Federal Cyber Defense Skilling Academy

FY25 Course Catalog

Cybersecurity and Infrastructure Security Agency

FEDERAL CYBER DEFENSE SKILLING ACADEMY

PROGRAM OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) Federal Cyber Defense Skilling Academy (Skilling Academy) provides virtual cybersecurity training at no cost for full-time federal employees, focusing on professional growth and interactive learning. This program is designed for participants at all levels, from beginners to advanced, who are looking to enhance their knowledge and skills in cybersecurity. The coursework is mapped to the NICE Workforce Framework for Cybersecurity and offers federal employees valuable experience to practice new skills.

MICRO-COURSES

In FY25, the Skilling Academy will be offering micro-courses, which are condensed,**self-paced,** 100% virtual training offerings, designed to equip federal employees with foundational and specialized cybersecurity skills. Each course emphasizes practical training to ensure that participants gain real-world experience in protecting and defending against cyber threats. Through this targeted training, participants will learn introductory skills to help prepare them to take on essential cybersecurity roles, enhancing the security and resilience of the nation's infrastructure. The self-paced nature of these micro-courses allows students to progress through the material at their own pace throughout the 40- or 80- hour course.

Please note, Skilling Academy Micro-course offerings do not include any third-party certification vouchers for participants to sit for a certification exam.

PATHWAYS

Skilling Academy Pathways are designed for students to go through an intense, full-time, 4 to 12-week accelerated training program. Pathway students are provided with valuable opportunities to practice cybersecurity skills in a 100% virtual environment. Pathway courses are **live** and led by an online instructor. Students will be required to attend Monday through Friday from 8 a.m. to 5 p.m. ET for the entire duration of the course (excluding federal holidays and predetermined session breaks). Students will not be able to maintain their alternative work schedule during the session.

ELIGIBILITY REQUIREMENTS AND HOW TO APPLY

Eligibility: All full-time federal employees, in any job series and any grade or grade equivalent for non-General Schedule (GS) employees, are eligible to apply to CISA's Federal Cyber Defense Skilling Academy. Government contractors are not permitted to participate.

Participation in the Skilling Academy is prioritized for individuals from Departments and Agencies within the Federal Civilian Executive Branch. Applications from other federal government entities are welcome and will be considered based on course availability and program requirements. Please speak with your supervisor before applying to ensure that you can fulfill the Skilling Academy's attendance requirements.

How to Apply: Interested applicants must submit a completed Supervisor and Applicant Agreement form to SkillingAcademy@cisa.dhs.gov.The form must be electronically signed using a digital certificate (i.e., PIV or CAC).

FY25 MICRO-COURSE DATES

Micro-Course Title & Session Number	Length	Course Start & End Date	Application Close Date*
IT Fundamentals – Session 1	2 weeks	1/27/2025 – 2/7/2025	1/10/2025
IT Fundamentals – Session 2	2 weeks	3/24/2025 – 4/4/2025	3/7/2025
IT Fundamentals – Session 3	2 weeks	6/2/2025 – 6/13/2025	5/16/2025
Intro to Forensic Analysis – Session 1	2 weeks	1/27/2025 – 2/7/2025	1/10/2025
Intro to Forensic Analysis – Session 2	2 weeks	4/21/2025 – 5/2/2025	4/4/2025
Intro to Forensic Analysis – Session 3	2 weeks	7/14/2025 – 7/25/2025	6/27/2025
Basics of Threat Analysis – Session 1	2 weeks	2/3/2025 – 2/14/2025	1/17/2025
Basics of Threat Analysis – Session 2	2 weeks	5/5/2025 – 5/16/2025	4/18/2025
Basics of Threat Analysis – Session 3	2 weeks	7/28/2025 – 8/8/2025	7/11/2025
Intro to Incident Response – Session 1	1 week	12/16/2024 – 12/20/2024	12/10/2024
Intro to Incident Response – Session 2	1 week	3/3/2025 – 3/7/2025	2/14/2025
Intro to Incident Response – Session 3	1 week	5/19/2025 – 5/23/2025	5/2/2025
Intro to Incident Detect/Response/Handling – Session 1	2 weeks	3/10/2025 – 3/21/2025	2/21/2025
Intro to Incident Detect/Response/Handling – Session 2	2 weeks	6/2/2025 – 6/13/2025	5/16/2025
Intro to Incident Detect/Response/Handling – Session 3	2 weeks	8/18/2025 – 8/29/2025	8/1/2025
Intro to Pen-Testing – Session 1	1 week	12/16/2024 – 12/20/2024	12/10/2024
Intro to Pen-Testing – Session 2	1 week	3/24/2025 – 3/28/2025	3/7/2025
Intro to Pen-Testing – Session 3	1 week	6/23/2025 – 6/27/2025	6/6/2025

