NETWORK INTELLIGENCE
Global cybersecurity provider

CSOCP
Certified Security Operations Center Practitioner

Certified Security Operations Center Practitioner (CSOCP)

16 hours of comprehensive workshop with Live DEMO

Batch 1: Asia & Middle East

Dates: February 21 – 24, 2022
Timing: 6 00 AM – 10 00 AM GMT

Batch 2: Americas & Europe

Dates: February 28 – March 3, 2022
Timing: 2 00 PM – 6 00 PM GMT

Course Fee:

Regular Participant – USD 200

ISACA/ISC2 Member – USD 150

INTRODUCTION:

The number of successful data breaches continues to increase everyday. Adversaries seem to have the upper hand, as many organizations fail to effectively detect and quickly respond to these breaches. Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams, and are often caught by surprise.

A Security Operations Center or SOC monitors enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints). The Security Operations Center allows an organization to enforce and test its security policies, processes, procedures and activities through one central platform that monitors and evaluates the effectiveness of the individual elements and the overall security system.

This course will cover the design, deployment and operation of the SOC. Once this course is completed, you will have the skills to perform your SOC responsibilities effectively.
Here, instructors will teach you the skills to analyse and detect threats to an organization through demonstrations, labs, and lectures.

The course covers the functional areas: Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment.
Security Operations Centers are used to monitor, detect, respond and mitigate threats to the organization.

WHO SHOULD ATTEND?

1.Cyber Security professionals
2.Blue Team Members
3.SOC Specialists
4.SOC Leaders and Managers

Course Contents

Security Operations Center Concepts (Day – 1)

- What is SOC
- Evolution of SOC
- Why is it required? (Objectives)
- SOC Infrastructure
- Log management
  - Computer Security Log Management
  - Log Management Infrastructure
  - Log Management Planning
  - Log Management Operational Process

SIEM (Security Information & Event Management) (Day - 2 & 3)

- Introduction to SIEM
- SIEM Architecture
- Logs and Events
- Understanding logs, various formats
- Log Baselining
- Aggregation and normalization
- Event Collection and Event Correlation
- Correlation Rules
- IBM QRadar
  - Components
  - Console Overview
  - LIVE Demo

Course Contents

Incident Response (Day - 4)

- Incident Response Plan
  - Purpose of Incident Response Plan
  - Requirements of Incident Response Plan
  - Preparation
- Incident Management
  - Purpose of Incident Management
  - Incident Management Process
  - Incident Management Team
- Incident Response Team
  - Incident Response Team Members
  - Incident Response Team Members Roles and Responsibilities
  - Developing Skills in Incident Response Personnel
  - Incident Response Team Structure
  - Incident Response Team Dependencies
  - Incident Response Team Services
  - Defining the Relationship between Incident Response, Incident Handling, and Incident Management
  - Incident Response Best Practices
  - Incident Response Policy
  - Incident Response Plan Checklist

- Incident Response and Handling Steps
  - Step 1: Identification
  - Step 2: Incident Recording
  - Step 3: Initial Response
  - Step 4: Communicating the Incident
  - Step 5: Containment
  - Step 6: Formulating a Response Strategy
  - Step 7: Incident Classification
  - Step 8: Incident Investigation
  - Step 9: Data Collection
  - Step 10: Forensic Analysis
  - Step 11: Evidence Protection
  - Step 12: Notify External Agencies
  - Step 13: Eradication
  - Step 14: Systems Recovery
  - Step 15: Incident Documentation
  - Step 16: Incident Damage and Cost Assessment
  - Step 17: Review and Update the Response Policies

Trainer Details

Mufaddal Taskin,
Lead Trainer
Network Intelligence

Mufaddal has over 26 years of diverse experience in technology solutions. His technical abilities span across Malware Analysis, Threat Hunting, Networks, Web Apps, Digital Forensics & Incident Response, Penetration Testing, SOC and ISO standards Compliance. Mufaddal has created custom course outlines as well as conducted the same for a variety of high technologies clients of Network Intelligence

Sujay Mendon,
Principal Consultant & Trainer: SOC & MDR
Network Intelligence

Having hands-on experience in both Red team and Blue team domain, Sujay was actively involved in setting up our Next Gen SOC. In his 9+ years of experience in delivery, pre-sales and regional business operations; he has gained strong competencies in business strategy, setting up SOC.

Registration form : https://forms.office.com/r/MMzbFbx6bc