ARANCIA

STRENGTHENING CYBER RESILIENCE

ARANCIA'S TABLETOP EXERCISE

REALISTIC TRAINING FOR REAL-WORLD THREATS

Arancia's Tabletop Exercises bring together executives, senior managers, and technical operators to simulate and respond to security breaches under the guidance of a CISO. This exercise is designed to develop the skills necessary to effectively manage and mitigate actual cyber incidents.

WHY CHOOSE US?

EXPERT GUIDANCE

Benefit from the expertise of seasoned CISOs who lead the exercises and provide invaluable insights.

TAILORED SCENARIOS

Customized simulations based on the latest threat landscape and specific to your organization's environment.

HANDS-ON TRAINING

Engage in realistic, hands-on training that mirrors actual cyber incidents, ensuring preparedness and confidence.

COMPREHENSIVE APPROACH

Cover both technical and soft skills, enhancing overall team performance and collaboration.

PROVEN METHODOLOGY

Our process is rooted in industry best practices and standards, ensuring thorough and effective training.

KEY BENEFITS

IDENTIFY GAPS

Uncover areas for improvement in existing response methodologies, tailored to client-specific scenarios.

REALISTIC TRAINING

Conduct on-site exercises that reflect the client's operational environment and enhance realistic scenario responses.

ENHANCED TEAM PERFORMANCE

Foster cooperative thinking and improve both individual and team performance in technical and soft skills required for resolution.

INCREASED AWARENESS

Provide real security awareness to executives, senior managers, and operational staff.

THREAT SCENARIOS

Corporate Website Hacked: Inflammatory messages posted using corporate branding.

Ransomware Attack: Compromising network and infrastructure services.

Data Leak by Third Party: Accidental release of corporate data.

Automated Attack: Malicious software remains undetected on the network.

Insider Threat: Disgruntled employee removes or sells corporate data.

External Data Breach: Hacker or competitor obtains corporate data.

Executive Extortion: Threat of releasing confidential data.

EXERCISE ROLLOUT & APPROACH

Session #1 – Senior Management (2 Hours)

- **Participants:** Legal/Risk, IT, HR, Communications, Business Operations, Finance.
- **Objective:** Overview of the evolving threat landscape and walkthrough of security incident scenarios.

Session #2 – IT Team (2 Hours)

- **Participants:** Service Desk, Application Dev/Ops, Network and Server Operations.
- **Objective:** Insight into recent incidents and a tabletop scenario for incident response.

Simulated Tabletop Exercise

- **Objective:** Simulate a live ransomware incident and review the incident response process.
- **Participants:** Technical team and senior leadership.
- **Goals:**
  1. **Containment and Recovery:** Determine necessary steps to contain and recover a compromised environment.
  2. **Roles and Responsibilities:** Clarify the roles of technical teams and senior leadership during an incident.

ARANCIA

Equip your organization with the skills and knowledge to tackle cyber threats head-on. Our tabletop exercises are designed to simulate real-world scenarios, providing your team with the experience and confidence needed to handle actual security breaches. Contact us today to schedule your tabletop exercise and fortify your organization's cybersecurity posture.