Certified SOC Analyst (CSA)

Course Description

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entrylevel and intermediate-level operations. CSA is a training and credentialing program that helps the candidate 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. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Key Outcomes

- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
- Gain experience and extensive knowledge of Security Information and Event Management.
- Able to develop threat cases (correlation rules), create reports, etc.
- Plan, organize, and perform threat monitoring and analysis in the enterprise.
- Able to prepare briefings and reports of analysis methodology and results.
- Gain understating of SOC and IRT collaboration for better incident response.

Exam Information

- Exam Title: Certified SOC Analyst
- Exam Code: 312-39
- Number of Questions: 100
- Duration: 3 hours
- Availability: EC-Council Exam Portal (please visit https://www. eccexam.com)
- Test Format: Multiple Choice
- Passing Score: 70%

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