Certified SOC Analyst

Modality: Virtual Classroom

Duration: 3 Days

What's Included:

- *Official EC Council Invitation to the virtual class*
- *Official EC Council Print or e-courseware included*
- *Official EC Council ilabs subscription*
- *EC Council Exam Voucher included*

About the Course:

The Certified SOC Analyst (CSA) program is designed as the first step for individuals aspiring to join a security operations center (SOC). This program focuses on equipping Tier I and Tier II SOC analysts with the necessary skills to perform entry-level and intermediate-level SOC operations. By emphasizing a holistic approach and providing hands-on lab exercises, the CSA program prepares individuals to identify and validate intrusion attempts, effectively use SIEM solutions and threat intelligence, and enhance threat detection capabilities. This program is essential in meeting the increasing demand for skilled SOC analysts who play a crucial role in detecting and responding to emerging cyber threats and protecting organizations from security incidents.

Course Objectives:

- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Gain basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities, attacker’s behaviors, cyber kill chain, etc.
- Able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
- Able to monitor and analyze logs and alerts from a variety of different technologies across
- multiple platforms (IDS/IPS, end-point protection, servers and workstations).
- Gain knowledge of Centralized Log Management (CLM) process.
- Able to perform Security events and log collection, monitoring, and analysis.
- Gain experience and extensive knowledge of Security Information and Event Management.
- Gain knowledge on administering SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Understand the architecture, implementation and fine tuning of SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Gain hands-on experience on SIEM use case development process.
- Able to develop threat cases (correlation rules), create reports, etc.
- Learn use cases that are widely used across the SIEM deployment.
- Plan, organize, and perform threat monitoring and analysis in the enterprise.

- Able to monitor emerging threat patterns and perform security threat analysis.
- Gain hands-on experience in alert triaging process.
- Able to escalate incidents to appropriate teams for additional assistance.
- Able to use a Service Desk ticketing system.
- Able to prepare briefings and reports of analysis methodology and results.
- Gain knowledge of integrating threat intelligence into SIEM for enhanced incident detection and response.
- Able to make use of varied, disparate, constantly changing threat information.
- Gain knowledge of Incident Response Process.
- Gain understating of SOC and IRT collaboration for better incident response

Audience:

- SOC Analysts (Tier I and Tier II)
- Network and security professionals involved in network security operations, including administrators, engineers, analysts, technicians, specialists, and operators.
- Cybersecurity Analyst
- Entry-level cybersecurity professionals
- Anyone who wants to become a SOC Analyst

Prerequisites:

The CSA program requires a candidate to have 1 year of work experience in the Network Admin/Security domain

Course Outline:

Module 1:
Security Operations and Management

Module 2:
Understanding Cyber Threats, IoCs, and Attack Methodology

Module 3:
Incidents, Events, and Logging

Module 4:
Incident Detection with Security Information and Event Management (SIEM)

Module 5:
Enhanced Incident Detection with Threat Intelligence

Module 6:
Incident Response