CYBERSECURITY ETHICAL HACKING PENETRATION TESTING TRAINING

ISGroup
Information Security

Cyber Threat Simulation

Realistic, repeated scenarios measuring how well the organisation detects and stops an attack

OBJECTIVE

Train people, processes and technology against realistic threats

Cyber Threat Simulation tests detection and response through controlled campaigns inspired by relevant adversaries.

Repeating scenarios over time turns a one-off test into measurable improvement.

ISGroup
Information Security

METHOD

Design, simulate and measure an end-to-end attack

Scenario

We select threat, objectives, vectors and rules of engagement.

Simulation

We execute controlled actions while observing detection and response.

Measurement

We reconstruct timelines, decisions, gaps and changes between campaigns.

ISGroup
Information Security

DELIVERY

Controlled phishing, malware, APT and DDoS scenarios

Scenarios combine people, endpoints, network, cloud and escalation processes according to business risk.

The simulation can focus on one vector or reproduce a complete attack chain.

Blue Team, SOC and management receive objectives and results aligned with their role.

ISGroup
Information Security

KEY STRENGTHS

Safe, repeatable exercises based on evidence

Realism

Techniques and objectives modelled on threats relevant to the sector.

Control

Limits, kill switches and escalation agreed before every activity.

Comparisa

Consistent metrics reveal improvements and regressions over time.

ISGroup
Information Security

OUTPUT

A concrete view of detection and response capability

Attack timeline with actions, detections and response times.

Detection gaps across people, processes, logs and controls.

Prioritised improvement plan for SOC and technical teams.

Executive summary on risk and resilience trends.

ISGroup
Information Security

Let's HACK together

ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

BOOK A MEETING
sales@isgroup.it
+39 045 4853232