FY25 PATHWAY DATES

Pathway Title & Session Number	Length	Course Start & End Date	Application Close Date*
Systems Security Analysis – Session 1	4 weeks	2/24/2025 – 3/21/2025	2/7/2025
Systems Security Analysis – Session 2	4 weeks	6/23/2025 – 7/18/2025	6/6/2025
Infrastructure Support – Session 1	4 weeks	3/3/2025 – 3/28/2025	2/14/2025
Infrastructure Support – Session 2	4 weeks	6/2/2025 – 6/27/2025	5/16/2025
Defensive Cybersecurity – Session 1	12 weeks	3/17/2025 – 6/13/2025	2/28/2025
Defensive Cybersecurity – Session 2	12 weeks	6/23/2025 – 9/26/2025	6/6/2025
AI/ML Pathway – Session 1	4 weeks	3/24/2025 – 4/18/2025	3/7/2025
AI/ML Pathway – Session 2	4 weeks	6/2/2025 – 6/27/2025	5/16/2025
AI/ML Pathway – Session 3	4 weeks	8/25/2025 – 9/19/2025	8/8/2025
Incident Response – Session 1	4 weeks	4/14/2025 – 5/9/2025	3/28/2025
Incident Response – Session 2	4 weeks	7/14/2025 – 8/8/2025	6/27/2025
Vulnerability Analysis – Session 1	4 weeks	4/21/2025 – 5/16/2025	4/4/2025
Vulnerability Analysis – Session 2	4 weeks	8/4/2025 – 8/29/2025	7/18/2025
Digital Forensics – Session 1	4 weeks	4/28/2025 – 5/23/2025	4/11/2025
Digital Forensics – Session 2	4 weeks	8/4/2025 – 8/29/2025	7/18/2025

**The application window may close when a course reaches a maximum number of applicants, which may be sooner than the stated application close date.*

IT Fundamentals Micro-Course

IT FUNDAMENTALS MICRO-COURSE

The **IT Fundamentals Micro-Course** is an **80-hour**, ten-day **self-paced** course that provides comprehensive knowledge in core IT and cybersecurity concepts. Students learn essential skills in operating systems, secure coding, Linux administration, network security, privacy compliance, and Python programming.

COURSE DESCRIPTION

The **IT Fundamentals Micro-Course** is a ten-day self-paced course that provides a comprehensive overview of core IT concepts and security principles. Starting with cybersecurity foundations and command-line basics, the program progresses through comprehensive Linux system administration, advanced secure coding practices, and privacy compliance. Participants gain extensive hands-on experience through cyber ranges, practical projects, and structured labs. The curriculum integrates essential components of system administration, security controls, cloud security, and programming fundamentals.

KEY LEARNING OUTCOMES

- Master IT foundations including operating systems, networking, and cloud computing
- Develop advanced Linux administration skills
- Learn secure coding practices and vulnerability mitigation
- Gain practical experience in system security
- Understand privacy regulations and compliance requirements
- Build Python programming skills for security testing

SUITABLE FOR ROLES IN

- IT Support Specialist
- System Administrator
- Security Analyst
- Network Administrator
- Cloud Support Engineer
- IT Security Specialist
- Application Security Analyst
- Security Operations Technician
- IT Compliance Specialist
- Junior Developer

Introduction to Forensic Analysis Micro-Course

INTRODUCTION TO FORENSIC ANALYSIS MICRO-COURSE

The **Introduction to Forensic Analysis Micro-Course** is an **80-hour**, ten-day **self-paced** training program providing comprehensive training in digital forensics, evidence handling, and security analysis. This extensive course equips students with advanced skills in digital forensic investigations, security assessment, and incident analysis.

