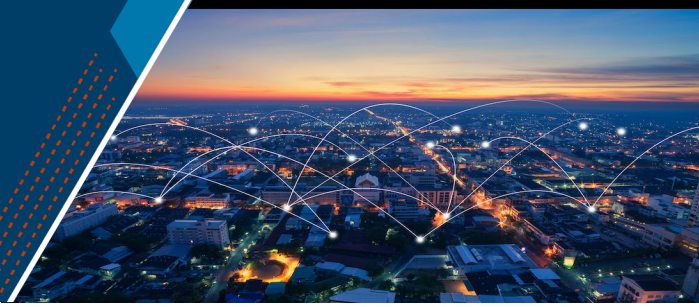
DEFENSIVE CYBERSECURITY PATHWAY



DEFENSIVE CYBERSECURITY PATHWAY

The **Defensive Cybersecurity Pathway** is a comprehensive 12-week, instructor-led cybersecurity training course designed to build expertise in cybersecurity defense and vulnerability analysis. Starting with foundational principles accessible to those with minimal technical background, participants progress through increasingly advanced topics including vulnerability detection, web application security, and cloud infrastructure assessments. The course combines theoretical knowledge with extensive hands-on experience using industry-standard tools and frameworks. By completion, students develop proficiency in computer architecture, operating systems, networking, cloud computing, and cybersecurity fundamentals. They gain practical experience in vulnerability assessments, security configurations, and compliance requirements while mastering the creation of technical documentation for various audiences. The course culminates with advanced concepts including Artificial Intelligence in vulnerability assessment, preparing graduates to tackle complex cybersecurity challenges in today's digital landscape.

KEY LEARNING OUTCOMES

- Implement basic system security controls
- Differentiate between cloud service models (IaaS, PaaS, SaaS)
- Understand the vulnerability management lifecycle
- Configure web servers securely
- Apply artificial intelligence and machine learning in vulnerability assessment

CAREER OPPORTUNITIES RELATED TO THIS SUBJECT

- Security Analyst
- Security Engineer
- Vulnerability Assessment Specialist
- Systems Security Administrator
- Cloud Security Engineer
- Information Security Specialist
- Security Operations Analyst
- IT Security Consultant

PATHWAY METRICS

- Course Duration: 12-Weeks (480 hours)
- CPE Credits: 480 Hours
- Certification: CompTIA Security+

This document is marked TLP: CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

PROFICIENCY LEVEL: CYBERSECURITY BASICS

Participants should have basic technical literacy and a general understanding of IT and cybersecurity principles; however, no prior hands-on experience with system security tools or frameworks is required. This course welcomes beginners by starting with essential concepts and then gradually building foundational skills in secure system design, analysis, and assessment.

Although this course is open to beginners, it includes hands-on practice, lab exercises, and real-world simulations, offering more advanced professionals the opportunity to further refine their skills and core competencies in practical scenarios.

TARGET AUDIENCE

This pathway is designed for individuals who want to build or strengthen their foundational skills in cybersecurity with a focus on systems security analysis. It is especially suited for:

- Aspiring cybersecurity analysts and entry-level security practitioners
- IT personnel expanding into security-focused roles
- Students or recent graduates with a technical background looking to specialize in system security
- Government staff supporting system administration, risk management, or compliance activities

RECOMMENDED PREREQUISITES:

While the prerequisites listed are recommended to help you successfully complete the course, they are not mandatory. If you are confident in your skills and capabilities and can dedicate the time needed to fully engage in the training material, we encourage you to apply. All Pathway courses are live instructor-led to help facilitate learning and skill development for participants across broad skill levels.

To ensure readiness for the hands-on and technical aspects of the course, participants should ideally have the following exposure and proficiencies prior to enrolling:

- Basic proficiency with computers and operating systems (Windows/Linux), command-line navigation, and general understanding of file systems, folders, and application usage.
- Basic understanding of IT systems, including patch management, software updates, and common misconfigurations. *No prior experience in system hardening, vulnerability scanning, or deep operating systems knowledge is needed.*
- Familiarity with threat intelligence and attack lifecycle (Cybersecurity Kill Change) and MITRE ATT&CK, and experience with firewalls, IDS/IPS, and endpoint protection.
- Comfort using basic command-line, including directory navigation, file operations, user commands, and introductory scripting capabilities. *No automation or tool-specific experience is required; however, it may be advantageous during training in lab environments.*

DEFENSIVE CYBERSECURITY COURSE OUTLINE

Week 1: Introduction to Computing and Security Basics: *A foundational introduction to computing and security fundamentals, combining theoretical concepts with hands-on experience in binary systems, operating systems, and command-line interfaces through virtual lab environments.*

Week 1 Learning Outcomes:

- Understand and explain basic binary and computing concepts
- Navigate operating system environments confidently
- Execute basic command-line operations
- Set up and manage virtual lab environments
- Apply fundamental security principles
- Interpret basic technical terminology
- Implement basic system security controls
- Document technical processes effectively

