



Certified Cybersecurity Associate (CCA) Program

The objective of this program is to provide learners with a practical introduction to cybersecurity through hands-on training in computer systems, networking, cloud security, and cybersecurity operations, preparing them for entry-level roles and the Certified Cybersecurity Associate (CCA) certification.

100 HOURS | <DATE> | FULLY ONLINE

- Provides a structured entry-level pathway into cybersecurity for beginners and career changers.
- Builds practical skills in computer systems, networking, and cybersecurity operations.
- Includes hands-on labs, case studies, and applied certification assessments.
- Covers cybersecurity fundamentals, Windows and Linux administration, cloud computing, and AI in cybersecurity.
- Delivered through an online learning platform with guided instruction and practical exercises.
- Ideal for individuals starting a cybersecurity career or expanding technical security skills.

TARGET AUDIENCE

- Individuals with basic computer knowledge and no prior cybersecurity experience
- Professionals looking to transition into cybersecurity roles
- IT and technology staff seeking practical cybersecurity skills
- Students and recent graduates exploring cybersecurity careers
- Anyone interested in cybersecurity fundamentals

THE INSTRUCTOR

This program is delivered through a dedicated learning platform and supported by experienced instructors with strong backgrounds in cybersecurity, IT systems, and digital technologies.

The training combines guided instruction, hands-on labs, case studies, and applied assessments to help participants build practical skills and prepare for certification.

ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.



FOUNDATIONS COURSE

This course offers a foundational introduction to cybersecurity, covering computer essentials, networking fundamentals, and cyber awareness. Learners will explore the core concepts of IT systems, digital networks, and common cyber threats.

MODULE 1

ORIENTATION

This module guides participants through the TechDX platform, covering navigation, learning materials, profile setup, and community access. Participants build the foundational confidence needed to begin their cybersecurity journey.

MODULE 2

INTRODUCTION TO CYBERSECURITY

This module introduces the world of cybersecurity and explores its role in protecting information and systems. Learners examine the landscape of cyber threats, the importance of ethical hacking, and the impact of cyberattacks in everyday life. It also introduces emerging technologies such as generative AI and large language models (LLMs), and their influence on cybersecurity.

Topics Covered:

- First Steps in Cybersecurity
- Cybersecurity Realm
- Cyberthreats
- Ethical Hacking
- Attacks in Our Daily Lives
- Gen AI & LLMs
- AI Threats and Trends in Modern Cybersecurity

MODULE 3

COMPUTER FOUNDATIONS

This module builds essential computer literacy skills by introducing learners to digital systems, core components, and the interaction between software and hardware. Topics include data, operating systems, and command-line interfaces.

Topics Covered:

- Living in a Digital Age
- Computer Components
- Operating Systems

MODULE 4

NETWORK FUNDAMENTALS

Learners are introduced to the fundamentals of digital networking and how information moves across systems. Topics include network types, architecture, addressing, the OSI model, and networking protocols. Learners also explore tools used to analyze network traffic.

Topics Covered:

- The Digital Network
- Building the Network
- Network Architecture
- Physical and Logical Addresses
- The OSI Model
- Networking Protocols
- Network Sniffers
- Analyzing Network Protocol Traffic

MODULE 5

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Malware Analysis
- Introduction to Local LLM Chatbot
- Your First Steps in Windows Command Execution
- Your First Steps in Linux Command Execution
- Home Network Protection Research
- Investigate HTTP vs. HTTPS
- FTP Credentials Exposure

CASE STUDY

The Olympics Cyber-Attack



SYSTEMS COURSE

This course offers a practical introduction to core cybersecurity systems and covers network administration, Windows system management, and Linux operations. Learners gain hands-on experience with essential tools and configurations used in modern IT environments.

MODULE 1

NETWORK ADMINISTRATION

This module introduces the role of a network administrator and the tools used to configure and secure networks. Learners gain hands-on experience with IP addressing, routers, switches, VLANs, and access control, while learning troubleshooting techniques.

