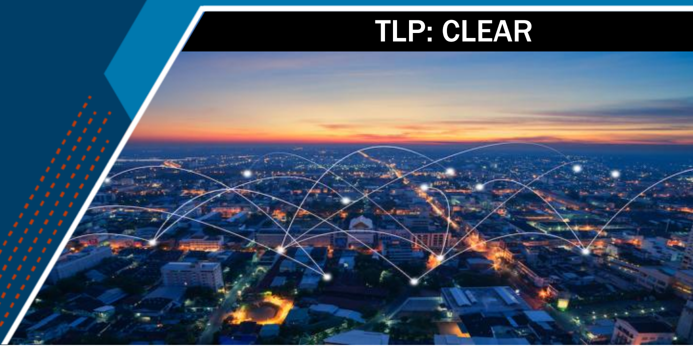
DEFENSIVE CYBERSECURITY PATHWAY



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 security tools, risk management, and security frameworks through virtual lab environments.*

Week 1 Learning Outcomes:

- Understand and apply fundamental security concepts including CIA Triad
- Identify and differentiate between physical and technical security controls
- Recognize common cyber threats, threat actors, and attack vectors
- Understand social engineering techniques and vulnerabilities
- Apply Risk Management Framework (RMF) steps and processes
- Comprehend the relationship between RMF and SDLC
- Implement NIST Cybersecurity Framework
- Understand cryptography basics and its role in security
- Navigate and configure virtual lab environments
- Execute basic change management procedures
- Document security processes and compliance requirements

Week 2: Security Architecture and Defense: *A comprehensive exploration of security architecture principles, focusing on access control models, secure network design, and defensive monitoring strategies through hands-on implementation of security controls and monitoring systems.*

Week 2 Learning Outcomes:

- Understand Identification, Authentication & Authorization (IA&A) systems
- Identify different access control models
- Recognize Area of Responsibility (AoR) based controls
- Comprehend secure network architecture principles and logical security zones
- Understand firewall configurations and remote access firewall architectures
- Identify IDS/IPS system capabilities and deployment options
- Navigate log monitoring and management solutions
- Recognize anti-malware defensive strategies
- Understand patch management processes
- Comprehend application whitelisting concepts
- Navigate Active Directory and Group Policy security features
- Execute basic internal security best practices for prevention
- Identify detection methods and monitoring approaches
- Document basic security architecture concepts

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:

- Understand cloud reference architecture and service deployment models (IaaS, PaaS, SaaS)
- Identify security aspects of virtualization and cloud model boundaries
- Comprehend principles of secure cloud computing and design requirements
- Navigate AWS key services and Microsoft Azure fundamentals
- Recognize methods for protecting sensitive information in the cloud
- Understand threat modeling concepts for cloud environments
- Identify cloud data security lifecycle and data retention requirements
- Comprehend Information Rights Management (IRM) and Digital Rights Management (DRM)
- Navigate cloud platform and infrastructure security features
- Understand cloud security strategies and operations
- Recognize cloud platform risks and shared responsibility models
- Identify third-party risks and management approaches

- Understand Cloud Security Alliance (CSA) STAR framework

Week 4: Security Operations Basics: *A practical introduction to security operations, combining essential network protocol analysis and security controls with hands-on exercises in network monitoring and access control fundamentals.*

Week 4 Learning Outcomes:

- Understand network protocols and their basic functionality
- Identify security implications of common network protocols
- Recognize secure protocol alternatives and their uses
- Comprehend different types of network security controls
- Understand implementation strategies for security controls
- Navigate methods for measuring control effectiveness
- Identify important security measurements and metrics
- Comprehend network monitoring strategies and approaches
- Recognize monitoring tool categories and selection criteria
- Understand alert configuration basics
- Navigate network access control policies
- Identify authentication methods and their applications
- Comprehend authorization control mechanisms
- Execute basic security operations documentation

Week 5: Vulnerability Management Foundations: *An overview of vulnerability management practices, featuring hands-on experience with IDS/IPS systems, network segmentation, and advanced firewall technologies through guided exercises.*

Week 5 Learning Outcomes:

- Understand IDS/IPS fundamentals and detection methods
- Identify different IDS/IPS system types and their uses
- Comprehend implementation strategies for detection systems
- Recognize signature development basics and rule creation principles
- Understand pattern matching concepts and false positive reduction
- Navigate IDS/IPS configuration and tuning methodologies
- Identify performance optimization approaches for security systems
- Comprehend network segmentation design principles
- Understand segmentation implementation strategies and security benefits
- Recognize next-generation firewall features and capabilities
- Navigate application control concepts and policies
- Identify advanced firewall policy requirements
- Execute basic vulnerability management processes
- Document detection and prevention configurations

Week 6: System Security Assessment: *A detailed exploration of system security evaluation techniques, focusing on SIEM (Security Information and Event Management) architecture, log analysis, and security analytics through hands-on implementation exercises.*

