INFOSECTRAIN

SOC Specialist

Training Course

Course Highlights

- 40 hrs of Instructor-led Training
- Access to the Recorded Sessions
- Session for Interview Prep
- Certified & Experienced Trainers

www.infosectrain.com

Tools Covered

FTK
FORENSIC TOOLKIT

AUTOPSY
DIGITAL FORENSICS

VOLATILITY

MAGNET
FORENSICS

MITRE
ATT&CK
& NAVIGATOR

MANY MORE...

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

Course Overview

SOC Specialists are at the core of the organization’s security teams, detecting and responding to suspicious activities and cyber threats as they arise. The SOC Specialist training course at InfosecTrain is tailored for candidates who want to learn how to avoid, identify, assess, and respond to cybersecurity threats and incidents. The course is the second in a series that comprises Part 1-SOC Analyst and Part 2-SOC Specialist. It aims to help you master over trending and in-demand technical expertise to perform advanced SOC operations. This training course will assist participants in securing the digital assets of their organization.

Target Audience

- SOC Analysts (L1, L2 or L3)
- SOC Administrators
- Security Consultants
- Senior SOC Consultant
- Incident Responder L1, L2
- Cyber Security Analysts
- Information Security Researcher
- Intermediate-level Information Security role
- Anyone Who wants to become SOC Specialist or Expert

Prerequisites

- InfosecTrain SOC Analyst L1 Training
- Advanced Operating System Concepts & Troubleshooting is recommended
- In-depth Knowledge of Windows and Linux Operating System
- Deep Knowledge of Information Security
- Intermediate or Expert Knowledge for SOC Operations Centre
- Working on L1 / L2 Role
- Minimum 2 years of experience in SOC

Our Expert Instructors

ABHISHEK SHARMA

10+ Years Of Experience

Information Security Consultant and Trainer

SANYAM NEGI

10+ Years Of Experience

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

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 : SOC Operations and Architecture

Domain 2 : Incident Responder & Forensics Specialists

Domain 3 : Malware Analysis

Domain 4 : Threat Hunting

Domain 5 : SIEM - Nervous System of SOC

Domain 1 : SOC Operations and Architecture

- ✓ Advance SOC Operations
- ✓ Building a successful SOC
- ✓ SOC Services: Security Monitoring, Incident Response, Security
- ✓ Analysis, Threat Hunting, Vulnerability Management, Log
- ✓ Management, Malware Analysis, etc.
- ✓ SOC Maturity Models, SOC-CMM
- ✓ SIEM and Automation
- ✓ SOAR
- ✓ EDR vs XDR
- ✓ MDR & MSSP

Domain 2 : Incident Responder & Forensics Specialists

- Incident Response Process Overview
- Digital Forensics in Incident Response
- The 6 A's of Forensics Process
- Anti - Forensics Techniques
- Evidence Destruction
- Volatile vs Non-Volatile Data
- Live Acquisition - KAPE
- Network Forensics **[Practical]**
    - Network Traffic Analysis
        - Post-Mortem Analysis
        - Real-Time Analysis
    - Tools : Wireshark, Network Miner, TCPDump, etc.
    - Introduction to Wireshark
    - PCAP Analysis - 1
    - Malware Traffic Analysis - 1
    - Malware Traffic Analysis - 2
    - System Forensics
        - Disk Based Forensics **[Practical]**
            - Concept of Disk Imaging - FTK Imager
            - Disk Analysis with Autopsy

- ✓ Memory Based Forensics [Practical]
  - ✓ Memory Acquisition - Ram Dump
  - ✓ Introduction to Volatility
  - ✓ Memory Analysis with Volatility
  - ✓ Identifying Malicious Processes with Volatility

Domain 3 : Malware Analysis

- Introduction to Malware Analysis
    - Why it is important
    - TWhat are Malwares?
    - Types of Malwares
    - Types of Malware Analysis
    - Concept of Sandboxing
    - Configuring Malware Lab
    - Installation, Settings, Snapshots
- Static Analysis [Practical]
    - PE Analysis
    - Strings
    - Hashing
    - Local and Online Scanning
    - YARA and yarGen
- Dynamic Analysis
    - Introduction to SysInternals
    - Process Monitoring
    - Autoruns
    - Port Monitoring
    - Anti-Sandboxing Techniques

