INCIDENT RESPONSE LEVEL 1

Incident Response 🕓 7 hours of content | 40 hours of practice | Final project

1. Attack & Defense Methodolgy

- Introduction
- MITRE ATT&CK
- Cyber Kill Chain
- TACTICS,TECHNIQUES & PROCEDURES
- Incident Response Methodolgy
- Proactive Hunt
- Live Analysis
- IOC's Vs IOA's
- Know Your Process
- Virtualization And Windows10 Lab

2. Threats And Scoping

- Host & Network Based Incidents
- Threats Types
- Threat Triage
- Operation System Visability
- PS Transcription And User SID

3. Endpoint Threat Artifects

- The Sysinternals Suite
- Process Explorer DeepDive
- Persistnce With Autoruns
- Autoruns CommandLine
- Exercise Scenario - Red Line Malware
- Unsigned Binary Detection
- Operation Detection Procmon
- Procmon Beautifier
- Exercise - Njrat
- Network Activity views
- Detect Source Zone Identifier
- System Resource Utilization Monitor
- RDP Cacheing
- ActivitiesCache

4. Windows Logs Analysis

- Windows Event Logs
- Event Logon Types
- Event Id's
- Event Log's Capabilities Demo
- Investigation Scenario Exercise
- Evtx Over TimeLine Explorer
- Sysmon
- Event Hunting

5. Registry Threat Artifects

- Qradar Log Activity
- Registry Structure
- Registry File Acquisition
- Registry Explorer
- Registry Point Ofs Interst
- Registry ASEPS
- UserAssist
- ShellBags
- SetupApi

6. Networking Threat Analysis

- Introduction To Wireshark
- Wireshark Statistics
- DNS Analysis
- DHCP Analysis
- HTTP Analysis
- Attack Scenarios Exercies
- SMB & MS-RPC Analysis
- Attack Scenario Exam

7. Evidence Of Execution

- JumpLists
- ShimCache
- AmCache

ITSAFE
POWERED BY CYSOURCE