INFOSECTRAIN

SOC Analyst

(Security Operations Center)

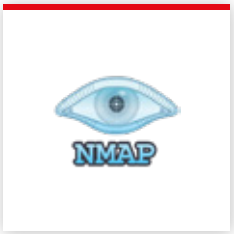
Hands-on Training

www.infosectrain.com

INFOSECTRAIN

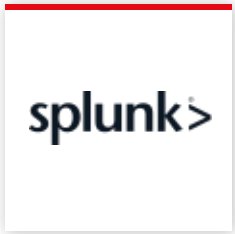
Tools Covered

ITSM Tools



Nmap

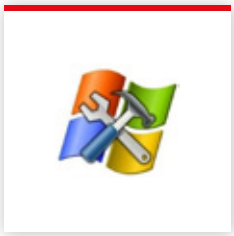
Metasploit



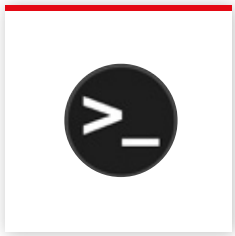
Splunk

Wireshark

CyberChef



Microsoft Sysinternals

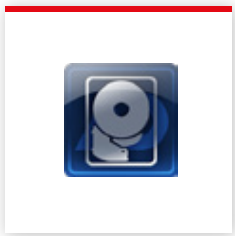


Terminal/Shell

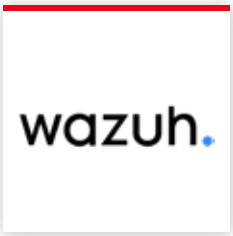
Maltego

AlienVault

MISP

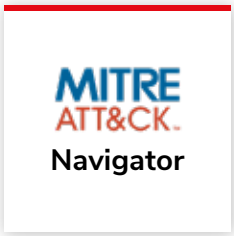


FTK Imager



Wazuh

MxToolbox



MITRE ATT&CK Navigator

volatility

Many more.....

INFOSECTRAIN

Course Highlights

- **48-Hour** Instructor-led Training
- Real-time Attack Simulations
- Access to Exclusive tools
- Case Study based Learning
- Project Integration
- Access Recorded Sessions
- Practical Approach
- Real-world Scenarios
- Interview Preparation

INFOSECTRAIN

About Course

As cyber threats become increasingly sophisticated, organizations require skilled professionals to safeguard their systems and data. The SOC (Security Operations Center) Analyst training course bridges this critical skills gap by offering an in-depth curriculum that spans the essentials of information security to advanced threat-hunting techniques.

Participants will explore critical areas such as SIEM operations, vulnerability management, malware analysis, and digital forensics, complemented by practical exposure to leading tools like Splunk, Wireshark, and MISP. This program emphasizes theoretical foundations and integrates hands-on labs that simulate real-world scenarios, equipping learners with the expertise to detect, analyze, and respond to complex cyber incidents effectively.

Course Objectives

- Understand the core principles of Information Security, including confidentiality, integrity, availability, non-repudiation, and managerial, technical, and operational security controls.
- Gain expertise in Security Operations Center (SOC) workflows, roles, and technologies to monitor and manage cyber threats effectively.
- Master the techniques for identifying and mitigating cyber threats like malware, ransomware, and Advanced Persistent Threats (APTs).
- Develop proficiency in vulnerability assessment and management, covering the complete lifecycle from asset identification to risk mitigation.
- Acquire hands-on experience in log management and analysis using tools like Splunk to detect anomalies and secure infrastructure.
- Build advanced skills in malware analysis, digital forensics, and incident response to investigate, contain, and remediate sophisticated cyber attacks.

INFOSECTRAIN

Target Audience

- Technical Support Engineers
- System Administrators
- Security Consultants
- Cyber Security Analysts
- Network Engineers
- Network Architects or Admin
- Security System Engineers
- SOC Analysts (L1 & L2)
- Information Security Researcher
- Aspiring Information Security Professionals
- Anyone Who Wants to Become a 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

INFOSECTRAIN

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.

