KLEAP Institute of
Information Security™

SOC Analyst

2026

SOC Analyst

3-MonthCourseOutline

ComprehensiveTrainingProgram

Duration: 3 Months | 12 Modules | Theory + Practical Labs

Part 1: SOC Foundations (Month 1) | Modules 1–5

Part 2: Detection & Analysis (Month 2) | Modules 6–9

Part 3: Intelligence & Response (Month 3) | Modules 10–12

PART 1 — SOC FOUNDATIONS (Month 1)

Module 1 Introduction to SOC

What is a Security Operations Center (SOC)?

- Definition, purpose, and business value of a SOC
- Role of a SOC in the overall security posture of an organization
- SOC vs CERT vs CSIRT — understanding the differences
- 24/7 monitoring, detection, analysis, and response workflow

SOC Tiers & Analyst Roles

- Tier 1 Analyst — alert triage and initial investigation
- Tier 2 Analyst — deeper incident analysis and escalation
- Tier 3 Analyst / Threat Hunter — proactive threat hunting
- SOC Manager — operations oversight and reporting
- Career path: SOC Analyst → Incident Responder → Threat Hunter

SOC Models

- In-house SOC — organization-owned and operated
- Managed SOC (MSSP) — outsourced to a security provider
- Hybrid SOC — combination of in-house and managed services
- Virtual SOC — remote team with no physical presence

SOC Metrics & KPIs

- Mean Time to Detect (MTTD) — how quickly threats are identified
- Mean Time to Respond (MTTR) — how quickly incidents are resolved
- False Positive Rate — percentage of incorrect alerts
- Alert volume and analyst workload management

Compliance & Regulatory Context

- Why organizations build SOCs — compliance, risk reduction, liability
- Relevant standards: ISO 27001, NIST CSF, PCI-DSS, HIPAA
- SOC's roleinaudit readiness and evidence collection

Practical Session

- Research andmap a real-world SOC analyst job description to tier roles
- Explore a SOCdashboard demo environment and identify alert types

Module 2 Lab Setup

Virtualization & Environment Overview

- Why a safe lab environment is critical for SOC training
- Types of hypervisors: Type 1 (bare-metal) vs Type 2 (hosted)
- Installing and configuring VirtualBox / VMware Workstation

Setting Up the SOC Lab

- Installing Ubuntu Server as a log source and target machine
- Installing Windows Server 2019 as an Active Directory environment
- Deploying Kali Linux as an attacker machine for simulated attacks
- Configuring host-only / NAT network adapters for isolation

Deploying Core SOC Tools

- Installing Splunk Free on Ubuntu — SIEM and log aggregation
- Setting up Security Onion — IDS/NSM all-in-one platform
- Installing Elastic Stack (ELK) — Elasticsearch, Logstash, Kibana
- Deploying Wazuh agent for host-based monitoring

Log Forwarding Configuration

- Configuring syslog on Linux to forward logs to SIEM
- Windows Event Forwarding (WEF) to collect Windows event logs
- Installing Filebeat / Winlogbeat log shippers
- Verifying logingestion in Splunk and Kibana dashboards

Practical Session

- Builda fullyfunctional 4-machine SOC lab (attacker, Windows target, Linux server, SIEM)
- Confirm logflow from all sources into Splunk
- Trigger a testevent and trace it from source to SIEM alert

Module 3 SOC Tools

SIEM — Security Information & Event Management

- What a SIEM does: collection, correlation, alerting, and reporting
- Key SIEM vendors: Splunk, IBM QRadar, Microsoft Sentinel, ArcSight
- Log sources: firewalls, IDS/IPS, endpoints, servers, cloud
- Use cases: brute force detection, lateral movement, data exfiltration

IDS / IPS

- Intrusion Detection System (IDS) vs Intrusion Prevention System (IPS)
- Network-based (NIDS) vs Host-based (HIDS) detection
- Signature-based vs anomaly-based detection methods
- Tools: Snort, Suricata, Security Onion

Endpoint Detection & Response (EDR)

- How EDR differs from traditional antivirus solutions
- Behavioral monitoring, process injection detection, memory analysis
- EDR tools overview: CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint
- Threat hunting capabilities within EDR platforms

Vulnerability Scanners

- Role of vulnerability scanning in the SOC workflow
- Tools: Nessus, OpenVAS, Qualys
- Interpreting scan results and mapping to CVEs
- Prioritizing remediation based on CVSS scores

Threat Intelligence Platforms (TIP)

