Cyber Readiness, Simulation & Resilience Program – 5-Day TOC

Day 1 – Cyber Readiness Foundations & Risk

Theory

- Cyber Threat Landscape & Business Impact
- Cyber Readiness vs Cyber Resilience
- Roles of Technical vs Business Teams
- Overview of Frameworks (NIST, ISO, CIS)
- Risk, Compliance & Insurance Perspective

Activity

- Identifying operational and financial impact

Day 2 – Security Awareness & User Simulations

Theory

- Common Attack Vectors (Phishing, Social Engineering)
- Human Risk & Insider Threats
- Security Best Practices for Users
- Identity & Access Security (Passwords, MFA)

Hands-on Labs

- Phishing simulation & detection
- Social engineering scenarios
- Credential security exercises

Day 3 – Technical Labs & Attack Simulations

Theory

- Attack Lifecycle (Kill Chain / MITRE ATT&CK;)
- Vulnerability & Exploitation Basics
- Network, Endpoint & Web Attacks Overview

Hands-on Labs

- Vulnerability scanning & exploitation
- Web application attack simulation
- Endpoint compromise scenario

Day 4 – Incident Response & Threat Detection

Theory

- Incident Response Lifecycle
- SOC & SIEM Concepts
- Threat Detection & Threat Hunting
- Communication during incidents

Hands-on / Simulation

- Log analysis & anomaly detection
- Live incident simulation
- Tabletop exercise

Day 5 – Cyber Readiness Measurement & Reporting

Theory

- Readiness & Resilience Metrics
- Risk Scoring & Maturity Models
- Trend Analysis & Improvement
- Framework Mapping (NIST, ISO, CIS)
- Regulatory & Insurance Readiness

Hands-on / Simulation

- Generating readiness reports
- Dashboard creation
- Executive presentation exercise