COURSE DESCRIPTION

The **Introduction to Forensic Analysis Micro-Course** is an intensive ten-day self-paced course that delivers a comprehensive coverage of digital forensics and related security concepts. The curriculum progresses from foundational IT concepts through advanced forensic techniques, incorporating extensive hands-on practice in digital evidence handling, Windows Registry analysis, and network security assessment. The course format allows for deeper exploration of cryptography, vulnerability management, and software security testing, while adding comprehensive coverage of ethical hacking and ISO compliance. Students gain extensive practical experience through multiple projects and labs, developing proficiency with industry-standard tools and methodologies. This comprehensive course equips learners with the introductory expertise needed to conduct thorough digital forensic investigations and security assessments in enterprise environments.

KEY LEARNING OUTCOMES

- Master core forensics skills in evidence handling and analysis
- Develop advanced security testing expertise
- Build comprehensive cryptography knowledge
- Gain advanced Windows forensics proficiency
- Master professional standards and compliance
- Develop ethical hacking capabilities
- Build advanced vulnerability assessment skills
- Learn network security fundamentals

SUITABLE FOR ROLES IN

- Digital Forensics Analyst
- Computer Forensics Examiner
- Digital Evidence Technician
- Security Investigation Analyst
- Incident Response Analyst
- Security Engineer
- Penetration Tester
- Compliance Analyst

Basics of Threat Analysis Micro-Course

BASICS OF THREAT ANALYSIS MICRO-COURSE

The **Basics of Threat Analysis Micro-Course** is an intensive **80-hour**, ten-day **self-paced** course that provides comprehensive knowledge in threat identification, analysis, and mitigation strategies. The program expands on foundational cybersecurity concepts and delivers in-depth coverage of threat modeling, vulnerability management, incident response, and advanced analysis techniques.

COURSE DESCRIPTION

The **Basics of Threat Analysis Micro-Course** is an intensive ten-day comprehensive self-paced training program that delivers an extensive overview of threat analysis concepts and security principles. The curriculum begins with essential cybersecurity foundations and progressively advances through specialized topics including network security, threat modeling, vulnerability management, incident response, and privacy law compliance. The course format allows for deeper exploration of each subject area, with additional hands-on exercises through cyber ranges, practical projects, and structured labs. The program integrates advanced components of threat identification, analysis, and mitigation strategies while providing extensive practice with industry-standard tools and methodologies.

KEY LEARNING OUTCOMES

- Master threat modeling frameworks, decomposition methods, and rapid prototyping techniques
- Develop comprehensive vulnerability management expertise
- Build advanced incident response capabilities
- Gain extensive traffic analysis proficiency
- Learn ethical hacking fundamentals and advanced techniques
- Understand privacy laws and compliance requirements
- Develop practical cryptography and cryptanalysis skills

SUITABLE FOR ROLES IN

- Threat Analyst
- Security Operations Analyst
- Vulnerability Management Analyst
- Security Incident Response Analyst
- Security Analyst
- ICS Security Analyst
- Privacy Compliance Analyst

Introduction to Incident Response Micro-Course

INTRODUCTION TO INCIDENT RESPONSE MICRO-COURSE

The **Introduction to Incident Response Micro-Course** is a **40-hour**, five-day **self-paced** course that provides entry-level training in incident response, detection, and handling. This foundational course equips students with essential cybersecurity knowledge and practical skills needed to identify, respond to, and manage security incidents in modern IT environments.

