

EC Council Official SOC Analyst (CSA)

Course Code

SC106

Duration

3 Days

Format

Classroom | Classroom/Virtual | Virtual

Overview

As the security landscape is expanding, a SOC team offers high quality IT-security services to actively detect potential cyber threats/attacks and quickly respond to security incidents. Organizations need skilled SOC Analysts who can serve as the front-line defenders, warning other professionals of emerging and present cyber threats.

The lab-intensive Certified SOC Analyst (CSA) program emphasizes the holistic approach to deliver the advanced knowledge of how to identify, validate and defend against cyber-attacks. The event is targeted at SOC Level 1 & Level 2 team members and their managers and those IT staff aspiring for a role in SOC.

Objectives

The goal of this course is to help you master how to use SIEM and other SOC tools to identify and protect the business from cyber threats. Candidates will learn to perform enhanced threat detection using the predictive capabilities of Threat Intelligence. You walk out the door with skills needed to be an effective SOC response team member as well as the internationally recognized SOC Analyst certification!

Content

- SOC processes, procedures,
- Technologies, and workflows.
- Security threats, attacks & vulnerabilities
- The cyber kill chain
- Recognize attacker tools & tactics
- Monitor and analyse logs and alerts
- Centralized Log Management (CLM)
- Log collection, monitoring, and analysis SIEM solutions
- Architecture & implementation
- Fine tuning of SIEM solutions
- Gain hands-on experience on SIEM use cases
- Able to develop threat cases SIEM Use cases
- Plan, organize, and perform threat monitoring
- Monitor emerging threat patterns
- Perform security threat analysis

Prerequisites

All delegates must have strong TCP/IP networking skills, equivalent of CompTIA Network+. All delegate must have strong IT Systems administration experience, equivalent of CompTIA A+ and CompTIA Server+. It is recommended that delegates have fundamental security experience, equivalent of our CISMP programme.

EC Council Official SOC Analyst (CSA)

Course Code

SC106

Duration

3 Days

Format

Classroom | Classroom/Virtual | Virtual

- Gain hands-on experience in alert triaging process.
- Threat intelligence
- Enhanced incident detection and response
- Gain knowledge of Incident Response Process