- What is Threat Intelligence and why it matters to SOC analysts
- MISP, OpenCTI, and commercial TIP solutions
- Integrating IOC feeds into SIEM for automated detection

Ticketing & Case Management

- Why structured case management improves incident handling
- Tools: TheHive, JIRA Service Management, ServiceNow
- Creating, escalating, and closing incident tickets

Practical Session

- Navigate andexplore the Splunk interface — search, dashboards, alerts
- Configure aSuricata rule and observe IDS alerts in Security Onion
- Run an OpenVAS scan against Metasploitable and review results

Module 4 Common Threats and Attacks

Malware Categories

- Viruses — self-replicating malicious code requiring a host file
- Worms — self-propagating across networks without user action
- Trojans — disguised as legitimate software to gain access
- Ransomware — encrypts files and demands payment for decryption
- Spyware / Adware — data collection and unwanted advertising
- Rootkits — deep OS-level persistence and stealth
- Botnets — networks of compromised hosts under attacker control

Network-Based Attacks

- Denial of Service (DoS) and Distributed DoS (DDoS)
- Man-in-the-Middle (MitM) — ARP spoofing, SSL stripping
- Port scanning and service enumeration with Nmap
- Packet sniffing — capturing cleartext credentials with Wireshark
- DNS hijacking and DNS amplification attacks

Credential-Based Attacks

- Brute force — automated password guessing
- Credential stuffing — using leaked username/password combos
- Password spraying — one common password across many accounts
- Pass-the-Hash (PtH) — lateral movement with NTLM hashes
- Kerberoasting — offline cracking of Kerberos service tickets

Social Engineering

- Phishing — deceptive emails to steal credentials or deliver malware
- Spear Phishing — targeted phishing against specific individuals
- Vishing — voice call-based deception
- Smishing — SMS phishing attacks
- Pretexting and Impersonation techniques

Insider Threats

- Malicious insiders — deliberate data theft or sabotage
- Negligent insiders — accidental exposure through poor practices
- Indicators ofinsider threat on SIEM (large file downloads, off-hours access)

Practical Session

- Simulate abrute-force SSH attack against a lab machine using Hydra
- Capture andanalyze attack traffic in Wireshark
- Identify theattack pattern in Splunk logs

PART 2 — DETECTION & ANALYSIS (Month 2)

Module 5 Security Operations Fundamentals

The SOC Workflow

- Alert triage lifecycle: receive → analyze → escalate → resolve
- True positive vs false positive vs false negative classification
- Priority assignment: Critical / High / Medium / Low / Informational
- SLA targets and escalation timelines for each severity level

Defence in Depth

- Layered security model — no single control is sufficient
- Perimeter security: firewalls, DMZ, network segmentation
- Endpoint security: AV, EDR, host-based firewalls, patch management
- Application security: WAF, input validation, secure coding
- Data security: encryption at rest and in transit, DLP solutions
- Identity security: MFA, PAM, least privilege principle
- Physical security controls and their role in defence in depth
- Monitoring and visibility as the final layer of defence

Zero Trust Architecture

- Core principle: 'Never trust, always verify'
- Micro-segmentation and identity-centric access control
- Continuous verification vs perimeter-based trust

Security Baselines & Hardening

- CIS Benchmarks — configuration standards for OSes and applications
- Windows hardening: disabling unnecessary services, GPO policies
- Linux hardening: SSH key authentication, firewall rules (UFW/iptables)
- Network device hardening: disable telnet, restrict SNMP

Log Management & Analysis

- Types of logs:Windows Event Logs, Syslog, Web Server logs, Firewall logs
- Critical WindowsEvent IDs: 4624 (logon), 4625 (failed logon), 4648, 4776, 7045
- Linux log files:/var/log/auth.log, /var/log/syslog, /var/log/audit/audit.log
- Log retentionpolicies and SIEM storage planning

Practical Session

- Analyze WindowsEvent Logs for failed logon attempts (Event ID 4625)
- Apply a CIShardening checklist to a lab Windows Server
- Identify securitymisconfigurations on a lab Ubuntu server

Module 6 Phishing Analysis

Understanding Phishing

- Phishing attack lifecycle: lure → delivery → infection → C2

- Types: spear phishing, whaling, business email compromise (BEC)
- Phishing kits — ready-made credential harvesting pages
- How attackers bypass spam filters and email gateways

Email Header Analysis

- Understanding email header fields: From, Reply-To, Return-Path, Received
- Identifying spoofed sender addresses and domain impersonation
- Tracing email path using Received headers and IP lookups
- SPF, DKIM, and DMARC — email authentication mechanisms
- Using MXToolbox and Google Admin Toolbox for header analysis