COURSE DESCRIPTION

The **Introduction to Incident Response Micro-Course** is an intensive five-day self-paced course that provides entry-level training in incident response, detection, and handling. This training course provides a comprehensive foundation to help students with understanding and managing security incidents. Beginning with core IT and cybersecurity fundamentals, the program progresses through network security, incident response processes, audit fundamentals, and advanced security concepts. Participants gain hands-on experience through practical exercises in both Windows and Linux environments, while learning essential incident response procedures and best practices. The curriculum builds from foundational knowledge to advanced concepts, incorporating elements of digital forensics, ICS/SCADA security, and IT fundamentals.

KEY LEARNING OUTCOMES

- Explore cybersecurity foundations in operating systems, networking, cloud computing, and command-line operations.
- Develop core IT competencies across system hardware, operating systems, and infrastructure management.
- Build incident response skills through fundamentals and hands-on penetration testing exposure.
- Gain ICS/SCADA expertise in operational environments, networking, and security management.
- Learn IT security fundamentals including network connectivity, application management, and data storage.

SUITABLE FOR ROLES IN

- Incident Response Analyst
- Security Operations Center (SOC) Analyst
- Security Incident Handler
- Cybersecurity Analyst
- IT Security Specialist
- Junior Security Engineer

Introduction to Incident Detection, Response and Handling Micro-Course

INCIDENT DETECTION, RESPONSE, AND HANDLING MICRO-COURSE

The **Introduction to Incident Detection, Response, and Handling Micro-Course** is an **80-hour**, ten-day **self-paced** course that provides comprehensive instruction in identifying, analyzing, and responding to security incidents in enterprise environments. The program builds from foundational security concepts through advanced incident handling techniques.

COURSE DESCRIPTION

The **Introduction to Incident Detection, Response, and Handling Micro-Course** is an intensive ten-day self-paced training that systematically progresses from essential cybersecurity foundations to advanced incident response techniques. The curriculum provides extensive coverage of network security, vulnerability management, digital forensics, and incident handling procedures. Students gain in-depth practical experience through cyber ranges, hands-on exercises, and real-world scenarios while learning systematic approaches to incident detection, analysis, and response. The program emphasizes both technical and procedural aspects of incident handling, including threat modeling, risk management, security architecture, and forensic analysis. The course format allows deeper exploration of each topic area with additional hands-on practice. This comprehensive course equips learners with the introductory skills needed to identify, respond to, and manage security incidents effectively in modern enterprise environments.

KEY LEARNING OUTCOMES

- Master incident response across the complete incident lifecycle
- Develop advanced threat detection and analysis capabilities
- Build comprehensive cybersecurity foundations
- Gain expertise in vulnerability assessment and management
- Learn digital forensics and evidence handling
- Understand enterprise risk management
- Develop security architecture skills
- Master threat modeling techniques

SUITABLE FOR ROLES IN

- IT Support Specialist
- System Incident Response Analyst
- SOC Analyst
- Security Operations Engineer
- Cyber Defense Analyst
- Threat Detection Specialist
- Security Incident Handler
- Digital Forensics Analyst
- Enterprise Security Architect

Introduction to Pen-Testing Micro-Course

INTRODUCTION TO PEN-TESTING MICRO-COURSE

The **Introduction to Pen-Testing Micro-Course** is a **40-hour**, five-day **self-paced** course that provides foundational knowledge and hands-on experience in ethical hacking. Participants learn key concepts like vulnerability management, network and web security, and advanced pentesting techniques.

COURSE DESCRIPTION

The **Introduction to Pen-Testing Micro-Course** is an intensive five-day self-paced course that provides a comprehensive introduction to ethical hacking and cybersecurity foundations. Beginning with cybersecurity fundamentals, command-line basics, and network protocols, the course advances through vulnerability management, web application security, and specialized pentesting techniques. Participants gain hands-on experience in areas like vulnerability discovery, exploitation, reconnaissance, and social engineering through structured labs and projects. Incorporating elements of the EC Council's ethical hacking framework, the curriculum covers key topics such as cloud security, Linux architecture, and IoT hacking. With 40 hours of content blending theoretical knowledge and practical skills, this course equips learners with the introductory expertise to conduct penetration testing and security assessments in real-world environments.

