skillcubator
learn and lead

IIBA® Endorsed Education Provider™

SOC (Security Operations Center) Analyst

Context

In today’s world, we all are surrounded by Information Technology (IT), whether it’s a conventional computer (desktop, laptops), or be it smartphones, tablets, cars, microwave etc., through which we access numerous software program/apps to perform our day-to-day tasks, whether for official purpose or personal work. These devices contain so much valuable information in the form of code, which is an organization’s proprietary artifact as well as highly confidential data, in the form of payment information, health records, tax records, email correspondence, trading data, photos, electronic files, which are stored and accessed via network. Furthermore, in the last decade, with applications and databases moving into the cloud, it has made digital assets more easily accessible but at the same time made them more vulnerable for theft and misuse.

In the recent years, there has been surge in malicious incidents, where in attempts were made to attack and hack into systems to steal code/data, injecting spyware, malware, ransomware into systems with a sole objective to corrupt systems, take control over them, or misuse confidential data. So, how do organizations safeguard their digital assets? Yes, you guessed that right. It’s through very strong cyber security policies, governance, framework, processes, and tools. Cybersecurity is the practice of securing applications, software, networks and data from modern-day digital threats and make them safe and secure from any unauthorized access.

Organizations have realized this imminent threat we are all facing and hence have stepped up the efforts to secure their software, hardware, data and networks and have started investing massively in cyber security domain. There is huge opportunity for individuals to upskill, reskill themselves in the field of cyber security and help organizations protect their digital assets from nefarious elements.

Is This **Program** Right for You?

SOC Analyst program is specifically designed for anyone without any prior experience in the cybersecurity field. In addition to SOC Analyst role, one can also apply for the following job roles, following the same training and placement program:

- Cybersecurity Analyst / Information Security Analyst
- Threat Intelligence Analyst
- Incident Responder / Incident Handler
- Security Operations Center (SOC) Technician
- Junior Forensics Analyst
- EDR Analyst / Endpoint Security Analyst
- Vulnerability Analyst / Vulnerability Management Specialist
- Security Analyst (Healthcare Sector - HIPAA)

Pre-**Requisites:**

- Basic familiarity with computers
- Working knowledge of MS Office suite (MS Word, Excel and PowerPoint)

