AjarAble

CERTIFIED SECURITY OPERATION CENTER (SOC) ANALYST

CSOCA

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

OVERVIEW

As you are reading this document, more than 100 successful hacking has occurred in the world per minute. With all the news stories about hackers, botnets, and breaches involving personal information, it's easy for the security message to sound over-used and tired. It's easy for people to say, "It won't happen here."

Currently, Security Operation Centre (SOC) Analyst role is being only used in Security Operation Centers (SOC) that are monitoring financial institutions. Instead, we can upscale every IT person in an organization by equipping them with the skillset of a SOC Analyst so that they have the ability to review logs and identify attacks that are happening in their own organization and enable their organization to respond to them effectively.

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

- Gain in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, 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 on 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, 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

- No prerequisites.

AUDIENCE

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

CERTIFICATION

Option 1: GlobalACE Certification
Certified SOC Analyst (CSOCA)

- The CSOCA examination is certified by the Global ACE Certification. The examination framework is designed to align with a set of relevant Knowledge, Skills and Attitudes (KSA) that is necessary for an Information Security Professional. Candidates will be tested via a combination of either continual assessment (CA), multiple choice questions (MC), theory/underpinning knowledge assessment (UK), practical assessment (PA), assignments (AS) or case studies (CS) as required.
- Candidates can take the examination at authorized examination centres in participating scheme member countries. Candidates who have successfully passed the CSOCA examination will be eligible to apply as an associate or professional member by fulfilling the membership criteria defined under the Global ACE Certification.
- Free Add-on: Free Membership access to KALAM Cybersecurity Collaboration & Community Skills Validation Platform

Option 2: Cybertronium Certification
Certified SOC Analyst (CSOCA)

- Exam Platform: KALAM
- Exam Format: Multiple Choice Question (MCQ)
- Exam Questions: 50 Questions
- Exam Duration is: 90 Minutes
- Exam Pass Mark: 70%
- Exam Fees: Inclusive in the Course Fees
- Free Add-on: Free Membership access to KALAM Cybersecurity Collaboration & Community Skills Validation Platform

AjarAble Consulting Sdn Bhd
41M, Jalan SS 21/1A, Damansara Utama, 47400 Petaling Jaya, Selangor
Contact: (+60)12 332 8535 | Email: info@ajarable.com | Website: www.ajarable.com

AjarAble

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

AjarAble Consulting Sdn Bhd
41M, Jalan SS 21/1A, Damansara Utama, 47400 Petaling Jaya, Selangor
Contact: (+60)12 332 8535 | Email: info@ajarable.com | Website: www.ajarable.com

- 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