CIBERSEGURIDAD ETHICAL HACKING PENETRATION TESTING FORMACIÓN

ISGroup
Information Security

Advanced Bug Bounty

Hackers éticos certificados buscan fallos: pagas solo por vulnerabilidades confirmadas

OBJETIVO

Investigación ofensiva continua con modelo pay per result

Investigadores seleccionados analizan aplicaciones y activos acordados sin el coste fijo de un assessment tradicional.

Cada recompensa corresponde a una vulnerabilidad válida, nueva y reproducible.

ISGroup
Information Security

MÉTODO

Del alcance a la remediation con un proceso controlado

Perímetro

Definimos activos, exclusiones, reglas y criterios de severidad.

Investigación

Hackers éticos certificados aplican técnicas manuales y específicas.

Validación

ISGroup verifica unicidad, reproducibilidad e impacto antes de la recompensa.

ISGroup
Information Security

MODALIDAD

Investigación dirigida, disclosure segura y costes previsibles

El programa puede operar por ventanas o continuamente sobre aplicaciones web, API y otros activos autorizados.

Un canal coordinado protege empresa e investigadores y evita informes incompletos.

El soporte continúa en el análisis técnico y la verificación de correcciones.

ISGroup
Information Security

PUNTOS FUERTES

Resultados validados por expertos en ataque y remediation

Selección

Investigadores identificados, competencias verificadas y acceso acorde al perímetro.

Control

Triage centralizado y ningún pago por duplicados o falsos positivos.

Impacto

Prioridades basadas en riesgo real, no solo en un score técnico.

ISGroup
Information Security

OUTPUT

Vulnerabilidades confirmadas y soporte a la corrección

Ficha técnica con escenario, impacto y reproducción.

Triage y severidad validados por ISGroup.

Guía de remediation para reducir el riesgo.

Retest para confirmar el cierre.

ISGroup
Information Security

Let's HACK together

ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

RESERVA UNA CITA
sales@isgroup.it
+39 045 4853232