CYBER
SECURITY XPERTS

Next-Gen Global SOC Analyst Pro with AI Threat Response

From Fresher to Global SOC Pro in 60 Days – Gain SOC L1, L2 & L3 Experience with AI-Powered Training, 120+ Real Incident, Hands-On Internship & 100% Job Placement with 200+ Partner Companies

+91-9503820287 cybersecxperts cybersecxperts cybersec_xperts Google Reviews cybersecxperts

Who Can Apply for the SOC Analyst 100% Job Placement Course?

- College Students (Final Year or Passouts)
- Graduates & Postgraduates (IT & Non-IT)
- Freshers from Any Background
- Career Switchers from Non-IT Fields Looking to Enter Cybersecurity
- Network & Information Security Professionals
- SOC L1 Analysts – Looking to Advance to L2/L3 Roles with Real-World Skills
- Working Professionals Seeking Career Growth
- Desktop Support / Technical Support Engineers
- System & Network Administrators

Why Choose Cyber Security Analyst as Your Career?

By 2025, 3.5 million cybersecurity jobs are expected to remain unfilled globally due to the shortage of skilled professionals.

1

Open to Any Graduate

Whether from IT or Non-IT Background, Anyone Can Become a Cybersecurity Analyst with the Right Training and Real Internship Experience.

2

Global Demand & Growth

Cybersecurity Offers Worldwide Opportunities and a Future-Proof Career

3

High Demand, Low Competition

Every company needs SOC analysts, but skilled SOC analysts are still rare

4

Fast Career Progression

Move from L1 to L3 roles within 1–3 years with hands-on experience

5

Attractive Salary

Cybersecurity Roles Offer Some of the Highest Packages in the IT Industry

Why Choose Cyber Security Analyst as Your Career?

6

Work with Leading Organizations

Opportunities in MNCs, banks, IT firms, and government sectors.

7

No Coding Required

Focus on investigation, detection, and real-time response in SOC roles.

8

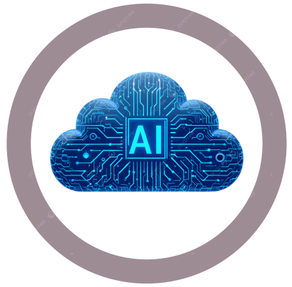
Remote Work Flexibility

A Work-from-Home Friendly Career with Global Clients, Anywhere in the World

9

Be a Digital Hero

Protect companies from cyber threats and play a critical role.



10

Ever-Evolving Field

Always growing with AI, Cloud, Threat Intelligence, and more

What is Required to Get into Cybersecurity?

We train you from scratch, give you real SOC internship experience, improve your communication skills, prepare you with mock interviews, and connect you directly with companies for job placements.

Operating efficiency

We provide everything you need to confidently start and grow your Cybersecurity career.

Fundamentals in IT & Domain Knowledge

We teach you everything from scratch, no prior experience needed.

Hands-on Real-Time Technical Experience

We are providing hands-on experience with a live internship in real company SOC environments.

English Communication Skills

We conduct daily practice sessions through team meetings to improve your English and make you confident for job interviews

Crack the Interview

We are providing 200+ real SOC Analyst interview questions, mock sessions, and detailed feedback on each answer to prepare you for real interviews.

Resume & Profile Building and Job Interview Calls

We are providing you with a customized resume, an optimized profile, and direct interview opportunities with our partner companies.

Course Overview

01

SOC Analyst Career

Become a Global SOC Analyst in Just 60 Days – From fresher to placed, with or without an IT degree.

02

Job Placement

100% Placement Guarantee — or Get Your Fees Back. We are with you until you get the job.

03

Real SOC Incidents

90+ Hours of Structured Learning + 120 Real SOC Incident Tickets.

04

Live Internship

Live Internship with Partner Company with dashboard access & alert handling, using industry tools like Splunk, CrowdStrike, Firewalls, IPS, WAF, Proxy, AWS, Windows, Linux & more.