Course Outline

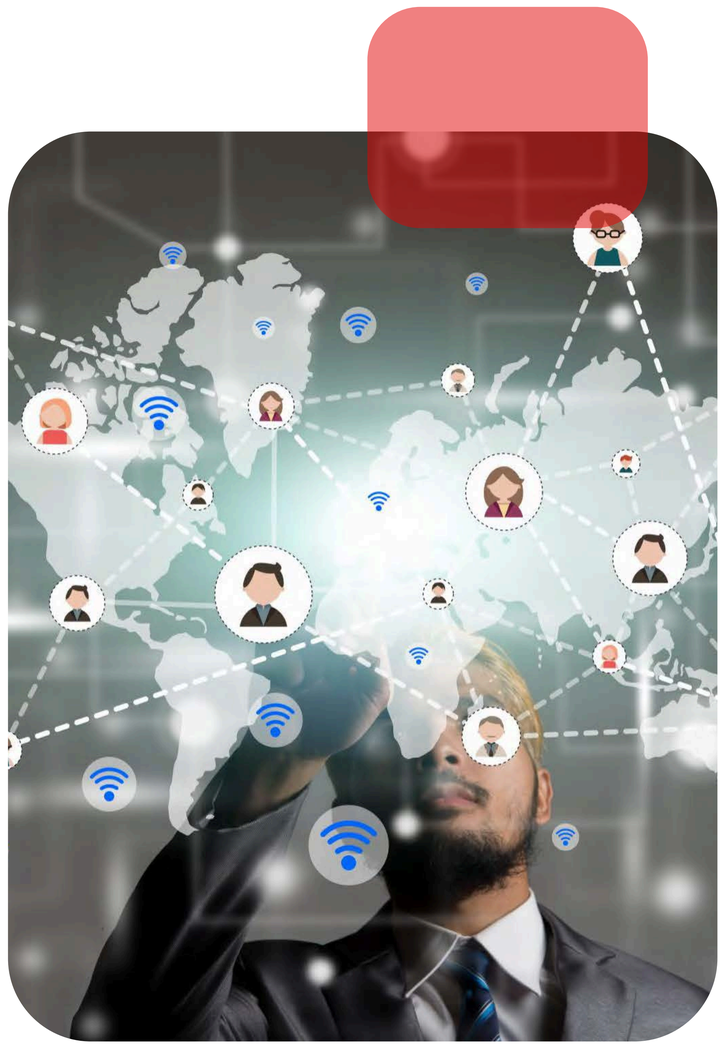
Module 01

Introduction to SOC and Cybersecurity Foundations (10 hours)

- **Overview of SOC:** Functions and operations of a Security Operations Center.
- **Roles of SOC Analysts:** Understanding L1, L2, and L3 responsibilities.
- **SOC Tools and Ticketing Systems:** Daily workflows and reporting.
- **Cybersecurity Fundamentals:** Core concepts like CIA Triad, threat actors, and vulnerabilities.

Module 02

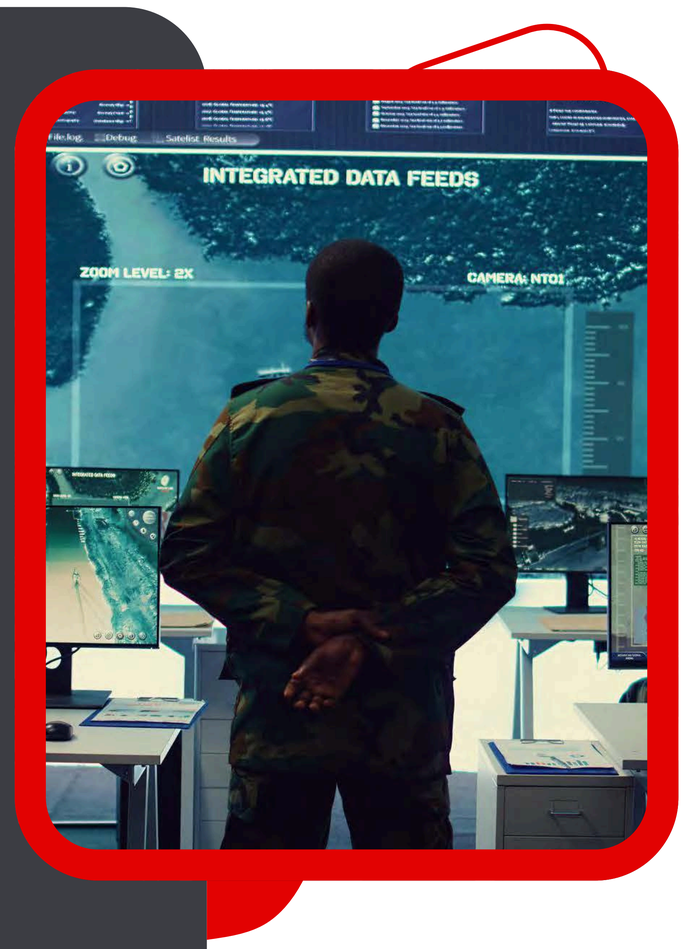
Networking Essentials for SOC Analysts (10 hours)



- **Networking Concepts:** IP addressing, TCP/IP, DNS, HTTP/HTTPS.
- **Common Network Protocols:** FTP, SSH, SSL, SNMP, etc.
- **Network Devices:** Firewalls, routers, IDS/IPS, switches.
- **Network Traffic Analysis:** Using Wireshark to capture and analyze traffic.

