AimNxt
School of Tech Leaders

BUILD CYBER SECURITY EXPERTISE WITH

SOC Analyst L1 & L2 Training Program

Accredited By:

NASSCOM® Certified Member

MSME Ministry of MSME, Govt. of India

DSCI PROMOTING DATA PROTECTION

www.aimnxt.org

10 Modules

Structured beginner-to-job-ready curriculum

Hands-On Labs

Real tools, real environments, real skills

Interview Ready

Mock interviews and exam preparation included

About the Program

The SOC L1 Training Program is a structured, **beginner-to-job-ready course** designed to develop the essential skills needed to operate as a Level 1 Security Operations Centre Analyst.

From foundational networking concepts to hands-on threat detection using industry tools like **Splunk, Wireshark, Nmap, and Seceon** — every module is built around real-world SOC workflows.

Graduates leave with the confidence, knowledge, and practical experience to crack interviews and **contribute from day one.**

Who Is This For?

- Fresh graduates entering cybersecurity
- IT professionals upskilling to security Aspiring SOC analysts & blue teamers
- Anyone preparing for security certifications

Course Curriculum Overview

Ten carefully sequenced modules take you from networking fundamentals all the way to live attack investigation and interview prep.

01

Networking Concepts

OSI & TCP/IP models, protocols, IP addressing

02

Intro to Cybersecurity

CIA Triad, SOC roles, threat actors, cryptography

03

Cyber Attacks

DDoS, SQLi, XSS, OWASP Top 10

04

Authentication & Threats

Zero-Trust, AAA, Defence in Depth

05

Frameworks & Analysis

MITRE ATT&CK, Kill Chain, Malware & Log Analysis

06

Security Analysis

Investigate threats at a deeper level through both static and dynamic techniques.

07

Log Analysis

Learn to extract critical signals from raw log data — a core SOC analyst skill.

08

SIEM & ERD Architecture

Operate enterprise-grade SIEM and EDR platforms used in production SOC environments.

09

Security Teams & MISC Concepts

Understand team dynamics, offensive/defensive roles, and the bigger security picture.

10

Lab & Practical Exercises

Get job-ready with real tool exposure, live attack simulations, and interview coaching.

Building Your Foundation

Thefirstthreemodulesestablishthebedrockknowledgeeverysocanalyst relies on daily — from network infrastructure to identity controls.

Module 01 — Networking Concepts

Understand topologies, firewalls, VPNs, routers, and switches. Master the OSI & TCP/IP models, the three-way handshake, IP addressing, and key protocols & ports that traffic flows through.

Module 02 — Introduction to Cybersecurity

Explore SOC roles & responsibilities, the CIA Triad, key terminology (threat actors, attack vectors, vulnerabilities), and cryptography fundamentals including encryption, hashing, and salting.

Attacks & Frameworks

Module 04 — Cyber Attacks

Dissect real-world attack techniques to sharpen your detection and response skills:

- DoS & DDoS Attacks Man-in-the-Middle Attack
- Brute-Force Attack
- SQL Injection, XSS & CSRF
- OWASP Top 10 — theoretical concepts

Module 05 — Frameworks

Apply the same industry-standard frameworks used by elite security teams worldwide:

Cyber Kill Chain — map attacker progression

Incident Response Life Cycle — structure your response

MITRE ATT&CK — catalogue adversary tactics and techniques

These frameworks form the analytical language of every professional SOC environment.

Security Analysis & Log Investigation

MODULES 06 – 07

Malware Analysis

Performboth**staticanalysis** (examining code without execution) and **dynamic analysis** (observing live behavior) to understand how malicious software operates and spreads.

Phishing & URL Analysis

Learnto dissectsuspicious emails, inspect headers, and analyze URLs to identify phishing campaigns 4 one of the most common attack vectors SOC analysts encounter.

Log Analysis & IOCs

Extractcriticalsignalsfrom raw log data. Master Windows Event IDs, understand the difference between events, alerts, and incidents, and identify **Indicators of Compromise (IOCs)**.

SIEM & EDR Architecture

MODULES - 08

Operate enterprise-grade platforms used in **production SOC environments** — the tools you'll use from your very first day on the job.

SIEM Hands-On

Work directly inside a SIEM platform to correlate events, build queries, and triage alerts at scale — just like a real SOC analyst.

EDR Hands-On

Investigate endpoint threats using an EDR tool, respond to detections, and practice incident documentation to industry standards.

Teams, Labs & Interview Prep

Module 09 — Security Teams & MISC Concepts

- **Red Team** — offensive simulation
- **Blue Team** — defensive monitoring
- **Purple Team** — collaborative improvement
- Vulnerability Assessment basics
- Penetration Testing concepts & types

Module 10 — Lab & Practical Exercises

- Hands-on lab environment setup
- Live tool usage: Nmap, Wireshark, Splunk, Seceon
  Attack workflow simulation & investigation
- PPT presentations & written exam
- **Mock interview preparation**

Graduates are fully equipped to clear L1 SOC analyst interviews with confidence.

Tools & Learning Outcomes

Everytoolinthisprogramisactivelydeployedinrealenterprise SOC environments — you graduate with **hands-on proficiency**, not just theoretical knowledge.

Nmap

Network discovery and port scanning for reconnaissance and asset mapping.

Wireshark

Deep packet inspection and traffic analysis for detecting anomalies.

Seceon

AI-driven threat detection and response for advanced SOC operations.

TryHackMe

Gamified learning labs to practice real-world attack and defence scenarios.

Splunk

Industry-leading SIEM platform for log ingestion, correlation, and alerting.

Success is Just a Call Away!

Request For Call Back

AimNxt
School of Tech Leaders

ADDRESS: AimNxt Technologies LLP,
6th floor, SAR AVENUE BUILDING,
Plot. No-1, HIG, Sy. No. 1009,
Phase- V KPHB, Kukatpally, Hyderabad-500072.

CONTACT: Phone: +91 91 5239 5239 | +91 9059 16 9059
Website: aimnxt.org | contact@aimnxt.org