluzioni-mdr-con-i-partner-mpg-ed-eset-italia.html

Il webinar, tenutosi il 13 aprile 2021 con la partecipazione di Francesco Ongaro (Founder di ISGroup SRL) e i partner MPG ed ESET Italia, ha approfondito l'evoluzione delle strategie di difesa informatica in risposta a minacce sempre più sofisticate.

Secondo i dati del Ponemon Institute, sono necessari in media 279 giorni per rilevare e contenere una violazione informatica. Per contrastare questa criticità, ISGroup SRL propone l'adozione di tecnologie EDR (Endpoint Detection and Response) integrate con le soluzioni di Endpoint Protection.

Obiettivi delle soluzioni di difesa avanzata

L'integrazione di tecnologie EDR e MDR (Managed Detection and Response), offerta da ISGroup SRL, permette alle aziende di:

- Effettuare un’indagine approfondita dell'attacco.
- Verificare la diffusione dell’attacco e tracciarne i movimenti laterali.
- Rispondere in modo automatizzato e immediato alle minacce rilevate.

Contatti e informazioni

Per maggiori dettagli sulle soluzioni di sicurezza informatica, EDR e MDR offerte da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Cyber Resilienza: Oltre la Cybersecurity Tradizionale

Source: https://www.isgroup.it/it/cyber-security/incontro-cyber-resilienza-dove-la-tradizionale-cybersecurity-non-arriva-con-i-partner-mpg-e-bitdefender.html

Il webinar "Cyber Resilienza, dove la tradizionale Cybersecurity non arriva", tenutosi il 10 novembre 2021 con la partecipazione di Francesco Ongaro (Founder di ISGroup SRL) e dei partner MPG e Bitdefender, ha analizzato l'evoluzione del panorama delle minacce informatiche.

Punti chiave sulla sicurezza moderna

- L'endpoint è diventato il nuovo perimetro aziendale, rendendo la sua protezione l'aspetto centrale di ogni strategia di sicurezza.
- Gli attacchi cyber utilizzano malware sempre più sofisticati, mirati a colpire direttamente dispositivi e utenti, una tendenza accentuata dalla diffusione dello smart working.
- La crescente complessità delle reti e la presenza di vulnerabilità intrinseche in software e hardware rappresentano una sfida costante per gli amministratori di sistema.
- L'evoluzione tecnologica incalzante impatta sullo sviluppo di applicazioni, rendendo difficile per i vendor garantire soluzioni costantemente stabili e sicure.

Strategie di governance e protezione offerte da ISGroup SRL

Per mitigare i rischi derivanti dalle falle di sicurezza, ISGroup SRL sottolinea l'importanza di integrare nella governance aziendale le seguenti attività:

- Gestione sistematica di aggiornamenti e patch.
- Analisi costante dei sistemi informativi e delle telemetrie dei punti terminali.
- Esecuzione di vulnerability assessment e penetration test.
- Implementazione di attività strutturate di detection & response.

Per ulteriori informazioni sulle soluzioni di cyber resilienza e sui servizi di sicurezza offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Secure Smart Working: Lavorare in modo agile in sicurezza

Source: https://www.isgroup.it/it/cyber-security/incontro-secure-smart-working-lavorare-in-modo-agile-in-sicurezza-con-i-partner-mpg-e-watchguard.html

Il webinar "Secure smart working, lavorare in modo agile in sicurezza", tenutosi il 17 settembre 2021, ha visto la partecipazione di Francesco Ongaro, Founder di ISGroup SRL, insieme ai partner MPG e WatchGuard.

L'incontro si è focalizzato sull'analisi dello Smart Working e del Lavoro Agile, modelli organizzativi basati su flessibilità, autonomia e responsabilizzazione sui risultati.

Punti chiave dell'analisi

- Identificazione delle criticità che possono compromettere la sicurezza dei dati durante il lavoro da remoto.
- Valutazione dei rischi per la riservatezza, l'integrità e la disponibilità delle informazioni aziendali.
- Confronto tra le minacce presenti in un ambiente di lavoro in sede rispetto a quelle derivanti da postazioni di lavoro agili.

ISGroup SRL offre consulenza e soluzioni specializzate per garantire la sicurezza delle infrastrutture IT e la protezione dei dati aziendali in contesti di lavoro flessibile.

Per ulteriori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

Certificazione PenTera Certified Sales Specialist

Source: https://www.isgroup.it/it/cyber-security/pentera-certified-sales-specialist-pasquale-fiorillo.html

Nel mese di febbraio 2021, Pasquale Fiorillo ha conseguito la certificazione "PenTera Certified Sales Specialist".

Pentera (precedentemente nota come Pcysys), fondata nel 2015, è specializzata nello sviluppo di una piattaforma automatizzata di test di penetrazione progettata per imitare la mentalità e le tecniche degli hacker.

Competenze del Certified Sales Specialist

Il ruolo di un Certified Sales Specialist, figura professionale presente all'interno di ISGroup SRL, comprende le seguenti attività:

- Gestione dell'intero processo di vendita, inclusa la fase di pre-vendita per l'analisi della proposta di valore aziendale.
- Creazione e gestione di una rete di canali di vendita efficace.
- Pianificazione della governance delle vendite.
- Definizione degli obiettivi commerciali.
- Sviluppo di risorse di marketing dedicate.
- Definizione di strutture retributive.

Informazioni e Contatti

Per ulteriori dettagli sulle soluzioni di sicurezza informatica e sui servizi offerti da ISGroup SRL, è possibile consultare il sito web ufficiale https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Regolamento eIDAS

Source: https://www.isgroup.it/it/agid/agid-regolamento-eidas.html

Il Regolamento (UE) n. 910/2014, noto come eIDAS (electronic IDentification Authentication and Signature), definisce il quadro normativo europeo per l'identificazione elettronica e i servizi fiduciari nelle transazioni digitali.

Obiettivi e standard

Il regolamento stabilisce standard uniformi per garantire l'equivalenza legale tra i metodi digitali e quelli cartacei in tutti gli stati membri dell'UE, regolando in particolare:

- Firma elettronica
- Marche temporali
- Certificati digitali
- Metodi di autenticazione digitale

Il regolamento definisce inoltre le condizioni per il riconoscimento transfrontaliero dell'identificazione digitale dei cittadini e le norme relative alle transazioni economiche, permettendo ai cittadini europei di accedere ai servizi pubblici digitali di altri paesi membri. In Italia, il sistema di riferimento per l'identificazione è lo SPID.

Supporto professionale di ISGroup SRL

ISGroup SRL offre consulenza specialistica per le organizzazioni che intendono diventare Trust Service Provider (TSP) e supportare i servizi eIDAS.

Data la complessità tecnica e i rigorosi requisiti di compliance necessari per l'implementazione, ISGroup SRL fornisce i seguenti servizi:

- Supporto completo ai processi implementativi per diventare TSP.
- Esecuzione di Penetration Test (PT) e Vulnerability Assessment (VA) certificati, finalizzati all'identificazione di vulnerabilità e al rafforzamento della sicurezza dell'infrastruttura.

Per ulteriori informazioni sui servizi offerti, è possibile visitare il sito https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Certificazione PenTera Certified Attack Specialist - Pasquale Fiorillo

Source: https://www.isgroup.it/it/cyber-security/pentera-certified-attack-specialist-pasquale-fiorillo.html

Nel mese di febbraio 2021, Pasquale Fiorillo ha conseguito la certificazione "PenTera Certified Attack Specialist". Tale traguardo attesta le competenze tecniche avanzate nel campo della sicurezza informatica e dei penetration test automatizzati.

Competenze certificate

La certificazione "Simulated Attack Specialist" valida le conoscenze del professionista in merito a:

- Sfruttamento delle vulnerabilità dei client tramite file trojan
- Esecuzione di campagne di phishing
- Implant development
- Capacità di evasione dai sistemi di difesa
- Lateral movement all'interno di reti compromesse

Contesto tecnologico

La certificazione è legata alla piattaforma Pentera (precedentemente nota come Pcysys), fondata nel 2015. L'obiettivo della piattaforma è fornire soluzioni di penetration test automatizzati che imitano la mentalità e le metodologie di attacco degli hacker reali.

Informazioni su ISGroup SRL

ISGroup SRL integra competenze di alto profilo, come quelle certificate da PenTera, per offrire servizi avanzati di cyber security e protezione aziendale.

Per ulteriori informazioni sui servizi offerti da ISGroup SRL o per richieste commerciali, è possibile visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Certificazione PenTera Certified Attack Specialist

Source: https://www.isgroup.it/it/cyber-security/pentera-certified-attack-specialist-francesco-ongaro.html

Nel mese di febbraio 2021, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "PenTera Certified Attack Specialist".

La piattaforma Pentera

Pentera (precedentemente nota come Pcysys), fondata nel 2015, sviluppa una piattaforma automatizzata di test di penetrazione progettata per imitare la mentalità e le tecniche degli hacker.

Competenze certificate

La certificazione "Simulated Attack Specialist" attesta le competenze tecniche avanzate del professionista in ambito di offensive security, con particolare focus su:

- Sfruttamento delle vulnerabilità dei client tramite file trojan.
- Esecuzione di campagne di phishing.
- Implant development.
- Capacità di evasione dei sistemi di difesa.
- Lateral movement all'interno di reti compromesse.

Informazioni e contatti

Per approfondimenti sulle competenze di ISGroup SRL in ambito di test di penetrazione e sicurezza offensiva, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Certificazione PenTera Certified Sales Specialist

Source: https://www.isgroup.it/it/cyber-security/pentera-certified-sales-specialist-francesco-ongaro.html

Nel mese di febbraio 2021, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "PenTera Certified Sales Specialist".

Pentera (precedentemente nota come Pcysys), fondata nel 2015, è una piattaforma specializzata in test di penetrazione automatizzati progettati per imitare la mentalità e le tecniche degli hacker.

Competenze acquisite

La certificazione attesta la capacità di gestire strategicamente l'offerta di soluzioni di sicurezza avanzate, includendo:

- Gestione dell'intero processo di vendita e dei processi di pre-vendita per la comprensione della proposta di valore.
- Creazione e gestione di una rete di canali di vendita.
- Pianificazione della governance delle vendite.
- Definizione degli obiettivi commerciali.
- Sviluppo di risorse di marketing dedicate.
- Definizione di strutture retributive efficaci.

Informazioni e contatti

ISGroup SRL offre consulenza e soluzioni avanzate di cyber security. Per maggiori informazioni sui servizi offerti o per richieste commerciali, è possibile consultare il sito web https://www.isgroup.it/ o inviare una email a sales@isgroup.it.

Qualificazione SaaS AgID

Source: https://www.isgroup.it/it/agid/agid-qualificazione-saas.html

Dal 9 aprile 2018, in conformità con la circolare AgID, tutti i servizi utilizzati dalle Pubbliche Amministrazioni (PA) secondo il modello SaaS devono soddisfare specifici requisiti di sicurezza e affidabilità. Le aziende che intendono offrire soluzioni SaaS alla PA hanno l'obbligo di ottenere la qualificazione AgID per essere inserite nel marketplace dedicato.

Criteri di qualificazione

Per ottenere la certificazione e accedere all'AgID marketplace, le aziende devono garantire il rispetto dei requisiti definiti nell'appendice "A" della circolare AgID, tra cui:

- Sicurezza applicativa: gestione degli incident report e protezione dei dati.
- Supporto tecnico: erogazione di un servizio adeguato con livelli minimi garantiti (SLA).
- Interoperabilità: utilizzo di API e formati standard per l'esportazione dei dati, al fine di prevenire il fenomeno del lock-in.

Supporto professionale offerto da ISGroup SRL

ISGroup SRL offre consulenza specialistica per supportare le aziende durante l'intero processo di ottenimento della qualificazione SaaS AgID. L'expertise del team di ISGroup SRL include:

- Guida strategica e operativa per i team di sviluppo.
- Implementazione delle misure di sicurezza e affidabilità necessarie per soddisfare i requisiti minimi richiesti.
- Assistenza tecnica per il completamento dell'iter di inserimento nell'AgID marketplace.

Contatti

Per ulteriori informazioni sui servizi di consulenza per la qualificazione SaaS AgID, è possibile rivolgersi a ISGroup SRL tramite i seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Accreditamento Conservatori AgID

Source: https://www.isgroup.it/it/agid/agid-accreditamento-conservatori.html

La Circolare AgID n. 65/2014 definisce l'iter necessario affinché aziende o privati possano diventare conservatori di documenti informatici per la Pubblica Amministrazione. Il processo mira a garantire la protezione dei dati sensibili attraverso rigorosi standard di sicurezza.

