AISECT LEARN
Better Education. Better Careers.

LIVE + SELF-PACED

CERTIFIED SECURITY OPERATIONS CENTRE

COURSE OVERVIEW

The Certified Security Operations Centre (CSOC) course is tailored to equip participants with the knowledge and expertise required to operate and defend modern security operations centers effectively. This comprehensive program focuses on providing a deep understanding of cybersecurity incident detection, response, and mitigation techniques. Through real-world simulations and hands-on exercises, students will learn how to analyze security events, identify potential threats, and implement proactive measures to protect critical infrastructure and sensitive data. By mastering the art of security incident handling and utilizing cutting-edge tools and technologies, individuals completing this course will be ready to play a pivotal role in safeguarding organizations from cyber threats, making them valuable assets in the cybersecurity landscape.

COURSE OBJECTIVE

The Certified Security Operations Centre (CSOC) course is tailored to empower learners with specialized expertise in establishing and operating effective security operations centers. Through hands-on training, participants will learn how to detect, analyze, and respond to security incidents efficiently. This course will prepare individuals to handle real-time cyber threats and ensure the continuous protection of an organization's critical assets.

WHAT YOU WILL LEARN

The Certified Security Operations Centre (CSOC) course offers participants an immersive experience in the world of security operations and incident response. Aspiring security analysts will develop a comprehensive understanding of cybersecurity fundamentals, learning about various cyber threats, attack vectors, and the tools used by threat actors. They will explore the methodologies employed to monitor, detect, and respond to security incidents effectively.

Throughout the course, participants will gain hands-on experience with security information and event management (SIEM) systems, intrusion detection systems (IDS), and threat intelligence platforms. They will also learn about security incident analysis and triage, as well as incident containment and eradication techniques.

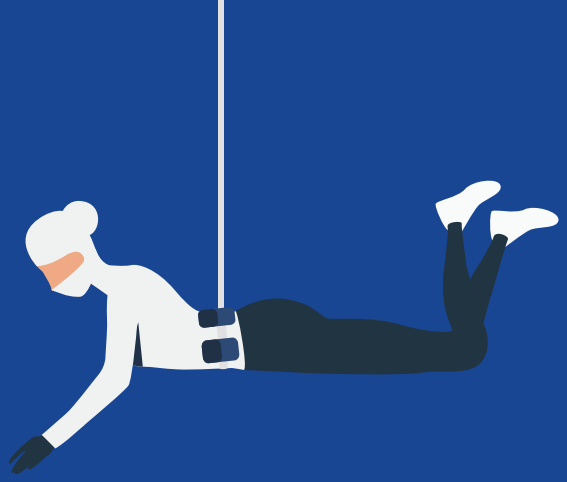
Participants will delve into real-world scenarios, simulating security incidents to practice their incident response skills in a controlled environment. They will also explore post-incident reporting and analysis, enabling them to improve future incident response strategies and strengthen overall cybersecurity posture.

By the end of the CSOC course, participants will be certified security professionals capable of operating and managing security operations centers, detecting and responding to security incidents proactively, and mitigating cyber threats efficiently.