KEY LEARNING OUTCOMES

- Master cybersecurity foundations including network protocols, cloud computing, and command-line operations.
- Develop vulnerability assessment skills such as scanning, classification, and remediation.
- Learn web application security techniques like exploiting vulnerabilities and mitigating risks.
- Gain hands-on experience in ethical hacking covering social engineering, wireless network attacks, and advanced exploitation.
- Understand Linux security fundamentals including architecture, scripting, and account management.

SUITABLE FOR ROLES IN

- Penetration Tester
- Ethical Hacker
- Cybersecurity Analyst
- Vulnerability Assessment Specialist
- SOC (Security Operations Center) Analyst
- Network Security Engineer

Systems Security Analysis Pathway

SYSTEMS SECURITY ANALYSIS PATHWAY

The **Systems Security Analysis Pathway** is a **4-week** live, **instructor-led** cybersecurity training course that equips professionals with essential skills in analyzing and securing modern IT infrastructures. Through hands-on labs and real-world simulations, participants master vulnerability assessment, system hardening, and security control implementation across traditional and cloud environments.

COURSE DESCRIPTION

The **Systems Security Analysis Pathway** is a comprehensive 4-week live, instructor-led cybersecurity training course designed to develop expertise in systems security analysis and protection. Starting with foundational security principles, participants progress through operating system hardening, network security, and application protection while gaining hands-on experience with industry-standard tools. The course emphasizes practical application through vulnerability scanning, firewall configuration, and intrusion detection across various environments. By course completion, students gain introductory skills to design and implement comprehensive security assessment strategies, execute full-scale vulnerability assessments, and effectively communicate findings through professional documentation.

KEY LEARNING OUTCOMES

- Set up and configure secure virtual environments for cybersecurity testing
- Implement system hardening techniques across Windows and Linux systems
- Identify and exploit common web application vulnerabilities
- Assess cloud infrastructure for security vulnerabilities

SUITABLE FOR ROLES IN

- Systems Security Analyst
- Security Engineer
- IT Security Specialist
- Infrastructure Security Analyst
- Security Operations Analyst
- Network Security Engineer
- Application Security Analyst
- Cloud Security Engineer

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: CompTIA Security+

Infrastructure Support Pathway

INFRASTRUCTURE SUPPORT PATHWAY

The **Infrastructure Support Pathway** is a **4-week** live, **instructor-led** cybersecurity training course that provides comprehensive hands-on experience in managing and troubleshooting essential IT infrastructure components. Through practical labs and real-world scenarios, participants master hardware, software, and network management while gaining expertise in cloud services integration and professional IT support delivery.

COURSE DESCRIPTION

The **Infrastructure Support Pathway** is a comprehensive 4-week live, instructor-led cybersecurity training course designed to prepare professionals for careers in IT infrastructure and support. Starting with foundational concepts, students' progress through hands-on labs and real-world scenarios, mastering essential components of modern IT systems including hardware, software, and networks. The course advances through virtual machine configuration, network device management, cloud services integration, and enterprise-level support scenarios. By course completion, participants develop proficiency in managing hybrid infrastructure environments, implementing IT best practices, and delivering professional support services. Whether starting in IT or enhancing existing skills, students gain both theoretical knowledge and practical experience needed to handle the complexities of today's rapidly evolving technology landscape.

KEY LEARNING OUTCOMES

- Configure and manage virtual machines across multiple operating systems
- Design and deploy secure wireless network solutions
- Implement comprehensive user account management
- Demonstrate proficiency in IT service delivery and support

SUITABLE FOR ROLES IN

- IT Support Specialist
- Systems Administrator
- Network Administrator
- Infrastructure Engineer
- Cloud Support Engineer
- Desktop Support Technician
- IT Service Desk Analyst
- Technical Support Engineer

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: CompTIA Network+

Defensive Cybersecurity Pathway

DEFENSIVE CYBERSECURITY PATHWAY

The **Defensive Cybersecurity Pathway** is a **12-week** live, **instructor-led** cybersecurity training course that provides comprehensive education in cybersecurity defense and vulnerability analysis. Through hands-on labs and real-world scenarios, participants master essential skills in identifying and mitigating vulnerabilities across networks, systems, and cloud environments.

