CyberHunt

BLUE TEAM / SOC SECURITY

Advanced SOC Analyst Program

Go beyond basic alert monitoring and master enterprise-grade SOC operations using Splunk, Microsoft Sentinel, SentinelOne, and Microsoft Defender. Designed for security professionals targeting L2/L3 SOC roles.

- Enterprise SIEM Investigation
- EDR/XDR Threat Response
- Incident Response Lifecycle
- Live Attack Simulations

5000+	95%	100+	24/7
Students Trained	Success Rate	Hiring Partners	Support

CyberHunt

Program Highlights

- 40-Hour Instructor-Led Training
- EC-Council Authorized Partner
- Practical Training on Latest Tools
- Telegram Group for Exam Support
- Learn from CEI Certified Trainers
- 98% Exam Pass Rate
- Post Training Support till Exam
- Access to Recorded Sessions
- Career Guidance & Mentorship

https://cyberhuntit.com/

CyberHunt

ABOUT COURSE

Advanced SOC Analyst Program

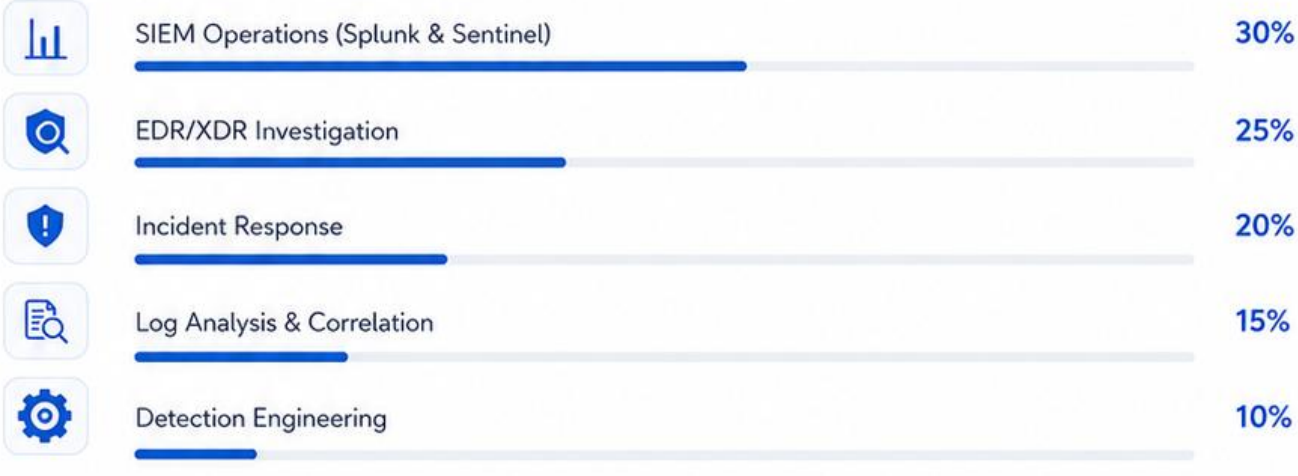
The Advanced SOC Analyst Program is a hands-on, enterprise-focused training designed to build expertise in Security Operations Center (SOC) monitoring, SIEM management, EDR/XDR investigation, cloud security monitoring, and incident response.

This program provides practical exposure to Splunk, Microsoft Sentinel, SentinelOne, Microsoft Defender for Endpoint, and Microsoft Defender for Office 365 — the same tools used in real enterprise SOC environments.

You will learn how to investigate real security alerts, correlate logs across multiple sources, detect advanced attacks, perform endpoint investigations, handle phishing and email-based threats, and respond to ransomware and lateral movement scenarios.

This course is designed to make candidates job-ready for L2/L3 SOC Analyst, SIEM Engineer, and Incident Responder roles.

SOC Analyst Skill Coverage



CyberHunt

Target Audience

- Security Analysts
- Ethical Hackers
- System Administrators
- Network Administrators
- Network and Security Engineers
- Cyber Security Managers
- Information Security Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components.

CyberHunt

Course Curriculum

Comprehensive SOC training with enterprise SIEM, EDR/XDR platforms and live attack simulations

01 SOC Operations & Incident Management

- SOC Architecture (L1, L2, L3)
- Roles & Responsibilities
- Security Monitoring Lifecycle
- Incident Response Lifecycle
- SLA & Escalation Matrix
- Ticketing Workflow & Documentation
- Alert Prioritization & Severity Classification

Practical: Handling simulated SOC tickets.

02 Log Management & Security Fundamentals

- Types of Logs (Windows, Linux, Firewall, Proxy, DNS)
- Log Collection & Normalization
- Event Correlation
- Log Parsing Techniques
- Identifying False Positives
- IOC vs IOB Detection

Practical: Analyzing raw logs to identify suspicious behavior.

03 Splunk SIEM – Complete Practical Training

splunk>

- Architecture & Setup: Splunk Components (Indexer, Forwarder, Search Head)
- Log Ingestion & Indexing
- SPL Query Writing: Basic & Advanced SPL Commands, Filtering & Aggregation
- Statistical & Time-Based Analysis
- Detection Engineering: Correlation Rule Creation & Alert Configuration
- Dashboard Creation & Use Case Development
- Brute Force, PowerShell Abuse & Privilege Escalation Detection

Practical: Create custom detection use case & investigate attack scenario.

04 Microsoft Sentinel (Azure Sentinel)

- Architecture & Data Connectors
- Connecting Log Sources & Azure Integration
- KQL Query Writing: Filtering, Parsing & Aggregation
- Time Series Analysis & Hunting Queries
- Analytics Rule Creation
- Playbooks (SOAR) & Automation for Incident Response
- Threat Intelligence Integration

Practical: Build KQL detection for phishing & lateral movement.

05 SentinelOne EDR/XDR

SentinelOne

- Agent Deployment & Architecture
- Behavioral AI Detection
- Threat Storyline Analysis
- Process Tree Investigation
- Ransomware Detection & Suspicious Process Execution
- Response Actions: Isolate Endpoint, Kill Process
- Rollback (Ransomware Recovery)

Practical: Investigate ransomware & lateral movement scenario.

06 Microsoft Defender for Endpoint

- Device Timeline Analysis
- Alert Investigation
- Advanced Hunting Queries
- ASR Rules & Endpoint Hardening
- Attack Surface Reduction Monitoring
- Live Response: Remote Investigation
- Collecting Digital Evidence

Practical: Detect credential dumping & persistence techniques.

07 Microsoft Defender for Email Security (Office 365)

- Phishing Detection & Email Threat Investigation
- Safe Links & Safe Attachments
- Email Header Analysis
- Threat Explorer Usage
- Anti-Phishing & Anti-Spam Policy Configuration
- Email Security Hardening

Practical: Full phishing investigation case study.

08 Incident Response & Advanced Investigation

- Malware Triage Basics
- Root Cause Analysis
- Timeline Reconstruction
- Lateral Movement Detection
- Data Exfiltration Investigation
- Reporting & Documentation

Practical: End-to-end incident handling simulation.

09 Use Case Development & Detection Engineering

- Creating High-Fidelity Alerts
- Reducing False Positives
- Mapping to MITRE ATT&CK
- Continuous Monitoring Improvement

Practical: Develop 5 enterprise-grade detection use cases.

CyberHunt

TRAINING ENQUIRIES

Have questions or need more information about our training programs? We're here to help!

For Training
+91 99599 06195
+91 93156 97737

Email
trainings@cyberhuntit.com

Website
www.cyberhuntit.com

Empowering Your Future
Industry-relevant training designed to upskill and empower you.

Follow us on