05

AI-Powered Threat Detection

AI-Powered Threat Detection & GenAI Risk Defense – Use AI tools to triage, investigate, and respond to modern cyber threats.

01

Build and Fine-Tune SOC Use Cases

Build and Fine-Tune 120+ SOC Use Cases and Detection Rules – Gain SOC L2 and L3-level expertise to advance your cybersecurity career.

02

Daily Team Meeting

Daily Team Meetings and Discussion Sessions – Improve English communication, build SOC teamwork confidence, and stay motivated to complete training and get placed.

03

Mock Interviews

Mock Interviews – Practice with 200+ company-verified questions and expert-guided answers.

04

Certified SOC Analyst

CyberSecXperts Certified SOC Analyst Certificate – Recognized by hiring partners and top security teams.

05

Flexible Time & Mentoring support

Flexible Learning Access – 24/7 from Any Device – Learn at your pace, with full support.

Security Tools You Will Learn in Training

Team Structure – Learn, Practice & Get Placed Together

02

Why Team Learning Works

Boost Motivation

Learn with your dedicated SOC team members.

Improve English Communication

Daily Microsoft Teams meetings for discussion, Q&A, and real SOC practice.

Real SOC Practice

Handle security incidents together like in a real company.

Stay on Track:

Support each other to complete training, internship & job prep on time.

Choose Your SOC Team (As per your daily availability)

Team Name	Time Slot (IST)	Good For
Morning Team	7:00 AM – 1:00 PM	Students & Freshers
Afternoon Team	1:00 PM – 7:00 PM	Day learners & non-working students
Evening Team	7:00 PM – 1:00 AM	Working professionals & part-time learners
Night Team	1:00 AM – 7:00 AM	Night-shift workers & global time zones
Flexible Team	Anytime	For working professionals with changing schedules

Security Responsibilities You Will Learn

Security Alert Monitoring & Triage

Monitor security alerts, filter false positives, and escalate real threats for investigation.

Security Alert Investigation

Analyze alerts in depth to confirm incidents, assess impact, and identify root causes.

Phishing Email Analysis

Analyze suspicious emails to detect malicious links, attachments, or spoofing attempts.

Malware Analysis

Analyze malicious files to understand their behavior, impact, and mitigation methods.

Security Responsibilities You Will Learn

IOC Management

Identify, track, and update malicious indicators to enhance threat detection and prevention.

Threat Hunting

Perform proactive threat hunting using IOC scoping and contextual analysis

SIEM Use case Writing

Create and fine-tune detection rules in SIEM to identify real threats and reduce false positives.

Threat Intelligence

Use threat intel feeds to detect and defend against emerging cyber threats

SOC Course Syllabus

Module 1: Computer Fundamentals

- Computer Components
- Computer Architecture
- Operating System and Types
- System Types
- Asset Management List

Module 2: Networking Fundamentals

- Networking Devices and Network Types
- OSI Model
- IP Addressing
- Port Numbers
- Network Protocols (TCP, UDP, ICMP, DNS, DHCP, HTTP, FTP, SMTP, SNMP, SSH, RDP)
- Network Segmentation and DMZs

Module 3: Cryptography

- Cryptography Fundamentals
- Encryption & Decryption
- Symmetric and Asymmetric Encryption
- Hashing & Hash Functions
- VPN and Its Uses
- HTTP vs HTTPS
- Digital Certificate

Module 4: SIEM

- SIEM Concepts and Architecture
- Splunk Installation & Configuration
- Log Sources and Log Management
- Event Correlation and Normalization
- Threat Detection and Alerting
- Monitoring the Health of Security Sensors and SIEM Infrastructure

Module 5: Malware Analysis

- Introduction to Malware Analysis
- Types of Malware (viruses, worms, trojans, rootkits, ransomware and more)
- Malware Analysis Techniques
- Malware Detection and Prevention
- Malware Functionality
- Sandboxing- Any-Run

