CYBERSECURITY ENGINEERING CAPSTONE

Advanced Security Engineering, Penetration Testing, Detection Engineering, Cloud Security & Cyber Defense

Target Audience

High School Students (Grades 9–12) and learners who have completed **Cybersecurity Specialist** or have strong foundational knowledge of networking, operating systems, Python, ethical hacking, vulnerability assessment, SIEM, threat hunting, digital forensics, incident response, cloud security, and security engineering. Prior professional cybersecurity experience is not required.

Program Pathway

Cybersecurity Foundations → Cybersecurity Practitioner → Cybersecurity Specialist → Cybersecurity Engineering Capstone

Total Duration

108 Hours

Delivery

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

Program Goal

The Cybersecurity Engineering Capstone program represents the advanced stage of the cybersecurity pathway and focuses on applying cybersecurity knowledge to **design, build, test, monitor, and improve secure technology environments**.

Students progress beyond individual security tools and techniques and begin working with cybersecurity from an **engineering and enterprise-defense perspective**. The program introduces advanced penetration testing, red team and blue team operations, advanced threat hunting, detection engineering, digital forensics, malware analysis concepts, cloud security engineering, Zero Trust architecture, DevSecOps, security automation, security orchestration, and enterprise security architecture.

Through instructor-led instruction, guided hands-on labs, security scenarios, attack-and-defense exercises, investigations, engineering activities, assessments, and a comprehensive final capstone, students learn to **identify security risks, engineer defensive controls, validate security architectures, investigate attacks, automate security operations, and communicate professional security recommendations**.

The program prepares students for advanced study and progression into cybersecurity engineering, security operations, penetration testing, cloud security, security architecture, threat detection, and related cybersecurity disciplines.

Program Structure

Module	Topic	Hours
Module 1	Advanced Penetration Testing & Red/Blue Team Operations	**22**
Module 2	Advanced Threat Hunting & Detection Engineering	**22**
Module 3	Advanced Digital Forensics, Malware Analysis & Incident Investigation	**20**
Module 4	Cloud Security Engineering, Zero Trust & DevSecOps	**22**
Module 5	Security Automation, Security Architecture & Engineering Capstone	**22**
Total		**108 Hours**

Curriculum

Module 1 – Advanced Penetration Testing & Red/Blue Team Operations

Students build upon Specialist-level ethical-hacking knowledge and learn how offensive and defensive security teams work together to identify, validate, and mitigate security weaknesses in controlled environments.

Topics:

Advanced Penetration Testing Methodology, Penetration Testing Lifecycle, Rules of Engagement, Scope Definition, Reconnaissance, Advanced Network Enumeration, Service Discovery, Vulnerability Validation, Attack-Surface Analysis, Exploitation Concepts, Privilege Escalation Fundamentals, Credential Security Testing, Password Attack Concepts, Active Directory Security Fundamentals, Windows Security Testing, Linux Security Testing, Web Application Security Testing, API Security Fundamentals, Authentication and Authorization Testing, Session Security, Injection Vulnerabilities, Security Misconfiguration, Controlled Exploitation, Post-Exploitation Concepts, Attack-Chain Development, Lateral Movement Concepts, Persistence Concepts, Command-and-Control Concepts, MITRE ATT&CK, Red Team Operations, Blue Team Operations, Purple Team Concepts, Attack Simulation, Defensive Validation, Security Control Testing, Network Defense, Endpoint Defense, Attack Detection, Threat Containment, Penetration Testing Documentation, Executive Security Reporting.

Module 2 – Advanced Threat Hunting & Detection Engineering

Students progress from security monitoring to designing and validating detection capabilities that identify sophisticated attacks across networks, endpoints, identities, and cloud environments.

