CYBERSECURITY ETHICAL HACKING PENETRATION TESTING SCHULUNG

ISGroup
Information Security

Cyber Threat Simulation

Realistische, wiederholte Szenarien messen, wie gut die Organisation Angriffe erkennt und stoppt

ZIEL

Menschen, Prozesse und Technik gegen realistische Bedrohungen trainieren

Cyber Threat Simulation prüft Detection und Response mit kontrollierten Kampagnen nach relevanten Angreifern.

Wiederholte Szenarien machen aus einem Einzeltest eine messbare Verbesserung.

ISGroup
Information Security

METHODE

Einen Angriff End to End planen, simulieren und messen

Szenario

Wir wählen Bedrohung, Ziele, Vektoren und Einsatzregeln.

Simulation

Wir führen kontrollierte Aktionen aus und beobachten Detection und Response.

Messung

Wir rekonstruieren Timeline, Entscheidungen, Lücken und Veränderungen.

ISGroup
Information Security

UMSETZUNG

Kontrollierte Phishing-, Malware-, APT- und DDoS-Szenarien

Szenarien verbinden Menschen, Endpoints, Netzwerk, Cloud und Eskalation passend zum Geschäftsrisiko.

Die Simulation fokussiert einen Vektor oder bildet eine vollständige Angriffskette ab.

Blue Team, SOC und Management erhalten rollengerechte Ziele und Ergebnisse.

ISGroup
Information Security

STÄRKEN

Sichere, wiederholbare Übungen auf Basis von Nachweisen

Realismus

Techniken und Ziele nach den für die Branche relevanten Bedrohungen.

Kontrolle

Grenzen, Kill Switch und Eskalation vor jeder Aktivität vereinbart.

Vergleich

Einheitliche Kennzahlen zeigen Fortschritte und Rückschritte.

ISGroup
Information Security

OUTPUT

Ein konkretes Bild der Detection- und Response-Fähigkeit

Attack Timeline mit Aktionen, Erkennung und Reaktionszeiten.

Detection Gaps bei Menschen, Prozessen, Logs und Kontrollen.

Priorisierter Verbesserungsplan für SOC und technische Teams.

Executive Summary zu Risiko und Resilienzentwicklung.

ISGroup
Information Security

Let's HACK together

ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

TERMIN VEREINBAREN

sales@isgroup.it

+39 045 4853232