Cybersecurity Specialist

Advanced Ethical Hacking, Threat Hunting, Digital Forensics & Security Engineering

Target Audience

High School Students (Grades 9–12) and learners who have completed **Cybersecurity Practitioner** or have basic knowledge of networking, operating systems, Python, vulnerability assessment, security monitoring, incident response, identity security, and cloud security. Prior advanced cybersecurity experience is not required.

Program Pathway

Cybersecurity Foundations → Cybersecurity Practitioner → Cybersecurity Specialist

Total Duration

96 Hours

Delivery

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

Program Goal

The Cybersecurity Specialist program builds upon the practical knowledge developed in Cybersecurity Practitioner and introduces students to advanced cybersecurity operations, ethical hacking, threat hunting, digital forensics, malware analysis, advanced security monitoring, cloud security, security engineering, and cybersecurity automation.

Students progress from performing basic security assessments to **analyzing sophisticated threats, investigating security incidents, conducting controlled security testing, developing defensive strategies, and designing security controls**.

Through instructor-led instruction, guided hands-on labs, security scenarios, assessments, investigations, and a final cybersecurity capstone, students develop practical skills for analyzing attacks, identifying threats, investigating incidents, strengthening security architectures, and recommending appropriate security controls.

The program prepares students for progression into an **Advanced Cybersecurity / Cybersecurity Engineering Capstone** pathway.

Program Structure

Module	Topic	Hours
Module 1	Advanced Network Defense & Ethical Hacking	**20**
Module 2	Threat Hunting, Advanced SIEM & Security Analytics	**20**
Module 3	Digital Forensics & Malware Analysis Fundamentals	**18**
Module 4	Advanced Incident Response, Cloud Security & Security Engineering	**20**
Module 5	Cybersecurity Automation & Specialist Security Capstone	**18**
Total		**96 Hours**

Curriculum

Module 1 – Advanced Network Defense & Ethical Hacking

Students build upon Practitioner-level network security and vulnerability-assessment skills and learn advanced techniques for analyzing, testing, and defending enterprise networks.

Topics:

Advanced Network Security, Defense-in-Depth, Secure Network Architecture, Network Segmentation, Micro-Segmentation, Zero Trust Concepts, Advanced Firewall Security, Next-Generation Firewalls, Network Access Control, Secure Routing and Switching, Network Device Hardening, Advanced VLAN Security, Wireless Security, Enterprise Wi-Fi Security, Rogue Access Points, Evil Twin Concepts, Network Attack Techniques, ARP Spoofing, DNS Attacks, Man-in-the-Middle Concepts, Denial-of-Service Concepts, Network Reconnaissance, Asset Discovery, Service Enumeration, Controlled Port Scanning, Vulnerability Identification, Ethical Hacking Methodology, Security Testing, Web Application Security Fundamentals, Authentication Testing, Authorization Testing, Injection Concepts, Session Security, Attack-Chain Analysis, MITRE ATT&CK Fundamentals, Security Control Validation, Network Defense Strategies, Security Testing Documentation.

Module 2 – Threat Hunting, Advanced SIEM & Security Analytics

Students progress from basic security monitoring to proactive threat hunting and advanced analysis of security events using SIEM and security analytics concepts.

Topics:

Advanced Security Operations, SOC Architecture, Threat Hunting Fundamentals, Threat Hunting Methodology, Security Analytics, Advanced Log Analysis, Windows Security Events, Linux Logs, Network Logs, DNS Logs, Firewall Logs, Authentication Logs, Cloud Logs, Log Collection, Log Normalization, Event Correlation, Security Baselines, Anomaly Detection Concepts, Indicators of Compromise, Indicators of Attack, Threat Intelligence, IOC Enrichment, IP and Domain Analysis, File Hash Analysis, Threat Actor Fundamentals, MITRE ATT&CK Tactics and Techniques, Detection Engineering, SIEM Architecture, SIEM Data Sources, SIEM Queries, Correlation Rules, Detection Rules, Alert Prioritization, Alert Triage, False Positive Analysis, Security Dashboards, Detection Use Cases, Endpoint Detection and Response Fundamentals, Network Detection Concepts, Threat Hunting Reports, SOC Documentation.

Module 3 – Digital Forensics & Malware Analysis Fundamentals

Students learn how cybersecurity investigators collect, preserve, and analyze digital evidence while developing an introductory understanding of malware behavior and investigation.

Topics:

Digital Forensics Fundamentals, Forensic Investigation Process, Digital Evidence, Evidence Identification, Evidence Collection, Evidence Preservation, Chain of Custody, Evidence Integrity, Hashing, File Metadata, File Systems, Windows Artifacts, Linux Artifacts, Browser Artifacts, Authentication Artifacts, Event Logs, System Logs, File Timeline Analysis, User Activity Analysis, Process Analysis, Network Connection Analysis, Memory Forensics Concepts, Disk Forensics Concepts, Forensic Imaging Concepts, Deleted File Concepts, Evidence Analysis, Timeline Reconstruction, Phishing Investigation, Account Compromise Investigation, Malware Investigation Fundamentals, Malware Types, Virus, Worm, Trojan, Ransomware, Spyware, Rootkit Concepts, Malware Delivery Methods, Malware Execution Concepts, Static Analysis Fundamentals, Dynamic Analysis Fundamentals, Strings Analysis, Malware Indicators, Suspicious Processes, Persistence Concepts, Command-and-Control Fundamentals, Sandbox Concepts, Forensic and Malware Reporting.

