Certified SOC Analyst

Purpose of the Class

This class will help the student to acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. It covers fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response.

Additionally, the student will learn to manage various SOC processes and collaborate with CSIRT at the time of need

Course Objectives

Upon successful completion of this course, the students will be able to:

1. Gain foundational knowledge of Security Operations Center (SOC) functions and architecture.

2. Understand adversary Tactics, Techniques, and Procedures (TTPs) and identify associated Indicators of Compromise (IoCs).

3. Develop skills in log management for effective monitoring and analysis.

4. Understand the role and functionality of Security Information and Event Management (SIEM) solutions in security operations.

5. Design and develop SIEM use cases for efficient incident detection and triage.

6. Leverage threat intelligence feeds to proactively detect emerging threats.

7. Learn and apply techniques for performing proactive threat hunting activities.

8. Develop skills to effectively respond to a wide range of cybersecurity incidents.
9. Investigate various types of security incidents using structured analysis techniques.
10. Perform basic malware analysis to identify and understand malicious behavior.
11. Detect threats within cloud-based network environments using appropriate tools and methodologies.

Module 01 – Security Operations and Management

OBJECTIVES:

Gain foundational knowledge of Security Operations Center (SOC) functions and architecture.

DISCUSSION THREAD:

Discuss the key technologies used in a SOC and how they support security operations

Module 02 – Understanding Cyber Threats, IoCs, and Attack Methodology

OBJECTIVES:

Understand adversary Tactics, Techniques, and Procedures (TTPs) and identify associated Indicators of Compromise (IoCs).

DISCUSSION THREAD:

- Discuss cyber threats, including their indicators, attack vectors, and underlying motivations
- Discuss various attack methodologies and frameworks that attackers use to conduct successful attacks

Module 03 – Log Management

OBJECTIVES:

Develop skills in log management for effective monitoring and analysis.

DISCUSSION THREAD:

- Discuss the local logging practices for different operating systems (Windows, Linux, and macOS),
- Discuss the infrastructure behind centralized logging and the systematic approach to logging, monitoring, and analysis in a centralized setup

Module 04 – Incident Detection and Triage in SOC

OBJECTIVES:

- Understand the role and functionality of Security Information and Event Management (SIEM) solutions in security operations.
- Design and develop SIEM use cases for efficient incident detection and triage.

DISCUSSION THREAD:

- Discuss different types of SIEM solutions
- Discuss implementing phased SIEM deployment
- Discuss creating effective use cases for incident detection and producing regular expression-based rules to detect and respond to cyberattacks

Module 05 – Proactive Threat Detection in SOC

OBJECTIVES:

- Leverage threat intelligence feeds to proactively detect emerging threats.
- Learn and apply techniques for performing proactive threat hunting activities.

DISCUSSION THREAD:

- Discuss the threat intelligence lifecycle and the threat analyst's role in it
- Discuss the different threat intelligence sources

Module 06 – Incident Response

OBJECTIVES:

Develop skills to effectively respond to a wide range of cybersecurity incidents.

DISCUSSION THREAD:

- Discuss the importance of Incident Response (IR) and its process flow
- Discuss the differences between SOC Playbook and SOC Runbook
- Discuss the best practices for EDR/XDR deployment in SOC

Module 07 – Forensics Investigation and Malware Analysis

OBJECTIVES:

- Investigate various types of security incidents using structured analysis techniques.
- Perform basic malware analysis to identify and understand malicious behavior.

DISCUSSION THREAD:

- Discuss the process involved in forensic investigation
- Discuss the SOC analyst’s approach to malware analysis

Module 08 – SOC for Cloud Environments

OBJECTIVES:

Detect threats within cloud-based network environments using appropriate tools and methodologies.

DISCUSSION THREAD:

- Discuss the fundamentals of Cloud SOC and the operational differences between Cloud SOC and On-Prem SOC
- Discuss implementing an SIEM solution using the services and third-party tools of different cloud providers AWS, Azure, and GCP