

Module 1: Networking Basics for SOC Analysts

1.1 Networking Fundamentals

What is Networking?

- Definition and importance in cybersecurity. Components of a
- network: Clients, servers, switches, and routers.

Network Models

Overview of OSI and TCP/IP models.

Key layers for SOC analysts:

- Layer 3 (Network): IP addresses and routing.
- Layer 4 (Transport): TCP/UDP and ports.
- Layer 7 (Application): HTTP, DNS, FTP, etc.

1.2 Network Protocols

- HTTP/HTTPS
- DNS
- DHCP
- FTP/SFTP
- SMTP/IMAP

Security-Relevant Protocols

- Syslog for log collection.
- SNMP for device monitoring.
- SSH for secure communication.

1.3 IP Addressing and Subnetting

- Basics of IPv4 and IPv6.
- Public vs. private IP addresses.
- Understanding subnet masks and CIDR notation.

1.4 Network Traffic and Monitoring

Ports and Services

- Well-known ports and their functions.
- Common services and their logs (e.g., web, email, DNS).

Packet Analysis Basics

- What is a packet? Understanding headers and payloads.
- Tools for packet analysis (Wireshark overview).

1.5 Network Security Concepts

- Firewalls and intrusion detection/prevention systems (IDS/IPS).
- VPNs and secure tunnelling.
- Proxy servers and their role in traffic monitoring.

Module 2: Introduction to Splunk and SOC Fundamentals

2.1 Introduction to Splunk

- What is Splunk? Overview and capabilities.
- Splunk's role in SOC operations.

Key components of Splunk:

- Splunk Enterprise
- Splunk Cloud
- Universal Forwarder

2.2 SOC Overview

- What is a Security Operations Center (SOC)?
- SOC tiers and analyst roles (Tier 1, Tier 2, Tier 3).
- Incident response lifecycle:
 - o Detection, analysis, containment, eradication, and recovery.

Module 3: Splunk Fundamentals for SOC

3.1 Setting Up Splunk

- Installing Splunk on Windows/Linux.
- Adding data sources to Splunk:
- Network logs
- Firewall logs
- Application logs

3.2 Search Processing Language (SPL) Basics

- Introduction to SPL syntax.
- Creating Knowledge Objects.
- Creating Reports, Alerts and dashboards for real time Use Cases

Basic SPL commands:

- search
- table
- fields
- stats
- Filtering and sorting results.

3.3 Field Extraction and Parsing

- Extracting fields from log data.
- Regex basics for field extraction.
- Custom field aliases and calculated fields.

Module 4: Advanced SPL and Query Building

4.1 Advanced SPL Techniques

- Using statistical commands (stats, chart, time chart).
- Event correlation across data sources (transaction).
- Creating lookup tables for enrichment.

4.2 Log Management

- Understanding log formats (JSON, Syslog, CSV).
- Parsing logs from network devices, firewalls, and servers.
- Normalizing logs using Common Information Model (CIM).

Module 5: Security Information and Event Management (SIEM)

5.1 Introduction to SIEM

- SIEM use cases in cybersecurity.
- Why Splunk is a powerful SIEM tool.

5.2 Threat Detection in Splunk

- Real-time alert creation.
- Examples of alerts:
 - Suspicious login attempts.
 - Excessive failed logins.
 - Data exfiltration anomalies.

5.3 Integration with Network Security Tools

- Onboarding logs from:
 - Firewalls (e.g., Palo Alto, Cisco ASA).
 - VPN and proxy servers.

Module 6: Threat Hunting with Splunk

6.1 Threat Intelligence

- Ingesting threat intelligence feeds.
- Matching IoCs (Indicators of Compromise) with logs.

6.2 Practical Threat Hunting

- Using SPL for threat hunting:
 - Identifying lateral movement.
 - Searching for abnormal port activity.
 - Analysing DNS queries for malware.

6.3 Leveraging MITRE ATT&CK Framework

- Mapping attack techniques to Splunk searches.
- Detecting TTPs (Tactics, Techniques, and Procedures).

Module 7: Incident Response and Forensics

7.1 Incident Investigation Workflow

- Identifying the scope of an attack.
- Analysing compromised endpoints.
- Tracing the attacker's path.

7.2 Network Forensics with Splunk

- Analysing network traffic logs.
- Investigating DNS and proxy logs.
- Correlating events from multiple network devices.

7.3 Automated Response

- Using Splunk SOAR for automated incident handling.
- Integrating Splunk with ServiceNow or Jira for case management.

Module 8: Splunk Enterprise Security (ES)

8.1 Overview of Splunk ES

- Features: Risk-based alerting, correlation searches, and data models.
- Understanding security domains in ES.

8.2 Risk-Based Alerting

- Configuring risk scores.
- Prioritizing alerts based on severity.

8.3 Splunk ES Dashboards

- Incident Review
- Security Posture
- Threat Intelligence

Module 9 :Reporting and SOC Automation

9.1 Dashboard Creation

- Building custom dashboards for monitoring.
- Best practices for visualization.

9.2 Report Generation

- Automating report generation for stakeholders.
- Customizing reports based on organizational needs.

9.3 Automation in SOC

- Automating alert actions:
 - o Email notifications
- Script execution

Module 10: Real-World Scenarios and Capstone Project

10.1 Real-World Scenarios

- Case Study 1: Investigating a phishing campaign.
- Case Study 2: Detecting and responding to a malware outbreak.
- Case Study 3: Analysing suspicious outbound traffic (data exfiltration).

10.2 Capstone Project

- Simulating a cyberattack in a lab environment.
- End-to-end workflow:
- Log ingestion
- Threat detection
- Incident response

Module 11: Interview and Certification Preparation

11.1 Splunk Certifications

- Preparing for:
- Splunk Core Certified User
- o Splunk Enterprise Security Certified Admin

11.2 SOC Analyst Interview Preparation

- Common interview questions and answers.
- Hands-on SPL exercises.
- Scenario-based problem-solving.

Module 12: Linux Fundamentals

- What is Linux? Importance in SOC operations. Linux distributions
- commonly used in cybersecurity:
- Understanding Linux file systems:
- /var/log, /etc, /bin, /usr.

12.2 Basic Linux Commands

- Navigation:
- ls, cd, pwd.
- File management:
- cat nano vi cp mv rm
- Process management:

12.3 Linux for SOC Analysts

- Reading and analyzing system logs:

Module 13: Cloud Computing Basics

13.1 Introduction to Cloud Computing

- What is cloud computing? Types of cloud services:
- Infrastructure-as-a-Service (IaaS)
- o Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS).

Cloud deployment models:

- Public, private, hybrid.

13.2 Popular Cloud Platforms

- Overview of AWS, Azure, and Google Cloud.
- **Key cloud services:**
- o Compute: EC2, Azure VMs, GCP VMs.
- Storage: S3, Azure Blob Storage, GCS.

13.3 Security in Cloud

- Shared responsibility model. Cloud security best
- practices: Access control Encryption

13.4 Working with Cloud Servers

- Setting up a virtual machine on AWS/Azure/GCP.
- Connecting to cloud servers using SSH. Monitoring
- cloud server logs.