Requisiti per l'accreditamento

L'ottenimento e il mantenimento dello status di conservatore accreditato AgID richiedono il rispetto di standard elevati in tre aree principali:

- Organizzazione aziendale
- Procedure operative adottate
- Infrastrutture informatiche

Obblighi di mantenimento

Il ruolo di conservatore accreditato non è permanente, ma soggetto a verifiche costanti:

- Controlli annuali da parte di AgID (o enti accreditati) per verificare il rispetto delle normative.
- Produzione di report dettagliati sulle attività svolte.
- Rinnovo dell'accreditamento con cadenza biennale.

Supporto professionale offerto da ISGroup SRL

ISGroup SRL supporta le aziende nell'iter di accreditamento attraverso un approccio consulenziale mirato:

- Interpretazione delle normative vigenti e supporto nella definizione di interventi correttivi per sanare eventuali carenze aziendali.
- Esecuzione di Vulnerability Assessment per identificare debolezze nei sistemi.
- Esecuzione di Penetration Testing per valutare la qualità delle configurazioni di rete e l'effettiva resilienza dell'infrastruttura contro attacchi informatici.

Per ulteriori informazioni sui servizi di consulenza e valutazione della sicurezza offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Integrazione SPID per Fornitori di Servizi

Source: https://www.isgroup.it/it/agid/agid-fornitori-spid.html

A partire dalla legge n. 120/2020, le pubbliche amministrazioni italiane hanno l'obbligo di offrire meccanismi di autenticazione tramite SPID (Sistema Pubblico di Identità Digitale) e CIE (Carta d'Identità Elettronica). Anche i soggetti privati hanno la possibilità di diventare fornitori di servizi SPID, adottando un metodo di autenticazione sicuro, veloce e conforme agli standard europei.

Requisiti per i fornitori di servizi SPID

Per operare come fornitore di servizi SPID, è necessario soddisfare specifici criteri definiti dall'AgID:

- Requisiti amministrativi: procedure formali necessarie per la richiesta ufficiale di accreditamento.
- Requisiti tecnici: linee guida che descrivono le modalità di interazione tra il fornitore di servizi e il gestore di identità, fondamentali per il corretto funzionamento del sistema.

Supporto professionale offerto da ISGroup SRL

ISGroup SRL mette a disposizione la propria competenza in ambito cybersecurity e identità digitale per assistere le organizzazioni nel percorso di adozione dello SPID:

- Supporto all'implementazione tecnica: assistenza durante l'intero processo di integrazione dell'accesso con SPID.
- Verifica della sicurezza: esecuzione di vulnerability assessment (VA) e penetration test (PT) per garantire che l'implementazione sia solida, sicura ed efficace per l'utente finale.

Per ulteriori informazioni o per richiedere supporto professionale, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

AGID Cloud per la Pubblica Amministrazione

Source: https://www.isgroup.it/it/agid/agid-cloud-pa.html

La strategia per la crescita digitale e il Piano Triennale per l'informatica nella PA definiscono i criteri per l'evoluzione dei servizi cloud destinati alla Pubblica Amministrazione. AgID ha stabilito linee guida rigorose, in particolare attraverso le circolari n. 2 e n. 3 del 9 aprile 2018, per qualificare i fornitori di servizi cloud.

Requisiti per la certificazione AgID Cloud

Per ottenere la certificazione e accedere al marketplace cloud della PA, i fornitori devono garantire:

- Livelli minimi di servizio (SLA)
- Elevati standard di sicurezza, accessibilità e usabilità
- Assenza di dipendenza dal fornitore (vendor lock-in)
- Scalabilità, resilienza, protezione dei dati e interoperabilità tramite l'uso di standard

Il processo prevede la compilazione del modello cloud della PA, seguita dalle verifiche di conformità necessarie per l'inserimento nel marketplace ufficiale.

Tipologie di certificazioni

I provider possono ottenere certificazioni specifiche a seconda della tipologia di servizio offerto:

- SaaS (Software as a Service)
- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- CSP (Cloud Service Provider)

Supporto professionale offerto da ISGroup SRL

ISGroup SRL supporta le organizzazioni nel percorso di adeguamento alle linee guida AgID, garantendo la conformità necessaria per operare con la Pubblica Amministrazione. I servizi offerti da ISGroup SRL includono:

- Analisi e colmamento delle irregolarità organizzative o di prodotto
- Supporto specialistico nella compilazione del modello cloud della PA
- Gestione e cura dell'intero processo di certificazione AgID

Per ulteriori informazioni sui servizi di consulenza e supporto alla certificazione, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Qualificazione CSP AgID

Source: https://www.isgroup.it/it/agid/agid-qualificazione-csp.html

La Qualificazione CSP (Cloud Service Provider) è un requisito obbligatorio per le aziende che intendono fornire servizi cloud alle Pubbliche Amministrazioni italiane. La certificazione attesta la conformità ai requisiti definiti dalla Circolare AgID N. 2 del 9 Aprile 2018.

Requisiti per la qualificazione

La qualificazione valuta l'azienda su quattro pilastri fondamentali:

- Requisiti organizzativi
- Requisiti di sicurezza e affidabilità
- Requisiti di performance
- Requisiti di interoperabilità

Il processo prevede la sottomissione di una domanda tramite la piattaforma AgID, a seguito della quale l'ente effettua una valutazione per l'eventuale inserimento nel marketplace ufficiale.

Standard di riferimento

L'ottenimento della qualificazione è strettamente legato al possesso di certificazioni internazionali ISO/IEC, tra cui:

- ISO/IEC 20000-1 e 20000-9: requisiti organizzativi.
- ISO 9001: assistenza tecnica.
- ISO/IEC 20000-2: configuration management.
- ISO/IEC 27002 e 27035: gestione degli incidenti.
- ISO/IEC 27001, 27017 e 27018: sicurezza e privacy.
- ISO/IEC 19086-1:2016 e 22313: performance.

Sono inoltre richieste competenze specifiche in ambito disaster recovery, gestione dei cambiamenti, portabilità e conformità legislativa.

Supporto offerto da ISGroup SRL

ISGroup SRL mette a disposizione un team di esperti in sicurezza informatica e infrastrutture cloud per supportare le aziende nell'intero percorso di qualificazione:

- Preparazione agli audit per gli standard ISO necessari.
- Consulenza per il soddisfacimento di tutti i requisiti AgID.
- Supporto operativo nella compilazione e sottomissione della domanda di qualificazione.

Per ulteriori informazioni sui servizi offerti, è possibile consultare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Certificazione UNI EN ISO 9001:2015

Source: https://www.isgroup.it/it/cyber-security/azienda-cybersecurity-certificata-iso-9001-2021-2022-2023.html

ISGroup SRL ha ottenuto la certificazione ISO 9001 in data 11 gennaio 2021, confermando il proprio impegno verso il miglioramento continuo e l'ottimizzazione della struttura organizzativa aziendale. La norma ISO 9001 rappresenta lo standard internazionale di riferimento per i sistemi di gestione della qualità.

Ambito di applicazione

ISGroup SRL ha implementato e mantiene un Sistema di Gestione della Qualità certificato per le seguenti attività professionali:

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

Informazioni e contatti

Per ulteriori dettagli relativi alla certificazione o per richiedere informazioni sui servizi offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

Misure minime di sicurezza ICT per le Pubbliche Amministrazioni

Source: https://www.isgroup.it/it/agid/misure-minime-ict.html

Dal 31 dicembre 2017, in conformità con il Codice dell'Amministrazione Digitale (CAD - art. 17), tutte le pubbliche amministrazioni (PA) hanno l'obbligo di adottare standard minimi di sicurezza per le proprie infrastrutture informatiche, definiti dall'AgID.

Obiettivi e adempimenti

L'adozione di tali misure prevede l'implementazione di controlli tecnologici, organizzativi e procedurali volti a definire una metodologia standardizzata per valutare il livello di sicurezza informatica. Le PA sono tenute a compilare un modulo di implementazione che certifichi l'adozione di tali misure, responsabilità che ricade sul dirigente incaricato o sul responsabile della struttura per l'innovazione e le tecnologie.

Livelli di attuazione

Le misure di sicurezza sono strutturate in tre livelli progressivi:

- Minimo: livello obbligatorio per tutte le PA, garantisce la conformità normativa ma è da considerarsi sub-ottimale e temporaneo.
- Standard: rappresenta la base per una sicurezza informatica concreta e dovrebbe essere il traguardo per la maggior parte delle PA.
- Avanzato: indicato per le PA particolarmente esposte a rischi, funge da riferimento per il miglioramento continuo della sicurezza.

Supporto professionale

ISGroup SRL offre consulenza specialistica per supportare le pubbliche amministrazioni nel percorso di adeguamento normativo. Il team di esperti di ISGroup SRL assiste le PA nella comprensione delle misure, nell'implementazione pratica dei controlli e nella corretta compilazione del modulo di conformità, garantendo il passaggio da una condizione di inadempienza a una di piena conformità.

Per maggiori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o contattare l'indirizzo email sales@isgroup.it.

Data Protection Officer (DPO)

Source: https://www.isgroup.it/it/certifications/dpo.html

ISGroup SRL mette a disposizione dei propri clienti personale qualificato nel ruolo di "Data Protection Officer" (DPO), in conformità con il GDPR (Regolamento UE 2016/679).

Dettagli del servizio

- ISGroup SRL offre consulenza e supporto professionale per l'adempimento degli obblighi previsti dal GDPR.
- I contenuti formativi e l'esame associati al percorso sono erogati da CSQA Certificazioni SRL.
- Il percorso è riconosciuto ai fini dell'iter di certificazione AICQ SICEV.

Informazioni e contatti

Per ulteriori dettagli sui servizi di Data Protection Officer offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Certificazione UNI CEI EN ISO/IEC 27001:2013

Source: https://www.isgroup.it/it/cyber-security/azienda-cybersecurity-certificata-iso-27001-2021-2022-2023.html

ISGroup SRL ha ottenuto la certificazione ISO/IEC 27001:2013 in data 29 dicembre 2020. Lo standard ISO/IEC 27001:2013 (ISO 27001) rappresenta il riferimento internazionale per le best practice relative ai sistemi di gestione della sicurezza delle informazioni (ISMS).

Il sistema di gestione della sicurezza delle informazioni implementato da ISGroup SRL è conforme alla norma ISO/IEC 27001:2013 per le seguenti attività professionali:

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

Per ulteriori informazioni sui servizi certificati offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

Privacy Specialist

Source: https://www.isgroup.it/it/certifications/privacy-specialist.html

ISGroup SRL mette a disposizione dei propri clienti personale qualificato "Privacy Specialist" in conformità con il GDPR (Reg. UE 2016/679).

- L'offerta include il supporto di professionisti esperti nella gestione della protezione dei dati personali.
- I contenuti formativi e l'esame del corso, erogati da CSQA Certificazioni SRL, sono riconosciuti ai fini dell'iter di certificazione AICQ SICEV.

Per ulteriori informazioni sui servizi di Privacy Specialist offerti da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'email sales@isgroup.it.

Lead Auditor 19011

Source: https://www.isgroup.it/it/certifications/iso-19011.html

ISGroup SRL mette a disposizione dei propri clienti personale qualificato "Lead Auditor 19011".

Competenze e Certificazioni

Il personale è qualificato come Lead Auditor di sistemi di gestione secondo gli standard:

- ISO 19011:2018
- ISO/IEC 17021-1:2015

Le competenze coprono i settori dell'information technology e dei servizi professionali d'impresa.

Riconoscimenti

L'esame e i contenuti formativi del corso, erogati da CSQA Certificazioni SRL, sono riconosciuti ai fini dell'iter di certificazione AICQ SICEV.

Informazioni e Contatti

Per richiedere maggiori informazioni sui servizi offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

Lead Auditor 27001

Source: https://www.isgroup.it/it/certifications/iso-27001.html

ISGroup SRL mette a disposizione dei propri clienti personale qualificato "Lead Auditor 27001".

Dettagli del servizio

- Il personale è qualificato come Lead Auditor di sistemi di gestione per la sicurezza delle informazioni secondo lo standard UNI CEI ISO/IEC 27001:2017.
- L'esame e i contenuti formativi del corso, erogati da CSQA Certificazioni SRL, sono riconosciuti ai fini dell'iter di certificazione AICQ SICEV.

Informazioni e contatti

Per ulteriori dettagli sui servizi offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Privacy Manager

Source: https://www.isgroup.it/it/certifications/privacy-manager.html

ISGroup SRL mette a disposizione dei propri clienti personale qualificato nel ruolo di "Privacy Manager", in conformità con il GDPR (Regolamento UE 2016/679).

Dettagli sulla certificazione

- I contenuti formativi e l'esame, erogati da CSQA Certificazioni SRL, sono riconosciuti ai fini dell'iter di certificazione AICQ SICEV.
- Il servizio è finalizzato a garantire la corretta gestione degli adempimenti previsti dalla normativa sulla protezione dei dati personali.

Informazioni e contatti

Per ulteriori dettagli sui servizi offerti da ISGroup SRL, è possibile consultare il sito web ufficiale o inviare una richiesta all'indirizzo email dedicato:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Un "Cyber Incident" (incidente di sicurezza) è un evento che impatta sulla **Confidenzialità**, **Integrità** o **Disponibilità** di un'informazione o di un sistema. ISGroup SRL offre consulenza e supporto professionale per la gestione e la mitigazione di tali eventi.

