Course Title: Security Operations Center (SOC) - Blue Teaming
Duration: 4 Months
Mode: Hybrid Classes
Level: Intermediate
Labs and Projects: 12 Practical Labs and Projects
Language: English

Month 1: SOC Fundamentals and Threat Detection

Module 1: SOC Fundamentals

- Introduction to SOC and Blue Team roles
- SOC structure and functions
- Key responsibilities of SOC analysts

Module 2: Threat Detection Frameworks

- Cyber Kill Chain: Understanding the stages of an attack
- MITRE ATT&CK Framework: Techniques and tactics for threat identification
- Lab: Mapping incidents to the Cyber Kill Chain

Module 3: Phishing Email Analysis

- Techniques for detecting phishing attempts
- Analyzing suspicious emails
- Lab: Phishing email investigation

Month 2: Attack Detection and Malware Analysis

Module 4: Detecting Web Attacks

- Common web attack techniques (SQL injection, XSS, CSRF)
- Investigating web attack patterns
- Lab: Investigate a simulated web attack

Module 5: Malware Analysis

- Introduction to malware analysis

- Static Analysis: Analyzing malware binaries
- Dynamic Analysis: Monitoring malware behavior
- Project: Setting up a malware analysis lab and analyzing malware samples

Month 3: Security Monitoring and Incident Management

Module 6: Security Solutions

- Overview of security solutions (firewalls, IDS/IPS, EDR)
- Lab: Configuring a basic EDR solution

Module 7: Network Log Analysis

- Identifying anomalies in network logs
- Techniques for log correlation
- Project: Analyzing a network log to identify incidents

Module 8: Security Information and Event Management (SIEM)

- Introduction to SIEM systems
- Splunk Setup and Configuration: Data ingestion and basic queries
- Project: Setting up Splunk and analyzing event logs

Month 4: Advanced Threat Intelligence and SOC Lab Projects

Module 9: Cyber Threat Intelligence (CTI)

- Gathering and analyzing threat intelligence
- Integrating CTI into SOC operations

Module 10: IT Security for Corporates

- Corporate security policies
- Best practices for maintaining security in a corporate environment

Module 11: Detecting Brute Force Attacks

- Identifying brute force patterns

- Automating detection using SIEM
- Lab: Implementing brute force attack detection

Capstone Projects:

- Project 1: Building a SOC Lab at Home
- Project 2: ELK SOC Setup
- Project 3: Wazuh XDR Implementation

Final Project:

- Adversary Simulation
    - End-to-end incident detection and response simulation
    - Creating a detailed SOC report

Skills Acquired:

- Threat detection and analysis
- Malware analysis techniques
- Security monitoring and incident management
- Network and log analysis
- Implementing and using SIEM tools (Splunk, ELK, Wazuh)
- Corporate IT security practices