Cybersecurity Practitioner

Network Security, Vulnerability Assessment & Security Operations

Target Audience

High School Students (Grades 9–12) and learners who have completed **Cybersecurity Foundations** or have basic knowledge of computers, operating systems, networking, Python, and cybersecurity concepts. Prior cybersecurity experience beyond the Foundations pathway is not required.

Program Pathway

Cybersecurity Foundations → Cybersecurity Practitioner

Total Duration

84 Hours

Delivery

Cohort-Based + Instructor-Led + Hands-On Labs

Program Goal

The Cybersecurity Practitioner program builds upon the foundational knowledge developed in Cybersecurity Foundations and introduces students to practical cybersecurity operations, network security, vulnerability assessment, ethical hacking fundamentals, security monitoring, incident response, identity and access management, and cloud security.

Students progress from understanding cybersecurity concepts to **applying security techniques in controlled and authorized environments**. Through instructor-led instruction, guided labs, security scenarios, assessments, and a final cybersecurity operations capstone, students develop practical skills for identifying vulnerabilities, analyzing security events, responding to incidents, and recommending security controls.

The program prepares students for progression into the **Cybersecurity Specialist** pathway.

Program Structure

Module	Topic	Hours
Module 1	Network Security & Secure Infrastructure	**18**
Module 2	Vulnerability Assessment & Ethical Hacking Fundamentals	**18**
Module 3	Security Monitoring, Threat Detection & SIEM Fundamentals	**16**
Module 4	Incident Response, Digital Investigation & Identity Security	**16**
Module 5	Cloud Security & Cybersecurity Operations Capstone	**16**
Total		**84 Hours**

Curriculum

Module 1 – Network Security & Secure Infrastructure

Students build upon networking knowledge from Cybersecurity Foundations and learn how networks are protected against unauthorized access, attacks, and security threats.

Topics:

Network Security Fundamentals, Secure Network Architecture, Network Attack Surface, Network Security Controls, Security Zones, Network Segmentation, VLAN Security, DMZ Fundamentals, Firewalls, Firewall Rules, Network Access Control, Router Security Fundamentals, Switch Security Fundamentals, Port Security, Wireless Security, Wi-Fi Security Standards, Secure Remote Access, VPN Security, Encryption Fundamentals, TLS & Secure Communication, Secure Protocols, DNS Security, DHCP Security, Network Traffic Analysis, Packet Analysis Fundamentals, Network Monitoring, Network Hardening, Secure Network Configuration, Common Network Attacks, Denial-of-Service Fundamentals, Man-in-the-Middle Attack Concepts, ARP Spoofing Concepts, Rogue Access Points, Network Security Policies.

Module 2 – Vulnerability Assessment & Ethical Hacking Fundamentals

Students learn how cybersecurity professionals identify weaknesses in systems and applications through authorized security testing. The module introduces ethical hacking methodology, vulnerability assessment, risk prioritization, and security remediation.

Topics:

Introduction to Ethical Hacking, Ethical Hacking Principles, Cybersecurity Ethics, Authorized Security Testing, Rules of Engagement, Attack Surface Fundamentals, Reconnaissance Fundamentals, Passive Reconnaissance, Active Reconnaissance Concepts, Asset Discovery, Service Discovery, Port Scanning Concepts, Vulnerability Assessment, Vulnerability Scanning Fundamentals, Security Misconfigurations, Outdated Software, Weak Authentication, Unnecessary Services, Web Application Security Fundamentals, Authentication Weaknesses, Authorization Issues, Input Validation, Injection Concepts, Cross-Site Scripting Fundamentals, Session Security, Password Security Testing Concepts, CVE Fundamentals, CVSS Fundamentals, Vulnerability Severity, Risk Prioritization, Security Findings, Vulnerability Reports, Remediation Recommendations, Responsible Disclosure.

Module 3 – Security Monitoring, Threat Detection & SIEM Fundamentals

Students learn how security teams monitor systems and networks to identify suspicious behavior, investigate security alerts, and detect potential cyber threats.

Topics:

Security Operations Fundamentals, Security Operations Center (SOC), Security Monitoring, Security Events, Security Alerts, Log Fundamentals, Windows Event Logs, Linux Logs, Application Logs, Firewall Logs, Network Logs, Authentication Logs, DNS Logs, Web Server Logs, Log Collection, Log Analysis, Event Correlation, Indicators of Compromise, Indicators of Attack, Suspicious Login Activity, Failed Authentication Attempts, Unusual Network Activity, Suspicious Processes, Malware Indicators, Phishing Indicators, Threat Intelligence Fundamentals, Threat Intelligence Sources, IP Addresses, Domains, URLs, File Hashes, Security Alerts, Alert Triage, False Positives, Threat Detection Fundamentals, SIEM Fundamentals, SIEM Components, SIEM Use Cases, Security Dashboards, Security Monitoring Workflows, Incident Escalation, Security Documentation.

Module 4 – Incident Response, Digital Investigation & Identity Security

Students learn how cybersecurity teams identify, investigate, contain, and respond to security incidents while applying identity and access controls to protect systems and data.