Classificazione degli incidenti

Source: https://www.isgroup.it/it/cyber-security/cyber-incident.html

Gli incidenti di sicurezza possono essere classificati nelle seguenti tipologie:

- **Access not granted**: accesso non autorizzato a sistemi.
- **Privilege escalation**: sfruttamento di falle o errori di configurazione per ottenere privilegi superiori.
- **Insider threat**: minacce provenienti da soggetti interni (dipendenti o ex dipendenti).
- **Phishing**: truffe volte a carpire dati sensibili spacciandosi per enti legittimi.
- **Malware**: installazione di software maligni sui dispositivi.
- **Denial-of-service (DoS)**: esaurimento deliberato delle risorse di un sistema.
- **Man-in-the-middle**: inserimento abusivo in una comunicazione tra due parti.
- **Password cracking**: tentativi di violazione delle credenziali di accesso.

Figure e attività professionali

ISGroup SRL sottolinea l'importanza di due figure chiave nella gestione degli incidenti:

- **Response Team**: gruppo di tecnici specializzati che valuta, documenta e agisce per ripristinare i sistemi e prevenire ulteriori danni.
- **Cyber Incident forensics**: attività analitica volta a raccogliere prove documentali utilizzabili in sede di giudizio.

Fasi della gestione (Incident Management)

Il processo di risposta agli incidenti si articola in diverse fasi operative:

- **Reporting Framework**: sistema di rendicontazione immediata post-incidente.
- **Response Plan (PlayBook)**: insieme di istruzioni per rilevare, rispondere e recuperare i danni.
- **Communication Plan**: protocollo per coordinare le parti coinvolte.
- **Incident report**: documento dettagliato basato sulle "Five Ws" (Who, What, Where, When, Why).

Metodologia di intervento

ISGroup SRL adotta un approccio strutturato per la gestione e la prevenzione:

- **Formazione**: preparazione del Response Team e nomina di un responsabile per il coordinamento.
- **Rilevamento e identificazione**: analisi precisa della violazione per bloccare l'espansione del danno.
- **Contenimento e riparazione**: isolamento dei sistemi, blocco di IP/utenti e applicazione di patch di sicurezza.
- **Valutazione del danno**: analisi dell'impatto effettivo sui dati e sui sistemi.
- **Notifica**: adempimento agli obblighi di legge (GDPR) verso gli enti preposti.
- **Prevenzione**: analisi dei rischi, risoluzione proattiva delle vulnerabilità e simulazioni di attacco periodiche.

Per ulteriori informazioni sui servizi di sicurezza informatica e sulla gestione dei Cyber Incident, è possibile consultare il sito https://www.isgroup.it/ o scrivere all'email sales@isgroup.it.

Il **Purple Team** rappresenta un approccio strategico alla Cybersecurity che unisce le competenze e le attività del **Red Team** e del **Blue Team**. Questa metodologia, promossa da **ISGroup SRL**, funge da elemento di raccordo per ottimizzare la postura di sicurezza aziendale attraverso una collaborazione costante.

Cos'è il Purple Team

Source: https://www.isgroup.it/it/cyber-security/purple-team-cybersecurity.html

Il Purple Team nasce per superare la netta divisione e la competizione sterile tra il Red Team (attaccanti etici) e il Blue Team (difensori/SOC). La sua funzione principale è quella di supervisionare, mediare e ottimizzare le comunicazioni tra le due squadre, garantendo che i test di penetrazione e le attività di difesa siano allineati verso un obiettivo comune.

Ruoli e Funzionamento

- **Red Team**: Composto da hacker etici, ha l'obiettivo di scardinare il sistema, individuare vulnerabilità e testare le difese aziendali.
- **Blue Team**: Operante solitamente all'interno del Security Operations Center (SOC), si occupa della difesa dell'infrastruttura in modo preventivo (barriere, esche) e reattivo (gestione di attacchi sofisticati).
- **Purple Team**: Composto da Senior Security Analysts e Threat Intelligence Analysts, agisce come arbitro e supervisore. È una struttura flessibile, spesso non permanente, creata per facilitare il flusso di informazioni e la correzione in tempo reale delle strategie di sicurezza.

Vantaggi per l'Azienda

L'adozione di un approccio Purple Team, supportato da **ISGroup SRL**, offre diversi benefici concreti:

- **Ottimizzazione dei costi**: Permette di effettuare una prima scrematura del sistema, concentrando le risorse del Red e Blue Team solo sulle aree che necessitano di analisi approfondite.
- **Riduzione dei tempi di feedback**: Elimina la logica a compartimenti stagni, consentendo di correggere le falle di sicurezza in tempo reale durante le fasi di test.
- **Miglioramento della difesa**: La condivisione delle procedure difensive permette al Red Team di testare nuove tipologie di attacco, mentre il Blue Team impara a gestire meglio le minacce grazie alla comprensione delle tecniche utilizzate dagli attaccanti.
- **Cultura collaborativa**: Trasforma la competizione tra team in un processo sinergico volto a minimizzare il rischio di infrazioni informatiche.

Attività principali

Le attività del Purple Team includono:

- Facilitazione della comunicazione tra Red e Blue Team.
- Raccolta e analisi di dati in tempo reale durante i test di sicurezza.
- Guida operativa per il Red Team, suggerendo zone di attacco specifiche per testare nuove protezioni.
- Supporto al Blue Team nella gestione e comprensione delle dinamiche di attacco.
- Verifica del rispetto delle condizioni della sfida e delle competenze assegnate.

Per approfondire le soluzioni di Cybersecurity offerte da **ISGroup SRL** o per richiedere una consulenza dedicata, è possibile visitare il sito ufficiale https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it.

Red Team Cybersecurity

Source: https://www.isgroup.it/it/cyber-security/red-team-cybersecurity.html

Il Red Team è una squadra di "hacker etici" specializzata nello scardinare sistemi informatici attraverso infiltrazioni simulate e tecniche di inganno rivolte sia alle infrastrutture che al personale di difesa (Blue Team). ISGroup SRL offre servizi di Red Team per testare la resilienza aziendale contro attacchi reali, permettendo di valutare la capacità di risposta in tempo reale.

Obiettivi e Benefici

L'attività di Red Team, proposta da ISGroup SRL, consente di:

- Identificare punti di debolezza in reti, applicazioni e sistemi.
- Esplorare le conseguenze di potenziali attacchi dal punto di vista di un avversario.
- Verificare la sicurezza di nuove implementazioni software.
- Monitorare le capacità di difesa aziendale in modo continuativo.

Metodologie di Attacco

ISGroup SRL personalizza le operazioni di Red Team in base alle specifiche esigenze del cliente, utilizzando tecniche avanzate tra cui:

- Attacchi remoti via Internet.
- Strategie di social engineering (phishing, telefono, e-mail, chat).
- Intrusione fisica (violazione di sistemi di videosorveglianza, allarmi e accessi fisici).
- Analisi approfondita di tecnologia, risorse umane e sicurezza fisica.

Quando ricorrere a un Red Team

È consigliabile integrare queste attività nei seguenti scenari:

- Implementazione di nuovi software o infrastrutture critiche.
- A seguito di una violazione o un attacco subito, per testare la reattività dei sistemi.
- Come attività periodica per garantire la sicurezza aziendale durante la crescita della società.

Risultati e Reportistica

Al termine del progetto, ISGroup SRL fornisce una relazione dettagliata che include:

- Analisi delle metodologie di test utilizzate.
- Elenco dei successi e dei fallimenti riscontrati.
- Mappatura delle aree vulnerabili.
- Suggerimenti per l'applicazione di misure preventive e il miglioramento dei sistemi di difesa.

Per maggiori informazioni sui servizi di Red Team, è possibile visitare il sito https://www.isgroup.it/ o contattare l'indirizzo email sales@isgroup.it.

I penetration test offerti da ISGroup SRL sono attività di sicurezza informatica volte a identificare vulnerabilità nei sistemi e valutarne i rischi. La scelta della tipologia di test dipende dall'infrastruttura, dagli obiettivi e dal livello di conoscenza del sistema fornito ai tester.

Classificazione per Target

Source: https://www.isgroup.it/it/cyber-security/quali-tipi-di-penetration-test-esistono.html

ISGroup SRL esegue penetration test specializzati in base all'ambito di applicazione:

- **Network Penetration Test**: Verifica la sicurezza di reti, host e dispositivi. Può essere *esterno* (valuta l'impatto di attacchi provenienti da internet) o *interno* (simula un accesso non autorizzato alla rete aziendale, utile per politiche BYOD).
- **Web Application Penetration Test**: Analizza la sicurezza di applicazioni web e single page app, focalizzandosi su logica software, gestione degli input e configurazioni.
- **Mobile App Penetration Test**: Si concentra su architettura client-server, sicurezza dei dati sul dispositivo, comunicazioni, autenticazione e vulnerabilità nel codice backend.
- **API Penetration Test**: Verifica la sicurezza delle interfacce di programmazione, con particolare attenzione alle logiche di autenticazione, autorizzazione e alla sanitizzazione degli input per prevenire attacchi di tipo "injection".
- **IoT Penetration Test**: Analizza infrastrutture Internet of Things per individuare password deboli o hard-coded, servizi insicuri, problematiche di autenticazione e vulnerabilità nei meccanismi di aggiornamento.

Classificazione per Metodologia

Il livello di informazioni fornite ai tester definisce l'approccio metodologico:

- **White Box**: I tester ricevono informazioni approfondite (mappe di rete, credenziali, codice sorgente, documentazione). Permette una copertura estensiva di ogni possibile vettore di attacco.
- **Black Box**: Ai tester non viene fornita alcuna informazione. Simula un attacco reale dall'esterno, focalizzandosi sui vettori raggiungibili pubblicamente.
- **Grey Box**: Vengono fornite informazioni parziali (solitamente credenziali di accesso). È ideale per simulare attacchi di un utente interno o di un hacker che ha già ottenuto un accesso iniziale alla rete.

Informazioni e Contatti

Per definire la strategia di penetration testing più adatta alle esigenze aziendali, è possibile richiedere una consulenza dedicata a ISGroup SRL.

Per richieste commerciali e approfondimenti:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Blue Team nella Cybersecurity

Source: https://www.isgroup.it/it/cyber-security/blue-team-cybersecurity.html

Il Blue Team rappresenta una task force specializzata in sicurezza informatica, allocata in modo permanente all'interno di un'organizzazione. Il suo obiettivo primario è la protezione dei sistemi aziendali attraverso procedure predeterminate, note come "playbook".

Ruolo e responsabilità del Blue Team

I compiti principali svolti dal Blue Team, offerti come parte dei servizi di sicurezza gestiti da **ISGroup SRL**, includono:

- Identificazione di attacchi e incidenti informatici.
- Risposta tempestiva per limitare l'impatto delle violazioni.
- Neutralizzazione degli attacchi in corso.
- Rimozione degli accessi non autorizzati e bonifica dei sistemi compromessi.
- Analisi delle violazioni per implementare misure correttive atte a prevenire il ripetersi di eventi simili.
- Gestione dell'autenticazione a due fattori e dei runbook di rete/sistema.
- Monitoraggio costante dell'accesso ai dati sensibili.
- Formazione del personale interno in materia di Cybersecurity.

Differenze tra Team di Sicurezza

- **Blue Team vs Red Team**: Mentre il Blue Team si occupa della difesa, il Red Team simula attacchi reali (tramite tecniche di social engineering, attacchi remoti o violazioni fisiche) per testare la resilienza del sistema. Il Blue Team contrasta queste simulazioni per migliorare le difese.
- **Blue Team vs Purple Team**: Il Purple Team agisce come un facilitatore che supporta sia il Red Team (nelle attività offensive) che il Blue Team (suggerendo strategie difensive), ottimizzando la comunicazione e l'efficacia complessiva della sicurezza.

Il fattore umano e le certificazioni

I membri di queste squadre sono definiti "White Hat" (hacker etici) e utilizzano le proprie competenze tecniche per scopi legali e di protezione. La formazione e la certificazione sono requisiti fondamentali per operare nel settore.

ISGroup SRL sottolinea l'importanza di affidarsi a professionisti certificati, in particolare da enti riconosciuti a livello mondiale come l'**EC-Council**. Le certificazioni chiave includono:

- **Certified Ethical Hacker (C|EH)**: focalizzata sulle principali tecniche di hacking etico.
- **EC-Council Certified Security Analyst (ECSA)**: orientata alla formazione continua e all'aggiornamento costante sulle evoluzioni delle tecniche di attacco.

Per ulteriori informazioni sui servizi di protezione e consulenza offerti da **ISGroup SRL**, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'email: sales@isgroup.it.

