CYBERSÉCURITÉ ETHICAL HACKING PENETRATION TESTING FORMATION

ISGroup
Information Security

Cyber Threat Simulation

Scénarios réalistes et répétés pour mesurer comment l'organisation détecte et stoppe une attaque

OBJECTIF

Entraîner personnes, processus et technologies face à des menaces réalistes

Cyber Threat Simulation vérifie détection et réponse par des campagnes contrôlées inspirées d'adversaires pertinents.

La répétition des scénarios transforme un test isolé en amélioration mesurable.

ISGroup
Information Security

MÉTHODE

Concevoir, simuler et mesurer une attaque end to end

Scénario

Nous sélectionnons menace, objectifs, vecteurs et règles.

Simulation

Nous exécutons des actions contrôlées en observant détection et réponse.

Mesure

Nous reconstruisons timeline, décisions, écarts et progrès entre campagnes.

ISGroup
Information Security

MODALITÉS

Phishing, malware, APT et DDoS contrôlés

Les scénarios combinent personnes, endpoints, réseau, cloud et processus d'escalade selon le risque.

La simulation peut cibler un vecteur ou reproduire une chaîne d'attaque complète.

Blue Team, SOC et direction reçoivent des objectifs et résultats adaptés à leur rôle.

ISGroup
Information Security

POINTS FORTS

Exercices sûrs, répétables et fondés sur des preuves

Réalisme

Techniques et objectifs modélisés sur les menaces pertinentes du secteur.

Contrôle

Limites, kill switch et escalades convenus avant chaque activité.

Comparais

Des métriques homogènes révèlent progrès et régressions dans le temps.

ISGroup
Information Security

LIVRABLES

Une vision concrète des capacités de détection et réponse

Attack timeline avec actions, détections et délais de réaction.

Detection gaps sur personnes, processus, logs et contrôles.

Plan d'amélioration priorisé pour SOC et équipes techniques.

Executive summary sur le risque et la résilience.

ISGroup
Information Security

Let's HACK together

ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

PRENDRE RENDEZ-VOUS

sales@isgroup.it

+39 045 4853232