FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

Course Overview

Threat hunting and incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident or contain propagating ransomware. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions. This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and ransomware operators.ate their moves and build better defenses.

Prerequisites

FOR508 is an advanced incident response and threat hunting course that focuses on detecting and responding to advanced persistent threats and organized crime threat groups. The course does not cover the basics of incident response policies or digital forensics.

Job Roles

- Incident Response Team
- Threat Hunters
- SOC Analysts
- Experienced Digital Forensic Analysts
- Detection Engineers
- Information Security Professionals
- Federal Agents and Law Enforcement Professionals
- Red Team Members
- Penetration Testers
- Exploit Developers

NICE Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Duration

6 Days

Certifications

GIAC Certified Forensic Analyst (GCFA)

Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: Incident Response and Cyber Investigations
TOPICS: Real Incident Response Tactics, Threat Hunting, Threat Hunting in the Enterprise, Incident Response and Hunting Across the Enterprise, Malware Defense Evasion and Identification, Malware Persistence Identification, Prevention, Detection, and Mitigation of Credential Theft

SECTION 2: Intrusion Analysis
TOPICS: Advanced Evidence of Execution Detection, Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs), Log Analysis for Incident Responders and Hunters, Investigating WMI and PowerShell-Based Attacks

SECTION 3: Memory Forensics in Incident Response & Threat Hunting
TOPICS: Endpoint Detection and Response (EDR), Memory Acquisition, Memory Forensics Analysis Process for Response and Hunting, Memory Forensics Examinations, Memory Analysis Tools

SECTION 4: Timeline Analysis
TOPICS: Malware Defense Evasion and Detection, Timeline Analysis Overview, Filesystem Timeline Creation and Analysis, Super Timeline Creation and Analysis

SECTION 5: Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics Detection
TOPICS: Volume Shadow Copy Analysis, Advanced NTFS Filesystem Tactics, Advanced Evidence Recovery

SECTION 6: The APT Threat Group Incident Response Challenge
The Intrusion Forensic Challenge requires analysis of multiple systems from an enterprise network with many endpoints.

Course Objectives

- Understand attacker tradecraft to perform compromise assessments
- Detect how and when a breach occurred
- Quickly identify compromised and infected systems
- Perform damage assessments and determine what was read, stolen, or changed
- Contain and remediate incidents of all types
- Track adversaries and develop threat intelligence to scope a network
- Hunt down additional breaches using knowledge of adversary techniques
- Build advanced forensics skills to counter anti-forensics and data hiding from technical subjects

GIAC Certified Forensic Analyst (GCFA)

The GIAC Certified Forensic Analyst (GCFA) certification focuses on core skills required to collect and analyze data computer systems. Candidates have the knowledge, skills, and ability to conduct formal incident investigations and handle advanced incident handling scenarios, including internal and external data breach intrusions, advanced persistent threats, anti-forensic techniques used by attackers, and complex digital forensic cases.

- Advanced Incident Response and Digital Forensics
- Memory Forensics, Timeline Analysis, and Anti-Forensics Detection
- Threat Hunting and APT Intrusion Incident Response