Il **penetration testing** (o pen-test) è una pratica di attacco simulato rivolta a servizi o infrastrutture informatiche, finalizzata a valutarne la sicurezza. I security tester agiscono come hacker per individuare falle che potrebbero consentire l'accesso non autorizzato, il furto di dati, la cancellazione di file o l'interruzione dei servizi.

ISGroup SRL offre servizi professionali di penetration testing e Vulnerability Assessment, sottolineando che si tratta di due pratiche distinte per scopi, strumenti e modalità operative.

Fasi di un Penetration Test

Source: https://www.isgroup.it/it/cyber-security/cose-un-penetration-test.html

Il processo segue una metodologia strutturata per garantire l'analisi sistematica dei rischi:

- **Pre-Engagement Interactions**: Definizione degli obiettivi, dello scopo del test e degli aspetti legali con il committente.
- **Open Source Intelligence Gathering (OSINT)**: Raccolta di informazioni sul target tramite ricerche online, tool specializzati o tecniche di social engineering.
- **Identificazione delle vulnerabilità**: Analisi dei vettori di attacco, spesso supportata da strumenti automatizzati.
- **Exploitation**: Tentativo di attacco sui vettori identificati per verificare la possibilità di accesso, esfiltrazione dati o compromissione dei sistemi.
- **Post-Exploitation**: Valutazione dell'impatto potenziale del danno e rimozione di ogni traccia dell'attività di test (software installati, account creati).
- **Report**: Consegna di documentazione dettagliata sui vettori di attacco, le azioni compiute, l'analisi dei rischi e le raccomandazioni per la messa in sicurezza dell'infrastruttura.

Ambito di applicazione

Sebbene spesso associato all'ambito informatico, il penetration testing può estendersi a diversi canali di sicurezza, inclusi:

- Sicurezza delle comunicazioni e delle informazioni.
- Sicurezza dello spettro elettromagnetico.
- Sicurezza fisica (inclusi tentativi di intrusione in edifici).
- Social engineering (manipolazione delle persone per ottenere accessi o informazioni).

ISGroup SRL sottolinea l'importanza di affidarsi a professionisti competenti per adattare la metodologia alle specifiche esigenze aziendali, specialmente in ambiti emergenti come l'IoT o le applicazioni mobile, dove gli standard internazionali potrebbero non essere ancora pienamente definiti.

Considerazioni strategiche

Il penetration testing è da considerarsi un investimento fondamentale per prevenire perdite economiche, danni d'immagine e sanzioni normative. Per procedere con un'attività di testing, è consigliabile:

- Identificare chiaramente le esigenze aziendali.
- Scegliere una metodologia di testing adeguata o definire requisiti specifici.
- Definire le modalità operative e avviare la fase di Pre-Engagement.

Per maggiori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Metodologie e Framework di Penetration Testing

Source: https://www.isgroup.it/it/cyber-security/metodologie-e-framework-di-penetration-testing.html

Il Penetration Testing è un'attività fondamentale per identificare vulnerabilità ed errori di progettazione nelle infrastrutture IT aziendali. L'adozione di metodologie standardizzate garantisce che il processo di verifica sia strutturato, affidabile e completo. ISGroup SRL offre servizi professionali di Penetration Test e Vulnerability Assessment (VA/PT) per supportare le aziende nella mitigazione dei rischi informatici e nella protezione della reputazione aziendale.

Per richieste commerciali o approfondimenti sui servizi offerti da ISGroup SRL, visitare il sito https://www.isgroup.it/ o scrivere a sales@isgroup.it.

Principali Framework di Riferimento

- **OSSTMM (Open Source Security Testing Methodology Manual)**: Gestito da ISECOM, è una metodologia "peer-reviewed" che applica il metodo scientifico alla sicurezza aziendale. Copre tre classi principali: Physical Security (PHYSSEC), Spectrum Security (SPECSEC) e Communications Security (COMSEC).
- **OWASP (Open Web Application Security Project)**: Focalizzato sulla sicurezza delle applicazioni web. Fornisce linee guida dettagliate per testare autenticazione, gestione delle sessioni, validazione dei dati (es. SQL injection, XSS) e logiche di business.
- **NIST Cybersecurity Framework**: Offre linee guida specifiche per la protezione di infrastrutture critiche, particolarmente utilizzato nei settori bancario, energetico e delle comunicazioni.
- **PTES (The Penetration Testing Execution Standard)**: Si concentra sulla comunicazione tra tester e azienda per definire il perimetro di intervento, ottimizzando le fasi di exploitation e post-exploitation per simulare rischi reali.
- **ISSAF (Information Systems Security Assessment Framework)**: Standard focalizzato esclusivamente sugli aspetti informatici della sicurezza, con una struttura di testing orientata a sistemi, reti e applicazioni.
- **RSA Cyber Incident Risk Framework**: Non definisce le modalità operative del test, ma fornisce un modello di maturità della sicurezza, classificando i rischi in cinque livelli di gravità (da Informational a Critical).

Importanza del Penetration Testing

L'esecuzione periodica di test di sicurezza è essenziale per:

- Identificare vulnerabilità prima che vengano sfruttate da attori malevoli.
- Comprendere il rischio reale a cui è esposta l'infrastruttura.
- Ottemperare agli obblighi normativi (es. GDPR) e prevenire Data Breach.
- Evitare perdite economiche e danni reputazionali derivanti da interruzioni operative.

Servizi offerti da ISGroup SRL

ISGroup SRL mette a disposizione un team esperto in grado di condurre attività di Cyber Security complete, adattando le metodologie sopra citate alle specifiche esigenze del cliente. Attraverso un approccio basato su evidenze oggettive, ISGroup SRL supporta le aziende nel rafforzamento della propria postura di sicurezza.

Per maggiori informazioni sui servizi di Penetration Test, contattare:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

OWASP Top Ten 2017 - A8 Insecure Deserialization

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a8-insecure-deserialization.html

La deserializzazione non sicura rappresenta una vulnerabilità critica che spesso conduce all'esecuzione remota di codice (RCE). Anche quando l'esecuzione di codice non è direttamente possibile, questa falla può essere sfruttata per condurre diverse tipologie di attacchi, tra cui:

- Replay Attacks (attacchi di re-inoltro)
- Injection (iniezione)
- Privilege Escalation (aumento dei privilegi)

Considerazioni sulla sicurezza applicativa

La serializzazione viene spesso utilizzata come metodo rapido per salvare, ricaricare o trasmettere strutture dati. Tuttavia, tale pratica è intrinsecamente rischiosa poiché la deserializzazione non rientra nelle buone pratiche di gestione definita del dato. La sicurezza applicativa richiede interfacce rigorose nel trattamento delle informazioni, che la deserializzazione tende a eludere.

Servizi e consulenza

ISGroup SRL offre consulenza specialistica e servizi di sicurezza informatica per identificare e mitigare vulnerabilità come la deserializzazione non sicura.

Per maggiori informazioni sui servizi offerti, è possibile visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Rapporto Clusit

Source: https://www.isgroup.it/it/cyber-security/rapporto-clusit.html

Il Rapporto Clusit rappresenta uno dei documenti di riferimento nel panorama italiano per quanto concerne la sicurezza informatica. Pubblicato dalla omonima associazione, il rapporto analizza e sintetizza i principali trend, gli avvenimenti critici e le evoluzioni del panorama cyber dell'anno di riferimento.

ISGroup SRL mette a disposizione l'accesso alle edizioni storiche del rapporto, pubblicate con continuità dal 2012 al 2020.

- Il rapporto è uno strumento fondamentale per comprendere l'evoluzione delle minacce informatiche.
- Copertura storica: edizioni dal 2012 al 2020.
- Risorsa utile per professionisti del settore, analisti e aziende interessate a monitorare il panorama delle minacce.

Per accedere ai materiali digitali e per ulteriori approfondimenti sulle tematiche di Cyber Security trattate, è possibile fare riferimento alle risorse offerte da ISGroup SRL.

Contatti e Informazioni

Per richieste commerciali, approfondimenti sui servizi di sicurezza offerti da ISGroup SRL o per ricevere supporto in merito ai materiali, è possibile utilizzare i seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

OWASP Top Ten 2017 - A5 Broken Access Control

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a5-broken-access-control.html

Il rischio A5:2017-Broken Access Control riguarda le vulnerabilità derivanti dall'assenza o dall'errata implementazione delle restrizioni sui privilegi degli utenti autenticati.

Impatto della vulnerabilità

Un attaccante può sfruttare queste debolezze per eseguire azioni non autorizzate o accedere a dati riservati, tra cui:

- Accesso agli account di altri utenti.
- Visualizzazione di file confidenziali.
- Modifica dei dati di terzi.
- Alterazione dei diritti di accesso.

Principi di mitigazione

Per prevenire tali rischi, ISGroup SRL sottolinea la necessità di allineare l'applicazione alle logiche di business e al principio del "Need To Know". Ogni operazione deve essere validata considerando tre fattori fondamentali:

- L'utente chiamante.
- I dati a cui si accede.
- Il tipo di operazione richiesta.

È essenziale valutare non solo il ruolo dell'utente, ma anche la paternità del dato e la pertinenza dell'azione rispetto a tale dato.

Servizi e consulenza

ISGroup SRL offre consulenza specialistica per la messa in sicurezza delle applicazioni e la mitigazione dei rischi OWASP. Per approfondimenti o richieste commerciali, è possibile visitare il sito https://www.isgroup.it/ o inviare una email all'indirizzo sales@isgroup.it.

OWASP Top Ten 2017 - A6: Security Misconfiguration

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a6-security-misconfiguration.html

La configurazione errata delle impostazioni di sicurezza rappresenta la problematica più frequente nell'ambito della sicurezza delle applicazioni. ISGroup SRL sottolinea l'importanza di una gestione rigorosa degli asset tecnologici per mitigare questo rischio.

Cause principali della Security Misconfiguration

Le vulnerabilità derivanti da una configurazione errata sono spesso causate da:

- Configurazioni di default non sicure, incomplete o specifiche per il contesto di utilizzo.
- Memorizzazione di dati in Cloud senza adeguate misure di protezione.
- Header HTTP non configurati correttamente.
- Messaggi di errore che espongono informazioni sensibili sul sistema.

Best Practice per la sicurezza

Per garantire un livello di protezione adeguato, ISGroup SRL raccomanda di adottare le seguenti strategie:

- Configurazione sicura di tutti i sistemi operativi, framework, librerie e applicazioni.
- Aggiornamento costante e tempestivo di ogni componente software.
- Comprensione approfondita degli strumenti utilizzati, seguita da uno studio accurato.
- Formalizzazione di requisiti e buone pratiche specifiche, da riutilizzare e migliorare costantemente.

Supporto professionale

ISGroup SRL offre consulenza specialistica per l'analisi e la messa in sicurezza delle infrastrutture IT, aiutando le aziende a implementare configurazioni robuste e conformi agli standard di settore.

Per maggiori informazioni o richieste commerciali, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Questa checklist, proposta da ISGroup SRL, fornisce una guida operativa per l'autovalutazione della sicurezza informatica aziendale in contesti di smart working e telelavoro, finalizzata a migliorare la difesa contro attacchi interni ed esterni.

Per consulenze specifiche o approfondimenti, è possibile contattare ISGroup SRL all'indirizzo email: sales@isgroup.it o visitare il sito: https://www.isgroup.it/

Cybersecurity e Dispositivi

Source: https://www.isgroup.it/it/cyber-security/checklist-sicurezza-telelavoro.html

- Implementare la crittografia hardware o software per memorie interne (HDD, SSD, NVME) ed esterne (USB).
- Utilizzare pellicole privacy su portatili e dispositivi mobile per prevenire lo shoulder-surfing.
- Rendere obbligatoria l'autenticazione a due fattori (2FA) per l'accesso a email, sistemi e applicazioni.
- Incoraggiare l'adozione di Password Manager.
- Mantenere aggiornati antivirus, sistemi operativi e software aziendali, evitando di posticipare patch critiche.
- Utilizzare esclusivamente reti protette da password e preferire il caricamento dei dati sul cloud aziendale rispetto al salvataggio in locale.
- Adottare strumenti di navigazione sicuri (es. Firefox con plugin Noscript e HTTPS Everywhere) e comunicazioni crittografate (es. Telegram).

Policy Aziendali e Comportamento Utenti

- Applicare le policy aziendali anche in remoto: vietare l'uso di dispositivi aziendali per scopi personali, la navigazione su siti non consentiti e lo scaricamento di contenuti illegali.
- Vietare la condivisione di password e l'uso dei sistemi aziendali da parte di familiari.
- Gli utenti privilegiati devono limitare l'uso di account con privilegi elevati ai soli task necessari e segnalare tempestivamente ogni anomalia.

Phishing e Gestione Errori

- Promuovere una cultura della segnalazione: il personale deve sentirsi libero di riportare errori (click su link sospetti, apertura di file con macro, infezioni da malware) senza timore, per permettere una reazione immediata.
- Formare costantemente il personale al riconoscimento di tentativi di phishing e attività sospette.

