Endpoint Security

Course Overview

This course covers how to assess the network, operating systems, and endpoints for vulnerabilities, and how to secure the network. It also covers skills to maintain the integrity, confidentiality, and availability in the network and data.

Benefits

The demand for security professionals continues to grow. Teach the foundational knowledge used in the workplace as a Cybersecurity Technician.

- ✓ Develop a cybersecurity foundation
- ✓ Offer the next step in exploring the many career possibilities in cybersecurity
- ✓ Build skills securing a network all the way to the edge, including hardware, software, and media

Course Details

Target Audience: Secondary and 2-year college vocational students; Reskilling to find a job in cyber

Estimated Time to Completion: 27 hours

Recommended Preparation: Introduction to Cybersecurity

Course Delivery: Instructor-led or Self-paced

Learning Component Highlights:
- ✓ 10 modules
- ✓ 31 Labs and Cisco Packet Tracer activities
- ✓ 40+ interactive activities & quizzes
- ✓ 1 final exam

Course Recognitions: Digital badge

Certification Alignment: CCST Cybersecurity

Recommended Next Course: Network Defense

Requirements

- ASC Alignment: Recommended
- Instructor Training: Optional
- Physical Equipment: Not required

Networking Academy

Endpoint Security

Scope and Sequence

Version 1.0

Contents

Target Audience

The Endpoint Security course is appropriate for learners with a high school reading proficiency, basic computer literacy, and interested in pursuing an entry-level job in the field of cybersecurity.

Prerequisites

There are no prerequisites for this course, although learners should have the following basic skills:

- Basic PC operating system navigation skills
- Knowledge of TCP/IP networking including network protocols, services, and processes

While not required, it is recommended that learners complete the following courses within the cybersecurity learning path:

- Introduction to Cybersecurity
- Network Essentials

Certification Alignment

This course, from the Junior Cybersecurity Analyst Career Path, aligns with the CCST Cybersecurity Certification (formerly known as IT Specialist Cybersecurity certification from Certiport).

Course Description

Endpoint Security has many features to help learners understand security concepts. The course design includes:

- Ten modules comprised of key topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.
- Each module contains practice and assessment activities such as a Check Your Understanding activity, a lab, or an activity using our network simulation tool, Cisco® Packet Tracer.
- Topic-level activities are designed to indicate a learner's mastery of course skills, enabling learners to gage understanding before taking a graded quiz or exam.
- Language describing concepts is designed to be easily understood by learners at a high school level.
- Assessments and practice activities focus on specific competencies are designed to increase retention and provide flexibility in the learning path.
- Multimedia learning tools, including videos and quizzes, address a variety of learning styles, stimulate learning, and promote knowledge retention.
- Labs and Packet Tracer simulation-based activities help learners develop critical thinking and complex problem-solving skills.
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and skills.
- Technical concepts are explained using introductory-level language.
- Embedded interactive activities break-up reading of large content blocks and reinforce understanding.
- The course emphasizes applied skills and hands-on experiences, while encouraging learners to consider additional Information Technology (IT) education.

Course Objectives

Endpoint introduces important foundational concepts in cybersecurity such as common attacks and attackers, threats, vulnerabilities, and risks, current trends in cybersecurity, network protocol and service vulnerabilities, Windows and Linux endpoints, and threat mitigation and defense. By the end of the course, learners can identify common threats and mitigation techniques, understand the concepts of threat, vulnerability, and risk, and gain experience analyzing common attacks, endpoint operation and security, and malware.

The course material will assist you in developing learner skills, including:

- Explain how threat actors execute some of the most common types of cyberattacks.
- Explain network security principles.
- Explain how TCP.IP vulnerabilities enable network attacks.
- Recommend measures to mitigate threats.
- Troubleshoot a wireless network.
- Explain how devices and services are used to enhance network security.
- Use Windows administrative tools.
- Implement basic Linux security.
- Evaluate endpoint protection and the impact of malware.
- Use cybersecurity best practices to improve confidentiality, integrity, and availability.

Equipment Requirements

Endpoint Security hands-on labs require equipment found in most home networks. Any lab that requires a more complex networking environment uses Packet Tracer, the network simulation tool.

Software

- Oracle Virtual Box
- Lab virtual machine OVA files
- Packet Tracer 8.0.1 or higher

Optional Lab Equipment

- Microsoft Windows host

Course Outline

Table 1 below details the modules and their associated competencies. Each module is an integrated unit of learning that consists of content, activities, and assessments that target a specific set of competencies. The size of the module depends on the depth of knowledge and skill needed to master the competency.