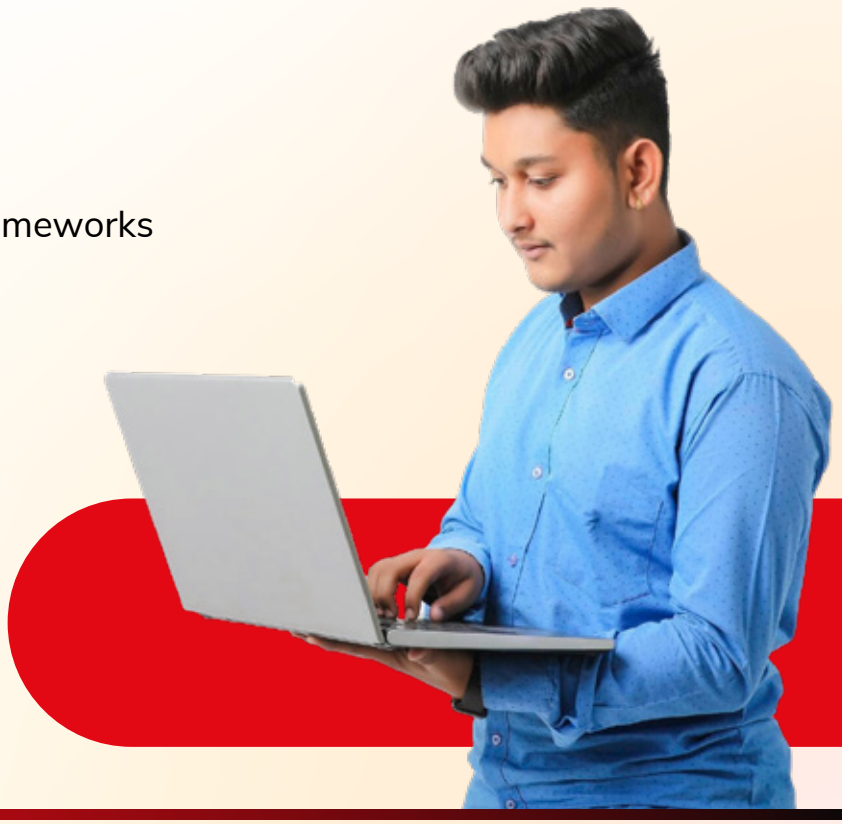
Abhishek is well versed in key aspects of Information Security including Security Operations Center, Web Application Security, Vulnerability Assessment, and some of the latest Information Security tools and technologies available in the market today. He's had exposure in delivering training to various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

INFOSECTRAIN

Course Content

Module 1 Introduction to Information Security

- Overview of Information Security
- Information Security vs. Cybersecurity
- Elements of Information Security
  - Confidentiality
  - Integrity
  - Availability
  - Non-Repudiation
- Security Controls
  - Managerial
  - Technical
  - Operational
- Introduction to Cybersecurity Frameworks
  - NIST
  - MITRE ATT&CK
  - ISO



Module 2 Security Operations Center (SOC) Foundations

- Introduction to Security Management
- Introduction to the Security Operations Center (SOC)
- Why Do We Need a SOC?
- Role of a SOC Analyst in Modern Cybersecurity
- SOC Tiers and Responsibilities
  - Tier 1
  - Tier 2
  - Tier 3
- Key SOC Technologies and Terminologies
- SOC Workflow

Module 3 Threat Landscape

- Types of Cyber Threats
  - Malware
  - Ransomware
  - Phishing
  - Insider Threats
- Overview of Advanced Persistent Threats (APTs)
- Understanding Attacks and Their Patterns

CASE STUDY

- MOVEit Data Breach
- SolarWinds Supply Chain Attack

Module 4 Vulnerability Management

- Understanding Vulnerability Assessment
- Types of Vulnerability Assessment
- Vulnerability Management Lifecycle
  - Asset Identification
  - Vulnerability Assessment
  - Risk Assessment
  - Remediation
  - Verification
  - Monitoring

Module 5 Log Management and Analysis

- Understanding Log Sources
  - Firewalls
  - IDS/IPS
  - Web Servers
  - Endpoints

- **Hands-On** with Centralized Logging Tool **(Splunk)**
- Identifying Anomalies in Logs

LAB

Analyzing Apache Server Logs for Intrusion Attempts

INFOSECTRAIN

Module 6 Threat Intelligence

- What is Threat Intelligence?
- Why Do We Need Intelligence?
- Threats, Threat Actors, APTs, and Global Campaigns
- Types of Threats
  - Network-Level
  - Web Application-Level
  - Host-Level
- Indicators of Compromise (IoCs) vs. Indicators of Attack (IoAs) vs. Precursors
- Traffic Light Protocol (TLP)
- Understanding the Pyramid of Pain

PRACTICAL LABS

- Collecting IoCs
- Exploring Threat Intelligence Platforms (e.g., Maltego, MISP)
- Checking IP/Domain Reputations
- Analyzing Malicious Files

Module 7 Threat Hunting Essentials

- Introduction to Threat Hunting
- Threat Hunting vs. Threat Detection
- Relationship Between Incident Response and Threat Hunting
- Threat Hunting Models
  - ✓ Hypotheses and Methodologies
  - ✓ Diamond Model of Intrusion Analysis
  - ✓ MITRE ATT&CK Framework

PRACTICAL LABS

- ✓ Network Traffic Analysis (Wireshark, Network Miner)
- ✓ Endpoint Process Analysis
  - → Memory Hunt - Volatility Framework
  - → Monitoring and Detecting USB drives in Windows
  - → Process Injection lab in Wazuh

Module 8 Security Information and Event Management (SIEM)

- What is SIEM and Why Do We Need It?
- SIEM Components
  - ✓ Security Information Management (SIM)
  - ✓ Security Event Management (SEM)