COURSE SKILL SET

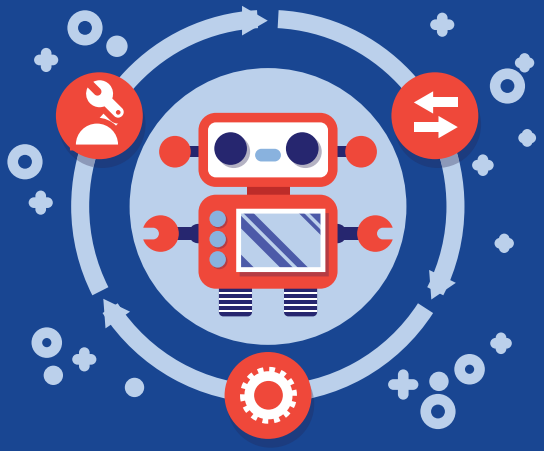
- Understand the basics of cybersecurity, the CIA Triad (Confidentiality, Integrity, Availability), and the hacking methodology.
- Learn about common cyber threats like Brute Force Attacks, Phishing, DoS, DDoS, and Man-in-the-Middle Attacks.
- Master the concepts of vulnerability, penetration testing, and cyber security controls.
- Familiarize yourself with Windows NT architecture, file systems, permissions, memory management, and processes.
- Gain proficiency in Linux command-line usage, managing users and groups, and working with Linux file systems.
- Understand the role of SOC, incident management, and incident response planning.
- Learn about SIEM architecture and its features, log analysis, and email analysis for SOC.
- Get acquainted with popular frameworks like NIST, COBIT, and PCI-DSS, and learn how to implement them.
- Acquire skills in analyzing and understanding different types of malware through static and dynamic analysis.
- Learn about VPN protocols, weaknesses, and how to set up and choose the right VPN provider.
- Understand various types of firewalls, including host-based and network-based firewalls on both Windows and Linux systems.
- Learn to set up a testing environment using virtual machines, such as VMware and VirtualBox.
- Understand email clients, protocols, and authentication, as well as email tracking, PGP, and GPG for encryption.
- Gain expertise in managing security incidents, incident response planning, and root cause analysis.
- Learn about cyber security policies, procedures, and standards that are essential for effective security practices.
- Familiarize yourself with social engineering tactics used by hackers and ways to protect against them.
- Learn about Linux tools used for penetration testing and how to secure Linux systems.
- Develop skills to raise security awareness among users and conduct security training programs.
- Gain knowledge about securing networks, detecting intrusions, and implementing network security measures.
- Acquire programming skills in Python, as it is widely used in cybersecurity for automation and analysis.

Instructor- Ajay Gautam | Cyber Security Expert
Instructor- Aman Roy | Cyber Security Expert
Duration- 2 Months
Eligibility- Any graduate with a Science stream
No. of Modules – 15 Modules
Language - English
Shareable certificate- Yes



PROGRAM SYLLABUS

Module 1 Introduction to Cybersecurity
Session 1.1 Introduction
Session 1.2 Why Cyber Security is Important?
Session 1.3 Role of cyber security enginner
Session 1.4 CIA Triad
Session 1.5 The Hacking Methodology
Session 1.6 The WhoIS Query
Session 1.7 Social Engineering
Session 1.8 Brute Force Attacks
Session 1.9 Phishing
Session 1.10 Bots and Botnets
Session 1.11 DoS and DDoS
Session 1.12 Pings
Session 1.13 Man in the Middle Attacks (MITM)



Module 2 Cyber Security Building blocks
Session 2.1 Malicious Codes and Terminologies
Session 2.2 Cybersecurity Breaches
Session 2.3 Penetration Testing and Methodologies
Session 2.4 Frameworks and Standards for Cybersecurity

Module 3 Basic concepts of Vulnerability
Session 3.1 Types of Hackers & Hacktivism
Session 3.2 Understanding Terminologies
Session 3.3 Vulnerability & Pentesting
Session 3.4 Cyber Security Controls
Session 3.5 Cyber Security Policies
Session 3.6 CVE & CVSS

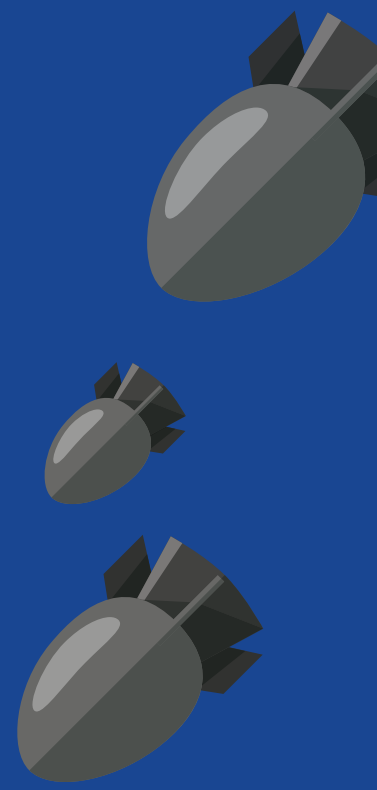
Module 4 Security Basics
Session 4.11 What is Cyber Kill Chain?
Session 4.12 Reconnaissance & Weaponization
Session 4.13 Delivery & Exploitation
Session 4.14 Installation, Command and control (C2) & Actions on Objectives

