Hands On Security Operation Center Analyst

1. Introduction To SOC

Section 1 - Lessons

- Introduction - Hands-On Security Operation Center Analyst
- SOC Analyst Roles & Duties
- Threats Handled by SOC Analyst
- SOC Tools, You Need
- Cyber Kill Chain Framework

2. Phishing Email Fundamentals

Section 2 - Lessons

- Types Of Phishing Attack
- Phishing Analysis Lab Setup
- Practical Phishing Email Analysis Lab-1
- Practical Phishing Email Analysis Lab-2 Part-1
- Practical Phishing Email Analysis Lab-2 Part-2
- Extract Indicator of Compromise of Phishing Email
- Malicious Email Attachments-Analysis
- Automated IOC Extraction from Phishing Email Part-1
- Automated IOC Extraction from Phishing Email Part-2
- Automated Malicious Shortcut (LNK) File Analysis
- Manual Malicious Shortcut (LNK) File Analysis

3. Network Security & Traffic Analysis

Section 3 - Lessons

- Network Analysis & Devices
- Common Ports & Services
- Malicious Traffic Analysis Tools
- Wireshark Basics
- Pcap File Analysis Lab – 1
- Pcap File Analysis Lab – 2
- Network Minor Basics
- Network Forenscis via Network Minor Lab -1
- Intrusion Detection & Prevention System
- Introduction to Snort
- IDS Snort Rule Lab -1
- IDS Snort Lab - 2

4. Endpoint Detection & Response (EDR)

Section 4 - Lessons

- Introduction to EDR
- Endpoint Security Monitoring
- Windows Core Artifacts
- Windows Event Logs
- Windows Scheduled Task
- Windows Autoruns
- Introduction to Sysmon
- Sysmon Event Log Analysis Lab -1
- Sysmon Event Log Analysis Lab - 2
- Wazuh Endpoint Detection & Response
- Wazuh Dashboard Setup Lab - 1
- Wazuh Agent Installation Lab – 2
- EDR Threat Detection Lab – 3

5. Threat Intelligence / Hunting

Section 5 - Lessons

- Introduction to Threat Intelligence
- Types of Threat Intel's
- Diamond Model
- Pyramid of Pain
- MITRE ATT&CK Basic
- MITRE ATT&CK Navigator
- MITRE ATT&CK Lab - 1
- MITRE ATT&CK Lab - 2
- Introduction to Yara Rules
- Malware detection using Yara Lab – 1
- Malware detection using Yara Lab – 1

6. Security Information & Event Management (SIEM)

Section 6 - Lessons

- Introduction to SIEM
- Architecture
- Deployment Models
- SIEM Log Types
- SIEM Log Formats
- SIEM Capabilities

- Log Analysis Lab – 1
- Introduction to Splunk
- Splunk Basics
- Splunk Queries
- Splunk Dashboard Setup - Lab
- Import Events in Splunk – Lab
- Attack Investigation via Splunk – Lab