INFOSECTRAIN

SOC Analyst L1 Training Course

Course Highlights

- 40 hrs of Instructor-led Training
- Access the Recorded Sessions
- Session for Interview Prep
- Post Training Support

INFOSECTRAIN

Tools Covered

ITSM TOOLS

NMAP

splunk>

WIRESHARK

CyberChef

>_

MALTEGO

ALIEN VAULT

MISP

MITRE ATT&CK & NAVIGATOR

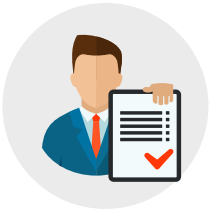
MANY MORE ...

INFOSECTRAIN

Why InfosecTrain?

40 hrs of Instructor-led Training

Hands-on Labs

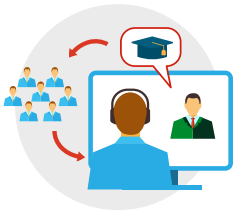


Scenario-based Learning

Session for Interview Prep

Career Guidance

Post Training Support



Telegram Discussion Group

Access to the Recorded Sessions

INFOSECTRAIN

Course Overview

SOC Analysts play a crucial position in today's security teams since they are on the front lines of cyber defense, identifying and responding to cyber threats as they occur.

The InfosecTrain's SOC Analyst training course is specifically created for aspiring and current SOC Analysts who want to learn how to prevent, identify, assess, and respond to cybersecurity threats and incidents. The course is the first level of a course series that includes Level 1-SOC Analyst and Level 2-SOC Specialist, and is specifically designed to assist you in mastering over trending and in-demand technical abilities to carry out numerous sophisticated SOC activities.

The course begins with the fundamentals of SOC teams and Blue Team operation architecture before moving on to more advanced topics such as digital forensics, incident response, threat intelligence, and SIEM (Security Incident and Event Management) solutions.

This training course also helps participants plan their preparation for the SOC Analyst certification examinations, which are required to obtain the most sought-after position in the SOC team.

INFOSECTRAIN

Target Audience

- Technical Support Engineers
- System Administrators
- Security Consultants
- Cyber Security Analysts
- Security System Engineers
- SOC Analysts (L1 & L2)
- Information Security Researcher
- Network Engineers
- Network Architects or Admin
- Entry-level Information Security role
- Anyone who wants to become SOC Analyst

Prerequisites

- Prior knowledge of networking fundamentals, OS basics, troubleshooting is recommended
- Experience as an entry-level SOC Analyst, Cyber Security Analyst, Information Security role
- Experience of two years in the Information Security domain

INFOSECTRAIN

Our Expert Instructors

BHARAT MUTHA

10+ Years Of Experience

SME - Blue Team Operations and Consultant

ABHISHEK SHARMA

5+ Years Of Experience

Information Security Consultant and Trainer

SANYAM NEGI

9+ Years Of Experience

CEH | CHFI | CTIA | CHFI | CND | CSA | Sec+ | Pentest+ | CySA+ | AWS Sec | AWS Architect

INFOSECTRAIN

Happy Learners Across the World

Tejas Rathod

InfosecTrain provided me with a fantastic environment in which to learn and complete SOC Analyst Training. It is extremely easy for me to grasp the concept quickly and have clarity about the topic because of the expert and experienced trainers

Jude Adio

I couldn't believe it would be an easy journey for a career change from nursing to certified SOC Analyst. I am proud to have completed this so easily with InfosecTrain.

Mahesh Gujar

It's a very good and informative session. It is great to have an instructor who keeps inspiring you throughout the course.

Iyyappan Vairavan

Trainer has extensive knowledge about the subject and has very good presentation skills. One of the good course to know more about the SOC. Really appreciate the trainer and the team.

INFOSECTRAIN

COURSE CONTENT

Domain 1 : Security Terminologies, OS Basics & Network Fundamentals

Domain 2: Blue Team Operations Architecture

Domain 3 : SIEM - Nervous System of SOC

Domain 4: Importance of Threat Intelligence

Domain 5: Basics of Incident Response & Forensics

INFOSECTRAIN

Domain 1 : Security Terminologies, OS Basics & Network Fundamentals

- Why do we need Security?
- CIA Triad
- Concept of AAA
- Hacking Concepts
- Types of Hackers
- Domains of Security
- Ethical Hacking Phases
- Types of Attacks
- Network Fundamentals
    - NOC vs SOC
    - The OSI Model
    - Network Devices
    - Network Tools – Firewall, IDS, IPS, VPN, Switches,
    - Routers
    - Ports and Services
    - Conducting a Port Scan with Nmap **[Practical]**