Topics:

Advanced Threat Hunting, Threat Hunting Lifecycle, Hypothesis-Driven Hunting, Intelligence-Driven Hunting, Threat Actor Analysis, Advanced IOC Analysis, Indicators of Attack, Behavioral Indicators, Tactics Techniques and Procedures, MITRE ATT&CK Mapping, Advanced Log Analysis, Windows Event Analysis, Linux Security Logs, Network Telemetry, DNS Analytics, Firewall Telemetry, Authentication Events, Endpoint Telemetry, Cloud Security Logs, SIEM Architecture, Advanced SIEM Queries, Event Correlation, Detection Engineering, Detection Logic, Detection Rules, Detection Use Cases, Behavioral Detection, Signature-Based Detection, Anomaly Detection, Baseline Analysis, Alert Engineering, Alert Prioritization, False Positive Reduction, Detection Validation, Detection Coverage, MITRE ATT&CK Coverage Mapping, Threat Intelligence Integration, IOC Enrichment, Security Dashboards, Endpoint Detection and Response, Network Detection and Response Concepts, Security Analytics, Threat Hunting Reports, Detection Documentation, Purple Team Detection Validation.

Module 3 – Advanced Digital Forensics, Malware Analysis & Incident Investigation

Students develop advanced investigative skills by analyzing digital evidence, reconstructing attack timelines, investigating compromised systems, and studying malware behavior in controlled environments.

Topics:

Advanced Digital Forensics, Forensic Investigation Lifecycle, Evidence Identification, Evidence Collection, Evidence Preservation, Chain of Custody, Evidence Integrity, Forensic Hashing, Disk Forensics, File-System Analysis, Windows Forensic Artifacts, Linux Forensic Artifacts, Browser Artifacts, Authentication Artifacts, Registry Analysis Fundamentals, Event Log Analysis, File Timeline Analysis, User Activity Reconstruction, Process Analysis, Network Connection Analysis, Memory Forensics Concepts, Memory Artifact Analysis, Deleted File Analysis, Data Recovery Concepts, Phishing Investigation, Credential Compromise Investigation, Account Takeover Investigation, Malware Investigation, Malware Families, Malware Delivery Techniques, Malware Execution, Static Malware Analysis, Dynamic Malware Analysis, Strings and Metadata Analysis, Suspicious File Analysis, Persistence Mechanisms, Process Injection Concepts, Command-and-Control Analysis, Sandbox Analysis, Malware Indicators, Attack Timeline Reconstruction, Root-Cause Analysis, Incident Evidence Correlation, Forensic Reporting, Investigation Presentation.

Module 4 – Cloud Security Engineering, Zero Trust & DevSecOps

Students learn how modern security engineering integrates cloud infrastructure, identity security, application security, Zero Trust principles, and secure software-development practices.

Topics:

Cloud Security Engineering, Cloud Security Architecture, Shared Responsibility Model, Cloud Identity and Access Management, Identity-Centric Security, Privileged Access Management, Authentication and Authorization, Role-Based Access Control, Least Privilege, Cloud Network Security, Virtual Networks, Security Groups, Network Access Controls, Cloud Firewalls, Secure Connectivity, Cloud Storage Security, Data Protection, Encryption, Key Management, Secrets Management, Cloud Logging, Cloud Monitoring, Cloud Security Posture Management Concepts, Cloud Misconfiguration Detection, Cloud Risk Assessment, Cloud Incident

Response, Zero Trust Architecture, Zero Trust Principles, Continuous Verification, Micro-Segmentation, Device and Identity Trust, Policy Enforcement, Application Security, Secure Software Development, DevSecOps Fundamentals, Security in CI/CD Pipelines, Source-Code Security, Dependency Security, Secrets Detection, Software Composition Analysis Concepts, Infrastructure-as-Code Security, Container Security Fundamentals, Image Security, Kubernetes Security Concepts, Security Testing Automation, Secure Deployment Practices, Cloud Security Documentation.

Module 5 – Security Automation, Security Architecture & Engineering Capstone

Students integrate the knowledge gained throughout the cybersecurity pathway to design and implement a comprehensive cybersecurity engineering solution.