- SIEM Capabilities
  - Aggregation
  - Correlation
  - Alerts
  - Reporting

HANDS-ON WITH SPLUNK

- Installation
- Rule Writing & Alert Creation
- Event Analysis

Module 9 Malware Analysis

- Malware Analysis Basics
- Static vs. Dynamic Analysis

PRACTICAL LABS

- PE Analysis
- YARA Rules
- Traffic Analysis (Using Wireshark)
- Setting Up a Malware Lab
- Anti-Sandboxing Techniques

INFOSECTRAIN

Module 10 Digital Forensics and Incident Response (DFIR)

- Phases of Incident Response
  - Preparation
  - Detection
  - Containment
  - Eradication
  - Recovery
- Incident Playbook Overview
- Ticketing System

DISSECTING PHISHING EMAILS (PRACTICAL)

- Identifying Red Flags in Phishing Emails
- URL Reputation Analysis
- File Reputation Analysis
- Authentication Mechanisms:
  - SPF
  - DKIM
  - DMARC

- The 6 A's of the Forensics Process
  - Acquisition
  - Authentication
  - Analysis
  - Attribution
  - Articulation
  - Audit

INFOSECTRAIN

ANTI-FORENSICS TECHNIQUES (PRACTICAL)

- Steganography Detection and Analysis

NETWORK FORENSICS (PRACTICAL)

- Network Traffic Analysis
- Real-Time vs. Post-Mortem Analysis

DATA RECOVERY (PRACTICAL)

- Recovering Deleted Data
- Live Acquisition (Magnetic RAM Capture)

- System Forensics
  - Disk Imaging with FTK Imager
  - Disk Analysis Using Autopsy

PRACTICAL LABS

- PCAP Analysis (Wireshark)
- File and Disk Artifact Investigation

INFOSECTRAIN

*Bonus Section

Your Final Steps to Mastery

- Incident Response Project
  - Attack Simulation
  - Detection & Remediation
  - Report Preparation
- Interview Preparation

INFOSECTRAIN

Testimonials

Karthik Rao Marthineni

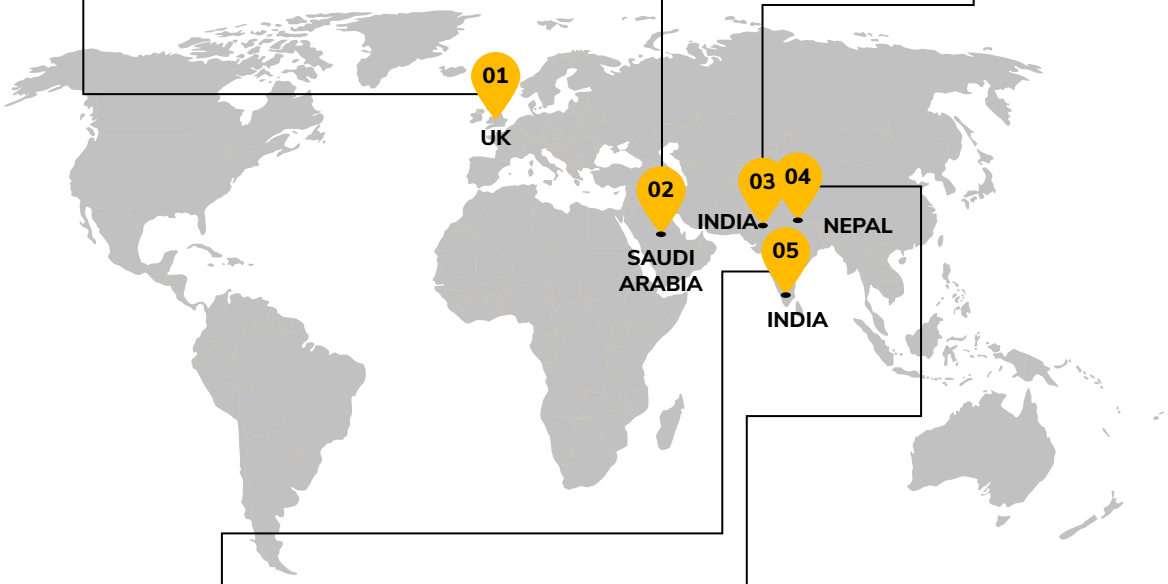
It's a great platform to learn the SOC analyst course online. The trainer is very patient and great at explaining the concept. I really liked the course. Thankyou!

Abdulaziz Abahussain

Overall, this training has equipped me with valuable skills and knowledge that I am excited to apply in my role. I couldn't have asked for a better team to guide me through this journey.

Abhiram KS

The trainer has great knowledge about the topic, and he knows what he is teaching us. Kudos to him. Thank you so much InfosecTrain.



Shubhranshu Mishra

It was a great experience,got opportunity to explore many new things and able to sort out doubts logically.

Dipendra Singh Mourya

I have learned the most about cyber security (SOC Analyst) from this organization. Our trainer, in particular, has given me the greatest advice and knowledge. Best Regards.

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on