NEXT IT CAREER
moving minds to right place

7 Years ANNIVERSARY

SOC Analyst Training

C|SA

Certified SOC Analyst

6TH Floor, Nilgiri Block,
ADITYA ENCLAVE,
604/B, Kumar Basti,
Ameerpet, Hyderabad,
Telangana 500016

+91-7995138210
+91-7013123485

contact@nextitcareer.com

About Next IT Career

Next IT Career Best Software Coaching Center in Hyderabad Corporate training is a function of human resource management that aims to provide the organization's employees with the knowledge and skills required to be successful. In turn, the growth of employees also contributes to the success of the business.
In recent years, Its also seen as a long-term strategic assignment rather than a cost center for the organization. The majority of companies have embraced 'continual learning' in it to promote employee growth both professionally and personally and acquire a highly skilled workforce as a result.

Corporate Training

Classroom Training

Online Training

NEXT IT CAREER
Moving minds to right place

Why Choose Us?

Training by Certified Instructors

Mock Interviews

Weekly Assignments

Project Training

Interview cracking tips

Resume Preparation

SOC ANALYST TRAINING PROGRAM

PHASE 1 — CYBERSECURITY FOUNDATIONS (DAY 1–5)

Day 1 — Introduction to Cybersecurity

Topics

- Cyber threat landscape
- Security domains
- Types of attackers

Practical

- Threat actor analysis

Day 2 — Security Concepts

Topics

- CIA triad
- Risk management
- Security controls

Exercise

- Risk assessment case study

Day 3 — SOC Architecture

Topics

- SOC tiers (L1, L2, L3)
- SOC workflows
- Detection pipeline

Exercise

- SOC workflow design

Day 4 — Security Frameworks

Topics

- NIST Cybersecurity Framework
- MITRE ATT&CK

Lab

- Map attacks using
- MITRE ATT&CK

Day 5 — Cyber Attack Lifecycle

Topics

- Kill chain
- Initial access methods
- Attack stages

Exercise

- Analyse a ransomware case study.

PHASE 2 — NETWORKING & OPERATING SYSTEMS (DAY 6–12)

Day 6 — Networking Fundamentals

Topics

- TCP/IP
- DNS
- HTTP

Tool

- Wireshark

Lab

- Analyze captured packets.

Day 7 — Network Security

Topics

- IDS vs IPS
- Firewall logs
- Port scanning

Lab

- Nmap scanning detection.

Day 8 — Windows Security

Topics

- Windows event logs
- Authentication events
- Active Directory basics

Tool

- Sysmon

Day 9 — Linux Security

Topics

- Linux authentication logs
- SSH attacks
- File monitoring

Lab

- Investigate failed SSH logins.

Day 10 — Endpoint Security

Topics

- EDR technologies
- Endpoint telemetry
- Behavioral monitoring

Platforms

- CrowdStrike
- Microsoft Defender

Day 11 — Log Analysis Fundamentals

Topics

- Log sources
- Event correlation
- Indicators of compromise

Exercise

- Analyse multi-source logs.

Day 12 — Threat Intelligence

Topics

- IOC enrichment
- OSINT intelligence sources

Tools

- Virus Total
- AbuseIPDB

PHASE 3 — SIEM OPERATIONS (DAY 13–20)

Day 13 — SIEM Fundamentals

Topics

- Log ingestion
- Event normalization
- Correlation rules

Tool

- Splunk Enterprise

Day 14 — Splunk Installation and Architecture

Lab

- Deploy Splunk in virtual lab.

Day 15 — Splunk Query Language

Topics

- SPL basics
- Filtering logs

Exercise

- index=windows EventCode=4625

Day 16 — Alert Creation

Topics

- Detection rules
- Alert thresholds

Exercise

- Create brute force detection alert.

Day 17 — Security Dashboards

Topics

- Visualization
- Incident metrics

Lab

- Build SOC dashboard.

Day 18 — Microsoft SIEM Ecosystem

Tool

- Microsoft Sentinel

Topics

- KQL queries
- Azure log ingestion

Day 19 — Detection Engineering

Topics

- Sigma rules
- Behaviour detection

Framework

- Sigma detection rules.

Day 20 — SOC Monitoring Simulation

Lab

- Investigate simulated attack logs.

Exercise

- Analyse multi-source logs.