COURSE DESCRIPTION

The **Defensive Cybersecurity Pathway** is a comprehensive 12-week live, 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 AI 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 AI/ML in vulnerability assessment

SUITABLE FOR ROLES IN

- 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
- Certification: CompTIA Security+

Artificial Intelligence and Machine Learning Pathway

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING PATHWAY

The **Artificial Intelligence and Machine Learning Pathway** is a **4-week** live, **instructor-led** cybersecurity training course that teaches essential skills in developing generative AI applications. Through hands-on labs and practical projects, participants master neural networks, natural language processing, and modern generative models like GANs, VAEs, and transformers.

COURSE DESCRIPTION

The **Artificial Intelligence and Machine Learning Pathway** is a comprehensive 4-week live, instructor-led cybersecurity training course designed to build expertise in generative AI development. Starting with AI/ML fundamentals, participants progress through advanced architectures and cutting-edge applications while gaining hands-on experience with industry-standard tools and frameworks. The course emphasizes practical implementation of neural networks, natural language processing, and pre-trained models, culminating in the development of complete generative AI systems. By completion, students will gain fundamental skills to design, develop, and deploy AI applications that address real-world challenges while considering ethical implications and best practices.

KEY LEARNING OUTCOMES

- Process and prepare data for machine learning applications
- Implement basic Generative Adversarial Networks (GANs)
- Design effective prompt engineering strategies
- Design and implement end-to-end generative AI systems

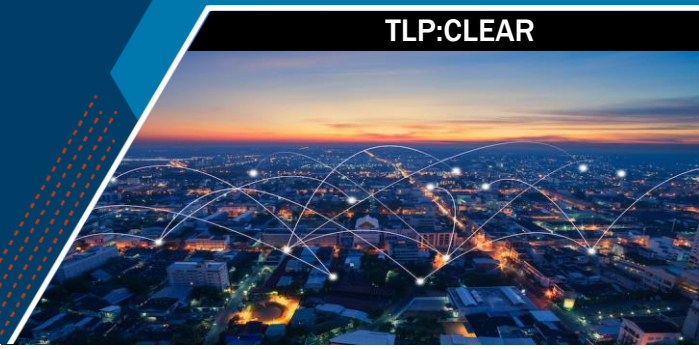
SUITABLE FOR ROLES IN

- Machine Learning Engineer
- AI Developer
- Data Scientist
- AI Research Engineer
- NLP Engineer
- Computer Vision Engineer
- AI Solutions Architect
- ML Operations Engineer

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: AWS Certified AI Practitioner

Incident Response Pathway



INCIDENT RESPONSE PATHWAY

The **Incident Response Pathway** is a **4-week** live, **instructor-led** cybersecurity training course that equips professionals with essential skills in cybersecurity incident handling. Through hands-on labs and real-world scenarios, participants master incident detection, analysis, containment, and recovery techniques across both traditional and cloud environments.

COURSE DESCRIPTION

The **Incident Response Pathway** is a comprehensive 4-week live, instructor-led cybersecurity training course designed to develop proficiency in managing the complete incident response lifecycle. Starting with foundational frameworks and methodologies, participants progress through advanced detection techniques, containment strategies, and recovery procedures. The course combines theoretical instruction with extensive hands-on labs, covering critical skills in malware detection, log analysis, network forensics, and SIEM tool usage. By completion, students are prepared to handle complex incidents across traditional and cloud environments, create professional documentation, and coordinate response efforts effectively. Whether beginning in incident response or enhancing existing expertise, participants gain both strategic and practical skills needed to address today's evolving threat landscape.