Module 5 Fundamentals of Windows Operating systems
Session 5.1 Windows NT Architecture
Session 5.2 File System in Windows
Session 5.3 File Permission in windows
Session 5.4 Managing Memory
Session 5.5 Password Hashing & SAM
Session 5.6 Windows Processes
Session 5.7 Windows Registry
Session 5.8 Introduction to PowerShell
Session 5.9 Installing windows Operating system in Virtual Box

Module 6 Linux Basics
Session 6.1 Overview of Operating System
Session 6.2 Working with Linux
Session 6.3 Linux Command Line Structure
Session 6.4 Sample Command Application
Session 6.5 Linux Directory Structure
Session 6.6 Flavours of Linux OS
Session 6.7 Linux File System & Directories
Session 6.8 Introduction to Kali Linux
Session 6.9 Installing Kali Linux in Virtual Box
Session 6.10 Managing Users & Groups
Session 6.11 Managing SSH in Kali Linux
Session 6.12 Hypervisors - Virtual Box, VM ware
Session 6.13 Tools Covered -- Python, Linux

Module 7 Blue Teaming & Cyber SOC
Session 7.1 Introduction to SOC
Session 7.2 Next Generation SOC
Session 7.3 Traditional SOC vs Next Generation SOC
Session 7.4 How to Build a SOC
Session 7.5 Working of SOC
Session 7.6 Introduction to SIEM Tools

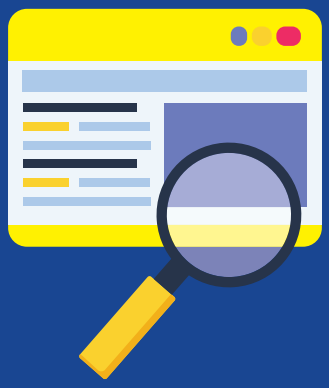
Session 7.7 Incident Management Process
Session 7.8 Lifecycle of an Incident
Session 7.9 Incident Response Team & Benefits
Session 7.10 Incident Response Plan
Session 7.11 How does Log Management help?
Session 7.12 Prevention, Detection & Investigation through Logs
Session 7.13 System Logs
Session 7.14 WAZUH Installation part 1
WAZUH Installation part 2
Session 7.15 WAZUH Configuration
Session 7.16 DNIF Installation
Session 7.17 DNIF Configuration
Session 7.18 Log Analysis - Sources & Event Collection
Session 7.19 Introduction To SIEM
Session 7.20 SIEM Architecture & Features Part 1
SIEM Architecture & Features Part 2
Session 7.21 Lab: Implementing SIEM - ELK
Session 7.22 Incident Response Process Part 1
Incident Response Process Part 2
Session 7.23 Email Analysis For SOC
Session 7.24 Lab: Analysing a Phishing Email
Session 7.25 Packet Analysis Using Wireshark



Module 8 Cyber Security Frameworks
Session 8.1 Introduction to NIST Framework
Session 8.2 Using NIST Framework
Session 8.3 Real World Case Studies
Session 8.4 Introduction to Cobit Framework
Session 8.5 Principles
Session 8.6 Cobit - Governance and Managing Objectives
Session 8.7 Business cases
Session 8.8 ISO Standard
Session 8.9 Implementation Over IT
Session 8.10 Fundamentals of PCI-DSS
Session 8.11 PCI DSS History
Session 8.12 Anatomy of Payment Flow
Session 8.13 Payment Attacks - Indian Perspective