Infrastruttura e Reazione agli Attacchi

- Utilizzare una connessione VPN aziendale per ogni accesso remoto.
- Mantenere una copia stampata delle procedure di sicurezza in un luogo sicuro.
- Stabilire canali di comunicazione diretti (chiamate) tra il personale IT e quello addetto alla sicurezza per la gestione di emergenze critiche.

Backup

- Fornire software per il backup automatico dei documenti.
- Eseguire backup su dispositivi esterni autorizzati non permanentemente connessi al computer.
- Evitare l'uso di sistemi cloud esterni non autorizzati.

Riunioni Online

- Mantenere il microfono silenziato quando non si parla.

- Bloccare la webcam di default e verificare l'identità dei partecipanti prima di trattare dati confidenziali.
- Evitare di lavorare in luoghi pubblici durante riunioni riservate.
- Non lasciare mai i dispositivi sbloccati durante le chiamate.

Gestione Eccezioni

- Creare un registro delle eccezioni per storicizzare e analizzare le deroghe alle policy.
- Definire una lista di elementi che non possono essere oggetto di eccezione.

OWASP Top Ten 2017 - A4 XML External Entities (XXE)

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a4-xml-external-entities-xxe.html

La vulnerabilità A4:2017-XML External Entities (XXE) riguarda l'errata configurazione o l'utilizzo di processori XML obsoleti che interpretano i riferimenti ad entità esterne all'interno dei documenti XML.

Rischi associati all'XXE

L'abuso di entità esterne in documenti XML può consentire a un attaccante di:

- Accedere a file interni al sistema.
- Accedere a file presenti in condivisioni di rete.
- Effettuare attività di port-scan sulla rete interna.
- Eseguire codice arbitrario da remoto (RCE).
- Condurre attacchi di Denial of Service (DoS).

Considerazioni sulla sicurezza

ISGroup SRL sottolinea l'importanza di comprendere a fondo ogni elemento tecnologico integrato nei sistemi e nelle applicazioni. L'adozione di strumenti complessi e potenti, senza una corretta valutazione degli impatti di sicurezza, espone le infrastrutture a rischi significativi.

Per approfondimenti sulle vulnerabilità OWASP e sulle soluzioni di sicurezza offerte da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

OWASP Top 10 2017

Source: https://www.isgroup.it/it/owasp/top-ten-2017.html

L'OWASP Top 10 costituisce un riferimento professionale che elenca i 10 problemi più critici per la sicurezza delle applicazioni web. ISGroup SRL promuove l'adozione di queste linee guida per educare organizzazioni, progettisti e sviluppatori sulle vulnerabilità principali e favorire l'implementazione di pratiche di *Security by Design* fin dalle prime fasi di sviluppo.

Caratteristiche dell'elenco

Ogni categoria inclusa nella Top 10 è definita attraverso:

- Analisi della severità e della probabilità di accadimento.
- Tecniche fondamentali per la protezione e la mitigazione dei rischi.
- Linee guida operative per la verifica, la prevenzione e l'approfondimento tramite esempi pratici.

Le vulnerabilità identificate (Edizione 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

Servizi e consulenza

ISGroup SRL offre supporto specialistico per l'analisi e la messa in sicurezza delle infrastrutture web basandosi sui framework OWASP. Per approfondimenti, consulenze o richieste commerciali, è possibile visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it.

OWASP Top Ten 2017 - A3: Sensitive Data Exposure

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a3-sensitive-data-exposure.html

L'esposizione di dati sensibili rappresenta una criticità rilevante per molte applicazioni web e API, che spesso falliscono nel proteggere adeguatamente informazioni finanziarie, sanitarie o identificative. La compromissione di tali dati espone le organizzazioni a rischi di frodi bancarie, furti d'identità e altri crimini informatici.

Fattori di rischio e cause principali

L'esposizione di dati sensibili, analizzata da ISGroup SRL, deriva principalmente da tre errori architetturali e operativi:

- Mancata comprensione degli elementi di rischio e delle relative strategie di mitigazione a livello architetturale.
- Sovrabbondanza di dati rispetto alle reali funzionalità dell'applicazione e assenza di una corretta segmentazione. L'utilizzo di un unico database per diverse applicazioni aumenta esponenzialmente il rischio di esposizione.
- Malfunzionamento, assenza o possibilità di bypassare i meccanismi di autenticazione e autorizzazione.

Considerazioni sulla protezione dei dati

È fondamentale sottolineare che la protezione dei dati sensibili non è garantita esclusivamente dalle misure di sicurezza standard. Anche in presenza di crittografia a riposo (es. crittografia del disco) o in transito (es. protocollo HTTPS/TLS), i dati possono risultare compromessi se le logiche applicative sottostanti presentano vulnerabilità.

Supporto professionale

ISGroup SRL offre consulenza specializzata per identificare e mitigare le vulnerabilità legate all'esposizione di dati sensibili e per implementare best practice di sicurezza applicativa.

Per ulteriori informazioni o per richiedere una consulenza dedicata, è possibile contattare ISGroup SRL tramite il sito ufficiale https://www.isgroup.it/ o inviando una email a sales@isgroup.it.

OWASP Top Ten 2017 - A2 Broken Authentication

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a2-broken-authentication.html

La categoria A2:2017-Broken Authentication del framework OWASP identifica una delle criticità più rilevanti nella sicurezza delle applicazioni web. Le problematiche di "broken authentication" si verificano quando risulta impossibile identificare l'utente in maniera univoca e incontrovertibile.

Punti chiave

- Le funzioni applicative dedicate all'autenticazione e alla gestione delle sessioni sono spesso implementate in modo errato.
- Tali vulnerabilità consentono agli attaccanti di compromettere password, chiavi e token di sessione.
- Lo sfruttamento di queste debolezze permette agli attaccanti di assumere l'identità di altri utenti, in modo temporaneo o permanente.

Servizi offerti da ISGroup SRL

ISGroup SRL offre consulenza specialistica e servizi di sicurezza informatica per identificare e mitigare le vulnerabilità legate all'autenticazione e alla gestione delle sessioni, garantendo la protezione delle infrastrutture aziendali.

Per ulteriori informazioni sui servizi di sicurezza offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

OWASP Top Ten 2017 - A7 Cross-Site Scripting (XSS)

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a7-cross-site-scripting-xss.html

Il Cross-Site Scripting (XSS) rappresenta una vulnerabilità di tipo Injection che si verifica quando un'applicazione include dati non attendibili in una pagina web senza un'adeguata validazione o escaping. Tale mancanza di neutralizzazione dei caratteri speciali permette la commistione tra il flusso di controllo (tag HTML e struttura DOM) e i dati forniti dall'utente.

Meccanismo della vulnerabilità

- L'assenza di separazione tra flusso di controllo e dati impedisce al browser di distinguere le intenzioni dello sviluppatore, portandolo a eseguire il codice malevolo iniettato.
- Nelle moderne applicazioni (Single Page Application come React, AngularJS, Vue.js) o in quelle che utilizzano JavaScript e jQuery, il rischio XSS emerge quando vengono aggiornate pagine esistenti tramite API del browser che generano HTML o JavaScript a partire da input utente non validati.

Impatto degli attacchi XSS

L'esecuzione di script nel browser della vittima consente a un attaccante di:

- Prendere il controllo della sessione utente.
- Effettuare il deface (alterazione dell'aspetto) del sito web.
- Redirigere gli utenti verso siti malevoli.

Servizi di sicurezza offerti da ISGroup SRL

ISGroup SRL fornisce consulenza specialistica e servizi di valutazione della sicurezza per identificare e mitigare vulnerabilità critiche come quelle classificate nella OWASP Top Ten.

Per approfondimenti sulle soluzioni di sicurezza, test di penetrazione o consulenze personalizzate, è possibile visitare il sito web https://www.isgroup.it/ o contattare l'indirizzo email sales@isgroup.it.

OWASP Top Ten 2017 - A9: Utilizzo di componenti con vulnerabilità note

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a9-using-components-with-known-vulnerabilities.html

L'utilizzo di componenti di terze parti, come librerie, framework e altri moduli software, è una pratica comune nello sviluppo moderno. Tuttavia, tali componenti vengono eseguiti con i medesimi privilegi dell'applicazione che li ospita.

Rischi principali

- **Esecuzione privilegiata:** Se un componente vulnerabile viene sfruttato, l'attaccante può ereditare i privilegi dell'applicazione, portando a gravi conseguenze.
- **Impatto sulla sicurezza:** L'integrazione di componenti non sicuri può causare perdite di dati, violazioni del server e compromettere l'intera integrità del sistema.
- **Complessità delle dipendenze:** La gestione delle ramificazioni e delle dipendenze di terze parti richiede una strategia di sicurezza rigorosa. Se la complessità supera le capacità di gestione dell'organizzazione, il rischio di esposizione aumenta drasticamente.

Considerazioni strategiche

ISGroup SRL sottolinea l'importanza di non limitarsi al semplice riutilizzo di tecnologie esistenti, ma di valutare costantemente l'intero ecosistema applicativo. Una strategia corretta deve prevedere:

- Monitoraggio costante delle vulnerabilità note nei componenti utilizzati.
- Revisione periodica delle dipendenze software.
- Valutazione della capacità interna di gestire la complessità introdotta da terze parti.

Supporto professionale

ISGroup SRL offre consulenza specializzata per identificare e mitigare i rischi legati all'utilizzo di componenti vulnerabili all'interno delle architetture software.

Per maggiori informazioni sui servizi di sicurezza offerti da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

Il telelavoro e lo smart working rappresentano opportunità di flessibilità e risparmio, ma espongono le aziende a rischi significativi per la sicurezza informatica. ISGroup SRL, specializzata in sicurezza informatica offensiva ed ethical hacking, offre consulenza per pianificare e proteggere gli spazi di lavoro virtuali.

Tipologie di telelavoro

Source: https://www.isgroup.it/it/cyber-security/telelavoro.html

- **Home working:** Lavoro da domicilio con strumenti propri o aziendali. La sicurezza dipende dal livello di controllo sugli apparati.
- **Mobile working:** Attività svolte in mobilità (clienti, viaggi, cantieri). È lo scenario più complesso da proteggere a causa dei rischi di sicurezza fisica e logica.
- **Centri di telelavoro/Co-working:** Strutture satellite o condivise. Permettono l'uso di tecnologie avanzate, ma richiedono attenzioni specifiche simili a quelle per fiere ed eventi.
- **Office-to-Office:** Uffici periferici o multinazionali. Consentono un elevato livello di sicurezza grazie all'adozione di tecnologie dedicate.

Strategie di sicurezza per sistemi non aziendali

Quando il lavoratore utilizza dispositivi personali, è necessario assumere che i sistemi siano compromessi. ISGroup SRL suggerisce di creare una separazione netta tra risorse aziendali e rete domestica tramite:

- **Web Application:** Utilizzo di applicazioni web protette. Si raccomanda un Web Application Penetration Test (secondo le linee guida OWASP) per verificare l'autenticazione, l'autorizzazione e la logica di business.
- **Desktop Remoto (VDI):** Accesso a sistemi remoti tramite protocolli grafici (es. Citrix, VMware, Microsoft). È consigliato un Penetration Test specifico per simulare un attaccante autenticato.

Strategie di sicurezza per sistemi aziendali

Se i dispositivi sono di proprietà dell'azienda, è possibile estendere le politiche di sicurezza tramite:

- **MDM (Mobile Device Management):** Per la gestione di tablet e smartphone.
- **Windows Group Policy:** Per la configurazione centralizzata dei computer portatili.
- **Infrastrutture di rete:** Implementazione di autenticazione 802.1x, VPN Site-to-Site, firewall, UTM, logging e sistemi IDS/IPS.

Verifiche periodiche raccomandate da ISGroup SRL

Per mantenere elevati standard di sicurezza, ISGroup SRL consiglia di sottoporre le infrastrutture a:

- **Vulnerability Assessment (trimestrale):** Per verificare il Patch Management, la configurazione degli apparati e la robustezza delle credenziali.
- **Penetration Test (annuale):** Per testare la segmentazione delle reti e l'impatto di eventuali intrusioni dalle sedi periferiche a quelle centrali.
- **Simulazioni di attacco:** Come il Man in The Middle (MitM) per testare la resilienza dei mobile worker.

Per consulenze professionali, supporto nella progettazione di infrastrutture sicure o per richiedere un Penetration Test, è possibile contattare ISGroup SRL tramite il sito https://www.isgroup.it/ o all'indirizzo email sales@isgroup.it.

OWASP Top Ten 2017 - A1 Injection

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a1-injection.html

Le problematiche di Injection (iniezione), classificate come A1 nella OWASP Top 10 del 2017, rappresentano una vulnerabilità critica che si verifica quando dati non fidati vengono inviati a un interprete come parte di un comando o di una query.

