SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

CYBERSECURITY SOC ANALYST (L1) + SIEM ENGINEER

Course Curriculum & Training Plan

Duration	16 - 20 Weeks | 120 - 150 Hours
Training Mix	60% Practical | 40% Theory
Target Audience	Beginners, Freshers, IT Support Engineers, System Administrators, Network Engineers, SOC L1 Analysts, Junior SIEM Engineers
Modules	18 Modules + Capstone Project

Website: https://secureflowinfotech.com

Phone: +91 91884 94949 / +91 91339 19666

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Table of Contents

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Module 1 — Computer Fundamentals

Introduction to Computers

Hardware Components

- CPU
- RAM
- Storage
- BIOS/UEFI

Virtualization

- Hypervisor
- VMware
- VirtualBox

Operating Systems

- Windows Architecture
- Linux Architecture
- Processes
- Services
- Memory
- Registry
- File Systems

Module 2 — Networking Fundamentals

Network Basics

- LAN
- WAN
- MAN
- PAN
- VLAN
- VPN

OSI Model

- Everylayer in detail (Layer 1-7)
- Examples of each layer
- Troubleshooting by layer
- Packet flow

TCP/IP Model & Protocols

- TCP
- UDP
- ICMP
- ARP
- DHCP
- DNS
- HTTP
- HTTPS
- FTP
- SFTP
- SMTP
- POP3
- IMAP
- SSH
- Telnet
- SNMP
- NTP
- RDP
- LDAP
- SMB
- NetBIOS

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

IP Addressing

- IPv4
- IPv6
- CIDR
- Subnetting (practical exercises)
- Gateway
- NAT
- PAT
- Broadcast
- Multicast
- Unicast

Network Devices

- Hub
- Switch
- Router
- Firewall
- Proxy
- IDS
- IPS
- WAF
- Load Balancer
- Reverse Proxy
- VPN Gateway

Packet Analysis (Wireshark)

- Packet Capture
- TCP Handshake
- DNS Resolution
- HTTP Traffic
- TLS Handshake
- ICMP
- Packet Filtering

Module 3 — Windows Administration

Core Topics

- Windows Architecture
- Services
- Event Viewer
- Windows Logs
- Registry
- Scheduled Tasks
- PowerShell Basics
- User Accounts
- Groups
- Permissions
- NTFS
- File Shares

Module 4 — Linux Administration

Core Topics

- Linux Architecture
- Users
- Groups
- Permissions
- SSH
- Cron Jobs
- systemd
- Services
- Package Management
- Journald
- Syslog
- rsyslog
- File Permissions
- Bash Basics

Module 5 — Active Directory

Core Topics

- Domain
- Forest
- Trust
- Domain Controller
- LDAP
- Kerberos
- NTLM
- Group Policy
- User Management

Organizational Units

Authentication Flow

Module 6 — Cybersecurity Fundamentals

Core Concepts

- CIA Triad
- AAA
- Risk
- Threat
- Vulnerability
- Exploit
- CVE
- CVSS
- Attack Surface
- Defense in Depth
- Zero Trust
- Least Privilege

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Module 7 — Cyber Attack Techniques

Malware

- Virus
- Worm
- Trojan
- Ransomware
- Spyware
- Rootkit
- Botnet
- Keylogger

Social Engineering & Credential Attacks

- Phishing
- Spear Phishing
- BEC
- Password Attacks
- Credential Stuffing
- Brute Force

Web & Application Attacks

- SQL Injection
- XSS
- CSRF
- SSRF
- Command Injection
- Reverse Shell
- Living Off The Land
- Insider Threat

Module 8 — Security Technologies

Core Tools

- Antivirus
- EDR
- XDR
- SIEM
- SOAR
- IAM
- PAM
- DLP
- CASB
- Email Security
- Secure Web Gateway
- MFA

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Module 9 — SOC Operations

SOC Structure

- L1
- L2
- L3
- Threat Hunting
- Incident Response
- DFIR
- SOC Manager

Daily Operations

- Shift Handover
- Ticket Creation
- Alert Monitoring
- Incident Escalation
- Documentation
- False/True Positive Analysis
- Playbooks
- Communication
- SLA
- Severity
- Priority
- Root Cause Analysis

Incident Lifecycle

- Detection
- Validation
- Investigation
- Containment
- Eradication
- Recovery
- Lessons Learned