URL & Link Analysis

- Identifying malicious URLs: lookalike domains, typosquatting, URL shorteners
- Safe URL defanging: replacing http with hxxp for safe sharing
- Analyzing URLs using VirusTotal, URLScan.io, and AnyRun
- Checking domain age and WHOIS registration details

Attachment Analysis

- Common malicious file types: .exe, .docm, .xlsm, .lnk, .iso, .zip
- Static analysis: examining file metadata, strings, and macros
- Dynamic analysis: detonating files in a sandbox (Any.run, Hybrid Analysis)
- Extracting IOCs from malicious documents using oletools

Phishing IOC Extraction

- Extracting sender IPs, URLs, and hashes from phishing samples
- Documenting IOCs in a structured format for SIEM ingestion
- Reporting phishing to upstream teams and ISPs

Practical Session

- Analyze aphishing email sample — extract headers, URLs, and attachments
- Submit attachment to Any.run sandbox and document findings
- Upload suspicious URL to URLScan.io and interpret the report
- Create an IOC report from the analyzed phishing email

Module 7 Splunk

Splunk Architecture & Components

- Forwarder — Universal vs Heavy Forwarder for log collection
- Indexer — stores and indexes incoming log data
- Search Head — user-facing interface for searching and dashboards
- Deployment Server — centralized forwarder configuration management

Splunk Search Processing Language (SPL)

- Basic search syntax: keywords, time ranges, and field filtering
- Pipe commands: stats, table, sort, dedup, eval, rex
- stats count by command for aggregation and counting events
- rex command for custom field extraction using regex

- where and search clauses for conditional filtering
- Subsearches and joins for correlating multiple data sources

Indexes, Sourcetypes & Data Inputs

- Understanding indexes and how data is partitioned
- Configuring sourcetypes for syslog, Windows events, and web logs
- Setting up data inputs: monitor, TCP/UDP, scripted inputs
- Index lifecycle management and data retention policies

Alerts & Scheduled Searches

- Creating real-time vs scheduled alerts
- Alert trigger conditions: number of results, per result, custom thresholds
- Alert actions: email notification, webhook, script execution
- Suppressing repeat alerts to reduce analyst fatigue

Dashboards & Visualizations

- Building SOC dashboards: timechart, single value panels, tables
- Using drilldowns to pivot from summary to raw events
- Creating executive dashboards for management reporting

Common SOC Detection Queries

- Detecting brute force: count failed logins by source IP
- Detecting privilege escalation: searches for Event ID 4672 and sudo commands
- Detecting lateral movement: Logon Type 3 across multiple hosts
- Detecting data exfiltration: large outbound data transfers

Practical Session

- Ingest Windows and Linux logs into Splunk
- Write SPL queries to detect brute force, privilege escalation, and suspicious logins
- Build a SOC monitoring dashboard with live alert panels
- Create a scheduled alert for failed login threshold breach

PART 3 — INTELLIGENCE & RESPONSE (Month 3)

Module 8 Threat Intelligence

What is Threat Intelligence?

- Definition: actionable, context-rich information about adversaries and threats
- Intelligence vs raw data vs information — understanding the distinction
- Consumers of threat intelligence: SOC analysts, CISOs, red teams

Types of Threat Intelligence

- Strategic intelligence — high-level trends for executive decision-making
- Operational intelligence — details about specific campaigns and actors
- Tactical intelligence — TTPs (Tactics, Techniques, Procedures) of threat actors
- Technical intelligence — specific IOCs: IP addresses, domains, hashes, URLs

Indicators of Compromise (IOCs)

- Types of IOCs: file hashes (MD5/SHA256), IP addresses, domain names, URLs, registry keys
- IOC lifecycle: discovery → validation → enrichment → sharing → expiry
- IOC management tools: MISP, OpenCTI, ThreatConnect
- Searching IOCs in VirusTotal, Shodan, and AlienVault OTX

MITRE ATT&CK Framework

- Overview of the ATT&CK matrix: Tactics → Techniques → Sub-techniques
- Enterprise vs Mobile vs ICS ATT&CK matrices
- Mapping real-world attacks to ATT&CK techniques
- Using ATT&CK Navigator to visualize threat actor coverage
- How SOC analysts use ATT&CK to improve detection rules

Threat Actor Profiling

- APT groups vs cybercriminal groups vs hacktivists
- Researching threat actors using public sources (CISA advisories, vendor reports)
- Nation-state actors: motivations, targets, and known TTPs
- Tracking actor campaigns using CTI platforms and reports