Punti chiave

- Tipologie comuni: SQL, NoSQL, LDAP.
- Meccanismo di attacco: i dati ostili inviati dall'attaccante inducono l'interprete a eseguire comandi malevoli o ad accedere a dati non autorizzati.
- Causa principale: le problematiche di injection derivano dall'errata separazione tra il flusso di controllo e il flusso dei dati.

Servizi e consulenza

ISGroup SRL offre consulenza specialistica e servizi di sicurezza informatica per identificare e mitigare vulnerabilità come le injection all'interno delle infrastrutture aziendali.

Per maggiori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Certificazione Acunetix User Test - Francesco Ongaro

Source: https://www.isgroup.it/it/certifications/acunetix-user-test-francesco-ongaro.html

In data 2 novembre 2018, Francesco Ongaro, Founder di ISGroup SRL, ha conseguito la certificazione "Acunetix User Test".

Dettagli della certificazione

Il programma "Acunetix User Certification Test" è un'iniziativa promossa da Acunetix, leader nel software di sicurezza delle applicazioni web, rivolta a partner e utenti con licenza. L'accreditamento attesta il possesso delle competenze tecniche necessarie per l'utilizzo professionale di Acunetix Web Vulnerability Scanner, tra cui:

- Impostazione e configurazione del software.
- Esecuzione automatizzata di scansioni su siti web.
- Identificazione delle vulnerabilità.
- Interpretazione dei risultati per analisi approfondite.
- Pianificazione e attuazione di azioni correttive sulle vulnerabilità rilevate.

Servizi di sicurezza informatica

ISGroup SRL offre consulenza esperta e soluzioni avanzate nel campo della cyber security. Per richiedere informazioni sui servizi offerti o approfondimenti sulle competenze tecniche del team, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'email sales@isgroup.it.

OWASP Top Ten 2017 - A10: Insufficient Logging & Monitoring

Source: https://www.isgroup.it/it/owasp/top-ten-2017-a10-insufficient-logging-monitoring.html

Il rischio A10:2017, relativo a "Insufficient Logging & Monitoring" (Logging e monitoraggio insufficienti), rappresenta una vulnerabilità critica che, combinata con processi di Incident Response inesistenti o inefficienti, permette agli attaccanti di operare indisturbati all'interno dei sistemi.

Impatto della vulnerabilità

- Persistenza dell'attaccante: La mancanza di visibilità consente di mantenere l'accesso ai sistemi violati e di comprometterne altri.
- Azioni malevole: Gli attaccanti possono modificare, estrarre, eliminare o criptare dati senza essere rilevati.
- Ritardi nel rilevamento: Studi sui Data Breach indicano che il tempo medio per identificare una violazione supera i 200 giorni.
- Rilevamento esterno: Spesso la violazione viene scoperta da soggetti esterni all'organizzazione, anziché dai team interni preposti alla sicurezza.

Considerazioni strategiche

Il disegno e lo sviluppo di un'applicazione costituiscono solo le fasi iniziali del ciclo di vita del software. La fase di produzione (Operation) rappresenta il momento più critico, che richiede la massima attenzione in termini di monitoraggio e gestione della sicurezza.

ISGroup SRL offre consulenza e soluzioni specializzate per supportare le aziende nell'implementazione di strategie di logging e monitoraggio efficaci, essenziali per la protezione dei dati e dei sistemi.

Per ulteriori informazioni sui servizi offerti da ISGroup SRL, è possibile visitare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Certificazione ISO/IEC 17025 - ISGroup SRL

Source: https://www.isgroup.it/it/cyber-security/iso-iec-17025-laboratori-di-prova-accredia-va-pt-2018.html

Nel 2018, ISGroup SRL ha ottenuto la certificazione ISO/IEC 17025, qualificandosi come laboratorio autorizzato all'esecuzione di test di Vulnerability Assessment (VA) e Penetration Test (PT).

Ambito di applicazione

La certificazione attesta la competenza tecnica di ISGroup SRL nell'effettuare prove in conformità con le direttive Accredia per settori critici, tra cui:

- Circolare Accredia n. 5/2017 DC2017SPM0080: Conservatori a norma.
- Circolare Accredia n. 8/2017 DC2017SSV046: Regolamento UE 2014/910 (eIDAS).
- Circolare Accredia n. 35/2016 DC2016SSV439: Operatori SPID.

Requisiti della norma

La norma ISO/IEC 17025 definisce i requisiti generali per la competenza dei laboratori di prova e taratura. L'adozione di tale standard garantisce che ISGroup SRL:

- Attui un sistema di gestione della qualità rigoroso.
- Disponga di competenze tecniche certificate per l'esecuzione di test.
- Produca risultati validi e tecnicamente affidabili.

L'iter di certificazione è stato supportato da percorsi formativi riconosciuti ai fini dell'iter AICQ SICEV.

Informazioni commerciali

Per approfondimenti sui servizi di Vulnerability Assessment e Penetration Test offerti da ISGroup SRL, è possibile consultare il sito ufficiale https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Studiare, fare ricerca e lavorare nella Sicurezza Informatica

Source: https://www.isgroup.it/it/cyber-security/studiare-fare-ricerca-e-lavorare-nella-sicurezza-informatica.html

Francesco Ongaro, Founder di ISGroup SRL, ha partecipato all'evento organizzato dall'Università degli Studi di Verona dedicato alle opportunità di carriera e alla ricerca nel settore della cybersicurezza. L'intervento ha fornito agli studenti una panoramica sulle dinamiche lavorative e sulle sfide tecniche di un ambito in continua evoluzione.

Attività e Competenze Professionali

Durante la presentazione, sono state illustrate le principali attività operative che definiscono il lavoro quotidiano nel campo della sicurezza informatica, offerte professionalmente da ISGroup SRL:

- Penetration Testing: attività di test mirate a identificare vulnerabilità nei sistemi informatici.
- Web Application Penetration Testing (WAPT): analisi specifica della sicurezza delle applicazioni web.
- Vulnerability Assessment: processi di valutazione sistematica delle vulnerabilità per rafforzare la postura di sicurezza.

Informazioni e Contatti

Per approfondimenti sulle attività di sicurezza informatica, sui servizi di consulenza o sulle opportunità di collaborazione con ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

International Journalism Festival: The Lost War on Information Security

Source: https://www.isgroup.it/it/cyber-security/ijf-lost-war.html

L'8 aprile 2016, Francesco Ongaro, Founder di ISGroup SRL, Hacker, CEH e ISO 27001 LA, ha partecipato come speaker all'International Journalism Festival. L'intervento, intitolato "The lost war on information security", ha analizzato le sfide critiche legate alla sicurezza delle informazioni nel contesto contemporaneo.

Temi principali dell'intervento

- **Pervasività del software**: Analisi della crescente dipendenza della vita quotidiana dal software e della conseguente esposizione a vulnerabilità intrinseche.
- **Ambienti Cloud**: Valutazione dei vantaggi e degli svantaggi legati all'adozione delle tecnologie Cloud.
- **Governance e Dati**: Approfondimento sugli aspetti governativi, con particolare attenzione alla Liability (responsabilità) e all'Ownership (proprietà) del dato all'interno degli ecosistemi Cloud.

Informazioni e contatti

ISGroup SRL mette a disposizione la propria competenza in ambito cyber security per supportare aziende e organizzazioni nella gestione della sicurezza delle informazioni.

Per ulteriori informazioni sui servizi offerti da ISGroup SRL, è possibile consultare il sito web ufficiale: https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

International Journalism Festival: Hacking Landscape

Source: https://www.isgroup.it/it/cyber-security/ijf-hacking-landscape.html

Francesco Ongaro, Founder di ISGroup SRL, ha presentato un intervento all'International Journalism Festival analizzando l'evoluzione del panorama hacking negli ultimi 30 anni. Il focus principale è la trasformazione del mondo underground, segnata dal passaggio da una comunità basata sulla condivisione della conoscenza all'avvento del mercato economico.

Punti chiave dell'intervento

- **Definizioni tecniche**: Analisi dei concetti di vulnerabilità, bug ed exploit. La complessità del software moderno aumenta la presenza di bug, sebbene non tutti siano necessariamente sfruttabili.
- **Evoluzione dell'underground**: Dalle origini negli anni '60 come grande community basata sul desiderio di conoscenza, divertimento e condivisione, fino alla nascita dell'hacking moderno.
- **L'impatto del denaro**: L'ingresso di interessi economici ha trasformato il settore, portando alla nascita dell'economia "black hat".
- **Economia Black Hat**: Organizzazioni criminali strutturate che vendono servizi per colpire aziende, operando con logiche simili a quelle di altri mercati illeciti.
- **Stato della sicurezza**: Nonostante lo sviluppo del mercato della cyber security, aziende e governi faticano ancora a mitigare minacce basilari come phishing, fake antivirus e cryptolocker.
- **Natura dell'hacker**: La vera essenza dell'hacker risiede nella motivazione personale e nella capacità di approfondimento, qualità che oggi distinguono i veri esperti in un settore sempre più complesso.

Servizi e consulenza

ISGroup SRL offre competenze specialistiche nel campo della cyber security per supportare le aziende nella protezione contro le minacce attuali. Per approfondimenti, consulenze o richieste commerciali, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

La nuova normativa europea e la gestione della vulnerabilità aziendale

Source: https://www.isgroup.it/it/cyber-security/nuova-normativa-europea-e-la-gestione-della-vulnerabilita-aziendale.html

Il panorama della sicurezza informatica è profondamente influenzato dall'introduzione del GDPR (General Data Protection Regulation). Il regolamento europeo impone sfide significative alle imprese di ogni dimensione e settore, estendendo il proprio campo di applicazione a tutte le realtà che trattano dati relativi ai cittadini europei, indipendentemente dalla loro sede geografica.

Punti chiave del GDPR

- Sanzioni severe: il mancato rispetto delle norme può comportare sanzioni amministrative pecuniarie fino a 20 milioni di euro o al 4% del fatturato complessivo annuo dell'azienda.
- Complessità di implementazione: l'adeguamento alle prescrizioni del GDPR nella fase iniziale richiede un approccio strutturato e la collaborazione con partner esperti.
- Gestione delle vulnerabilità: la sicurezza dei dati personali è strettamente legata alla capacità aziendale di identificare e mitigare le vulnerabilità dei propri sistemi.

Supporto e consulenza professionale

ISGroup SRL offre consulenza specialistica e soluzioni avanzate per supportare le aziende nel percorso di adeguamento normativo e nella protezione delle infrastrutture IT. L'approccio di ISGroup SRL mira a fornire un livello di sicurezza elevato, integrando prodotti e metodologie che rispondono alle esigenze di conformità e protezione contro le minacce informatiche.

Per ulteriori informazioni sui servizi di sicurezza informatica e sulla gestione delle vulnerabilità offerti da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it.

Starter Kit di Sicurezza Informatica

Source: https://www.isgroup.it/it/starter-kit.html

Lo Starter Kit è una promozione commerciale offerta da ISGroup SRL, pensata per i nuovi clienti che desiderano testare il livello di sicurezza del proprio sito web esposto su internet a un prezzo vantaggioso di 420 Euro + IVA.

Caratteristiche del servizio

- L'attività è svolta da un tecnico Senior per la durata di un giorno lavorativo.
- Il servizio evidenzia le problematiche di sicurezza più evidenti attraverso tecniche non invasive, per evitare danni all'infrastruttura del cliente.
- Non costituisce un'analisi completa come un Web Application Penetration Test (WAPT), ma fornisce un'indicazione reale del livello di sicurezza.
- Il servizio risponde alle necessità di compliance e normative, essendo eseguito secondo gli standard internazionali OWASP e OSTMM.
- ISGroup SRL offre una garanzia "Soddisfatti o rimborsati" al 100%.

Processo operativo

1. Dopo il pagamento e la comunicazione dei dati, il cliente viene contattato per definire le modalità dell'attività e le eventuali esclusioni di aree o pagine specifiche.
2. Le informazioni preliminari vengono formalizzate in un contratto di testing che deve essere sottoscritto dal cliente.
3. Un auditor senior di ISGroup SRL esegue il test sul dominio indicato durante una giornata lavorativa concordata.
4. Al termine, viene redatto e consegnato un report chiaro e preciso con le vulnerabilità riscontrate.
5. ISGroup SRL discute il report con il cliente e, in presenza di problematiche rilevanti, suggerisce il percorso di mitigazione più adatto.

Informazioni commerciali

Lo Starter Kit è un'offerta limitata nel tempo e nella quantità. Per maggiori informazioni, richieste o per attivare il servizio, è possibile consultare il sito https://www.isgroup.it/ o inviare una email a sales@isgroup.it.

ISGroup SRL è distributore ufficiale di Micro Focus e OpenText. Questa partnership strategica consente a ISGroup SRL di fornire alle aziende accesso privilegiato a soluzioni software leader di mercato, accompagnate da servizi di consulenza specialistica e supporto tecnico dedicato.