Topics:

Cybersecurity Engineering Principles, Enterprise Security Architecture, Security Architecture Frameworks, Defense-in-Depth, Security Control Design, Preventive Controls, Detective Controls, Corrective Controls, Identity Security, Network Security Architecture, Endpoint Security Architecture, Cloud Security Architecture, Zero Trust Architecture, Security Segmentation, Security Policy Design, Risk Assessment, Threat Modeling, Attack-Path Analysis, Security Requirements, Security Control Selection, Security Architecture Review, Security Automation, Python Security Automation, Automated Log Analysis, IOC Processing, Hash Analysis, IP and Domain Analysis, Security APIs, Threat Intelligence Automation, Automated Security Validation, Security Configuration Auditing, Security Orchestration, SOAR Concepts, Automated Incident Response, Security Workflow Design, DevSecOps Automation, Security Monitoring Automation, Reporting Automation, Automation Security Risks, Error Handling, Secure Coding, Security Logging, Capstone Planning, Security Architecture Design, Security Testing, Attack Simulation, Detection Validation, Incident Investigation, Risk Analysis, Security Control Recommendations, Technical Documentation, Executive Reporting, Final Presentation, Capstone Defense.

Hands-On Learning

Students learn through instructor-led lessons, advanced cybersecurity demonstrations, controlled penetration-testing exercises, red team and blue team simulations, threat-hunting investigations, detection-engineering activities, digital-forensics investigations, malware-analysis exercises, cloud-security assessments, Zero Trust architecture activities, DevSecOps security

exercises, Python-based security automation, security-architecture design, incident-response simulations, and an enterprise-style **Cybersecurity Engineering Capstone**.

Students progressively move from **performing security activities to engineering, validating, automating, and defending complete cybersecurity environments**.

What Students Build

Students develop practical experience with:

- Advanced penetration testing methodology
- Red team and blue team operations
- Purple team security validation
- Attack-chain analysis
- Active Directory security fundamentals
- Advanced network and web security testing
- MITRE ATT&CK-based security analysis
- Advanced threat hunting
- Detection engineering
- SIEM detection development
- EDR and network detection concepts
- Threat intelligence integration
- Detection coverage analysis
- Advanced digital forensics
- Malware investigation and analysis
- Attack timeline reconstruction
- Incident investigation and root-cause analysis
- Cloud security engineering
- Zero Trust architecture
- Identity and privileged-access security
- DevSecOps security
- Container and infrastructure security fundamentals
- Security architecture design
- Threat modeling and risk analysis
- Python-based security automation
- Security orchestration concepts
- Automated security validation
- Security-control design
- Enterprise security documentation
- Executive security reporting
- Final cybersecurity engineering capstone

Recommended Lab Requirements

Each student should ideally have:

- Windows or Mac desktop/laptop
- **8 GB RAM minimum**
- **16 GB RAM recommended**
- **40 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 activities.

Virtual machines, isolated laboratory networks, cloud environments, cybersecurity training platforms, SIEM platforms, security monitoring environments, and controlled attack-and-defense environments may be used for penetration testing, threat hunting, detection engineering, digital forensics, malware-analysis demonstrations, incident-response exercises, cloud-security engineering, DevSecOps activities, Zero Trust exercises, and security automation.

A dedicated GPU is **not required**.

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

Program Outcome

Students who complete **Cybersecurity Engineering Capstone** will have progressed from foundational cybersecurity concepts to advanced **security engineering and enterprise cyber defense**.

They will understand how offensive security, defensive security, threat intelligence, detection engineering, digital forensics, incident response, cloud security, Zero Trust, DevSecOps, automation, and security architecture work together as part of a modern cybersecurity program.

The capstone provides students with experience in **designing, testing, analyzing, automating, and defending cybersecurity environments**, preparing them for advanced academic programs, cybersecurity competitions, internships, and future pathways in

cybersecurity engineering, penetration testing, security operations, threat detection, cloud security, security architecture, and related fields.