NETWORK INTELLIGENCE

introducing

Certified Security Operations Center Practitioner(CSOCP)

A 16 Hours Online SOC Training

Schedule & Fees

Batch 1: Americas & Europe

Dates: 18 - 21, July 2022

Time: 1:00 PM To 5:00 PM (GMT)

Mode: Online- GoToWebinar

Batch 2: Asia & Middle East

Dates: 25 - 28, July 2022

Time: 6:00 AM To 10:00 AM (GMT)

Mode: Online GoToWebinar

Course Fees:

Regular Participant: USD $ 150

ISACA/ISC2 Member : USD $ 120

Introduction

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

An information security operations center is where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops, and other endpoints) are monitored, assessed, and defended. The CSOC (Cybersecurity Operations Centre) 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 CSOC. Once this course is completed, you will have the skills to perform your SOC responsibilities effectively.
Here, instructors will teach you the skills to analyze 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 Centres are used to monitor and detect threats to the organization.

In line with these objectives, we are pleased to announce 16 hours of training spread across 4 days on "Certified Security Operations Center Practitioner (CSOCP)."

CSOCP
Certified Security Operations Center Practitioner

NETWORK INTELLIGENCE

Day 1

Security Operations Center Concepts

- 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

Day 2&3

SIEM (Security Information & Event Management)

- 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

Day 4

Incident Response

- 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

CSOCP
Certified Security Operations Center Practitioner

NETWORK INTELLIGENCE

Day 4

- 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

Day 4

- 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

Udit Pathak,
Principal Consultant – Compliance and Audit,
Network Intelligence.

Udit Pathak currently serve as Principal Consultant at Network Intelligence focusing on Information Security audits (PCI DSS, ISO 27001, HIPAA, cloud security, etc.), Data privacy audit and implementation, application security assessment, vulnerability assessment. He delivered many trainings to ISACA and ISC2 chapters. He has delivered excellent trainings across the globe on various cyber security topics like Payment security, Forensics, Threats & Malware, Mobile App and Web App etc..

Mufaddal Taskin,
Cybersecurity Training Specialist,
Network Intelligence.

Mufaddal has over 26 years of diverse experience in technology solutions and cyber security. He currently serves as a cybersecurity Training Specialist at NI His work mainly focuses on Payment Security Audits Security, Vulnerability Assessment and Penetration Testing for NI. His technical abilities span across Networks, Web & Mobile Apps, Incident Response, Cyber Threat Intelligence, SOC and ISO standards Compliance. Mufaddal has created custom course outlines on cyber security as well as conducted the same for a variety of high technologies clients and partners of NI.

Registration Link : https://forms.office.com/r/5AL2WFDS2t

CSOCP
Certified Security Operations Center Practitioner

NETWORK INTELLIGENCE