Introduction to Cyber security

- Evolution of Cyber Security
- Cyber Security Awareness & Situational Context
- Cyber Security Skills Gap
- Information Security vs Cyber Security
- Cyber Security Objectives and Goals
- Cyber Security Roles and Career Pathways

Network Fundamentals (Prerequisites)

- Evolution of Cyber Security
- Cyber Security Awareness & Situational Context
- Cyber Security Skills Gap and Industry Demand
- Information Security vs Cyber Security
- Cyber Security Objectives and Principles
- Cyber Security Roles and Career Pathways
- Infrastructure Terminology and Components
- Security-Focused Network Design Principles
- Network Topology and Architecture
- OSI Model and TCP/IP Framework
- IPv4 and IPv6 Addressing
- Essential Network Ports and Protocols
- Firewalls and Intrusion Prevention Systems (IPS)
- VPN Technologies and VPN Concentrators
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Proxy Servers and Load Balancers
- Network Access Control (NAC)
- Zero Trust Architecture
- Secure Mail Gateways

Security Operations Center (SOC)

Security Operations Center (SOC)

- SOC Overview
- SOC Team Structure
- SOC Roles and Responsibilities

SOC Analyst Tiers

- Tier 1 Responsibilities
- Tier 2 Responsibilities
- Tier 3 Responsibilities

SOC Operations & Workflow

- SOC Workflow and Escalation Path
- Alert Lifecycle Stages
- Incident Response Phases
- Types of Alerts Handled in SOC
- Daily SOC Monitoring Activities

SOC Performance & Metrics

- Key Performance Indicators (KPIs) and Metrics

Log Management in SOC

- Log Collection Strategy
- Log Parsing and Normalization
- Key SOC Log Sources
- Firewall Logs
- IDS/IPS Logs
- DNS Logs
- Endpoint Logs (Sysmon / EDR)
- Active Directory Logs
- Cloud Logs (AWS CloudTrail, Azure Activity Logs)

SIEM & Detection Engineering

- Use Case Design in SIEM

- Rule Writing (SPL – Splunk, AQL – QRadar)
- MITRE ATT&CK Mapping to Alerts

Threat Detection & Response

- Threat Hunting Basics
- Alert Enrichment Techniques
- Alert Suppression and False Positive Handling

SOC Tools & Processes

- Ticketing System Integration (ServiceNow, JIRA)
- Shift Handover Protocol

SIEM and EDR Focus

SIEM

- Introduction to SIEM
- Overview of Splunk Architecture
- Splunk Data Ingestion and Indexing
- Writing SPL Queries
- Splunk Dashboards and Alerts
- QRadar Architecture and Flow Collection
- QRadar Rule Creation using CRE
- AQL Querying in QRadar

EDR

- Introduction to EDR
- SentinelOne Architecture
- SentinelOne Agent Capabilities
- Remote Response Actions
    - Kill Process
    - Quarantine
    - Rollback

Malware Analysis

Malware Analysis

- Introduction to Malware Analysis
- Malware Categories
    - Virus
    - Worm
    - Trojan
    - Ransomware
    - Spyware
    - Rootkit
    - Fileless Malware
- Malware Behavior and Infection Chain

Static Analysis

- Static Analysis Fundamentals
- File Header and Metadata Check
- String Extraction (strings, FLOSS)
- PE Header Inspection
- Hashing (MD5, SHA256) and Use Cases

Dynamic Analysis

- Dynamic Analysis Overview
- Sandbox Analysis (Any.run, Cuckoo)
- Tools for Monitoring Malware Behavior
    - ProcMon
    - RegShot
    - Wireshark
    - TCPView

Reverse Engineering Basics

- Introduction to Reverse Engineering
- Disassemblers (Ghidra, IDA Free)

- Debuggers (x64dbg, OllyDbg)
- Packers and Obfuscation

Indicators of Compromise (IOCs)

- IOC Extraction Process
- Types of IOCs
    - File Hashes
    - Registry Keys
    - IP Addresses and Domains
    - File Names

Email Security

Email Security & Phishing Analysis

- Overview of Email-Based Threats
- Anatomy of a Phishing Email
- Spear Phishing vs Generic Phishing
- Business Email Compromise (BEC)
- Malware Delivery via Email
- Spoofing and Lookalike Domains

Email Authentication & Headers

- Email Header Components
- Email Flow and Received Headers
- SPF Record Validation
- DKIM Signature Verification
- DMARC Policy Enforcement

Email Security Tools

- Microsoft Defender for Office 365
- Cisco Email Security Appliance (ESA)
- Proofpoint
- Mimecast

- Email Sandbox Solutions

SOC Response to Phishing Incidents

- SOC Response to Phishing
- IOC Search in Mailboxes
- Quarantining and Purging Malicious Emails
- User Awareness and Reporting Channels

Threat Intelligence

Threat Intelligence

- Threat Intelligence Fundamentals
- Threat Intelligence Lifecycle Stages

Types of Threat Intelligence

- Strategic Threat Intelligence
- Tactical Threat Intelligence
- Operational Threat Intelligence
- Technical Threat Intelligence

Indicators of Compromise (IOC)

- IOC Formats (IP, Hash, URL, Domain)

Threat Intelligence Sources & Feeds

- VirusTotal
- AlienVault OTX
- Recorded Future
- Shodan
- URLScan.io

Threat Frameworks & SIEM Integration

- MITRE ATT&CK Overview
- IOC Enrichment in SIEM

Digital Forensics (Basic)

Digital Forensics

- Introduction to Digital Forensics
- Role of Forensics in Incident Response

Evidence Handling

- Evidence Identification
- Chain of Custody Requirements
- Legal Considerations for Digital Evidence

Disk & File Forensics

- Disk Imaging using FTK Imager
- File Recovery and Analysis

System & Application Artifacts

- Windows Registry Artifact Locations
- Browser History and Cache Inspection
- Event Log Collection

Analysis Techniques

- Timeline Analysis Basics
- Memory Analysis using Volatility

Investigation Outcomes

- Role of Forensics in Root Cause Analysis

Cloud Security

Cloud Security Fundamentals

- Cloud Security Fundamentals
- Shared Responsibility Model

Cloud Threat Landscape

- Common Cloud Infrastructure Threats
- Misconfigured Storage Buckets (e.g., S3)

- Cloud Resource Exploitation
- Unmonitored API Calls and Access Keys
- Credential Theft from Code Repositories
- Cloud Identity and Access Attacks
- Lateral Movement in Cloud Environments
- Lack of Visibility and Logging in Cloud

Mobile Security – Threats Only

Cloud Security Fundamentals

- Cloud Security Fundamentals
- Shared Responsibility Model

Cloud Infrastructure Threats

- Cloud Infrastructure Threats
- Misconfigured Storage Buckets (e.g., S3)
- Cloud Resource Exploitation
- Unmonitored API Calls and Access Keys
- Credential Theft from Code Repositories
- Cloud Identity Attacks
- Lateral Movement in Cloud Environments
- Lack of Visibility and Logging