Certified SOC Analyst- Forensic Academy

Offered by: Forensic Academy

Overview Details~

The **Certified SOC Analyst – Forensic Academy** is a comprehensive 2-month training program designed to equip aspiring cybersecurity professionals with the skills needed to operate effectively within a Security Operations Center (SOC). This certification focuses on real-world threat detection, incident response, log analysis, and foundational digital forensics. It bridges the gap between theoretical knowledge and practical SOC operations, preparing candidates for Tier 1 and Tier 2 analyst roles.

Duration: Two Months

Training Fees: INR 25,000/- *(~~30,000~~)*

Certification:

- ISO Certified
- Registered under **MSME**, Government of India
- Format: Instructor-led / Online / Hybrid
- Audience: Aspiring SOC Analysts, Security Enthusiasts, Tier 1/2 Security Analysts, Forensic Analyst

ENROLL FOR SOC ANALYST TRAINING

Installement Option also Available

Contact us for Registration and More Details:

+91 8437138319 | sales@forensicacademy.in

www.forensicacademy.in

Module 1: Introduction to SOC & Threat Landscape

- What is SOC? Roles & Responsibilities
- SOC Architecture and components
- Cybersecurity kill chain & MITRE ATT&CK
- Threat actors, TTPs, and attack vectors
- Understanding Incident Response lifecycle

Module 2: Network & Endpoint Security Fundamentals

- TCP/IP and OSI Model refresher
- Common network protocols & packet analysis
- Endpoint security basics (Windows, Linux)
- Common attacks: MITM, DNS Poisoning, spoofing
- Firewall, IDS/IPS, AV/EDR concepts
- Wireshark, TCPDump & Tshark
- Server Network Capturing Automation
- Network Infrastructure Working
- Interanet or Internet -Model
- Network Security Architecuture Concept working

Module 3: System Attack Practical Analysis

- MITM Attack
- Network Security Attack
- DdoS analysis
- Packet Log Monitoging
- Cloud Monitoging
- Real Time System Monitoring
- Logs ANALYSIS
- Manual analysis
- /var/log

Module 4: SIEM Tools & Log Analysis

- Understanding SIEM (Security Information and Event Management)
- SPLUNK & WAZUH
- Configuration and Forwarder
- Splunk Monitoring Dashboard
- Log Sources: windows, Linux, Firewall, Proxy, Mail
- Log Parsing
- Building alerts custom dashboards

Module 5: Threat Intelligence & Malware Analysis Basics

- What is Threat Intelligence (TI)
- OSINT tools & Platforms
- IOC, TTP, STIX/ TAXII standards
- Malware types and delivery mechanisms
- Static and dynamic analysis
- Virustotal, hybrid analysis, kape sandboxie
- Extract and analyze simple IOCs

Module 6: Digital Forensics process

- Forensics and chain of custody
- Memory, disk and network forensics
- File System: NTFS, FAT32, EXT
- Evidence acquisition and preservation
- Windows and linux artificats
- Autopsy | FTK Imager
- Analyze deleted files, and recover artifacts

Module 7: Incident Detection and Triage

- Email Phishing Analysis
- Brute-force attack detection
- Lateral movement identification
- Alert investigation lifecycle
- Escalation and ticketing
- Detect and respond to simulated attack
- Create incident tickets and perform triage

Module 8: Incident Response & Reporting

- IR Policies and playbooks
- Phases or IR: Preparation to lessons learned
- Role of SOC in containment & eradication
- Writing effective incident reports
- Communication and escalation plans
- Real-time incident reports

The **Certified SOC Analyst (CSA)** training offered by **Forensic Academy** is a foundational program designed to equip aspiring cybersecurity professionals with the essential knowledge and practical skills required to work effectively in a **Security Operations Center (SOC)** environment.

This course bridges the gap between beginner-level cyber security enthusiasts and SOC roles, offering hands-on exposure to modern-day security operations, threat detection, incident response, and log analysis using real-world scenarios.

Whether you're aiming to become a Tier I or Tier II SOC Analyst, this certification sets the groundwork for a successful cybersecurity career by building your understanding of **SIEM tools**, **threat intelligence**, **incident detection**, and **forensic investigation**.