INFOSECTRAIN

EC-Council Accredited Training Center

C|SA

Certified SOC Analyst

Course Agenda

sales@infosectrain.com | www.infosectrain.com

Index

Learning 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

Course Outline

Module 01: Security Operations and Management

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

Module 03: Incidents, Events, and Logging

Module 04: Incident Detection with Security Information and Event Management (SIEM)

Module 05: Enhanced Incident Detection with Threat Intelligence

Module 06: Incident Response

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com