- Windows Operating System Fundamentals **[Practical]**
  - Investigating Windows Operating System
  - Windows Event Logs
  - Windows Registry
  - Scheduled Tasks
  - File Analysis
  - SysInternals Suite
  - Command Prompt
  - Sysmon (System Monitor)
- Linux Operating System Fundamentals **[Practical]**
  - Linux Directory Services
  - Most useful Linux Commands in SOC
  - Events Logs in Linux
  - Linux System Services

INFOSECTRAIN

Domain 2: Blue Team Operations Architecture

- Why do we need SOC?
- What is SOC?
- Functions of SOC
- SOC Models & Types
- SOC Teams & Roles
- Incidents vs Events
- True vs False Incident Categories
- Concept of Logging
    - Local Logging vs Centralized Logging
- Log Management & Log Analysis
    - Log Management needs
    - Concept of Log Analysis
    - Web Server Logs
    - Firewall Logs
    - SSH Logs
    - Windows Event Logs
    - Using Regex for Log Analysis **[Practical]**
- SOC Workflow: ITSM Workflow
- ITSM Tools: Service Now, JIRA, BMC, Request Tracker, etc.

INFOSECTRAIN

Domain 3 : SIEM – Nervous System of SOC

- Why do we need SIEM?
- What is SIEM?
  - Security Information Management (SIM)
  - Security Event Management (SEM)
- SIEM guidelines and architecture
- SIEM Capabilities: Aggregation, Correlation, Reporting, Storage, Alerts, etc.
- Using Splunk **[Practical]**
  - Section Introduction
  - Installing Splunk
  - UI Navigation
  - Search Queries using SPL
  - Creating Alerts & Dashboard

INFOSECTRAIN

Domain 4: Importance of Threat Intelligence

- What is Threat?
- Why do we need Intelligence?
- Introduction to Threat Intelligence
- Threats, Threat Actors, APTs & Global Campaigns
  - Network Level Threats
  - Web App Level Threats
  - Host Level Threats
- IOCs vs IOA vs Precursors
- Traffic Light Protocol (TLP)
- Pyramid of Pain **[Practical]**
- Collecting Threat Intelligence **[Practical]**
  - Paid vs Open-Source Intelligence Gathering
- Types of Threat Intelligence
  - Strategic Threat Intelligence
  - Operational Threat Intelligence
  - Tactical Threat Intelligence
  - Technical Threat Intelligence
- Enhanced Detection with Threat Intelligence
- Maltego, MISP, STIX, TAXII, etc. **[Practical]**

INFOSECTRAIN

Domain 5: Basics of Incident Response & Forensics

- Forensics Fundamentals
  - File Systems
  - Hard Disk Drive Basics
  - Forensics Process **[Practical]**
  - Digital Evidence and Handling
  - Order of Volatility
  - Chain of Custody
  - Hashing & Integrity

- Email Forensics
  - How Electronic Mail Works
  - Anatomy of an Email
  - What is Phishing?
  - Types of Phishing
    - Spear Phishing
    - Whaling
    - Impersonation
    - Typosquatting and Homographs
    - Sender Spoofing
    - URL Shortening
    - Business Email Compromise

- Analysing Phishing Emails **[Practical]**
  - Analysing Artifacts
  - Red Flags of Phishing Emails
  - URL Reputation
  - File Reputation
  - SPF
  - DKIM
  - DMARC
  - Manual & Automated Analysis

- Incident Response
  - Introduction to Incident Response
  - What is an Incident Response?
  - Why is IR Needed?
  - Incident Response Lifecycle – NIST SP 800 61r2
  - Incident Response Plan: Preparation, Detection & Analysis, Containment, Eradication, Recovery, Lessons Learned
  - Incident Response and Security Operations Integration
  - Case Study: Cyber Kill Chain in Incident Response

- Lockheed Martin Cyber Kill Chain
  - What is it, why is it used ?
  - Case Study: Monero Crypto-Mining

- MITRE ATT&CK Framework **[Practical]**
  - What is it, why is it used ?
  - Matrices in Mitre
  - Mapping Data with Mitre
  - Case Study 1: APT3
  - Case Study 2: OilRig

INFOSECTRAIN

SOC Analyst Course Benefits

Hiring Companies

TATA CONSULTANCY SERVICES

IBM

EY

wipro

accenture

HCL

Source: Glassdoor

www.infosectrain.com | sales@infosectrain.com