Domain 4 : Threat Hunting

- Introduction to Threat Hunting
- Threat Hunting vs Threat Detection
- Incident Response & Threat Hunting Relationship
- Types of Hunts
- Threat Hunting Hypothesis
- Threat Hunting Model
- Diamond Model of Intrusion Analysis
- LOTL & GTFO Bins based Techniques
- Malware Campaigns & APTs
- MITRE ATT&CK Framework [Practical]
    - Pre and Post Compromise Detection with Mitre ATT&CK
    - Hunting Hypothesis and Methodology

Network Traffic Hunting [Practical]

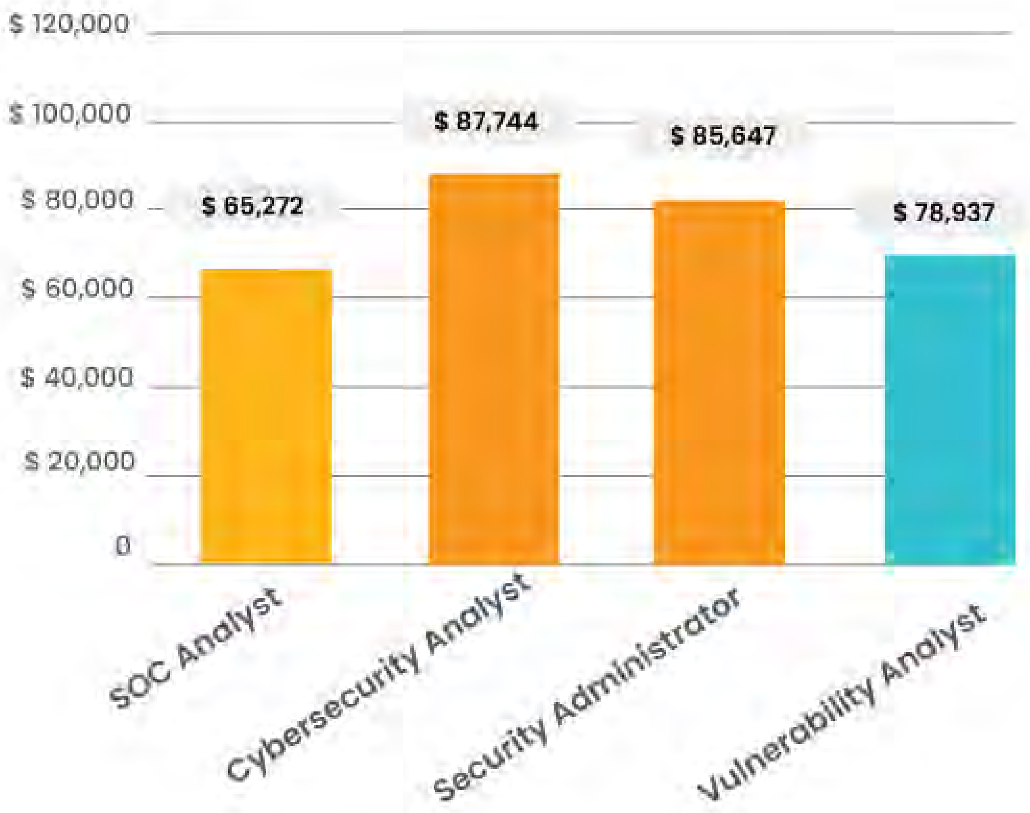
- Section Introduction
- HTTP and HTTPS traffic suspects
- Network Hunting and Forensics
- Wireshark, Network Miner

- Endpoint Hunting [Practical]
  - Introduction
  - Windows Processes
    - Smss.exe
    - Winlogon.exe
    - Wininit.exe
    - Services.exe
    - Lsass.exe
    - Svchost.exe
    - Taskhost.exe
    - Explorer.exe
  - Endpoint Baselines

Domain 5 : SIEM - Nervous System of SOC

- Using IBM QRadar [Practical]
  - Introduction to QRadar
  - QRadar SIEM Component Architecture and Data Flow
  - Using QRadar SIEM User Interface
  - Working with Logs
  - Working with Events of an Offense
  - Investigating Events & Flows
  - Developing Custom Rules
  - Creating Reports

SOC Specialist Course Benefits



Hiring Companies

tcs TATA CONSULTANCY SERVICES

IBM

EY

wipro

accenture

HCL

Source: Glassdoor

INFOSECTRAIN

www.infosectrain.com I sales@infosectrain.com