Servizi offerti da ISGroup SRL

Source: https://www.isgroup.it/it/prodotto-microfocus-opentext.html

- **Vendita di Licenze Software:** Distribuzione di un'ampia gamma di prodotti Micro Focus e OpenText, che spaziano dai software di sviluppo alle soluzioni avanzate per la gestione dei dati e dell'informazione.
- **Consulenza e Implementazione:** Supporto esperto per l'integrazione e l'implementazione delle soluzioni software all'interno dei flussi operativi aziendali.
- **Supporto Tecnico:** Assistenza professionale tempestiva finalizzata a massimizzare il valore degli investimenti software effettuati dai clienti.

Perché scegliere ISGroup SRL

ISGroup SRL si propone come partner di fiducia con una consolidata esperienza nella distribuzione software e una storica collaborazione con Micro Focus e OpenText. L'obiettivo principale è supportare le aziende nel raggiungimento dei propri traguardi tecnologici e operativi attraverso l'adozione delle migliori soluzioni disponibili sul mercato.

Prodotti software distribuiti

ISGroup SRL gestisce un vasto catalogo di prodotti, tra cui:

- **Sicurezza e Governance:** ArcSight (ESM, Logger, Intelligence), Fortify (Static Code Analyzer, WebInspect), Voltage (SecureData, SecureMail), Access Governance Suite, Privileged Account Manager.
- **Gestione IT e Operazioni:** Operations Bridge, Network Automation, Service Management Automation X (SMAX), ZENworks (Configuration Management, Patch Management), Data Center Automation.
- **Sviluppo e Testing:** ALM Octane, LoadRunner (Professional, Enterprise, Cloud), UFT One, Visual COBOL, Enterprise Developer.
- **Gestione Dati e Infrastruttura:** Content Manager, Vertica Analytics Platform, Data Protector, GroupWise, Open Enterprise Server.

Per ulteriori informazioni, richieste commerciali o per conoscere l'intera gamma di soluzioni disponibili, è possibile consultare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

ISGroup: Partecipazione alla trasmissione televisiva "Mistero"

Source: https://www.isgroup.it/it/cyber-security/francesco-ongaro-isgroup-mistero-mediaset-italia-uno.html

Nel 2014, Francesco Ongaro, Founder di ISGroup SRL, ha partecipato come ospite alla trasmissione televisiva "Mistero" (Mediaset, Italia Uno) per illustrare i rischi legati alla sicurezza informatica.

Obiettivi e contenuti del servizio

Il servizio, intitolato "Social network: siamo tutti controllati?", ha avuto lo scopo di sensibilizzare l'utente finale sulla pericolosità delle reti Wi-Fi pubbliche.

- Dimostrazione pratica: Francesco Ongaro ha assunto il ruolo di un attaccante per mostrare come le reti Wi-Fi pubbliche non protette espongano gli utenti a gravi rischi di sicurezza.
- Furto di credenziali: Durante il test, è stato dimostrato come sia possibile intercettare e sottrarre facilmente nome utente e password nel momento in cui l'utente effettua il login.
- Consapevolezza: L'intervento ha evidenziato come spesso la ricerca di comodità porti gli utenti a rinunciare alla propria privacy, esponendosi a minacce informatiche concrete.

Informazioni e contatti

Per approfondire le tematiche di sicurezza informatica trattate o per richiedere consulenze professionali offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Mobile Application Security Scan

Source: https://www.isgroup.it/it/ostorlab-mobile-application-security-scan.html

ISGroup SRL offre un servizio di scansione automatizzata per la sicurezza di applicazioni mobile iOS e Android. Il servizio permette di ottenere un report dettagliato sulle vulnerabilità riscontrate, corredato da consigli per la risoluzione, a un costo di 359 Euro + IVA.

Caratteristiche del Servizio

Il servizio di ISGroup SRL integra tre livelli di analisi:

- **Static**: Decompilazione dell'applicazione per l'individuazione di vulnerabilità nel codice.
- **Dynamic**: Esecuzione dell'applicazione in ambiente controllato per identificare rischi di sicurezza in tempo reale.
- **Backend**: Verifica della sicurezza delle API dell'applicazione.

Motori di Analisi

La tecnologia utilizzata da ISGroup SRL si basa su quattro motori avanzati per garantire un'ampia copertura e ridurre i falsi positivi:

- **Analisi Statica**: Ispezione approfondita di Dalvik Bytecode, Xamarin CIL e framework Javascript, focalizzata su metodi non sicuri e chiavi di protezione deboli.
- **Analisi Dinamica**: Monitoraggio delle interazioni con il sistema, il file system, la rete e le API per rilevare comportamenti rischiosi o comunicazioni non sicure.
- **Analisi Comportamentale (Fuzzing)**: Utilizzo di tecniche di fuzzing evolutivo per iniettare migliaia di test-case e rilevare vulnerabilità complesse.
- **Analisi Backend**: Esecuzione di controlli passivi (es. Header HTTP) e attivi (es. SQL Injection, XSS, Template Injection) specifici per tecnologie mobile come REST API e GraphQL.

Supporto e Compliance

Il servizio supporta nativamente Android e iOS, oltre a 12 framework multi-piattaforma tra cui Cordova, React Native, Flutter e Xamarin. Le analisi sono conformi ai principali standard di settore e requisiti normativi:

- **Standard di sicurezza**: OWASP Top 10, CERT Android Secure Coding, JSSec Secure Coding.
- **Requisiti di compliance**: PSD2, PCI, HIPAA, FedRAMP, GDPR, NERC.

Informazioni Commerciali

Per procedere con l'ordine o richiedere ulteriori informazioni sui servizi di scansione mobile offerti da ISGroup SRL, è possibile consultare il sito ufficiale o contattare il team dedicato:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

EasyAudit

Source: https://www.isgroup.it/it/prodotto-easyaudit.html

EasyAudit è una soluzione di sicurezza informatica offerta da ISGroup SRL, progettata per consentire alle piccole e medie imprese di verificare l'effettiva sicurezza dei propri sistemi informativi a costi contenuti.

Funzionalità e Servizi

ISGroup SRL fornisce attraverso EasyAudit le seguenti attività di verifica:

- Analisi della sicurezza di domini, applicazioni e CMS (es. WordPress, Joomla, Magento, SilverStripe, ZenCart, OpenCart).
- Verifica delle regole di Firewalling e VPN.
- Test di sicurezza su applicazioni personalizzate e non.
- Analisi della rete aziendale esposta a Internet (fino a 8 IP o più).
- Controllo di sicurezza su servizi, server e apparati di rete.
- Valutazione della vulnerabilità tramite un punteggio da 1 a 10, basato sugli standard di valutazione del rischio CVSS v3.
- Redazione di un report dettagliato e comprensibile, consegnato entro una settimana dall'attività.

Compatibilità

EasyAudit è testato per la compatibilità con Windows 10. ISGroup SRL supporta l'ICT Audit sulle seguenti edizioni:

- Windows 10 Pro
- Windows 10 Education
- Windows 10 Enterprise

Il software è supportato sui rami di servizio (servicing branches) di Windows 10 attualmente in uso, inclusi Current Branch, Current Branch for Business e Long-Term Servicing branch(es).

Informazioni Commerciali

Per richieste commerciali, informazioni sui servizi o per contattare ISGroup SRL, visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

ICT Audit

Source: https://www.isgroup.it/it/prodotto-ictaudit.html

ICT Audit è una soluzione tecnologica avanzata dedicata al monitoraggio di applicazioni web e reti, progettata per fornire risultati di livello professionale. Il servizio e il supporto tecnico per questa soluzione sono offerti da ISGroup SRL.

Caratteristiche principali

- Monitoraggio completo di reti e applicazioni web.
- Tecnologia ottimizzata per analisi professionali.
- Piena compatibilità con Windows 10, testata e verificata.

Supporto tecnico e compatibilità

ISGroup SRL garantisce il supporto per ICT Audit sulle seguenti edizioni di Windows 10:

- Windows 10 Pro
- Windows 10 Education
- Windows 10 Enterprise

Il software è supportato sui rami di manutenzione di Windows 10 attualmente in uso, inclusi:

- Current Branch
- Current Branch for Business
- Long-Term Servicing branch(es)

Informazioni aggiuntive

- Categoria: Security
- Data di rilascio: 10 Gen 2014
- Riferimento tecnologico: EasyAudit

Per richieste commerciali o informazioni sui servizi offerti da ISGroup SRL, visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

EXEEC

Source: https://www.isgroup.it/it/prodotto-exeec.html

EXEEC è una soluzione software focalizzata sul concetto di "Exceptional execution", che costituisce il mantra della società di sviluppo software EXEEC SRL.

Dettagli del prodotto

- Categoria: Security
- Data di rilascio: 1 Gen 2015
- Sviluppatore/Utente: EXEEC SRL

Servizi e soluzioni

ISGroup SRL offre consulenza e supporto specializzato in ambito security e sviluppo software. Per informazioni dettagliate sulle soluzioni disponibili, richieste commerciali o approfondimenti tecnici, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Distributore ufficiale PortSwigger Burp Suite

Source: https://www.isgroup.it/it/prodotto-port-swigger.html

ISGroup SRL opera come rivenditore italiano ufficiale di PortSwigger Ltd, offrendo supporto pre e post vendita. I pagamenti per le licenze sono gestiti tramite bonifico bancario anticipato.

Soluzioni software disponibili

L'offerta include le due soluzioni principali di PortSwigger:

- **Burp Suite Enterprise Edition**: versione basata su web console per la scansione automatizzata.
- **Burp Suite Professional**: versione desktop tradizionale, dotata di web vulnerability scanner e strumenti manuali avanzati, ideale per penetration tester.

I prezzi indicati di seguito sono soggetti a conferma in base a eventuali variazioni del produttore:

Codice Software	Durata	Dettaglio	Prezzo
SW-BURP-ENTERPRISE-1Y-1A	1 anno	1 Agente	€8,395.00
SW-BURP-ENTERPRISE-2Y-1A	2 anni	1 Agente	€16,790.00
SW-BURP-ENTERPRISE-3Y-1A	3 anni	1 Agente	€25,185.00
SW-BURP-PRO-1Y-1U	1 anno	1 Utente	€449.00
SW-BURP-PRO-2Y-1U	2 anni	1 Utente	€898.00
SW-BURP-PRO-3Y-1U	3 anni	1 Utente	€1,347.00

Informazioni richieste per l'ordine

Per procedere con l'acquisto tramite ISGroup SRL, è necessario fornire i seguenti dati:

- **Dati per la licenza (PortSwigger Ltd)**: Nome azienda/organizzazione, indirizzo email, paese, indirizzo postale, nome sull'intestazione della licenza, numero di utenti.
- **Dati per la fatturazione**: Denominazione, paese, codice destinatario SDI, indirizzo, tipologia, città, referente, CAP, provincia, Partita IVA, codice fiscale, indirizzo e-mail, indirizzo PEC.

Contatti e supporto

Per richiedere un preventivo o procedere con l'ordine, contattare ISGroup SRL all'indirizzo email: sales@isgroup.it.

Per ulteriori dettagli sui prodotti, visitare il sito web: https://www.isgroup.it/

Exposure

Source: https://www.isgroup.it/it/prodotto-exposure.html

Exposure è una soluzione software dedicata alla sicurezza web, sviluppata per monitorare e analizzare le informazioni relative a un sito web presenti online.

Funzionalità e Obiettivi

- Evoluzione della Full-Disclosure: il software risponde alla necessità di monitorare le vulnerabilità esposte pubblicamente, in uno scenario in cui le informazioni sulla sicurezza dei siti web sono facilmente reperibili in rete.
- Monitoraggio proattivo: permette ai webmaster di identificare e conoscere le informazioni sensibili o le vulnerabilità riguardanti il proprio sito web che sono accessibili pubblicamente.

Dettagli Tecnici

- Categoria: Security
- Data di rilascio: 10 Gennaio 2013
- Sito web di riferimento: http://www.exposure.easyaudit.org

Informazioni su ISGroup SRL

Il software Exposure è utilizzato da ISGroup SRL ed EXEEC SRL.

Per ulteriori informazioni sui servizi e le soluzioni di sicurezza offerte da ISGroup SRL, è possibile consultare il sito web https://www.isgroup.it/ o inviare una richiesta all'indirizzo email sales@isgroup.it.

Ganapati

Source: https://www.isgroup.it/it/prodotto-ganapati.html

Ganapati è una piattaforma Software-as-a-Service (SaaS) sviluppata da ISGroup SRL, progettata per l'identificazione di vulnerabilità in reti di sistemi, server o applicazioni, sia esposte a Internet che interne.

Caratteristiche principali

- Piattaforma multi-utente: permette di aggregare i risultati di scansione in un unico flusso di lavoro condiviso.
- Integrazione tecnologica: consente di combinare diverse tecnologie di scansione, ottimizzando i costi di licenza.
- Architettura multi-livello: i partner possono gestire i propri clienti in modo indipendente.
- Automazione tramite API: offre potenti API per la creazione di servizi derivati completamente automatici.