Module 6: EDR – CrowdStrike

- Endpoint Detection and Response (EDR)
- Forensics and Investigation of Endpoint Incidents
- Indicators of Compromise(IoC)(Email, Network, Host-based,Behavioural indicators
- Endpoint Security Concepts and Architecture
- Host-based Intrusion Detection and Prevention (HIDS/HIPS)
- Device Control and USB Blocking
- User Behavior Monitoring and Analytics

Module 7: Network Security

- Network Security Diagram
- Firewall: Palo Alto
- IDS/IPS: TippingPoint
- Network Traffic Analysis using Wireshark
- Virtual Private Network (VPN)
- **Network Attacks Covered:**

1. DNS Amplification Attack 2. DHCP Starvation Attack
3. TCP/UDP Flood Attack 4. DoS/DDoS Attacks Network Layer and Application Layer

Module 8: Web Security

- Web Application Architecture
- HTTP and HTTPS Communication
- HTTP Methods, Requests and Responses
- Cookies and Sessions
- Web Application Firewall (WAF): Imperva
- OWASP Top 10 Security Risk

Module 9: Cyber Attack Investigation and Response

- Incident Response Process
- Incident Classification and Prioritization
- Incident Notification and Communication
- Incident Preparation, Detection and Reporting
- Triage and Analysis
- Containment and Neutralization
- Eradication
- Post-Incident Activities
- Cyber Kill Chain
- MITRE ATT&CK Framework
- Malware infections: Viruses, Trojans, Ransomware
- Phishing Attacks
- Spear-phishing Attacks
- Social Engineering Attack
- Phishing email Analysis
- Denial-of-service (DoS) attacks
- Brute-force attacks
- Account compromised
- Unauthorized access
- Data breaches
- Advanced persistent threats (APTs)
- Website defacements
- Man-in-the-Middle Attack
- SQL Injection Attack
- Password Attack
- Web Attacks
- IOC-Indicator of Compromise
- URL Analysis
- IP Analysis
- Insider threats

Module 10: Threat Hunting

- Types of Treat Hunting
- Threat Hunting Use Cases
- Threat Hunting Tools
- Threat Hunting Scenarios
- Use of Threat Intelligence in Hunting
- Data Collection and Analysis
- Review threat intelligence feeds and investigate IOCs
- Integration with SIEM, EDR

Module 11: Threat Intelligence

- Threat Intelligence Platforms and Analysis
- Threat intelligence Integration with Security Tools (such as SIEM, Firewall, Proxy, Email Gateway, and EDR)
- Identify and Ingest IOCs Into Applicable Security Controls
- Review Detection Coverage of IOCs
- IOCs submission for coverage

Module 12: Vulnerability Management

- Vulnerability Assessment
- Vulnerability Management Life Cycle
- Vulnerability Scanning: Credential scan and Non-Credential scan
- Vulnerability Prioritization and Remediation
- Patch Management and Asset Management
- Reporting and metrics

Module 13: Penetration Testing

- Importance of Ethical hacking
- Bug Bounty Program
- Types of Hackers
- Penetration testing life cycle
- Reconnaissance, Vulnerability scanning, Exploitation, Privilege escalation, Post-exploitation

Our Partner Companies for Placement

Career Launchpad — From Training to Offer

Fee Structure & Enrollment

Our SOC Analyst Training & Internship program Fees Structure.

Total Fees Indian Students: INR ₹30,000

1st Installment	₹15,000
2nd Installment	₹15,000

Total Fees For International Students: USD $400

1st Installment	USD $200
2nd Installment	USD $200

Scan the QR Code to Registration

CYBER
SECURITY XPERTS

THANK TOU

+91-9503820287

info@cybersecxperts.com

www.cybersecxperts.com

cybersecxperts

cybersecxperts

cybersec_xperts