Topics Covered:

- The Network Administrator Arsenal
- Cisco Foundations
- Network Addressing
- IP Address Assignment
- DHCP & NAT
- Switches
- Initial Device Configuration
- Switch Port Security
- Network Routers
- Router Configuration
- VLANs
- ACLs
- Network Monitoring & Troubleshooting

MODULE 2

WINDOWS SYSTEM ADMINISTRATION

This module covers the essentials of managing and securing Windows environments at both client and server levels. Learners work with applications, processes, file systems, and security tools such as Active Directory and Group Policy.

Topics Covered:

- Windows Environment
- Applications, Processes, and Services
- File System and Data Management
- Windows Registry
- Windows Client
- Command Prompt
- Users and Groups
- Windows Client Security
- Windows Server
- Active Directory (AD)
- Group Policy (GPO)
- Domain Name System (DNS)
- Host Encryption
- Windows Firewall
- Account Security Policies

MODULE 3

LINUX SYSTEM ADMINISTRATION

This module develops Linux administration skills, including command-line operations, file systems, permissions, and system configuration. Learners also practice monitoring and troubleshooting techniques.

Topics Covered:

- Linux Environment
- File System Structure
- Linux Command Line Structure
- File System Navigation
- Advanced Operators
- Input, Output, and Redirection
- System Monitoring and Management
- Managing Users & Groups
- Linux Permissions
- System Configuration
- Package Management
- Linux Server Administration

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Exploring DHCP Configuration
- Configure Administrative Functions
- Port Security – Configure & Verify
- Initial Router Configuration
- Processes with Task Manager in Windows
- Windows Management Commands
- Windows Server Configuration
- Creating & Managing AD Objects
- Basic GPO Configuration
- Configuring DNS
- User Password Policies
- Basic Linux Commands
- Linux Pipelines
- Essentials of Linux Group Management
- Web Server Configurations

CASE STUDY

SIEM in Action



OPERATIONS COURSE

This course introduces key operational areas of cybersecurity including cloud security, AI-driven defense, and threat management. Learners explore cloud technologies, generative AI applications, and cybersecurity frameworks.

MODULE 1

CLOUD COMPUTING

This module introduces virtualization and cloud technologies. Learners explore cloud service models, deployment types, and network management, while gaining hands-on exposure to AWS environments and cloud security practices.

Topics Covered:

- Virtualization
- Networking and Security in Virtual Environments
- Cloud Computing
- Service Models
- Deployment Types
- Cloud Network Management
- Amazon Web Services (AWS)
- Cloud Monitoring
- Cloud Security
- Cloud Regulations and Standards
- Cloud Security Best Practices
- Serverless Computing
- Containerization

MODULE 2

CYBERSECURITY FUNDAMENTALS

This module provides an overview of core cybersecurity defense practices. Learners study cybercrime, threat actors, vulnerabilities, and frameworks used in modern security operations.

Topics Covered:

- Cybersecurity and Cybercrime
- Building Your Defenses
- Cybersecurity Teams
- Cybersecurity Frameworks
- NIST Framework
- MITRE Framework
- Cyber Kill Chain Framework
- Defense in Depth (DID)
- Threat Actors
- Vulnerabilities
- Exploits
- Threats
- Malware

MODULE 3

AI IN CYBERSECURITY (LLMS)

This module explores the role of artificial intelligence in cybersecurity. Learners examine how AI tools support analysis, automation, and security tasks, along with associated risks and ethical considerations.

Topics Covered:

- Machine Learning & AI
- GenAI Landscape
- LLM Foundations
- Automated Security Analysis
- Managing Security Tasks with LLMs
- Responsible AI and Ethical Implications
- LLM Vulnerabilities
- Preparing for a Cybersecurity Role

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Intro to Virtualization
- EC2 Instance Creation
- EC2 Instance CMD Commands
- Secure AWS IAM
- Secure AWS VPC
- CVE Research & Analysis
- VNC Exploitation
- Network at Risk – Part 1
- Network at Risk – Part 2
- LLM Chat Configurations
- LLM-Powered Log Analysis
- LLM02:2025 – Sensitive Information Disclosure

CASE STUDY

- Case Study: Identifying Security Incidents
- NOC Case Study: Resolving a Network Outage
- SOC Case Study: Mitigating a Ransomware Attack
- The MediWell Case Study
- Case Study: Elysium (CVE-2024-19876)
- Case Study: EternalBlue