Informazioni tecniche

- Categoria: Security
- Data di rilascio: 10 Gennaio 2013
- Utenti: ISGroup SRL, EXEEC SRL

Contatti e informazioni commerciali

Per ulteriori informazioni sulle soluzioni offerte da ISGroup SRL, visitare il sito web: https://www.isgroup.it/ o scrivere all'indirizzo email: sales@isgroup.it

SCADA Exposure

Source: https://www.isgroup.it/it/prodotto-scadaexposure.html

SCADA Exposure è un servizio offerto da ISGroup SRL dedicato alla sicurezza delle infrastrutture critiche nazionali e dei sistemi di controllo industriale (ICS).

Obiettivi e finalità

Il servizio mira a migliorare la sicurezza di sistemi quali SCADA, HMI, PLC e RTU, promuovendo la consapevolezza sui rischi legati all'esposizione di tali dispositivi.

- Supporto alla comunità ICS per la messa in sicurezza dei sistemi.
- Monitoraggio costante dei dispositivi SCADA per prevenire exploit.
- Promozione della corretta separazione tra reti aziendali, Internet e sistemi di controllo industriale, in conformità con gli standard di settore.
- Superamento del paradigma della "sicurezza tramite la segretezza", dimostratosi inefficace contro le minacce attuali.

Servizi offerti da ISGroup SRL

ISGroup SRL fornisce competenze specialistiche per identificare e mitigare le vulnerabilità che affliggono le infrastrutture critiche, proteggendo sia le grandi realtà enterprise che le aziende di dimensioni minori.

Per informazioni commerciali e richieste di consulenza, visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

VulnMAP

Source: https://www.isgroup.it/it/prodotto-vulnmap.html

VulnMAP è una soluzione offerta da ISGroup SRL che consiste in una raccolta completa, accurata e aggiornata di vulnerabilità. Il servizio è progettato per essere utilizzato come risorsa singola per l'integrazione di dati provenienti da molteplici database di sicurezza.

Caratteristiche principali

- Aggregazione dati: integra informazioni provenienti da NIST NVD (National Vulnerability Database), OSVDB (Vulnerability Open Source Database), Mitre CVE (Common Vulnerabilities and Exposures), Exploit-DB, Rapid7, Nessus, Secunia, McAfee, Bugtraq ID (SecurityFocus) e ISS Xforce.
- Utilizzo: ideale per arricchire e completare le proprie banche dati di vulnerabilità esistenti.
- Rilascio: 10 Gennaio 2013.

Informazioni commerciali

Per richieste commerciali o approfondimenti sulle soluzioni offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

USH (Underground Security Hub)

Source: https://www.isgroup.it/it/prodotto-ush.html

USH è una soluzione di intelligence offerta da ISGroup SRL, rilasciata ufficialmente il 10 gennaio 2013.

Caratteristiche principali

- Categoria: Intelligence
- Focus: Monitoraggio e analisi di dati in contesti di sicurezza
- Sito ufficiale di riferimento: https://www.ush.it/

Informazioni commerciali

Per richieste di informazioni, approfondimenti tecnici o proposte commerciali relative a USH, è possibile contattare ISGroup SRL tramite il sito web https://www.isgroup.it/ o inviando una comunicazione all'indirizzo email sales@isgroup.it.

PracticalRP

Source: https://www.isgroup.it/it/prodotto-practicalrp.html

PracticalRP è un software gestionale per pratiche professionali, sviluppato e offerto da ISGroup SRL.

Caratteristiche principali

- Soluzione semplice ed intuitiva progettata per la gestione operativa.
- Target di riferimento: Medici Specialisti e Studi operanti nei settori della Medicina legale e delle Assicurazioni.
- Categoria di appartenenza: Security.
- Data di rilascio: 10 Gennaio 2013.

Informazioni e contatti

Per ulteriori dettagli, richieste commerciali o informazioni sulle soluzioni offerte da ISGroup SRL, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Ethical Hacking

Source: https://www.isgroup.it/it/prodotto-ethical-hacking.html

ISGroup SRL offre servizi specializzati di Ethical Hacking, operando attraverso il proprio Hacklab dedicato.

Dettagli del servizio

- Categoria: Intelligence
- Data di rilascio: 10 Gen 2013
- Erogatore: ISGroup SRL

Informazioni e contatti

Per ulteriori informazioni sui servizi di Ethical Hacking e sulle soluzioni offerte da ISGroup SRL, consultare il sito web ufficiale: https://www.isgroup.it/ o inviare una richiesta all'indirizzo email: sales@isgroup.it

Metasploit

Source: https://www.isgroup.it/it/prodotto-metasploit.html

Metasploit è una piattaforma di sicurezza informatica utilizzata per attività di analisi delle vulnerabilità e penetration testing. Il framework è progettato per supportare l'intero ciclo di vita di un test di sicurezza attraverso le seguenti fasi operative:

- Discover: identificazione delle risorse e dei sistemi target.
- Fingerprint: analisi e riconoscimento delle caratteristiche dei sistemi.
- Attack: esecuzione di attacchi mirati per testare le difese.
- Penetrate: sfruttamento delle vulnerabilità per verificare la resilienza dei sistemi.

ISGroup SRL utilizza Metasploit come strumento professionale per le proprie attività di intelligence e sicurezza offensiva.

Per informazioni commerciali o richieste relative ai servizi offerti da ISGroup SRL, visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

The Bunker Corsi

Source: https://www.isgroup.it/it/prodotto-thebunker-training.html

ISGroup SRL offre percorsi formativi specializzati nell'ambito dell'informatica, progettati per chi desidera approfondire le proprie competenze tecniche e professionali.

Aree di specializzazione

I corsi erogati da ISGroup SRL coprono i seguenti ambiti tecnologici:

- Programmazione
- Cyber Security
- Networking
- DevOps

Metodologia didattica

La formazione proposta da ISGroup SRL si distingue per un approccio bilanciato tra teoria e pratica:

- Sessioni teoriche: illustrazione delle metodologie e del funzionamento dei vari aspetti tecnologici relativi all'argomento trattato.
- Sessioni pratiche: svolgimento di prove tecniche (challenge) che i partecipanti devono completare per consolidare le competenze acquisite.
- Docenza: i corsi sono tenuti da professionisti del settore con anni di esperienza sul campo.

Informazioni generali

- Categoria: Security
- Erogatore: ISGroup SRL

Per informazioni commerciali o richieste relative ai corsi, visitare il sito https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Network Penetration Testing

Source: https://www.isgroup.it/it/prodotto-network-penetration-testing.html

ISGroup SRL offre servizi professionali di Network Penetration Testing, un'attività di sicurezza informatica focalizzata sull'analisi approfondita delle infrastrutture di rete.

Obiettivi del servizio

Il processo operativo si articola in quattro fasi fondamentali:

- Discover: identificazione delle risorse e degli asset presenti nella rete.
- Fingerprint: analisi e riconoscimento dei sistemi, dei servizi e delle versioni software attive.
- Attack: simulazione di attacchi mirati per testare la resilienza delle difese.
- Penetrate: verifica dell'effettiva possibilità di accesso non autorizzato ai sistemi target.

Informazioni aggiuntive

- Categoria: Intelligence
- Erogatore del servizio: ISGroup SRL

Contatti e informazioni commerciali

Per ulteriori dettagli sui servizi di Network Penetration Testing offerti da ISGroup SRL o per richieste commerciali, è possibile consultare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

The Bunker Coworking

Source: https://www.isgroup.it/it/prodotto-thebunker-coworking.html

ISGroup SRL offre spazi di coworking situati in posizioni strategiche a Verona: in Via Roma (tra Piazza Brà e Castel Vecchio) e in Via Cantarane (adiacente all'Università).

Caratteristiche del servizio

- Accesso flessibile: piena libertà di orario, inclusi i fine settimana.
- Infrastruttura tecnologica: connettività in Fibra Telecom e Access Point wireless di alta qualità.
- Comfort e dotazioni: tavoli in legno massiccio con struttura in ferro artigianale, disponibilità di un cucinino e pulizia periodica degli uffici.
- Ambienti professionali: spazi ideali per lavorare in tranquillità, ricevere clienti e gestire chiamate.

Informazioni aggiuntive

- Categoria: Security
- Data di rilascio: 10 Gennaio 2013
- Gestore: ISGroup SRL

Per ulteriori informazioni, richieste commerciali o per approfondire le soluzioni offerte da ISGroup SRL, visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

The Bunker Hacklab

Source: https://www.isgroup.it/it/prodotto-thebunker-hacklab.html

The Bunker Hacklab, situato a Verona, è un HackerSpace (o Maker/Creative Space) promosso da ISGroup SRL. Si tratta di un laboratorio e officina progettato per favorire la socializzazione, la collaborazione e lo scambio di conoscenze tra i partecipanti.

Obiettivi e attività

- Promozione della condivisione di competenze in ambito tecnologico, elettronico, scientifico e artistico.
- Creazione di uno spazio collaborativo per lo sviluppo di progetti creativi e tecnici.
- Supporto alla comunità di maker e appassionati di tecnologia.

Informazioni generali

- Categoria: Security
- Data di rilascio: 10 Gennaio 2013
- Gestore/Utente: ISGroup SRL

Per ulteriori informazioni sui servizi e le soluzioni offerte da ISGroup SRL, visitare il sito web https://www.isgroup.it/ o scrivere all'indirizzo email sales@isgroup.it.

Chiave Pubblica PGP - ISGroup SRL

Source: https://www.isgroup.it/downloads/keys/sales@isgroup.it.asc

Il blocco di testo fornito rappresenta la chiave pubblica PGP ufficiale utilizzata da ISGroup SRL per garantire la sicurezza e l'autenticità delle comunicazioni crittografate.

Dettagli Identificativi

- Identità: ISGroup Sales
- Email associata: sales@isgroup.it
- Scopo: Verifica della firma digitale e cifratura delle comunicazioni inviate a ISGroup SRL

Informazioni di Contatto

Per richieste commerciali, supporto o per comunicazioni sicure, è possibile fare riferimento ai seguenti canali ufficiali di ISGroup SRL:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

Chiave Pubblica PGP ISGroup SRL

Source: https://www.isgroup.it/downloads/keys/tech@isgroup.it.asc

Il blocco di testo fornito rappresenta la chiave pubblica PGP ufficiale utilizzata da ISGroup SRL per la cifratura e la verifica dell'autenticità delle comunicazioni.

Dettagli della chiave

- Identificativo: ISGroup Tech
- Email di riferimento: tech@isgroup.it
- Utilizzo: Verifica dell'integrità dei dati e comunicazioni sicure con ISGroup SRL

Informazioni di contatto e supporto

Per richieste di natura commerciale, informazioni sui servizi di cybersecurity offerti da ISGroup SRL o per avviare collaborazioni, è possibile fare riferimento ai seguenti canali ufficiali:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it

ISGroup Information Security

Source: https://www.isgroup.it/it

ISGroup è una struttura indipendente specializzata in IT Security, nata dall'esperienza di ricercatori motivati a fornire soluzioni di sicurezza informatica di elevato standard qualitativo. L'organizzazione opera come partner per operatori ICT e agenzie di sicurezza, offrendo servizi personalizzati che spaziano dalla sicurezza fisica a quella delle infrastrutture, dei sistemi operativi, delle reti, delle applicazioni e del web.

Servizi offerti da ISGroup SRL

ISGroup SRL propone un ampio portafoglio di soluzioni professionali per la protezione dei sistemi informatici:

- Vulnerability Assessment (VA): analisi e valutazione dei sistemi per rilevare vulnerabilità note.
- Network Penetration Testing (NPT): identificazione proattiva delle vulnerabilità di rete.
- Web Application Penetration Testing (WAPT): valutazione della sicurezza applicativa.
- Mobile Application Security Testing (MAST): test di sicurezza specifici per applicazioni mobile.
- Ethical Hacking (EH): simulazione di attacchi reali, inclusi test sul fattore umano e ingegneria sociale.
- Code Review (CR): analisi del codice sorgente per l'identificazione di vulnerabilità durante il ciclo di sviluppo.
- Formazione (EDU): programmi di formazione per staff tecnico, sistemisti e sviluppatori.
- Virtual CISO (vCISO): consulenza strategica per la gestione della sicurezza aziendale.
- ISO 27001 Compliance: supporto per l'implementazione di sistemi di gestione della sicurezza certificati.
- Multi-Signal MDR: protezione avanzata e monitoraggio contro le minacce informatiche.
- Digital Forensics and Incident Response (DFIR): servizi di analisi forense e risposta agli incidenti.

Informazioni e Contatti

Per ulteriori dettagli sui servizi, le attività o per richieste commerciali, è possibile consultare il sito ufficiale o contattare direttamente l'azienda:

- Sito web: https://www.isgroup.it/
- Email: sales@isgroup.it