KEY LEARNING OUTCOMES

- Configure and maintain a basic incident response environment
- Configure and utilize SIEM tools for effective incident detection
- Implement effective containment strategies for various incident types
- Security Operations Engineer
- Utilize cloud-native security tools for incident handling

SUITABLE FOR ROLES IN

- Incident Response Analyst
- SOC Analyst
- Cybersecurity Analyst
- Security Operations Engineer
- Threat Response Engineer
- Digital Forensics Specialist
- Security Incident Handler
- IT Security Specialist

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: EC-Council Certified Incident Handler (ECIH)

Vulnerability Analysis Pathway

VULNERABILITY ANALYSIS PATHWAY

The **Vulnerability Analysis Pathway** is a **4-week** live, **instructor-led**, cybersecurity training course that teaches professionals how to identify, assess, and manage security vulnerabilities across digital systems. Through hands-on labs and real-world scenarios, participants learn essential skills in vulnerability scanning, web application security, and enterprise-level vulnerability management, preparing them to tackle modern organizational security challenges.

COURSE DESCRIPTION

The **Vulnerability Analysis Pathway** is a comprehensive 4-week live, instructor led cybersecurity training course designed to equip IT and cybersecurity professionals with the critical skills needed to identify, assess, and manage vulnerabilities across various digital environments. Starting with foundational concepts, participants progress through hands-on labs and real-world scenarios, mastering key tools and techniques for vulnerability scanning, system assessments, and web application security. By course completion, students develop proficiency in executing comprehensive vulnerability assessments, utilizing industry-standard tools and OWASP methodologies to identify and analyze security weaknesses in both systems and web applications. The course advances through vulnerability chaining, custom script development, and enterprise-level management, teaching students to effectively prioritize risks using vulnerability scoring systems and communicate findings through detailed technical reports. Whether starting out or deepening existing expertise, participants gain practical experience in implementing enterprise-level vulnerability management programs, conducting specialized assessments, and understanding complex attack paths – all essential skills for tackling today's most pressing organizational security challenges.

KEY LEARNING OUTCOMES

- Configure and manage virtual machines across multiple operating systems
- Design and deploy secure wireless network solutions
- Implement comprehensive user account management and access control systems
- Demonstrate proficiency in IT service delivery and support

SUITABLE FOR ROLES IN

- System & Network Administrators
- Cloud Support Engineer
- IT & Security Operations Professionals
- Cybersecurity Incident Responder
- Information Security Specialist
- Vulnerability Management Specialist
- Network Security Engineer

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: CompTIA CySA+

Digital Forensics Pathway

DIGITAL FORENSICS PATHWAY

The **Digital Forensics Pathway** is a **4-week** live, **instructor-led** cybersecurity training course that equips professionals with essential skills in digital evidence handling and analysis. Through hands-on labs and real-world scenarios, participants master forensic tools and techniques for investigating devices, networks, and cloud environments.

COURSE DESCRIPTION

The **Digital Forensics Pathway** is a comprehensive 4-week live, instructor-led cybersecurity training course designed to develop expertise in conducting thorough and legally sound digital investigations. Starting with foundational forensic concepts, participants progress through device-level, network, and cloud forensics while gaining hands-on experience with professional tools and techniques. The course emphasizes proper evidence handling, chain of custody, and analysis methodologies across various digital platforms. By completion, students gain introductory skills to conduct comprehensive forensic investigations, document findings professionally, and adapt to emerging forensic challenges in hybrid environments, all while maintaining legal and ethical compliance.

KEY LEARNING OUTCOMES

- Apply core cybersecurity principles to digital forensic investigations
- Analyze Windows system artifacts for forensic evidence
- Capture and analyze network traffic using Wireshark
- Conduct forensic investigations in cloud environments

SUITABLE FOR ROLES IN

- Digital Forensics Investigator
- Incident Response Analyst
- Computer Crime Investigator
- Forensics Consultant
- eDiscovery Specialist
- Law Enforcement Digital Forensics Expert
- Corporate Forensics Analyst
- Cybersecurity Investigator

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: EC-Council Computer Hacking Forensic Investigator (CHFI)