

CERTIFIED SECURITY OPERATION CENTER (SOC) ANALYST

CSOCA

Duration: 5 days; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

A security operations centre (SOC) is a facility operating 24 x 7 x 365, where enterprise information systems (data centres, servers, networks, desktops and other endpoints) are monitored, assessed, and defended around the clock. SOC Analysts are the backbone for the operations of a SOC. This course prepares you to be ready for the real-world challenges of a SOC Analyst.

OBJECTIVES

As more enterprises guided by the current state of cybersecurity, compliance and regulations are either setting up their own SOC or outsourcing SOC activities to MSSPs, there is an acute shortage of SOC Analysts / Professionals who understand all the SOC technologies and how to handle them to achieve cyber-resilience for customers.

- Gain in-depth knowledge of security threats, attacks, vulnerabilities, attackers' behavior, cyber kill chain, SOC processes, procedures, technologies, and automation workflows
- Understand the MITRE ATT&CK Framework and able to identify attacker techniques, tactics, and procedures (TTP) to investigate indicators of compromise (IOCs) and provide automated / manual responses to eliminate the attack/incident
- Understand SOC and its processes, roles, responsibilities and implementation models
- Able to monitor and work on alerts generated based on various log sources. Ex: IDS/IPS, AV, EDR, Firewall, Network Monitoring applications, etc.
- Gain in-depth knowledge on all the latest defense technologies that are used in next generation SOC deployments. Ex : NGAV, SIEM, EDR, XDR, SOAR, TI, UEBA, IAM/PAM, etc.
- Gain knowledge of Incident Response Methodology, processes and in-depth knowledge on how to integrate SOC processes with Incident Response processes and learn how to automate them as a single workflow
- Able to understand the concepts of Threat Intelligence and gain in-depth knowledge on how to integrate Threat Intelligence with the SIEM, SOAR, EDR and other SOC technologies to reduce the Mean time to Detect (MTTD) and Mean time to Respond (MTTR)

PREREQUISITES

Not applicable.

AUDIENCE

Cybersecurity Analysts, Network and Security Administrators, Entry-level cybersecurity professionals, New recruits into a SOC environment.

COURSE CONTENTS

Module 1: Introduction to Cyber Security & Latest Attack Trends

- What is Security, Vulnerabilities & O-Days, Attack life Cycle, Different Attack Vectors
- Threats Vs. Risks, Why Perimeter defenses are failing? Why Anti-Virus is not enough?
- Financial Implications of a Cyber Attack
- Business Email Compromise (BEC) (Demo)
- Ransomware (Demo)
- Advanced Persistent Threat (Demo)
- File-less Malwares (Demo)
- Mobile Malwares (Demo)
- Identity Theft (Demo)
- Web Data Breach (Demo)
- Malvertising (Demo)
- Payment Gateway based attacks (Demo)
- Social Media based attacks (Demo)
- Password based attacks (Password Stuffing, Account Takeover, Phishing, etc) (Demo)
- State sponsored attacks (Case Study)
- Distributed Denial of Service (Case Study)
- Insider Threat (Case Study)

Module 2: Security Operations Center (SOC) – Introduction

- What is a Security Operations Center and why we need it ?
- NOC vs. SOC
- Overview of CARTA
- SOC v1.0 vs SOC v2.0
- SOC v2.0 : Components
- Security Operations Center roles and responsibilities
- SOC team roles and responsibilities
- Challenges of Security Operations Center
- Measuring the ROI of Security Operations Center

Module 3: Understanding Attack DNA

- What is MITRE ATT&CK Framework?
- Tactics, Techniques and Procedures (TTP)

- Indicators of Compromise (IoC) and Indicators of Attack (IoA)
- Mapping to ATT&CK from Raw Data – Lab

Module 4: Latest Cybersecurity Defence Technologies

- Anti-Virus & Next Generation Anti-Virus (NGAV)
 - How it works and Where is the Gap ?
- Deep Learning & Machine Learning & Artificial Intelligence
 - Cybersecurity use cases
- Security Information and Event Management (SIEM)
 - How it Works ?
 - Understanding Logs & Log Correlation
 - SIEM Deployment options
 - Application Level Incident Detection Use Case Examples
 - Network Incident Detection Use Case Examples
 - Host Malware Incident Detection Use Case Examples
 - Understanding why SIEM is not enough and why Noise/False Positives ?
 - Lab / Demo
- Endpoint Detection and Response (EDR)
 - How it Works ?
 - EDR vs. NGAV
 - Understanding Memory and Process Detection & Mapping
 - What is Managed Detection and Response
 - Understanding various Response actions
 - Lab / Demo
- Security Orchestration, Automation and Response (SOAR)
 - Alert / Notification Handling Challenges
 - Why SOAR ?
 - Sample Automated Playbooks
 - Lab / Demo
- Cyber Range
 - Cyber Range Components
 - Cyber Range Simulation Scenarios
- Data Leakage Prevention (DLP)
- User Behavior Analytics
- Identity Management
- Virtual Dispersive Networking (VDN)

Module 5: Cybersecurity Incident Response

- Introduction to Incident Response
 - Types of Computer Security Incidents
 - Fingerprint of an Incident
 - Incident Categories & Incident Prioritization
 - Why Incident Response?
 - Incident Reporting
- Incident Response & Handling Methodology
- Incident Response Plan
- Incident Response and Handling : Identification, Incident Recording, Initial Response, Communicating the Incident, Containment, Formulating a Response Strategy, Incident Classification, Incident Investigation, Data Collection, Forensic Analysis, Evidence Protection, Systems Recovery, Incident Documentation, Incident Damage and Cost Assessment, Review and Update the Response Plan and Policies

- Incident Response Checklist and Best Practices
- CSIRT & its best practices
- Incident Response Team
- Incident Tracking and Reporting
- Incident handling : Real Word examples and exercises on Malware, Web Application attacks, Email attacks and Insider attacks.

Module 6: Threat Intelligence & Threat Hunting

- Introduction to Threat Intelligence
 - Understanding Threats, Threat Modeling and Risk
 - What is Threat Intelligence
 - Need for Threat Intelligence
 - Benefits of Threat Intelligence
 - Types of Threat Intelligence
 - Threat Intelligence Life Cycle
 - Sources of Threat Intelligence
 - Technologies contributing to Threat Intelligence (SIEM, EDR, Log Sources)
 - Incident Response & Threat Intelligence
 - Applications of Threat Intelligence
 - Threat Intelligence Frameworks (CIF, MISP, TAXII)
 - Role of Threat Intelligence Analyst & Threat Hunters
 - Role of Threat Intelligence in SOC operations
- Setting up Threat Intel Framework
 - Enterprise Threat Landscape Mapping
 - Scope & Plan Threat Intel Program
 - Setup Threat Intel Team
 - Threat Intelligence Feeds, Sources & Data Collections
 - Open source Threat Intel Collections (OSINT and more)
 - Dark Web Threat Intel Collections
 - SIEM / Log Sources Threat Intel Collections
 - Public Web data Threat Intel Collections (Maltego, OSTRiCa, and more)
 - Threat Intel collections with YARA
 - EDR Threat Intel Collections
 - Incorporating Threat Intel into Incident Response
 - Threat Intel & Actionable Contextual Data
- MISP Lab