Table 1: Module Title and Objective

Module Title / Topic Title	Objective
Module 1: Cybersecurity Threats, Vulnerabilities, and Attacks	
1.0 Cybersecurity Threats, Vulnerabilities, and Attacks	Explain how threat actors execute some of the most common types of cyberattacks.
1.1 Common Threats	Explain the threats, vulnerabilities, and attacks that occur in the various domains.
1.2 Deception	Identify the different deception methods used by attackers to deceive their victims.
1.3 Cyber Attacks	Describe some common types of network attacks.
1.4 Wireless and Mobile Device Attacks	Describe common types of wireless and mobile device attacks.
1.5 Application Attacks	Describe types of application attacks.
Module 2: Securing Networks	
2.0 Securing Networks	Explain network security principles.
2.1 Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
2.2 IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
2.3 The Command Structure	Describe the command structure of Cisco IOS software.
2.4 Basic Device Configuration	Configure a Cisco IOS device using CLI.
2.5 Save Configurations	Use IOS commands to save the running configuration.
2.6 Ports and Addresses	Explain how devices communicate across network media.
2.7 Configure IP Addressing	Configure a host device with an IP address.
2.8 Verify Connectivity	Verify connectivity between two end devices.
Module 3: Attacking the Foundation	
3.0 Attacking the Foundation	Explain how TCP/IP vulnerabilities enable network attacks.
3.1 IP PDU Details	Explain the IPv4 and IPv6 header structure.
3.2 IP Vulnerabilities	Explain how IP vulnerabilities enable network attacks.
3.3 TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities enable network attacks.
Module 4: Attacking What We Do	
4.0 Attacking What We Do	Recommend measures to mitigate threats.
4.1 IP Services	Explain IP service vulnerabilities.
4.2 Enterprise Services	Explain how network application vulnerabilities enable network attacks.
4.3 Mitigating Common Network Attacks	Recommend basic threat mitigation measures.
Module 5: Wireless Network Communication Devices	
5.0 Wireless Network Communication Devices	Troubleshoot a wireless network.
5.1 Wireless Communications	Explain how wireless devices enable network communication.
5.2 WLAN Threats	Describe threats to WLANs.
5.3 Secure WLANs	Troubleshoot a wireless connection.
Module 6: Network Security Infrastructure	
6.0 Network Security Infrastructure	Explain how devices and services are used to enhance network security.
6.0 Zone-Based Policy Firewalls	Implement Zone-Based Policy Firewall using the CLI.
6.1 Security Devices	Explain how specialized devices are used to enhance network security.
6.2 Security Services	Explain how services enhance network security.
Module 7: The Windows Operating System	
7.0 The Windows Operating System	Use Windows administrative tools.
7.1 Windows History	Describe the history of the Windows Operating System.
7.2 Windows Architecture and Operations	Explain the architecture of Windows and its operation.
7.3 Windows Configuration and Monitoring	Use Windows administrative tools to configure, monitor, and manage system resources.
7.4 Windows Security	Explain how Windows can be kept secure.

Module 8: Linux Overview	
8.0 Linux Overview	Implement basic Linux security.
8.1 Linux Basics	Explain why Linux skills are essential for network security monitoring and investigation.
8.2 Working in the Linux Shell	Use the Linux shell to manipulate text files.
8.3 Linux Servers and Clients	Use the Linux command line to identify servers that are running on a computer.
8.4 Basic Server Administration	Use commands to locate and monitor log files.
8.5 The Linux File System	Use commands to manage the Linux file system and permissions.
8.6 Working with the Linux GUI	Explain the basic components of the Linux GUI.
8.7 Working on a Linux Host	Use tools to detect malware on a Linux host.
Module 9: System and Endpoint Protection	
9.1 Defending Systems and Devices	Use processes and procedures to protect systems.
9.2 Antimalware Protection	Explain methods of mitigating malware.
9.3 Host-based Intrusion Prevention	Recommend endpoint security measures.
9.4 Application Security	Use malware investigation tools to learn malware features.
9.1 Defending Systems and Devices	Use processes and procedures to protect systems.
Module 10: Cybersecurity Principles, Practices, and Processes	
10.0 Cybersecurity Principles, Practices, and Processes	Use cybersecurity best practices to improve confidentiality, integrity, and availability.
10.1 The Three Dimensions	Use hashes to verify the integrity of files.
10.2 States of Data	Compare the three states of data.
10.3 Cybersecurity Countermeasures	Compare the types of cybersecurity countermeasures.