FORENSIC ANALYSIS

Definition of training:

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 syndicates.

Advanced Incident Response and Threat Hunting Education will help you to:

- 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 the adversary
- Build advanced forensics skills to counter anti-forensics and data hiding from technical subjects.

This training is an advanced incident response and threat hunting training focused on detecting and responding to advanced persistent threats and groups of organized crime threats. The training does not cover the fundamentals of incident response policies or digital forensics.

Duration:

2 Instructors / 6 Days

Place:

Online Platform

Target group:

Incident Response Team Members, Threat Hunters, SOC Specialists, Experienced Digital Forensic Specialists, Information Security Professionals, Federal Agents and Law Enforcement Professionals, Red Team Members, Penetration Testers and Exploit Developers

Participation prerequisite:

We recommend that attendees should have a background in Windows Forensics prior to attending this education.

Document:

Certificate of participation

Forensic Analysis_ENG.11/2022_V1