Module 4 – Advanced Incident Response, Cloud Security & Security Engineering

Students integrate advanced incident-response techniques with cloud security and security-engineering principles used to protect modern technology environments.

Topics:

Advanced Incident Response, Incident Classification, Incident Severity, Incident Coordination, Incident Analysis, Advanced Containment, Eradication Strategies, Recovery Planning, Incident Communications, Breach Investigation, Account Compromise Response, Malware Incident Response, Ransomware Response Fundamentals, Phishing Campaign Response, Insider Threat Concepts, Evidence Preservation, Root Cause Analysis, Post-Incident Analysis, Lessons Learned, Security Engineering Fundamentals, Security Architecture, Defense-in-Depth, Secure-by-Design Principles, Security Control Selection, Preventive Controls, Detective Controls, Corrective Controls, Administrative and Technical Controls, Zero Trust Security, Identity-Centric Security, Privileged Access Management Fundamentals, Advanced IAM, Cloud Security Architecture, Cloud IAM, Cloud Network Security, Cloud Access Policies, Cloud Storage Security, Encryption, Key Management Fundamentals, Cloud Logging, Cloud Monitoring, Cloud Security Posture Concepts, Cloud Misconfiguration Detection, Cloud Incident Response, Cloud Security Risk Assessment, Security Architecture Documentation.

Module 5 – Cybersecurity Automation & Specialist Security Capstone

Students learn how automation and scripting can improve cybersecurity operations and integrate the knowledge gained throughout the Specialist pathway into a comprehensive cybersecurity project.

Topics:

Cybersecurity Automation Fundamentals, Python for Security Automation, Security Scripting, File and Directory Analysis, Log Processing, Automated IOC Analysis, IP and Domain Analysis, Hash Analysis, Security Data Processing, Automated Security Checks, Security APIs, Alert Enrichment, Security Orchestration Concepts, SOAR Fundamentals, Automated Incident Workflows, Security Reporting Automation, Vulnerability Data Processing, Threat Intelligence Automation, Security Configuration Validation, Automated Security Monitoring, Defensive Scripting, Secure Coding Practices, Automation Risks, Error Handling, Security Logging, Threat Modeling, Security Assessment Methodology, Risk Analysis, Security Architecture Review, Security Control Recommendations, Capstone Planning, Security Investigation, Threat Analysis, Security Testing, Defensive Design, Security Documentation, Final Presentation.

Hands-On Learning

Students learn through instructor-led lessons, cybersecurity demonstrations, controlled ethical-hacking activities, advanced network-defense exercises, vulnerability assessments, SIEM investigations, threat-hunting scenarios, digital-forensics activities, malware-analysis exercises, cloud-security assessments, Python security-automation activities, incident-response simulations, security-engineering exercises, assessments, and a final **Cybersecurity Specialist Capstone**.

Students progressively move from **understanding security concepts to applying, analyzing, investigating, engineering, and defending cybersecurity environments**.

What Students Build

Students develop practical experience with:

- Advanced network defense and secure architecture

- Network segmentation and Zero Trust concepts
- Advanced firewall and wireless security
- Ethical hacking and controlled security testing
- Vulnerability and attack-surface analysis
- Web-security testing fundamentals
- MITRE ATT&CK and attack-chain analysis
- Threat hunting and security analytics
- SIEM and detection engineering
- IOC and threat-intelligence analysis
- Security alert investigation
- Digital forensics and evidence preservation
- Timeline and artifact analysis
- Malware-analysis fundamentals
- Phishing and account-compromise investigations
- Advanced incident response
- Root-cause analysis
- Cloud security architecture
- Cloud IAM and cloud monitoring
- Cloud misconfiguration analysis
- Security engineering and defense-in-depth
- Python-based security automation
- Security orchestration concepts
- Risk assessment and security-control design
- Professional cybersecurity documentation
- Final Specialist cybersecurity assessment

Recommended Lab Requirements

Each student should ideally have:

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

Windows or Mac systems are recommended.

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

Virtual machines, cloud environments, cybersecurity training platforms, and isolated laboratory networks may be used for ethical hacking, vulnerability assessment, SIEM investigation, threat hunting, digital forensics, malware-analysis demonstrations, incident-response scenarios, cloud-security exercises, and security automation.

A dedicated GPU is **not required**.

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

Next Step

Students who complete **Cybersecurity Specialist** will have developed advanced skills in ethical hacking, network defense, threat hunting, SIEM, digital forensics, malware analysis, incident response, cloud security, security engineering, and cybersecurity automation.

Students can progress to:

Cybersecurity Engineering Capstone

The next pathway can introduce **Advanced Penetration Testing, Red Team and Blue Team Operations, Advanced Threat Hunting, Malware Reverse Engineering, Advanced Digital Forensics, Detection Engineering, Security Architecture, DevSecOps, Cloud Security Engineering, Advanced Zero Trust, Security Automation, Security Orchestration, and an enterprise-level cybersecurity engineering capstone.**