Module 03

Threat Intelligence and MITRE ATT&CK Framework (12 hours)



- **Threat Intelligence:** Importance in SOC operations and threat hunting.
- **MITRE ATT&CK Framework:** Understanding attacker tactics, techniques, and procedures (TTPs).
- **Practical Applications:** Utilizing the MITRE ATT&CK Framework for detection and incident response.

Module 04

Wazuh and Open-Source Threat Intel Tools (12 hours)

- **Wazuh SIEM:** Installing and configuring Wazuh for log collection and correlation.
- **Log Analysis and Alerts:** Using Wazuh to detect threats and generate alerts.
- **Open-Source Tools:** Using OSINT tools like Shodan and VirusTotal.

Module 05

Malware and Malware Analysis (15 hours)

- **Introduction to Malware:** Types (viruses, worms, trojans, ransomware, etc.).
- **Malware Analysis Techniques:** Static and dynamic analysis methods.
- **Sandboxing and Reverse Engineering:** Using tools like Cuckoo Sandbox for dynamic analysis.

Module 06

Endpoint Detection and Response (EDR) (12 hours)

- **Introduction to EDR:** Role of EDR in SOC operations.
- **Popular EDR Tools:** CrowdStrike, Carbon Black, Microsoft Defender.
- **EDR and Incident Response:** Detecting, containing, and remediating endpoint-based attacks.

Module 07

Firewalls and Security Controls (10 hours)

- **Firewall Concepts:** Types (stateful, stateless, NGFW) and configurations.
- **Firewall Logs:** Analyzing logs for signs of attacks or breaches.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** Role in detecting threats.

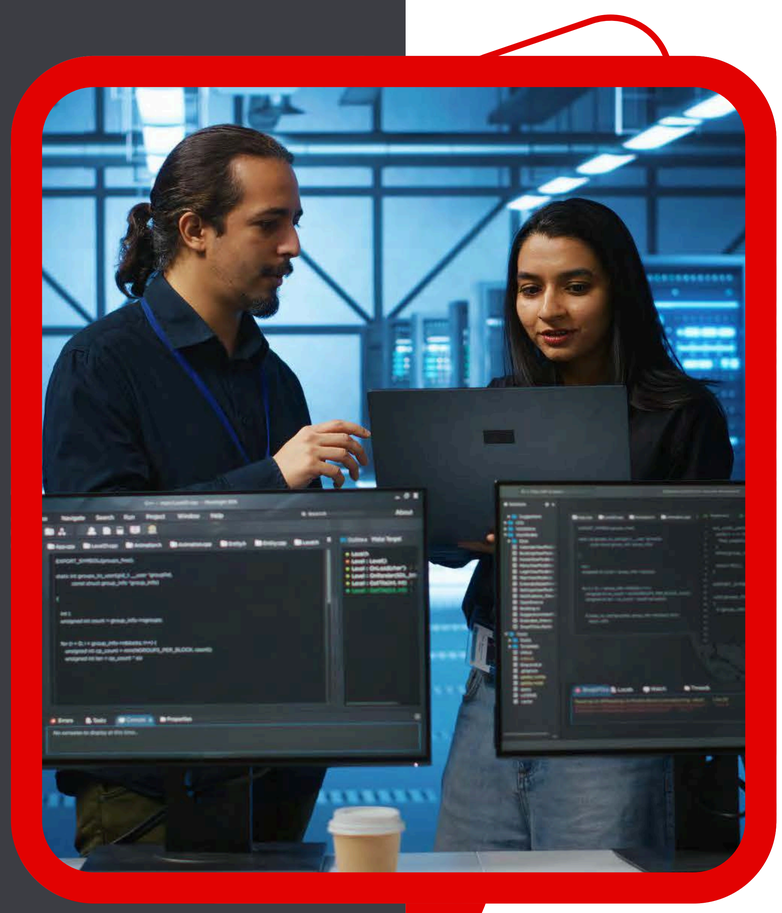
Module 08

SIEM Fundamentals and Splunk Basics (15 hours)

- **Introduction to SIEM:** Importance in centralized monitoring and alerting.
- **Splunk Basics:** Data ingestion, search, creating alerts, and dashboards.
- **Log Sources:** Understanding firewall, server, and endpoint logs.