Week 2: Networking Fundamentals: *A comprehensive exploration of computer networking principles, focusing on practical experience with network analysis tools and protocols through guided exercises in traffic analysis and network troubleshooting.*

Week 2 Learning Outcomes:

- Explain TCP/IP protocols and the OSI model
- Using Wireshark for basic packet analysis
- Perform network traffic analysis
- Understand network topologies
- Execute basic network troubleshooting
- Map network communications
- Identify common network protocols
- Recognize basic network security issues

Week 3: Cloud Computing Essentials: *An introduction to cloud computing technologies, providing hands-on experience with major cloud platforms while exploring service models and security considerations through practical exercises.*

Week 3 Learning Outcomes:

- Differentiate between cloud service models (IaaS, PaaS, SaaS)
- Create and manage basic cloud instances
- Implement cloud security best practices
- Apply the shared responsibility model
- Navigate major cloud platforms
- Configure basic cloud services
- Understand cloud networking concepts
- Implement basic cloud security controls

Week 4: Security Operations Basics: *A practical introduction to security operations, combining essential tool usage and log analysis with incident response fundamentals through hands-on exercises in security monitoring and documentation.*

Week 4 Learning Outcomes:

- Utilize essential security tools
- Analyze basic system logs
- Follow incident response procedures
- Apply security frameworks
- Create security documentation
- Implement security monitoring basics
- Understand security operations workflow
- Perform basic security assessments

Week 5: Vulnerability Management Foundations: *An overview of vulnerability management practices, featuring hands-on experience with professional scanning tools and practical training in vulnerability assessment methodologies through guided exercises.*

Week 5 Learning Outcomes:

- Understand the vulnerability management lifecycle
- Use CVE and CVSS scoring systems
- Configure basic vulnerability scanners
- Operate Nessus and OpenVAS
- Interpret vulnerability scan results
- Create basic vulnerability reports
- Prioritize vulnerability remediation
- Implement vulnerability management processes

Week 6: System Security Assessment: *A detailed exploration of system security evaluation and hardening techniques, focusing on practical implementation of security controls and patch management through real-world system assessments.*

Week 6 Learning Outcomes:

- Assess system security baselines
- Identify system misconfigurations
- Implement system hardening techniques
- Manage system patches effectively
- Conduct system security audits
- Document security findings
- Create system hardening guidelines
- Verify security controls

Week 7: Network Vulnerability Analysis: *An advanced examination of network security assessment, combining port scanning and enumeration techniques with wireless security evaluation through comprehensive hands-on exercises.*

Week 7 Learning Outcomes:

- Perform comprehensive port scanning
- Execute network enumeration
- Assess network services
- Evaluate wireless network security
- Implement network security controls
- Conduct network vulnerability assessments
- Create network security baselines
- Document network security findings

Week 8: Vulnerability Assessment Tools: *A thorough review of professional vulnerability assessment tools, emphasizing advanced scanning configurations and enterprise-scale implementation through practical exercises with industry-standard platforms.*

Week 8 Learning Outcomes:

- Master advanced vulnerability scanner features
- Create custom scan policies
- Compare multiple tool results
- Generate professional reports
- Optimize scan configurations
- Interpret complex scan results
- Manage enterprise vulnerability programs
- Implement automated scanning solutions

Week 9: Web Technologies and Security: *A comprehensive introduction to web security testing, featuring hands-on experience with professional tools and practical training in identifying common web vulnerabilities through guided assessments.*

Week 9 Learning Outcomes:

- Understand HTTP/HTTPS protocols
- Configure web servers securely
- Use Burp Suite and OWASP ZAP
- Identify common web vulnerabilities
- Assess web architecture security
- Implement web security controls
- Test web application security
- Document web security findings

Week 10: Web Application Security Assessment: *An advanced exploration of web application security testing, focusing on authentication, session management, and injection vulnerabilities through practical exercises with professional testing tools.*

Week 10 Learning Outcomes:

- Test authentication mechanisms
- Evaluate session management
- Assess input validation
- Identify XSS and SQL injections
- Use advanced Burp Suite features
- Create web application test plans
- Generate web security reports
- Recommend security improvements

Week 11: Cloud Security Assessment: *A specialized review of cloud security evaluation, covering container security and serverless architectures through hands-on exercises with cloud-native security tools and platforms.*

Week 11 Learning Outcomes:

- Assess cloud infrastructure security
- Evaluate container security
- Understand serverless security
- Using cloud security tools
- Implement cloud security controls
- Conduct cloud security audits
- Create cloud security baselines
- Document cloud security findings

Week 12: Integration and Advanced Concepts: *A culminating integration of security concepts with emerging technologies, featuring a comprehensive capstone project and CTF exercise focused on* real-world *vulnerability assessment scenarios.*

Week 12 Learning Outcomes:

- Apply AI/ML in vulnerability assessment
- Complete comprehensive security assessments
- Write professional security reports
- Prioritize security findings
- Participate in CTF exercises
- Present security findings
- Integrate multiple security tools
- Develop comprehensive security programs