SOC Tier 1 Training Programme

Offered by See Security See Secure Consulting

A unique training programme aimed for IT professionals who wish to embark on the exciting profession of SOC analyst.

Including preparation for the CCNA-Cyber Ops, CompTIA-CySA+ and the EC Council-ECIH certifications.

SeeSecure

The domains covered in this comprehensive training programme relates to the core skills and knowledge you need to know to working and operating a SOC & IR centers.

The graduates of this training shall understand the theoretical and practical components associated with their roles as SOC analysts. Therefore, the course is rich in hands-on practices which closely accompanied the theoretical topics addressed in this training.

Students can also attempt the CCNA-Cyber Ops and / or the CompTIA-CySA+ and / or the EC Council-ECIH certifications.

SOC Tier 1 Training Programme

A unique training programme aimed for IT professionals who wish to embark on the exciting profession of SOC analyst.

About See Security College

See Security College is a highly specialized and international cybersecurity college. One of seven colleges of its kind, our college offers training programs aimed for absolute beginners to more advanced professionals. The college delivers its study programs worldwide, through the See Security International brand as well as well-known governmental and special cybersecurity agencies.

See-Security's CEO, Mr. Avi Weissman is one of the leaders of the Israeli cyber industry and serves as an advisor and commentator to the Israeli government for the regulation of cyber professions. Further, Mr. Weissman was the co-founder of the Israeli Forum for Information Security (IFIS) together with Maj. Gen. (Res.) and former head of the National Security Council, Yaakov Amidror. In addition to his role in leading the college, Avi is also a co-CEO of a cyber human resources company, See-HR and a cybersecurity consulting company, See Events – Managed SIEM/SOC.

About See Secure Consulting

See-Secure is an information security consultancy company specializing in Managed SIEM- SOC, Cyber security architecture, IT regulatory compliance and standards, secure designing of information systems, IT risk management, Business Continuity Management and Disaster Recovery Planning.

Our Consulting Division of our company provides solutions for information security requirements, including the information security regulations on varied sectors Financial, Health Care, Critical Infrastructure, Insurance and more.

Our consulting division is known internationally for its security experts, jurisdiction and international capabilities. Business knowledge accumulated in the Consulting Division provides our clients with the professional solutions at the highest quality, while applying the experience accumulated worldwide.

Key Features	
Cost	9,900 NIS (tax included)
Aaudience	Advanced
Orientation	Technical, theoretical, and applicative knowledge
Objectives	To train IT professionals who wish to embark on the exciting profession of SOC analyst.
Entry requirements	Practical knowledge in OS and networking
Certifications	CCNA-Cyber Ops, CompTIA-CySA+ and EC Council ECIH
Academic hours	100
Homework	Total of 200 homework assignments
Course format	Class lectures and online synchronized lessons

About the SOC Programme

The domains covered in this comprehensive training programme relates to the core skills and knowledge you need for working and operating SOC & IR centers.

The graduates of this training shall understand the theoretical and practical components associated with their roles as SOC analysts. Therefore, the course is rich in hands-on practices which closely accompanied the theoretical topics addressed in this training.

A *SOC analyst* is a cybersecurity professional who works as part of a team to monitor and fight threats to an organization's IT infrastructure, and to assess security systems and measures for weaknesses and possible improvements. The *SOC* in the job title stands for *security operations center;* this is the name for the team, which consists of multiple analysts and other security pros, and often works together in a single physical location. A SOC may be an internal team serving a single enterprise or an outsourced service providing security for one or more external clients.

SOC analyst is a job title held by infosec newbies and more experienced pros alike. The job can be a great steppingstone into a cybersecurity career.

There are three main Tiers (or level of expertise) in this progression:

- **Tier 1 SOC analysts** are *triage specialists* who monitor, manage, and configure security tools, review incidents to assess their urgency, and escalate incidents if necessary.
- **Tier 2 SOC analysts** are *incident responders,* remediating serious attacks escalated from Tier 1, assessing the scope of the attack and affected systems, and collecting data for further analysis.
- **Tier 3 SOC analysts** are threat hunters, working proactively to seek out weaknesses and stealthy attackers, conducting penetration tests, and reviewing vulnerability assessments. Some Tier 3 analysts focus more on doing deep dives into datasets to understand what is happening during and after attacks. [adapted from: Josh Fruhlinger, SOC analyst job description, salary, and certification]

Other graduates may proceed to advanced studies in Forensics or Malware Analysis.

Target Audience

The programme is aimed for students with a background in IT who wish to develop a career in SOC and Incident Response. A familiarity with OP and Networking is essential.

Entry Requirements

You will not be tested on these requirements for enrolment. However, we emphasize that without background knowledge it will be difficult to keep up with materials covered throughout the course and even more challenging to pass the exams and assignments. The following are expected:

1. Prior knowledge in IT: OS and Networking
2. Passing an admission interview
3. Good command of the English language

Pedagogical Requirements

1. Attendance in 85% of the sessions
2. Passing grade (70 and above) in each of the exams and assignments
3. In technical modules – ”hands-on” practice labs in class and at home.

Academic Faculty

Our lecturers live and breathe cyber with a deep knowledge of the world of IT systems and networking and have extensive experience in

establishing SOC and IR centres in Israel and abroad.