Module 09

Cyber Forensics (12 hours)



- **Digital Forensics:** Importance in SOC.
- **Memory and Disk Forensics:** Using tools like FTK Imager, Autopsy, and Volatility.
- **File System and Network Forensics:** Investigating compromised machines.

Module 10

HIPAA and Compliance (8 hours)

- **HIPAA Overview:** Importance in healthcare environments.
- **Security and Privacy Rules:** Ensuring compliance in SOC operations.
- **HIPAA Risk Assessments:** Identifying vulnerabilities in healthcare settings.

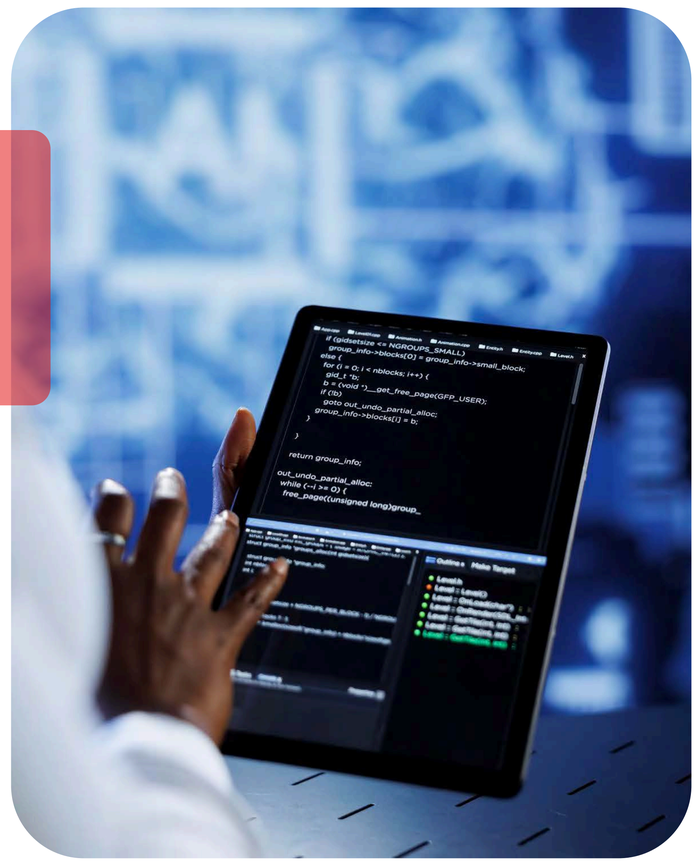
Module 11

Data Loss Prevention (DLP) (10 hours)

- **DLP Fundamentals:** Protecting sensitive information from leaving the organization.
- **DLP Tools:** Configuring policies and monitoring data flows.
- **DLP Incident Response:** Managing alerts and incidents involving data exfiltration.

