SAVORY MINDS
BUILD SKILLS. SECURE FUTURES.

SOC ANALYST
COMPLETE COURSE SYLLABUS

LEARN. PRACTICE. ANALYZE. DEFEND.

From fundamentals to real-world SOC operations – become industry ready.

LIVE TRAINING BY WORKING PROFESSIONALS
Learn from real SOC experts with 6+ years of experience.

HANDS-ON LABS & REAL SCENARIOS
Work on live attacks, logs, and case studies.

END-TO-END SOC OPERATIONS
Covers People, Process and Technology.

CERTIFICATE OF COMPLETION
Industry-recognized course completion certificate.

PLACEMENT SUPPORT & CALL REFERRALS
Resume support, mock interviews & real job opportunities.

COURSE STRUCTURE – 10 MODULES

01 INTRODUCTION TO CYBER SECURITY & SOC
- Overview of Cyber Security
- SOC Structure & Functions
- SOC Analyst Roles & Responsibilities
- Threat Landscape & Attack Lifecycle

DURATION: 4 HRS

02 NETWORKING FUNDAMENTALS
- OSI & TCP/IP Model
- IP Addressing & Subnetting
- Protocols & Ports
- Network Devices
- Wireshark Basics

DURATION: 6 HRS

03 LINUX FUNDAMENTALS FOR SOC
- Linux Installation & Navigation
- File System & Permissions
- User & Process Management
- Package Management
- Essential Linux Commands

DURATION: 6 HRS

04 LOG MANAGEMENT & ANALYSIS
- Understanding Logs
- Log Sources (Windows, Linux, Network)
- Centralized Logging
- Log Analysis Techniques

DURATION: 6 HRS

05 THREAT DETECTION & ANALYSIS
- Indicators of Compromise (IOC)
- MITRE ATT&CK Framework
- Threat Hunting Basics
- Alert Triage & Prioritization

DURATION: 8 HRS

06 SIEM FUNDAMENTALS (ELASTIC STACK)
- Introduction to SIEM
- ELK Stack Overview
- ElasticSearch Basics
- Log Ingestion with Beats
- Kibana Dashboards

DURATION: 10 HRS

07 KQL QUERIES & ALERTING
- KQL Basics
- Filtering & Searching Data
- Advanced KQL Queries
- Creating Alerts
- Visualization in Kibana

DURATION: 8 HRS

08 WINDOWS SECURITY ESSENTIALS
- Windows OS Internals
- Event Logs (System, Security, Application)
- Windows Security Features
- PowerShell Basics

DURATION: 6 HRS

09 MALWARE ANALYSIS FUNDAMENTALS
- Malware Types
- Static Analysis Basics
- Dynamic Analysis Basics
- Tools: VirusTotal, Hybrid Analysis, Basic Reverse

DURATION: 6 HRS

10 INCIDENT RESPONSE & CASE MANAGEMENT
- Incident Response Lifecycle
- Containment, Eradication, & Recovery
- Case Documentation
- Reporting & Communication

DURATION: 6 HRS

TOOLS & TECHNOLOGIES YOU WILL MASTER

Linux · Wireshark · Elastic Stack · Kibana · Windows · PowerShell · VirusTotal · YARA · MITRE ATT&CK · MISP

WHAT YOU WILL ACHIEVE

- Monitor, detect & respond to security threats
- Analyze logs & incidents like a professional
- Work with SIEM tools & threat intelligence
- Handle real-world SOC scenarios with confidence
- Build a strong foundation for a high-growth SOC career

REAL TRAINING
No PPTs. Only practical, hands-on learning.

REAL SUPPORT
24/7 doubt solving & mentor guidance.

REAL RESULTS
Job-ready skills for high-demand roles.

REAL CAREERS
Placement support till you get placed.

SCAN TO ENROLL

SECURE TODAY. DEFEND TOMORROW.

JOIN SAVORY MINDS. BECOME A SOC ANALYST.