

Comprehensive Cybersecurity Roadmap

Prepared for ISOC: A structured, phased learning pathway designed to build elite operational, analytical, and governance capabilities without prerequisite gaps.

Design Philosophy: This curriculum arranges courses progressively from foundational IT and networking to advanced security operations, threat intelligence, detection engineering, and purple teaming, alongside distinct GRC and offensive tracks.

MASTER FLOW ARCHITECTURE

Network → Security → SOC → SIEM → IR/DFIR → Threat Hunting / Purple Team

COMPLETE ROADMAP STAGES

- Phase 0: IT & Computer Fundamentals
- Phase 1: CompTIA Network+
- Phase 2: Cisco CCNA
- Phase 3: Linux + Windows Server / AD
- Phase 4: CompTIA Security+
- Phase 5: Network Security & Firewalls
- Phase 6: Wireshark & Traffic Analysis
- Phase 7: SOC Analyst Tier 1
- Phase 8: SIEM (Splunk / ELK)
- Phase 9: SOC Analyst Tier 2
- Phase 10: Incident Response
- Phase 11: DFIR
- Phase 12: Threat Hunting + Intelligence
- Phase 13: Detection Engineering
- Phase 14: Purple Team
- Phase 15: ISO 27001 (ISMS / GRC)
- Phase 16 & 17: CISM & CISSP Management
- Optional: CEH → Pentesting → OSCP

IT & Computer Fundamentals

Prerequisite baseline knowledge required before Network+ to understand computer systems and network services.

HARDWARE & OS FUNDAMENTALS

- Hardware Fundamentals
- CPU / RAM / Storage
- Operating Systems
- Windows Fundamentals
- Linux Fundamentals
- Files & Filesystems
- Processes & Services

SYSTEM ARCHITECTURE & CLOUD

- Users & Groups
- Command Line Interface
- Virtualization
- Client / Server Concept
- Application / Service Concept
- Cloud Computing Concepts

Core Objective: Master how a computer system and network service function under the hood.

CompTIA Network+

Comprehensive foundational network infrastructure principles and protocol operations.

NETWORK FUNDAMENTALS

- OSI Model & TCP/IP Model
- Encapsulation & Ethernet
- MAC Address & IP Address
- IPv4 & IPv6
- Subnetting & CIDR
- Public / Private IP
- Unicast / Multicast / Broadcast

PROTOCOLS & SWITCHING

- TCP, UDP, ICMP, ARP
- DNS, DHCP, HTTP / HTTPS
- SSH, FTP / SFTP, SMTP
- IMAP / POP3, SNMP, NTP
- Switch & VLAN Architecture
- Access & Trunk Ports, STP
- MAC Address Table

ROUTING & TROUBLESHOOTING

- Router & Routing Table
- Static & Dynamic Routing
- Default Gateway & NAT
- OSPF Fundamentals
- ping, traceroute, nslookup
- ipconfig / ifconfig / ip
- netstat / ss, arp, route

Cisco CCNA

Translating theoretical network principles into hands-on practical implementation skills.

CORE SYLLABUS

- Ethernet, VLANs & Trunking
- STP & Inter-VLAN Routing
- IPv4 / IPv6 Subnetting & Routing
- OSPF, NAT, DHCP & DNS
- ACLs & Wireless Networking
- Network Security Fundamentals
- Network Automation Fundamentals
- Network Troubleshooting

PRACTICAL LABS

- Cisco Packet Tracer Environment
- Small Network Design Lab
- VLAN Configuration Lab
- Routing Configuration Lab
- DHCP Deployment Lab
- ACL Security Lab
- Troubleshooting Simulation Lab

Linux + Windows Server / Active Directory

Essential operating system and directory services architecture critical for Security Operations.

LINUX & LINUX SECURITY

- Architecture, CLI & Filesystem
- Users, Groups, Permissions & Processes
- Services, systemd & Package Mgmt
- Bash Scripting, SSH & Networking
- Firewalls, Logs, Monitoring & Backup
- Authentication & SSH Security
- System Logs, Audit Logs & Monitoring

WINDOWS SERVER & ACTIVE DIRECTORY

- Architecture & Active Directory Domains
- Domain Controllers, OUs & Group Policy
- DNS, DHCP & File Services
- PowerShell & Windows Event Logs
- Authentication: Kerberos & NTLM
- Windows Security & Monitoring
- Identity, Auth, Authz & GPO Auditing

CompTIA Security+

Core security principles, infrastructure hardening, and defensive operations.