Case Management

- Ticketing
- Evidence Collection
- Timeline
- Documentation

Incident Response Planning

- Cyber Kill Chain
- MITRE ATT&CK; Framework
- Incident Response Plan (IRP)
- IR Team Roles & Responsibilities
- Escalation Matrix
- Communication Plan

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Module 10 — Log Management

Log Sources

- Windows Logs
- Linux Logs
- Firewall Logs
- DNS Logs
- Proxy Logs
- VPN Logs
- DHCP Logs
- Email Logs
- Authentication Logs
- Cloud Logs

Log Formats

- Syslog(RFC3164 / RFC5424)
- JSON
- CEF
- LEEF
- CSV
- XML
- UDP / TCP / TLS transport

Log Collection

- Agent Based
- Agentless
- API
- Syslog
- Event Forwarding

Module 11 — SIEM Fundamentals

SIEM Architecture

- Collection Layer
- Collector
- Parser
- Normalization
- Indexing
- Search Layer
- Detection Engine
- Dashboards
- Storage

SIEM Concepts

- Parsing
- Normalization
- Enrichment
- Correlation
- Aggregation
- Retention
- Archive

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Module 12 — SIEM Engineering

Log Source Onboarding

- Windows
- Linux
- Firewall
- DNS
- VPN
- Proxy
- Cloud
- SaaS

Data Collection

- Syslog
- API
- Agents
- Forwarders
- Event Hub

Parsing & Normalization

- Regex
- Grok
- JSON
- XML
- CSV
- Field Extraction
- Common Schema
- Field Mapping
- Timestamp Handling
- Hostname Resolution

Data Validation

- Log Verification
- Parsing Validation
- Duplicate Detection
- Time Synchronization
- Data Quality Checks

Detection Engineering

- IOCDetection
- Behavioral Detection
- Threshold Rules
- Sequence Rules
- Correlation Rules
- Statistical Detection
- Risk-based Detection
- Alert Tuning

Rule Management

- Rule Creation
- Rule Testing
- Rule Deployment
- Version Control
- Performance Optimization
- False Positive Reduction

Dashboards

- KPI Dashboards
- Executive Dashboards
- SOC Dashboards
- Compliance Dashboards

Use Cases

- Brute Force
- Impossible Travel
- Privilege Escalation
- Lateral Movement
- Malware Detection
- PowerShell Abuse
- DNS Tunneling
- Data Exfiltration
- BEC Detection
- Insider Threat

Module 13 — Threat Intelligence

Core Topics

- IOC
- TTP
- MITRE ATT&CK;
- Cyber Kill Chain
- Threat Feeds
- IOC Enrichment

Reputation Services

Module 14 — Cloud Security

Core Topics

- AWS Basics
- Azure Basics
- Google Cloud Basics
- Cloud Identity
- CloudLogs

CloudTrail

Azure Activity Logs

Microsoft 365 Logs

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Module 15 — Email Security

Core Topics

- EmailHeaders
- SPF
- DKIM
- DMARC
- Phishing Analysis
- URL Analysis
- Attachment Analysis

Module 16 — SOC Hands-on Lab

Lab Activities

- Install Windows Server
- Install Linux
- Configure Active Directory
- Configure Syslog
- Configure Windows Event Forwarding
- Generate Logs
- Install SIEM
- Create Dashboards
- Write Detection Rules
- Investigate Incidents

SECURE FLOW INFOTECH
Secure Solutions. Smart Flow. Seamless Future.

Module 17 — SIEM Engineering Lab

Lab Activities

- Onboard5Log Sources
- Parse Custom Logs
- Create Parsers
- Normalize Fields
- Build Correlation Rules
- Tune False Positives
- Build Dashboards
- Troubleshoot Log Collection
- Troubleshoot Parsing Failures
- Optimize Performance

Module 18 — Professional Skills & Capstone Project

Professional Skills

- SOC Documentation
- Writing Incident Reports
- Customer Communication
- Shift Handover Notes
- Change Management
- ITIL Basics
- Interview Preparation
- Resume Building
- Mock Interviews

Capstone Project — integrates everything learned

- Builda lab with Windows Server, Active Directory, Linux, and a firewall
- Deploy a SIEM platform and onboard at least 5 log sources
- Validate ingestion, create parsers, and normalize custom logs
- Develop and tune 10 detection rules mapped to MITRE ATT&CK;
- Build SOC dashboards for monitoring, investigations, and executive reporting
- Produce professional documentation, including onboarding guides, rule documentation, incident reports, and a final project presentation

Website: https://secureflowinfotech.com

Phone: +91 91884 94949 / +91 91339 19666