CONCEPT

Cyber Incident Response, SOC Operations and Threat Hunting with MITRE ATT&CK

CONCEPT

Cyber Incident Response, SOC Operations and Threat Hunting with MITRE ATT&CK

Technical depth: Practitioner · **Practical mode:** Simulation

Introduction

Security operations centres receive thousands of alerts a day, yet intrusions still go unnoticed for weeks and incidents are often contained late because triage, escalation and evidence handling are improvised. Adversaries who avoid signature-based detection are found only by teams that hunt for them deliberately. This Core Concept course builds the response and hunting routines a SOC needs, using NIST SP 800-61 Rev. 3, ISO/IEC 27035 and MITRE ATT&CK, then tests them under time pressure. Participants leave with an Incident Response and Threat Hunting Playbook Set for their own SOC.

Course Objectives

- Classify security events by severity and escalate them using a defined matrix aligned to NIST SP 800-61 Rev. 3 and ISO/IEC 27035
- Analyse alerts and intrusions with MITRE ATT&CK, the Diamond Model and threat intelligence exchanged in STIX and TAXII
- Investigate incidents on SIEM and EDR data while preserving evidence under ISO/IEC 27037
- Contain, eradicate and recover from ransomware, account compromise and email fraud incidents
- Plan and run hypothesis-driven and intelligence-led threat hunts using PEAK and TaHiTI
- Produce an Incident Response and Threat Hunting Playbook Set ready for SOC management sign-off

Target Audience

- SOC analysts responsible for alert triage, investigation and escalation
- Incident responders and CSIRT members who contain and recover from security incidents
- Threat hunters and detection engineers who build and tune detection content
- Threat intelligence analysts who supply indicators and adversary context to the SOC
- Security operations shift leads who coordinate response during live incidents

Course Outline

Day 1: Incident Response and SOC Foundations

- Incident Response in NIST CSF 2.0 and NIST SP 800-61 Rev. 3
- ISO/IEC 27035-1:2023 Incident Management Phases
- SOC Operating Models, Analyst Tiers and the FIRST CSIRT Services Framework
- SOC Capability Assessment with SOC-CMM
- Incident Severity Classification and Escalation Matrix

Day 2: Adversary Models and Detection Standards

- MITRE ATT&CK Enterprise Tactics, Techniques and Procedures
- Cyber Kill Chain and the Diamond Model of Intrusion Analysis
- Pyramid of Pain and Indicator Quality Assessment
- Threat Intelligence Exchange with STIX 2.1 and TAXII 2.1
- Detection Rule Writing in Sigma and YARA

Day 3: Investigation, Containment and Recovery

- SIEM Alert Triage and Log Source Correlation Workflow
- EDR Investigation and Endpoint Triage Collection
- Evidence Handling and Chain of Custody under ISO/IEC 27037
- Containment, Eradication and Recovery Decision Tree
- Incident Status Reporting and Stakeholder Notification Log

Day 4: Threat Hunting and Complex Incidents

- Hypothesis-Driven Hunting with the PEAK Framework
- Intelligence-Led Hunting Using the TaHiTI Methodology
- Hunting Living-off-the-Land Techniques through ATT&CK Mappings
- Ransomware and Business Email Compromise Response Playbooks
- Post-Incident Review, Detection Gap Analysis and MTTD and MTTR Metrics

Day 5: Response Simulation and the Playbook Set

- Ransomware Outbreak Simulation: Triage to Containment
- Cloud Account Compromise Simulation: Scoping and Recovery
- Threat Hunt Execution on a Supplied Log Dataset
- Incident Response and Threat Hunting Playbook Set Drafting
- Simulation Debrief and Playbook Defence

Skills You Will Gain

- Alert Triage
- Intrusion Analysis
- Digital Evidence Preservation
- Incident Containment
- Detection Engineering
- Threat Hunting
- Threat Intelligence Application
- Post-Incident Review

Why Attend This Course

- Return to work with an Incident Response and Threat Hunting Playbook Set, already exercised under simulated pressure
- Make faster and more consistent escalation decisions during the first hour of an incident
- Find adversary activity that existing alerts miss by running structured hunts on your own data
- Compare response practice with SOC teams from other sectors and countries facing similar adversaries

Conclusion

A SOC is judged by how quickly it finds an intrusion and how cleanly it contains it. This course moves from incident response standards and SOC operating models, through adversary frameworks and detection formats, to investigation, evidence handling, containment and structured threat hunting. The final day tests those routines in timed simulations and turns them into an Incident Response and Threat Hunting Playbook Set that participants take back to their team, giving them repeatable procedures for the next incident they face.