Module 12

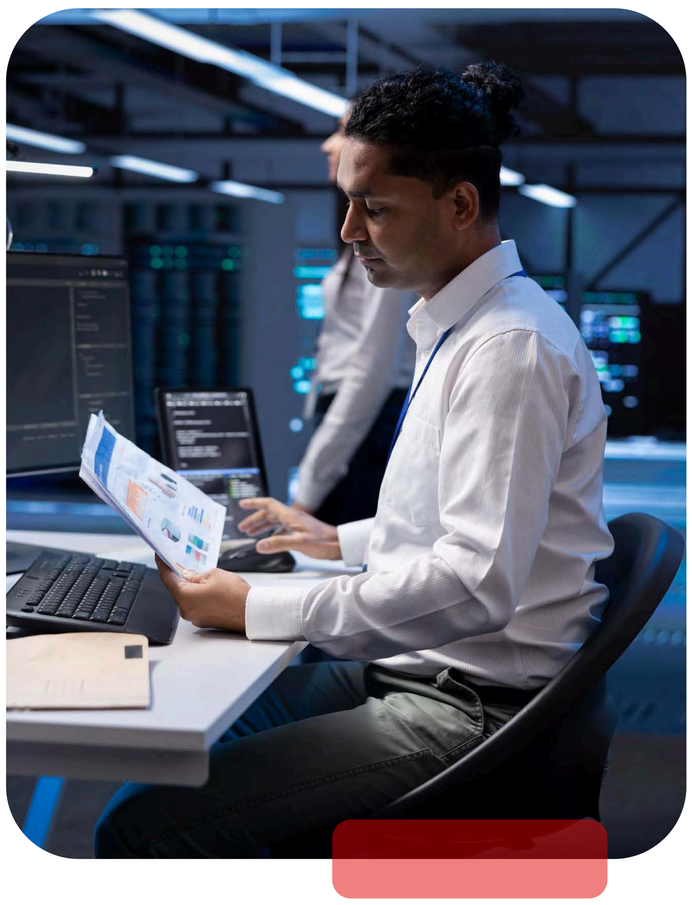
Incident Response and Handling (12 hours)



- **Incident Detection and Playbooks:** Methods for detecting phishing, malware, and ransomware attacks.
- **Containment and Eradication:** Isolating affected systems and removing threats.
- **Post-Incident Reporting:** Documenting and improving processes.

Module 13

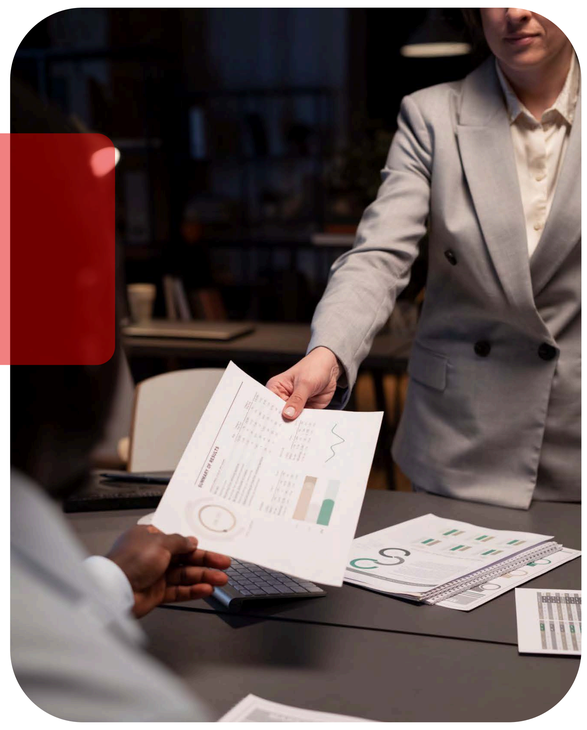
Security Operations Tools and Hands-On Practice (10 hours)



- **Vulnerability Scanning:** Using Nessus or OpenVAS for detecting vulnerabilities.
- **Intrusion Detection Tools:** Configuring Snort or Suricata for monitoring network traffic.

