SOC Analyst Training Program

Hands-On SIEM | Real Attack Detection | Job-Ready Skills
Become a Level-1 / Level-2 SOC Analyst with real-time labs, live attack simulations, and enterprise-grade tools.

Program Highlights

- **100% Practical SOC Lab Training**
- **SIEM (Elastic Stack) Hands-On**
- **Alert Triage & Incident Investigation**
- **MITRE ATT&CK-Driven Detection**
- **Email, Endpoint, Network & Cloud Security**
- **Capstone Project + Mock Interviews**
- **Ideal for Freshers & IT/Security Professionals**

Program Duration
3 Months | 90 Days | Day-Wise Practical Schedule

MODULE BREAKDOWN
Module 1: SOC Fundamentals & Lab Setup (Week 1)

- **SOC Architecture & Analyst Roles**
- **Cyber Kill Chain & Attack Lifecycle**
- **MITRE ATT&CK Framework**
- **Windows & Linux Log Fundamentals**

Labs:

- **SOC Virtual Lab Setup (Ubuntu, Windows)**
- **Attack Lifecycle Mapping**
- **Windows Event IDs (4624, 4625)**
- **Linux Auth Log Analysis**

Module 2: SIEM Foundations & Log Ingestion (Week 2)

- **SIEM Architecture & Use Cases**
- **Windows & Linux Log Ingestion**
- **Sysmon Deployment**
- **Dashboard Creation**

Labs:

- **Elastic Stack Installation**
- **Winlogbeat & Filebeat Configuration**
- **Sysmon Telemetry Analysis**
- **Custom Kibana Dashboards**

Module 3: Alert Triage & Investigation Workflow (Week 3)

- Alert Triage Methodology
- Brute Force Detection
- Process Creation Analysis
- False Positive Handling
- Incident Documentation

Labs:

- Detection Rule Creation
- Sysmon Event Analysis
- Alert Tuning & Classification
- Professional Incident Report Writing

Module 4: Network Traffic Analysis & Threat Intelligence (Week 4)

- Network Fundamentals for SOC
- PCAP & Malicious Traffic Analysis
- Threat Intelligence Platforms
- Firewall & DNS Log Analysis

Labs:

- Wireshark Traffic Filtering
- C2 Detection from PCAP
- VirusTotal, AbuseIPDB, OTX
- DGA & High-Entropy Domain Detection

Module 5: Email Security & Phishing Analysis (Week 5)

- Email Security Fundamentals
- Phishing Detection & IOC Extraction
- SPF, DKIM & DMARC
- Malicious Attachments

Labs:

- Email Header Analysis
- Phishing Investigation
- Macro Analysis
- Email Alert Triage

Module 6: Endpoint Detection & Malware Basics (Week 6)

- EDR Fundamentals
- Suspicious Process Investigation
- File Reputation Analysis
- Malware Behavior Analysis

- Persistence Detection

Labs:

- Wazuh EDR Configuration
- PowerShell & WMI Investigation
- Sandbox Report Analysis
- Registry Persistence Hunting

Module 7: Advanced Detection & SOAR (Week 7)

- Web Attack Detection
- Insider Threat Indicators
- Cloud Log Analysis (Intro)
- SOAR & Case Management
- Advanced Correlation Rules

Labs:

- Web Log Analysis (SQLi, Scans)
- Insider Threat Detection Rules
- TheHive Case Management
- Multi-Stage Attack Correlation

Module 8: Capstone Project & Interview Prep (Week 8)

- End-to-End SOC Investigation
- Multi-Stage Attack Detection
- Incident Response & Reporting
- Mock Interviews

Capstone Labs:

- Simulated Phishing → Exfiltration Attack
- SIEM Monitoring & Alert Triage
- MITRE ATT&CK Mapping
- Final Presentation

Career Outcomes

✓ SOC Analyst (L1 / L2)

✓ SIEM Analyst

✓ Cyber Security Analyst

✓ Threat Monitoring Analyst

Tools Covered

Elastic Stack | Kibana | Sysmon | Wazuh
Wireshark | VirusTotal | AbuseIPDB
TheHive | MITRE ATT&CK

SIEM Tools and SOC Technologies You Will Master (9-12 Week)
You will work with 12 tools across the 3-month program — from foundational analysis tools to enterprise-grade SIEM. Below is the full tool set with the context in which each is used.

Tool / Technology	Category	How You Use It in This Course
IBM QRadar	Primary SIEM	Analyst, Admin, and Engineer level — alert investigation, rule tuning, log source config
Wireshark	Network Analysis	Capture and analyse network packets — used in incident investigation labs
Kali Linux	Security OS	Ethical hacking introduction and penetration awareness modules
Nessus	Vulnerability Scanning	Understand how attackers identify weaknesses — context for SOC alert triage
CyberChef	Data Analysis	Decode and analyse email payloads, encoded malware strings
Sysinternals Suite	Endpoint Forensics	Process monitoring, autoruns, malware behaviour analysis on Windows
Snort / Suricata	NIDS/NIPS	Write and test intrusion detection rules, understand signature-based detection
SOAR Platforms (concepts)	Automation	Security Orchestration, Automation and Response — L2 and L3 context
EDR Tools (concepts)	Endpoint Detection	Endpoint alert triage, isolation workflows, agent-based detection
XDR (concepts)	Extended Detection	Extended detection and response — cross-layer visibility for senior SOC roles
Google Dorks	OSINT / Threat Intel	Open-source intelligence gathering for threat hunting and IOC research
Firewalls and IPS	Perimeter Security	Log reading, rule interpretation — foundational for all SOC log analysis work

Enroll Now
AimNxt Technologies
+91 91 5239 5239 | +91 9059 16 9059