SECURITY & NETWORK SECURITY

- CIA Triad, AAA & Non-repudiation
- Security Controls, Defense in Depth
- Zero Trust, Risk, Vulnerability & Threat
- Attack Surface Management
- Firewalls, IDS, IPS, VPN
- Network Segmentation & Secure Protocols
- Wireless Security & NAC

IAM, CRYPTOGRAPHY & OPERATIONS

- MFA, SSO, RBAC & Privileged Access
- Identity Management Systems
- Encryption, Hashing, Symmetric/Asymmetric
- Digital Signatures, PKI, Certificates, TLS
- Logging, Monitoring & Vulnerability Mgmt
- Incident Response, Risk Mgmt & Compliance

Network Security & Firewalls

Deploying advanced network protection mechanisms and enterprise firewall platforms.

NETWORK SECURITY & FIREWALLS

- Security Architecture & Defense in Depth
- Network Segmentation & VLAN Security
- ACLs, IDS/IPS, WAF & DDoS Concepts
- VPN, Remote Access & Zero Trust
- Firewall Architecture & Security Policies
- NAT, Application Control & URL Filtering
- TLS Inspection, High Availability & Logging

FORTINET & PALO ALTO PLATFORMS

- Fortinet Admin, Routing, NAT & Policies
- FortiGate VPN, Auth, IPS & Web Filtering
- Application Control, Logging & HA
- Palo Alto Admin, Security Policies & NAT
- Routing, VPN & User Identification
- Threat Prevention, URL Filtering & HA

Wireshark & Network Traffic Analysis

Deep protocol analysis and suspicious traffic investigation using Wireshark.

PROTOCOL ANALYSIS

- Ethernet, ARP, IPv4 & IPv6
- TCP, UDP & ICMP Protocol Mechanics
- DNS & DHCP Transaction Analysis
- HTTP & TLS Protocol Inspection

WIRESHARK INVESTIGATIONS

- Packet Capture & PCAP Management
- Display Filters, Conversations & Endpoints
- Follow TCP Stream & DNS Investigation
- TCP Handshake & Connection Analysis
- Suspicious Traffic & Incident Analysis

SOC Analyst — Tier 1

Entering the Security Operations Center with operational monitoring and alert triage.

SOC FUNDAMENTALS

- SOC Architecture & Roles
- Security Monitoring
- Events, Logs & Alerts
- Ticket Management
- Incident Classification
- Severity & Priority
- Escalation & Documentation

ALERT TRIAGE

- Alert Investigation Workflow
- False Positives vs. True Positives
- IOC Tracking & Analysis
- IP, Domain, URL & Hash Evaluation
- Phishing Indicators
- Authentication Events
- Endpoint & Network Events

MITRE ATT&CK

- Tactics, Techniques & Procedures
- Attack Lifecycle Framework
- Mapping Alerts to ATT&CK Matrix

SIEM (Splunk / ELK Stack)

Core log management, correlation, and event monitoring platforms.

SIEM FUNDAMENTALS

- Log Collection & Ingestion
- Parsing & Normalization
- Correlation & Detection
- Alerting & Dashboards
- Investigation & Monitoring

SPLUNK TRACK

- Data Inputs & Indexes
- Events, Fields & Search
- Splunk Search Processing Language (SPL)
- Reports, Dashboards & Alerts
- Correlation & Data Models
- Detection Rules

ELK / ELASTIC STACK

- Elasticsearch & Logstash
- Kibana & Beats
- Elastic Agent Deployment
- Data Ingestion & Indexing
- Querying & Dashboards
- Elastic Security Detection

SOC Analyst — Tier 2

Advancing from alert triage to deep technical investigation and threat hunting.

ADVANCED INVESTIGATION

- Advanced Alert Investigation
- Threat Hunting Methodologies
- Threat Intelligence Integration
- MITRE ATT&CK Deep Alignment
- Attack Chain Analysis

FORENSICS & ENGINEERING

- IOC Correlation & Hunting
- Endpoint & Network Investigation
- Root Cause Analysis (RCA)
- Detection Engineering Concepts
- Incident Escalation & Reporting

Incident Response

Managing security incidents through structured operational lifecycles.

Preparation ↓ Detection ↓ Analysis ↓ Containment ↓ Eradication ↓ Recovery ↓ Lessons Learned

RESPONSE OPERATIONS

- Incident Classification & Severity
- Evidence Collection Procedures
- IOC Management & Tracking
- Active Investigation Workflows
- Containment Strategies & Isolation

RESOLUTION & REVIEW

- Eradication & System Recovery
- Documentation & Communication
- Escalation Paths & Procedures
- Incident Report Generation
- Post-Incident Review (Lessons Learned)

DFIR (Digital Forensics & Incident Response)

Digital evidence preservation and deep forensic examination methodologies.