Module 14

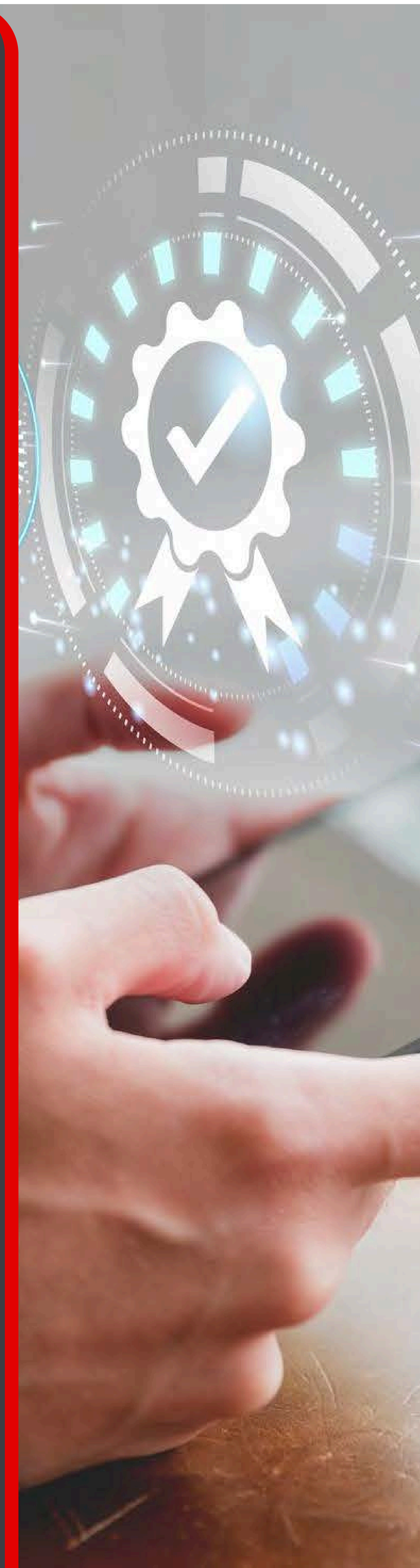
Final Project and Case Studies (9 hours)



- **Case Studies:** Real-world incidents and responses.
- **Final Project:** End-to-end SOC simulation with malware detection, incident response, and threat hunting.

Features

- Training Program as per Latest Industry Demand
- Learn from IIBA Endorsed Education Provider
- Access to Learning Management System (LMS)
- Free PSM-I and PSPO-I Training Included in the Package
- Certified Instructors with 20 plus years of experience
- Plenty of Case Studies, In-class Exercises, Quizzes, and Take-home Assignments
- Usage of Industry-Standard tools
- Personalized Resume, LinkedIn Profile makeover, and Cover Letter
- Interview Prep Guide (With real-world scenarios and questions/answers from live interviews)
- Comprehensive lab work
- Experiential Learning through Case Studies



Software/Tools

Used for this training

- Wazuh (SIEM)
- Splunk (Log Management and SIEM)
- Wireshark (Network Traffic Analysis)
- TryHackMe and LetsDefend (Gamified Cybersecurity Platforms)
- Cuckoo Sandbox (Malware Analysis)
- Shodan and VirusTotal (Threat Intelligence)
- Nessus or OpenVAS (Vulnerability Scanning)
- Snort or Suricata (Intrusion Detection Tools)
- FTK Imager, Autopsy, Volatility (Forensics Tools)
- Microsoft Office (Word, Excel, PowerPoint)
- Microsoft Visio, Gliffy, Lucidchart
- Jira
- Confluence