PHASE 4 — INCIDENT RESPONSE (DAY 21–28)

Day 21 — Incident Response Lifecycle

Topics

- Preparation
- Detection
- Containment

Framework

- NIST IR model.

Day 22 — Malware Basics

Topics

- Malware types
- Execution patterns

Lab

- Malware sandbox analysis.

Day 23 — Digital Forensics

Tool

- Autopsy
- Volatility

Day 24 — Network Forensics

Tools

- Wireshark deep analysis.

Day 25 — Ransomware Investigation

Case Study

- Enterprise ransomware attack.

Day 26 — Threat Intelligence Integration

Tool

- Recorded Future
- Mandiant Intelligence

Day 27 — SOC Playbooks

Topics

- Incident runbooks
- Escalation procedures

Day 28 — Investigation Lab

Complete attack investigation exercise.

PHASE 5 — THREAT HUNTING (DAY 29–35)

Day 29 — Threat Hunting Methodology

Topics

- Hypothesis-driven hunting

Day 30 — Behavioral Analytics

Topics

- anomaly detection
- attack patterns

Day 31 — MITRE ATT&CK Hunting

Hunt credential dumping.

Day 32 — PowerShell Attacks

Detect malicious scripts.

Day 33 — Lateral Movement Detection

Detect PsExec activity.

Day 34 — Detection Engineering

Build detection rules.

Day 35 — Threat Hunting Campaign

Perform full hunt exercise.

PHASE 6 — CLOUD SOC OPERATIONS (DAY 36–40)

Day 36 — Cloud Security Fundamentals

Topics

- cloud attack surface
- shared responsibility model

Day 37 — AWS Security Monitoring

Topics

- Amazon GuardDuty

Day 38 — Azure Security Monitoring

Tools

- Microsoft Defender for Cloud

Day 39 — Container Security

Topics

- Kubernetes threats
- container escape attacks

Day 40 — Cloud Incident Response

Exercise

- Investigate IAM compromise.

PHASE 7 — AUTOMATION & AI SOC (DAY 41–45)

Day 41 — Security Automation

Topics

- SOAR platforms
- Automation workflows

Tools

- Cortex XSOAR
- Splunk SOAR

Day 42 — Python for SOC

Topics

- log parsing
- API integration

Day 43 — AI in SOC Operations

Tool

- Microsoft Security Copilot

Topics

- AI assisted investigations
- automated threat detection

Day 44 — SOC Metrics & Reporting

Topics

- MTTR
- MTTD
- SOC KPIs

Day 45 — Capstone SOC Project

Project

Build a Tasks

- Deploy SIEM
- generate attack logs
- create detection rules
- investigate incident
- produce incident report

Final Deliverables: Participants should complete..

NEXT IT CAREER
Moving minds to right place

Our Other Courses

Trending Software Testing courses

- Manual Testing
- Selenium Automation
- Tocsa
- ETL Testing
- Performance Testing
- API Testing
- Load runner
- J-meter
- Neo load

Most Trending Courses

- Data Science
- Data Analytics
- Scrum Master

Most Demand Courses

- AWS DevOps
- Azure DevOps
- Power BI
- Java Full Stack
- Python Full Stack
- Cyber Security

NEXT IT CAREER
Moving minds to right place

Our Recruitment Partners

TCS TATA CONSULTANCY SERVICES | genpact | accenture | NOUS INFOSYSTEMS | TestingXperts Passion For Perfection

cognizant | CGI | Capgemini | NTT | wipro

yatra | Deloitte. | EMERSON | IGT | Qualcomm

glance | Ford | EXL | Cigniti Software Quality Assured | zeta

goibibo.com | HCL | HDFC BANK | ARTECH INTELLIGENCE IS HUMAN | Caliber Deliver More. Deliver Excellence

Myntra | Infosys | IBM | aprovesign | DQ Labs Run by IITians

paytm | syngenta | Tech Mahindra | aspire SYSTEMS attention. always. | FedEx

Convertcart | { expleo } | Sotiotech Collaborate • Execute • Impact | AllCloud | ARTECH INTELLIGENCE IS HUMAN

Our Branch

Address: #407, Crescent arcade, Madhapur, Hyderabad

+91 - 7995138210
+91 - 7013123485

contact@nextitcareer.com

Our Infrastructure