DIGITAL FORENSICS

- Digital Evidence & Preservation
- Chain of Custody Standards
- Disk Forensics & Filesystem Artifacts
- Memory Forensics & Volatile Data
- Windows, Linux & Browser Artifacts
- Timeline Analysis & Reconstruction

INVESTIGATION & REPORTING

- Host & Network Investigation
- Malware Analysis Concepts
- IOC Analysis & Root Cause Analysis
- Evidence Correlation
- Forensic Report Preparation

Threat Hunting + Threat Intelligence

Proactive adversary hunting and threat intelligence feed integration.

HUNTING FRAMEWORKS

- Threat Hunting Fundamentals
- Hypothesis-Based Hunting
- IOC Hunting & TTP Hunting
- MITRE ATT&CK Alignment

OPERATIONAL HUNTING

- Endpoint, Network & DNS Hunting
- Authentication & SIEM Hunting
- EDR Hunting Queries
- Threat Intelligence Integration
- Detection Gaps Identification

Detection Engineering & Purple Team

Creating custom detections and integrating Red and Blue team operations.

Red Team ↔ Purple Team ↔ Blue Team

DETECTION ENGINEERING

- Detection Fundamentals & Logic
- SIEM & EDR Detection Rules
- Sigma Rule Concepts
- IOC & TTP-Based Detection
- False Positive Reduction & Testing

PURPLE TEAM OPERATIONS

- Purple Team Fundamentals
- Adversary Emulation & Simulation
- TTP Analysis & Control Validation
- Detection Gap Analysis
- Defensive Improvement & Metrics

ISO 27001 (ISMS / GRC)

Information Security Management Systems, risk frameworks, and auditing standards.

AWARENESS

- Information Security
- ISMS Frameworks
- CIA Triad Principles
- Risk-Based Approach
- Security Policies

IMPLEMENTATION

- ISMS Scope & Assets
- Risk Assessment
- Risk Treatment Plans
- Statement of Applicability
- Policies, Procedures & Goals
- Continuous Improvement

AUDITING

- Audit Principles & Planning
- Audit Checklists & Evidence
- Interviews & Findings
- Nonconformity Tracking
- Corrective Actions & Reporting

CISM & CISSP (Management & Architecture)

Executive management, governance, and advanced security architecture.

CISM GOVERNANCE DOMAINS

- Information Security Governance
- Information Security Risk Management
- Information Security Program
- Incident Management Leadership

CISSP EIGHT DOMAINS

- Security & Risk Management
- Asset Security & Architecture
- Communications & Network Security
- Identity & Access Management (IAM)
- Security Assessment & Testing
- Security Operations & Software Security

Offensive Security (CEH → Pentesting → OSCP)

Optional offensive security curriculum for penetration testing and red teaming.

CEH (CERTIFIED ETHICAL HACKER)

- Reconnaissance & Scanning
- Enumeration & Vulnerability Assessment
- Network & Web Security
- Wireless & Social Engineering
- Cryptography & Malware Concepts
- Cloud & IoT Security

PENETRATION TESTING

- Recon & Vulnerability Identification
- Security Testing Methodologies
- Linux, Windows & Web Applications
- Active Directory Exploitation
- Privilege Escalation Concepts
- Reporting & Remediation

OSCP-LEVEL ADVANCED

- Advanced Networking & Scripting
- Enumeration & Vulnerability Analysis
- Exploitation & Privilege Escalation
- Active Directory & Web Security
- Pivoting Concepts & Reporting

ISOC Strategic Career Framework

Structuring professional development tracks based on organizational goals.

SOC OPERATIONS TRACK

IT Fundamentals → Network+ → CCNA → Linux + Windows/AD → Security+ → Network Security/Firewall → Wireshark → SOC Tier 1 → SIEM → SOC Tier 2 → Incident Response → DFIR → Threat Hunting → Detection Engineering → Purple Team

MANAGEMENT & GRC TRACK

Security+ → ISO 27001 → ISMS / Risk Management → CISM → CISSP

OFFENSIVE SECURITY TRACK

Network+ → Linux → Security+ → CEH → Pentesting → Advanced Pentesting → OSCP

Strategic Note: SOC/SIEM/IR roles focus primarily on the operational path. ISO 27001/CISM/CISSP serve GRC and management, while CEH/OSCP cater to penetration testing.