Available formats for this course

01

Live Online Instructor-Led Training

03

Private Group Training

Self-Paced training

02

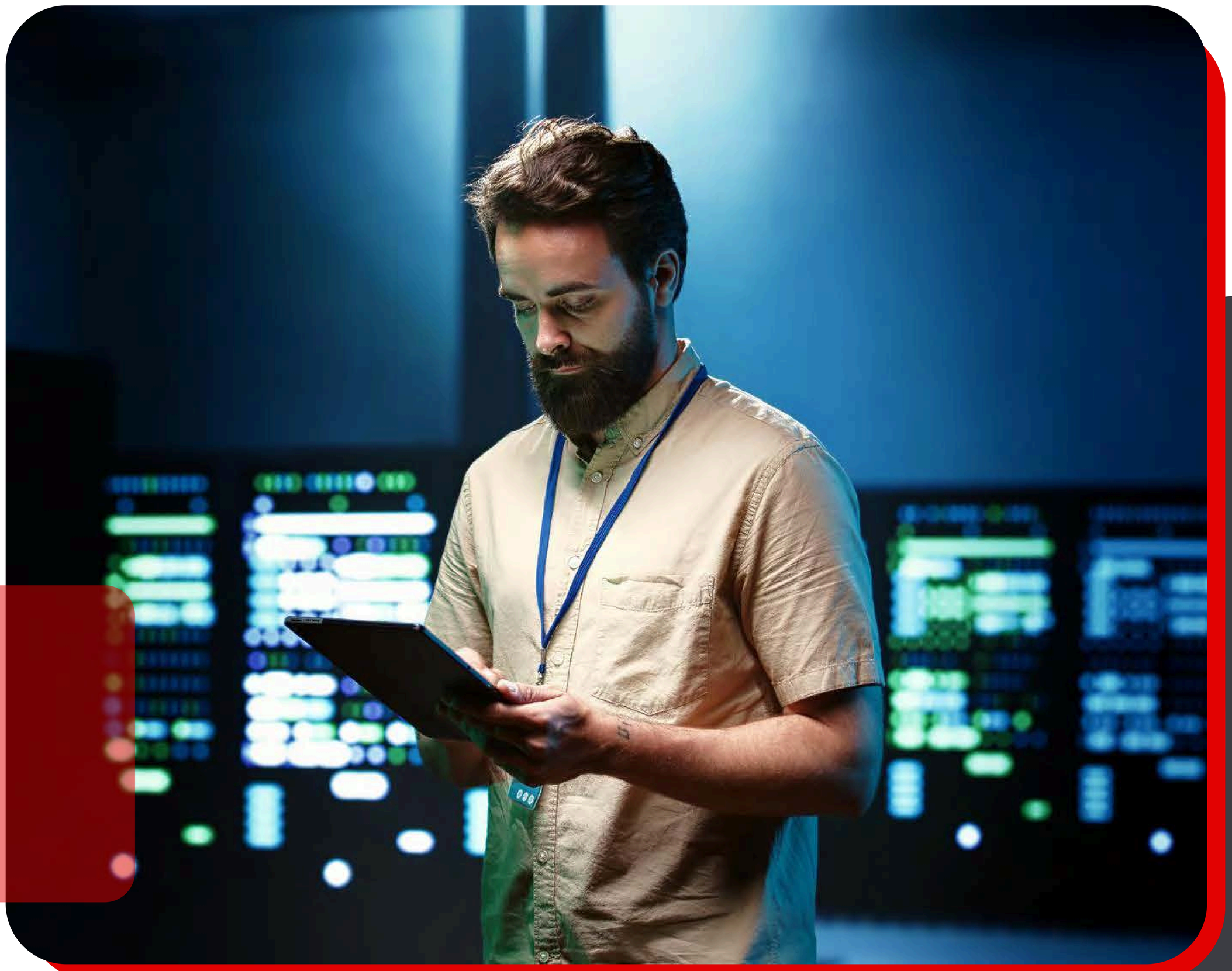
Duration

- **12 weeks. x** (Monday, Tuesday, Wednesday and Thursday from 00:00 PM EST to 00:00 PM EST).

- **Core Training Hours:** 160 hours.

Fees

1500 USD / 2100 CAD + Tax



Frequently Asked Questions (FAQs)

What is the role of SOC Analyst and what do they do?

An SOC Analyst's role is to monitor, detect, and respond to security threats within an organization. They are part of Security Operations Center (SOC) and use specialized tools and techniques to identify, analyze, and respond to suspicious activities to protect applications from cyber threats.

How is SOC Analyst different from an Incident Responder?