Module 9 Malware Analysis
Session 9.5 Introduction Ransomware Part 1

Introduction Ransomware Part 2
Introduction Ransomware Part 3
Session 9.6 Building Ransomware
Session 9.7 Executing a ransomware
Session 9.8 Analysing the results
Session 9.9 Introduction to Malware Analysis
Session 9.10 Static Analysis
Session 9.11 Practical Static Analysis
Session 9.12 Malware Dynamic Analysis
Session 9.13 Lab: Malware analysis - Sample1
Session 9.14 Lab: Malware Analysis - Sample2 Part 1
Lab: Malware Analysis - Sample2 Part 2
Session 9.15 Introduction to File Less Malwares Part 1
Introduction to File Less Malwares Part 2
Session 9.16 Fileless Malware Analysis



Module 10 Virtual private network (VPN)
Session 10.1 Which VPN protocol is best to use and why?
Session 10.2 VPN Weaknesses
Session 10.3 Setting up an OpenVPN client on Linux
Session 10.4 Choosing the right VPN provider

Module 11 Firewalls
Session 11.1 Firewalls – Host-based, network-based and virtual
Session 11.2 Windows - Host Based Firewalls - Windows Firewall
Session 11.3 Linux - Host Based Firewalls - iptables
Session 11.4 Linux - Host Based Firewalls - UFW, gufw & nftables
Session 11.5 Use iptables to Build Source NAT
Session 11.6 Use iptables to Build Destination NAT
Session 11.7 Using iptables' Match and Target Extensions

Module 12 Testing environment using virtual machines
Session 12.1 Introduction to Setting up a Testing Environment
Using Virtual Machines
Session 12.2 Vmware
Session 12.3 Creating virtual machines - [VirtualBox options]
Session 12.4 Ubuntu Linux - [Virtual system installation]
Session 12.5 Cloning virtual machines
Session 12.6 Basic configuration of a virtual satellite and its
system - [VMs Snapshots]

Session 12.7 Virtual satellite network -
[Ubuntu Linux network configuration]
Session 12.8 Basic firewall network configuration -
[preparation for NAT]
Session 12.9 IP FORWARD and NAT - [iptables: MASQUERADE, POSTROUTING, save rules & restore]
Session 12.10 Telnet server setup - [2 rules from Troski behind us, Putty, Windows client]
Session 12.11 Kali Linux 2022

Module 13 Email: security, Privacy and Anonymity

Session 13.1 Introduction
Session 13.2 Clients, Protocols and Authentication
Session 13.3 Email Weaknesses
Session 13.4 PGP, GPG & Privacy
Session 13.5 PGP & GPG Clients
Session 13.6 Windows - PGP & GPG
Session 13.7 Tail - PGP & GPG
Session 13.8 PGP & GPG Weaknesses
Session 13.9 Improving OpenPGP Security -
Best Practices - Part 1
Session 13.10 Improving OpenPGP Security - Primary and Subkeys - Part 2
Session 13.11 Improving OpenPGP Security - Smartcards/ Yubikey - Part 3
Session 13.12 Email Tracking & Exploits
Session 13.13 Email Anonymity & Pseudonymity
Session 13.14 TorBirdy
Session 13.15 Remailers
Session 13.16 Choosing an Email Provider
Session 13.17 Email Alternatives (Guerrilla Mail)
Session 13.18 Email Spoofing

Module 14 Security Incident Management

Session 14.1 Security Incident Management
Session 14.2 Incident Response Plan
Session 14.3 Incident Management Concepts and Practices
Session 14.4 Integration with DR and BCP
Session 14.5 Recovery Terms
Session 14.6 Incident Classification Methods

Session 14.7 Damage Containment
Session 14.8 Re-plan
Session 14.9 Roles and Responsibilities
Session 14.10 Incident Response Tools and Equipments
Session 14.11 Reliability of Evidence
Session 14.12 Validation of Evidence
Session 14.13 Incident Response Reporting and Procedures
Session 14.14 Root Cause Analysis
Session 14.15 Business Impact Analysis
Session 14.16 Detecting and Analyzing Security Events
Session 14.17 Incident Management System

Module 15 Job roles
Session 15.3 Engineer Trainee
Session 15.5 Security Analyst
Session 15.7 Analyst Security Operations Centre