Topics:

Incident Response Fundamentals, Incident Response Lifecycle, Preparation, Detection, Analysis, Containment, Eradication, Recovery, Lessons Learned, Incident Classification, Incident Severity, Incident Response Plans, Incident Documentation, Incident Communication, Evidence Preservation, Digital Forensics Fundamentals, Digital Evidence, Chain of Custody, File Metadata, File Hashes, Timeline Analysis, Basic Digital Artifacts, Phishing Investigation, Malware Investigation Fundamentals, Account Compromise Investigation, Security Breach Scenarios, Identity & Access Management, IAM Fundamentals, Authentication, Authorization, Accounting, User Accounts, Groups & Roles, Role-Based Access Control, Least Privilege, Privileged Accounts, Password Policies, Multi-Factor Authentication, Single Sign-On Fundamentals, Access Reviews, Account Monitoring, Credential Theft, Account Takeover, Secure Identity Practices.

Module 5 – Cloud Security & Cybersecurity Operations Capstone

Students are introduced to cloud-security concepts and apply the knowledge developed throughout the Practitioner pathway to a practical cybersecurity operations project.

Topics:

Cloud Computing Fundamentals, IaaS, PaaS & SaaS, Cloud Deployment Models, Cloud Security Fundamentals, Shared Responsibility Model, Cloud Identity & Access Management, Cloud Users & Roles, Least Privilege in Cloud Environments, Cloud Authentication, Virtual Networks, Cloud Network Security, Security Groups, Network Access Controls, Cloud Firewalls, Cloud Storage Security, Data Protection, Encryption at Rest, Encryption in Transit, Cloud Logging, Cloud Monitoring, Cloud Security Alerts, Cloud Misconfiguration Risks, Publicly Exposed Resources, Credential Security, Account Compromise, Cloud Threats, Cloud Incident Response, Security Automation Fundamentals, Cybersecurity Operations, Security Policies, Risk Assessment, Security Controls, Security Documentation, Capstone Planning, Security Assessment, Security Recommendations, Final Presentation.

Cybersecurity Operations Capstone

Students apply concepts from the Practitioner pathway to a controlled cybersecurity scenario involving:

- Asset and risk identification
- Network-security analysis
- Vulnerability identification
- Security misconfiguration analysis
- Log and alert analysis
- Threat identification
- Identity and access review
- Cloud-security assessment
- Incident-response planning
- Security-control recommendations
- Security assessment documentation
- Final presentation

Hands-On Learning

Students learn through instructor-led lessons, cybersecurity demonstrations, network-security exercises, authorized vulnerability-assessment activities, security-monitoring exercises, log-analysis activities, incident-response scenarios, identity-security activities, cloud-security exercises, assessments, mini-projects, and a final Cybersecurity Operations Capstone.

Students progressively move from **understanding security concepts to applying, analyzing, documenting, and responding to cybersecurity situations**.

What Students Build

Students develop practical experience with:

- Network security and secure network architecture
- Firewalls and network access controls
- Network segmentation and wireless security
- VPNs and secure communication
- Network traffic and packet analysis
- Network hardening
- Vulnerability assessment
- Asset and service discovery
- Ethical hacking methodology
- Security misconfiguration identification
- CVE and CVSS fundamentals

- Vulnerability prioritization
- Security findings and remediation
- Security monitoring and alert analysis
- Windows and Linux logs
- Network, firewall, and authentication logs
- Indicators of compromise
- Threat detection fundamentals
- SIEM fundamentals
- SOC workflows and alert triage
- Incident response
- Digital investigation fundamentals
- Evidence preservation
- Phishing and account-compromise investigation
- Identity and access management
- Role-based access control
- Least privilege
- Multi-factor authentication
- Cloud security fundamentals
- Cloud IAM and network security
- Cloud logging and monitoring
- Cloud misconfiguration risks
- Cybersecurity risk assessment
- Security documentation
- Incident-response planning
- Final cybersecurity operations assessment

Recommended Lab Requirements

Each student should ideally have:

- Windows or Mac desktop/laptop
- **8 GB RAM minimum**
- **16 GB RAM recommended**
- **20 GB+ free storage recommended**

Windows or Mac systems are recommended.

Students may use Linux through a virtual machine or cloud-based environment for selected cybersecurity labs.

Virtual machines, cloud-based environments, cybersecurity training platforms, and isolated laboratory networks may be used for selected vulnerability assessment, network security, monitoring, and incident-response exercises.

A dedicated GPU is **not required** for this program.

All scanning, vulnerability assessment, ethical hacking, and security-testing activities should be conducted only in **authorized laboratory environments or systems where explicit permission has been provided**.

Next Step

Students who complete **Cybersecurity Practitioner** will have developed practical skills in network security, vulnerability assessment, security monitoring, threat detection, incident response, identity security, and cloud security.

Students can progress to the next pathway:

Cybersecurity Specialist

The Specialist pathway can introduce advanced areas such as **Advanced Ethical Hacking, Penetration Testing, Threat Hunting, Malware Analysis, Digital Forensics, Advanced SIEM, Security Engineering, Advanced Network Defense, Cloud Security Engineering, Security Automation, Advanced Incident Response, and Security Architecture.**