SOC Analyst focuses primarily on monitoring and the initial analysis of security alerts. Incident Responders take on more specialized tasks, investigating incidents thoroughly, containing threats, and minimizing damages. Incident Response roles often require deeper expertise in handling security events.

What will I learn in this training program?

You'll gain key skills in cybersecurity, including threat detection, incident response, malware analysis, and practical experience with SOC tools like SIEM platforms (e.g., Splunk, Wazuh), EDR tools, and network analyzers like Wireshark. The course also includes hands-on labs and real-world case studies for job-ready experience.

Do I need any prior knowledge or experience to join this course?

Basic IT skills and an understanding of networking concepts (like IP addresses, DNS, and TCP/IP) are useful but not required. The program starts with the fundamentals and progresses advanced skills, so it's accessible even for beginners. This program can be done by anyone. But your commitment is required for us to get you a job.

How long will the training program take to complete?

The entire training program will take between 120-150 hours, covering all topics in depth. Total hours may vary depending on the cohort's ability to grasp all the topics and complete all the required lab work.

Will there be any tools/software used as part of the training?

Yes! The course includes hands-on labs using the following list of software:

- Wazuh (SIEM)
- Splunk (Log Management and SIEM)
- Wireshark (Network Traffic Analysis)
- TryHackMe and LetsDefend (Gamified Cybersecurity Platforms)
- Cuckoo Sandbox (Malware Analysis)
- Shodan and VirusTotal (Threat Intelligence)
- Nessus or OpenVAS (Vulnerability Scanning)
- Snort or Suricata (Intrusion Detection Tools)
- FTK Imager, Autopsy, Volatility (Forensics Tools)
- Microsoft Office (Word, Excel, PowerPoint)
- Microsoft Visio, Gliffy, Lucidchart
- Jira

Will I receive a certificate after finishing the program?

Absolutely yes. You will receive a Certificate of Completion from Skillcubator (USA), an IIBA Premium-Level Endorsed Education Provider (EEP). Additionally, this training will also prepare you for industry-recognized certifications such as CompTIA Security+, Certified SOC Analyst (CSA), and Certified Incident Handler (GCIH).

What kind of job opportunities are available after this training?

SOC Analysts and Incident Responders are in high demand across industries such as finance, healthcare, government, and tech. This training qualifies you for SOC Analyst and Incident Response roles and helps you advance to more senior positions as you gain experience.

Is this program suitable for those new to cybersecurity?

Yes! This program is designed for both beginners and those with some IT experience, starting with cybersecurity and networking basics.

Does the program offer support for job placement after completion?

Of course. This is a job-based training, which means the sole objective of this program is to upskill/reskill an individual in the field of cybersecurity and help them transition as Cybersecurity professional. This program includes (a) Training (b) Resume Building, LinkedIn Profile makeover, Cover Letters (c) Interview Preparation (d) Job Placement and (e) Post-Placement support.

How does this course differ from general cybersecurity programs?

This course is uniquely focused on SOC and Incident Response roles, combining foundational knowledge with practical, hands-on labs, real-world case studies, and interactive learning. It emphasizes skills and tools specifically for SOC environments.

What kind of salary can I expect with an SOC Analyst role?

An SOC Analysts typically earn between 80,000 USD and 100,000 USD GPA (Gross Per Annum), depending on location, industry, and experience. Incident Responders often draw higher salaries as they gain expertise.

Is there any programming/coding involved in this training?

No. There is no programming/coding involved in this training program.

Are there remote jobs in Cybersecurity domain?

Yes. There are plenty of jobs in cybersecurity domain, which are 100% remote or partially remote.

How will you help me find a suitable job after the training is completed?

We have an in-house team of IT Recruiters, who will market your resume across our clients. Additionally, we also have agreement with top-tier IT staffing firms in USA and Canada, which help you get umpteen job opportunities.

What is an average time to get a job?

Statistically speaking 2-3 months (after the training is finished) is a normal timeframe to get a job.