Week 6 Learning Outcomes:

- Assess SIEM architecture components and deployment models
- Implement basic SIEM design considerations
- Configure log source integration from multiple systems
- Identify various log source types and collection methods
- Implement parser configuration for log normalization
- Develop basic correlation rules for security events
- Configure logic implementation for event detection
- Create security alerts based on correlation rules
- Implement SIEM analytics capabilities
- Design security dashboards for monitoring

- Develop basic security reports
- Configure key security metrics
- Assess system security posture using SIEM data
- Document SIEM implementation and findings

Week 7: Network Vulnerability Analysis: *An advanced examination of network security assessment, combining endpoint security technologies and application control strategies with comprehensive hands-on exercises in detection and response.*

Week 7 Learning Outcomes:

- Assess endpoint security fundamentals and protection types
- Implement endpoint deployment strategies
- Configure endpoint management solutions
- Deploy EDR (Endpoint Detection and Response) capabilities
- Implement automated response features
- Integrate EDR with existing security infrastructure
- Develop application control and whitelisting strategies
- Create application control policies
- Implement application control methods
- Configure endpoint monitoring strategies
- Design alert configurations for endpoint threats
- Develop response procedures for endpoint incidents
- Assess network vulnerabilities through endpoint analysis
- Document endpoint security architecture and findings
- Implement network security controls

Week 8: Vulnerability Assessment Tools: *A thorough review of professional vulnerability assessment tools, emphasizing system hardening, patch management, and configuration standards through practical exercises with industry-standard platforms.*

Week 8 Learning Outcomes:

- Implement security baselines and configuration standards
- Develop hardening strategies for diverse systems
- Assess system vulnerabilities using professional tools
- Configure Windows security hardening measures
- Implement Linux security best practices
- Deploy OS-specific security controls
- Develop patch management strategies
- Implement patch deployment methods
- Test patch effectiveness and system stability
- Create configuration management policies
- Implement change control procedures
- Develop documentation for security requirements
- Assess configuration compliance
- Validate hardening effectiveness
- Generate vulnerability assessment reports

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:

- Assess web application architecture and security components
- Identify and analyze common web vulnerabilities
- Implement web application security controls

- Analyze OWASP Top 10 vulnerability categories
- Evaluate attack methods and vectors
- Develop defense strategies for web applications
- Implement secure development practices and coding standards
- Configure input validation and output encoding
- Deploy authentication and authorization mechanisms
- Implement session management controls
- Configure Web Application Firewalls (WAF)
- Develop WAF rules and policies
- Create monitoring strategies for web applications
- Test web application security posture
- Document web security findings and recommendations

Week 10: Web Application Security Assessment: *An advanced exploration of web application security testing, focusing on security automation, SOAR platforms, and automated response capabilities through practical exercises with orchestration tools.*

Week 10 Learning Outcomes:

- Implement Security Orchestration, Automation and Response (SOAR) platforms
- Evaluate automation use cases for web application security
- Develop implementation strategies for security automation
- Design security playbooks for incident response
- Implement playbook logic and decision trees
- Test and validate playbook effectiveness
- Configure API integrations for security tools
- Develop tool integration workflows
- Implement automated data flow between systems
- Create automated response strategies
- Configure automation rules and triggers
- Validate automated response procedures
- Assess web application security through automated testing
- Generate automated security reports
- Document automation workflows and procedures

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

Week 11 Learning Outcomes:

- Perform comprehensive cloud security assessments
- Evaluate multi-cloud security architectures
- Implement advanced IAM configurations across cloud platforms
- Develop enterprise-level role management strategies
- Create and enforce complex access policies
- Design secure multi-region VPC architectures
- Configure advanced security group rules and network ACLs
- Implement zero-trust network security in cloud environments
- Deploy advanced storage security controls
- Configure encryption key management systems
- Implement data loss prevention (DLP) strategies
- Assess cloud compliance and governance
- Automate cloud security monitoring and response
- Generate executive-level cloud security reports
- Validate cloud security controls against frameworks

Week 12: Integration and Advanced Concepts: *A culminating integration of all security concepts with focused preparation for the CompTIA Security+ certification exam through comprehensive review, practice questions, and a hands-on Capture The Flag (CTF) exercise.*

Week 12 Learning Outcomes:

- Summarize fundamental security concepts for certification readiness
- Master CompTIA Security+ exam objectives and domains
- Complete practice questions and certification-focused labs
- Demonstrate proficiency in security control implementation
- Participate in Capture The Flag (CTF) security challenges
- Apply vulnerability assessment and exploitation techniques in CTF scenarios
- Execute performance-based questions and simulations
- Analyze practice test results to identify knowledge gaps
- Develop exam-taking strategies and time management skills
- Synthesize security concepts across multiple domains
- Validate hands-on security skills through CTF competition