Sharing Intelligence

- STIX — StructuredThreat Information Expression data format
- TAXII — TrustedAutomated eXchange of Intelligence Information protocol
- ISACs and ISAOs— sector-specific intelligence sharing communities
- Operating underTraffic Light Protocol (TLP) — TLP:RED, AMBER, GREEN, WHITE

Practical Session

- Search an IOC(IPaddress or file hash) across VirusTotal, OTX, and Shodan
- Map a recentransomware attack to MITRE ATT&CK techniques
- Import an IOCfeedinto MISP and browse the shared intelligence

Module 9 Cyber Kill Chain

Overview of the Kill Chain Model

- Developed by Lockheed Martin as a framework for understanding intrusions
- Purpose: identify attacker actions at each phase to detect and disrupt
- Kill Chain vs MITRE ATT&CK — complementary frameworks

Phase 1: Reconnaissance

- Passive reconnaissance: OSINT, WHOIS, LinkedIn profiling, Google Dorking
- Active reconnaissance: Nmap scans, DNS enumeration, banner grabbing
- Defender action: monitor for scan activity, limit public information exposure

Phase 2: Weaponization

- Attacker creates malicious payload (malware, exploit, malicious document)
- Pairing exploit with backdoor for post-compromise access
- Defender action: threat intelligence feeds to identify known weaponization tools

Phase 3: Delivery

- Phishing emails, watering hole attacks, USB drops, supply chain compromise
- Web application exploits delivering payloads
- Defender action: email gateway filtering, user awareness training

Phase 4: Exploitation

- Triggering vulnerability to execute attacker code on target
- Common exploits: CVE-based RCE, macro execution in Office documents
- Defender action: patch management, application whitelisting

Phase 5: Installation

- Installing backdoor or RAT for persistent access
- Techniques: registry Run keys, scheduled tasks, WMI subscriptions
- Defender action: EDR behavioral monitoring, file integrity monitoring

Phase 6: Command & Control (C2)

- Attacker communicates with compromised host via C2 channel
- Common C2 protocols: HTTP/S, DNS tunneling, social media
- C2 frameworks: Cobalt Strike, Metasploit, Sliver, Havoc
- Defender action: DNS monitoring, outbound traffic analysis, proxy logs

Phase 7: Actions on Objectives

- Data exfiltration, ransomware deployment, lateral movement, sabotage
- Attacker achieves mission goal at this final phase
- Defender action: DLP monitoring, honeypots, SOC investigation and response

Practical Session

- Map a simulated attack lab scenario to each Kill Chain phase
- Identify whichKill Chain phase a set of SIEM alerts belongs to
- Draft a detection strategy for each phase using available SOC tools

Module 10 Pyramid of Pain

Overview of the Pyramid of Pain

- Created by David Bianco to illustrate attacker cost of IOC changes
- Higher levels cause more pain to attackers when defenders block them
- Used to prioritize what detections deliver the most defensive value

Level 1: Hash Values (Trivial)

- File hashes: MD5, SHA1, SHA256 identify specific malware samples
- Attacker workaround: recompile or modify one byte to change the hash
- Value: good for blocking known malware but trivial for attacker to bypass
- Tools: VirusTotal, SIEM hash IOC matching

Level 2: IP Addresses (Easy)

- C2 server IPs, download servers, exfiltration destinations
- Attacker workaround: migrate to a new IP or use cloud/CDN infrastructure
- Value: useful but short-lived due to ease of IP rotation
- Enrichment tools: Shodan, AbuseIPDB, GreyNoise

Level 3: Domain Names (Simple)

- C2 domains, phishing domains, malware distribution sites Attacker
- workaround: register new domain (low cost, fast)
- Value: slightly more painful — attacker must update infrastructure
- Monitoring: DNS query logs in SIEM, passive DNS databases

Level 4: Network / Host Artifacts (Annoying)

- Unique network patterns: URI paths, User-Agent strings, beacon intervals
- Host artifacts: registry keys, file paths, mutex names, pipe names
- Attacker workaround: requires code changes, increasing cost
- Value: significantly more disruptive — forces retooling

Level 5: Tools (Challenging)

- Malware families, attack frameworks (Cobalt Strike, Mimikatz), custom tools
- Attacker workaround: develop or purchase new tooling — expensive and time-consuming
- Value: very high — losing a tool disrupts operations for weeks
- Detection: YARA rules, EDR behavioral signatures, tool-specific IOCs

Level 6: TTPs (Tough)

- Tactics, Techniques, and Procedures — how the attacker operates
- Behavior-based detection that is independent of any specific tool or IOC
- Attacker workaround: extremely costly — requires retraining and rethinking operations
- Value: highest — forces attacker to fundamentally change methodology
- Mapped directly to MITRE ATT&CK techniques for detection engineering

Practical Session

- Given a malware report, categorize each IOC on the Pyramid of Pain
- Write a behavioral SIEM detection rule at the TTP level vs a simple hash rule

- Compare the detection lifetime of a hash-based rule vs a TTP-based rule

Module 11 Incident Response

What is Incident Response?