Certifications

See-Security certificate will be awarded to students who fulfil the pedagogical requirement.

Certified SOC Analyst

Students can also attempt the CCNA-Cyber Ops and / or the CompTIA-CySA+
and / or the EC Council- ECIH certifications.

Remarks

a) Registration for external examinations is the responsibility of the student
b) The programme will open only if there are enough enrolled students
c) The registration fee is not refundable.

Outline of the Programme

Main Topics
Module 0: Course Introduction
Module 1: Information Security Basics
Module 2: Security Operations
Module 3: Monitoring & Analysis
Module 4: Threat & Vulnerability
Module 5: Monitoring & Intrusion
Module 6: Incident Response
Module 7: Windows Security Monitoring
Module 8: SIEM system

CISCO CERTIFIED CCNA CYBER OPS

CompTIA CySA+

E|CIH EC-Council Certifie Incident Handler

Curriculum

Module 0: Course Introduction

Welcome to SOC Analyst Course

- Message to the Student
- Welcome
- Today's Cybersecurity Analyst

Module 1: Information Security Basics

Information Security Terminology

- Information Security
- CIA
- Defense in depth
- Information Security Solutions

Module 2: Security Operations

SOC Operation

- Legacy vs Modern Security Operations
- Three Pillars
- People
- SOC Structure
- Tiered SOC Model
- Tireless SOC Model
- Processes
- SOC Charter
- Onboarding
- Security information and event management (SIEM) review

Module 3: Monitoring & Analysis of Common Protocols

SIEM & Monitoring Basics

- Technology - SIEM
- McAfee SIEM Foundation
- Log Collection
- Main Data Sources
- Network
- Network Traffic by Layer
- Network Traffic Collection
- Endpoint Traffic
- SIEM Terms & Definitions
- Event Examples
- Example of Security Solutions Alerts
- Type of SIEM Alerts
- High Severity Alert Flow
- Technology - Incident Management System
- Threat Intelligence Platform
- SOAR
- Automation

Module 4: Threat & Vulnerability Management

Incident response process.

Utilization of threat intelligence to support organizational security

- Threat Intelligence and its importance
- Definitions
- Intelligence sources
- Confidence levels
- Indicator management
- Threat classification
- Collection
- Commodity malware
- Attack frameworks
- Threat research
- Threat modeling methodologies

Module 5: Monitoring & Intrusion Data Analysis

1. **Analyze data as part of security monitoring activities**
   - Heuristics
   - Trend analysis
   - Endpoint
   - Network
   - Log review
   - Impact analysis
   - E-mail analysis
2. **Hardening controls to improve security**
   - Permissions
   - Allow list (previously known as whitelisting)
   - Blocklist (previously known as blacklisting)
   - Firewall
   - Intrusion prevention system (IPS) rules
   - Data loss prevention (DLP)
   - Endpoint detection and response (EDR)
   - Network access control (NAC)
   - Sinkholing
   - Malware signatures - Development/rule writing
   - Sandboxing
   - Port security

3. **Proactive threat hunting**
   - § Establishing a hypothesis
   - § Profiling threat actors and activities
   - § Threat hunting tactics - Executable process analysis
   - § Reducing the attack surface area
   - § Bundling critical assets
   - § Attack vectors
   - § Integrated intelligence
   - § Improving detection capabilities

Module 6: Incident Response

1. **Incident response process**
   - § Response coordination with relevant entities
   - § Factors contributing to data criticality
2. **Incident response procedure**
   - § Preparation
   - § Detection and analysis
   - § Containment
   - § Eradication and recovery
   - § Post-incident activities
3. **Potential indicators of compromise**

Incident Response in action

- § Network-related
- § Host-related
- § Application-related
- § Real life Incident Response cases

Module 7: Windows Security Monitoring

Introduction to Windows Security Monitoring

- § Windows Auditing Subsystem
- § Security Monitoring Scenarios
- § Local User Accounts
- § Local Security Groups
- § Microsoft Active Directory
- § Active Directory Objects
- § Authentication Protocols
- § Operating System Events
- § Logon Rights and User Privileges
- § Windows Applications
- § Filesystem and Removable Storage
- § Windows Registry
- § Network File Shares and Named Pipes

Module 8: SIEM system

1. **Getting to know the SIEM (Sentinel, QRadar, Splunk)**
   - § Introduction to **Azure Sentinel** SIEM interface, dashboard, logs, devices
   - § Introduction to **QRadar** SIEM interface, dashboard, logs, devices
   - § Introduction to **WatchDog-Splunk** SIEM interface, dashboard, logs, devices
   - § Architecture Overview
   - § Devices and Settings
   - § Data Sources
   - § Event Analysis
   - § Aggregation
   - § Watch Lists and Policy Editor
   - § Query Filters
   - § Rule Correlation
   - § Alarms
2. **Gaining Hands on experience**
   - § Working on the SIEM - queries, detection, analysis
   - § Domain User activity, Anti-Virus, Perimeter Defense, firewall, Correlation Engine…
3. **Detecting & Analyzing Attack scenarios**
   - § SIEM scenarios and analysis