INFOSECTRAIN

SOC Analyst

(Security Operations Center) Hands-on Training

www.infosectrain.com

Tools Covered

- ITSM Tools
- Nmap
- Metasploit
- Splunk
- Wireshark
- CyberChef
- Microsoft Sysinternals
- Terminal/Shell
- Maltego
- AlienVault
- MISP
- Gophish
- Hack the Box (HTB)
- MxToolbox
- MITRE ATT&CK Navigator
- Many more......

Course Highlights

- **40-Hour** LIVE Instructor-led Training
- Certified Instructors
- Scenario-based Learning
- Hands-on Practice on Latest Tools
- Access to Recorded Sessions
- Career Guidance & Interview Prep
- Extended Post Training Support

Course Overview

Security Operations Center or SOC Analysts play a crucial role in today's security teams since they are on the front lines of cyber defense, identifying and responding to cyber threats as they occur. InfosecTrain's SOC Analyst hands-on 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 specifically designed to assist you in mastering techniques 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 through hands-on practice on the latest SOC tools.

Target Audience

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

Pre-requisites

Basic Knowledge of:

- Networking fundamentals
- OS basics & Troubleshooting is recommended
- Basics of Information Security
- Basics of Cyber World & Security
- Beginner or Fresher for SOC Operations Centre
- Working on Information Security Role

Our Expert Instructor

SANYAM NEGI

10+ Years of Experience

CEH | CSA | CND | CHFI | CTIA | CCISO | Security+ | Pentest+ | CySA+

An Information Security Consultant & Trainer with over 10+ years of hands-on experience with specializations in Security Operations Center, Threat Hunting and DevOps, Web Application Security, Vulnerability Assessment, Incident Handling & Response among others.

Sanyam is proficient in crafting customized training programs and courseware focused on Security Solutions with extensive expertise in providing consultations to a diverse clientele on cyber security and information security strategy. He's got an outstanding track record in achieving high exam success rates for professionals. His penchant for teaching with examples and simplifying complex topics are his key strengths.

ABHISHEK SHARMA

10+ Years of Experience

ISO 27001 LA | ISO 27001 LI | CySA+ | Security+ | Pentest+ | CSA | CTIA | ECIH | AZ-104

An Information Security expert with 10+ years of experience as an instructor delivering training to government and non-government organizations around the globe.

Abhishek is well versed in key aspects of Information Security including Security Operations Center, Web Application Security, Vulnerability Assessment, and some of the latest Information Security tools and technologies available in the market today. He's had exposure in delivering training to various corporate teams and in managing Information Security for different sectors, including banking, telecom, e-commerce, retail, healthcare and IT, among others.

Course Content

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

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.

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

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]

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

Educate. Excel. Empower.

www.infosectrain.com | sales@infosectrain.com