- Definition: structured approach to detecting, containing, and recovering from incidents
- IR vs emergency response vs disaster recovery
- Why IR plans are essential for minimizing breach impact

NIST Incident Response Lifecycle

- Phase 1: Preparation — IR plan, playbooks, team roles, tooling
- Phase 2: Detection & Analysis — alerts, log analysis, triage, scope assessment
- Phase 3: Containment — short-term containment, evidence preservation
- Phase 4: Eradication — remove malware, close entry points, patch vulnerabilities
- Phase 5: Recovery — restore systems, monitor for recurrence, re-enable services
- Phase 6: Post-Incident Activity — lessons learned, report, process improvement

IR Playbooks & Procedures

- What is a playbook — step-by-step guide for specific incident types
- Ransomware playbook: isolate host → image disk → notify management → rebuild
- Phishing playbook: block sender → analyze attachment → reset compromised creds
- Brute force playbook: block IP → audit affected accounts → enforce MFA
- Insider threat playbook: preserve evidence → HR coordination → access revocation

Digital Forensics for IR

- Evidence handling: chain of custody, write blockers, disk imaging
- Volatile evidence collection: memory dump, running processes, network connections
- Disk forensics: timeline analysis, deleted file recovery, artifact carving
- Tools: Autopsy, Volatility, FTK Imager, Velociraptor

Containment Strategies

- Network isolation: VLAN quarantine, firewall block, port shutdown
- Host isolation: EDR network isolation, disabling network adapters
- Account disablement: disabling compromised user and service accounts
- When to contain immediately vs preserve for investigation

Threat Hunting

- Proactive vs reactive hunting — searching without prior alerts
- Hypothesis-driven hunting using MITRE ATT&CK
- Hunting with Splunk: searching for LOLBins, PowerShell abuse, lateral movement
- Creating detections from hunting findings to improve SOC coverage

IR Communication & Reporting

- Stakeholder communication during an incident: IT, management, legal, PR
- Breach notification obligations — GDPR, CERT-In (India), US state laws
- Writing a post-incident report: timeline, impact, root cause, remediation
- Lessons learned session and IR plan improvements

Practical Session

- Simulate aransomware incident in the lab and follow the IR playbook
- Conduct memory forensics on a compromised VM using Volatility
- Write a complete post-incident report for a simulated phishing compromise
- Build a threat hunt in Splunk for signs of lateral movement

Module 12 Final Capstone Project

Project Overview

- Students perform a complete SOC analyst simulation across a 3-day exercise
- Covers monitoring, detection, analysis, threat intelligence, and incident response
- Evaluated on accuracy, thoroughness, and quality of documentation

Day 1: Monitoring & Detection

- Ingest simulated attack data into Splunk SIEM
- Triage and classify alerts by severity and attack type
- Identify true positives, false positives, and escalation candidates

Day 2: Investigation & Analysis

- Conduct deep-dive analysis on escalated alerts
- Extract and enrich IOCs using VirusTotal, OTX, and Shodan
- Map attack to the Cyber Kill Chain and MITRE ATT&CK framework
- Analyze phishing email, malicious attachment, and C2 communication artifacts

Day 3: Response & Reporting

- Execute IR playbook for identified incident type
- Perform containment actions in the lab environment
- Conduct basic forensic triage using Autopsy or Volatility
- Produce a full incident report with timeline, IOCs, impact assessment, and remediation

Labs Used

- Security Onion — network traffic monitoring and IDS alerts
- Splunk — log ingestion, SIEM detection, and dashboards
- Wazuh — host-based alert generation
- Any.run / Hybrid Analysis — malware sandbox analysis
- Autopsy / Volatility — digital forensics analysis

KIIS

15th Floor 1502 Segment Spaces,
Manjeera Trinity Corporate, KPHB,
Kukatpally, Hyderabad- 500072

Email us - **kiis@kleap.in**

Call Us - **+91 9398514034**