CYBERIUM ARENA

Description

Dive deep into the realm of Threat Hunting with this comprehensive, hands-on training. Begin with foundational concepts, then master advanced techniques, from endpoint forensics to network analysis. Engage in real-world scenarios and labs, exploring everything from machine learning applications to ethical considerations. By the end, emerge as a skilled threat hunter, adept at identifying and mitigating evolving cybersecurity challenges.

THREAT HUNTING

Module 1: Intro to Threat Hunting

Dive into threat hunting setup and strategies. Understand proactive vs. reactive cybersecurity, explore the Cyber Kill Chain and MITRE ATT&CK frameworks, and master tools like SIEM and EDR. Harness threat intelligence sources and simulate real-world threats in configured labs.

Setting Up the Hunting Environment
Proactive vs. Reactive Cybersecurity
Cyber Kill Chain and MITRE ATT&CK Framework
SIEM, EDR, and Threat Intelligence Platforms
Configuring a Lab for Simulated Threats
Logs, Network Traffic, and Endpoint Data
Sources of Threat Intelligence
Feeding Intelligence into Hunting Tools

Module 2: Practical Simulations

Delve into advanced threat hunting methodologies, from hypothesis-driven tactics to heuristic-based approaches. Master the art of detecting network lateral movements, C2 communications, and data exfiltration attempts. Enhance your skills in memory forensics, uncovering persistence mechanisms, and identifying elusive fileless malware techniques.

Hunting Techniques and Tactics
Hypothesis-Driven Hunting
Pattern and Anomaly Detection
Heuristic-Based Approaches
Detecting Lateral Movement within a Network
Command and Control (C2) Communications
Identifying Data Exfiltration Attempts
Memory Analysis and Forensics
Detecting Persistence Mechanisms
Uncovering Fileless Malware Techniques

Module 3: Network Hunting

Dive into network threat hunting, from deep packet inspection to DNS monitoring. Identify suspicious traffic, encrypted threats, and leverage machine learning techniques. Explore insider threat detection, honeypot strategies, and real-world breach analysis.

Deep Packet Inspection and Analysis
Baselining Network Behavior
DNS Monitoring and Analysis
Identifying Suspicious Traffic Patterns
Uncovering Encrypted Threats
Threat Hunting using Machine Learning
Hunting for Insider Threats
Honeypots and Deception Technologies
Analyzing Real-World Breaches and APTs

Module 4: Response and Remediation

Embark on a journey through threat hunting and incident response, delving into forensic analysis and containment strategies. Master post-incident evaluations, ensure continuous monitoring, and integrate threat intelligence into hunting practices. Conclude with robust backup and disaster recovery protocols.

Threat Hunting and Incident Response
Forensic Analysis
Containment and Mitigation Strategies
Post-Incident Analysis
Continuous Monitoring
Threat Intelligence in Threat Hunting
Backup and Disaster Recovery

NX Defense | LEVEL: 5 | DURATION: 40h