Networking Academy

Cybersecurity Essentials

Scope and Sequence

Version 3.0

Contents

Introduction

Every day, Cybersecurity threats are growing in complexity and scale. In their Global Risks Report (2021) publication, even the World Economic Forum listed Cybersecurity failure among the top 5 global risks, along with threats like extreme weather and infectious diseases. At the same time, organizations everywhere seek new cybersecurity talent. However, due to a skill gap, a predicted 3.5 million cybersecurity jobs globally will likely go unfilled for a skill gap by 2025. Educators are critical to helping close this skills gap by kickstarting the cybersecurity career journeys of their students. Cybersecurity Essentials 3.0 has been designed to help educators prepare students to take the first stepping stone on their cybersecurity career journey. After completing the course, students can find job roles such as Junior Cybersecurity Analyst, Cybersecurity Technician, Cybersecurity Support, Cybersecurity Specialist, or Tier 1 Help Desk Support. Or, they can continue their education towards associate and professional level cybersecurity job roles with courses like CyberOps Associate, Network Security, etc.

Target Audience

The Cybersecurity Essentials 3.0 course is designed for learners as a starting point for cybersecurity careers. It equips learners with entry-level job skills across the three-course domains: Endpoint Security, Network Defense, and Cyber Threat Management. These domains provide an integrated and comprehensive learning experience for an entry-level Junior Cybersecurity Analyst role. Course topics include cybersecurity threats and attacks, threat mitigation, vulnerabilities in protocols and network services, Linux and Windows endpoint security, common network defense measures and architectures, vulnerability and risk management, and cybersecurity incident response. The course includes hands-on labs using Virtual Machines, Packet Tracer activities, and research-based lab experiences. The course is appropriate for learners of many ages and education levels, primarily at high schools, colleges, and NGOs focusing on retraining opportunities.

Prerequisites

Learners are expected to have the following skills:

- High school reading level
- Basic computer literacy
- Basic PC operating system navigation skills
- Basic internet usage skills
- Knowledge of TCP/IP networking, including network protocols, services, processes, and basic configuration of networking devices such as routers and switches

Certification Alignment

This course aligns with Cisco Certified Support Technician (CCST) Cybersecurity certification objectives.

Course Description

In this course, learners develop workforce readiness skills and build a foundation for success in cybersecurity-related careers. With video and rich interactive media support, participants learn, apply, and practice cybersecurity knowledge and skills through a series of in-depth, hands-on experiences and simulated activities that reinforce their learning.

Cybersecurity Essentials teaches comprehensive cybersecurity concepts and skills at the entry level, from threat mitigation and defense to post-incident forensics. Learners will progress from basic cybersecurity concepts to experiences in assessing vulnerabilities and risks later in the curriculum.

Cybersecurity Essentials includes the following features:

- This course consists of three domains.
- The three domains align with common knowledge, skills, and abilities required in the cybersecurity workforce at the entry level.
- Each offering is comprised of multiple modules. Each module consists of multiple topics.
- Each module includes an interactive Check Your Understanding interactive assessment, interactive self-assessment activity, or some other way to assess understanding, such as a multiple-choice quiz, lab, or a Packet Tracer activity. These assessments are designed to tell learners if they have a good grasp of the module content, or if they need to review before continuing. Learners can ensure their level of understanding well before taking a graded quiz or exam. Check Your Understanding quizzes do not affect the learner's overall grade.
- Students learn the basics of a comprehensive set of skills that are carried out by cybersecurity team members in a wide range of organizations.
- The language used to describe cybersecurity concepts is designed to be easily understood by learners at all levels and embedded interactive activities help reinforce comprehension.
- Assessments and practice activities are focused on specific competencies to increase retention and provide flexibility in the course.
- Multimedia learning tools, including videos, games, and quizzes, address a variety of learning styles and help stimulate learning and promote increased knowledge retention.
- Hands-on labs and Cisco® Packet Tracer simulation-based learning activities help students develop critical thinking and complex problem-solving skills.
- Embedded assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.
- Cisco Packet Tracer activities are designed for use with the latest version of Packet Tracer.

Course Objectives

Cybersecurity Essentials is designed for learners who want to start their cybersecurity career journey. Cybersecurity Essentials prepares students to take their first stepping stone toward entry-level or continuing their education toward associate and professional level job roles. These course materials assist in developing the skills necessary to do the following:

- Explain how threat actors execute some of the most common types of cyber attacks.
- 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 impacts of malware.
- Use cybersecurity best practices to improve confidentiality, integrity, and availability.
- Explain approaches to network security defense.
- Implement some of the various aspects of system and network defense.
- Configure local and server-based access control.
- Implement access control lists (ACLs) to filter traffic and mitigate network attacks.
- Explain how firewalls are implemented to provide network security.

- Implement Zone-Based Policy Firewall using the CLI.
- Recommend cloud security requirements based on a given cloud scenario.
- Determine the cryptographic techniques that are required to ensure confidentiality, integrity, and authenticity.
- Explain how security technologies affect security monitoring.
- Use different types of logs and records to store information regarding hosts and the network.
- Explain the process of evaluating alerts.
- Create documents and policies related to cybersecurity governance and compliance.
- Use tools for network security testing.
- Evaluate threat intelligence sources.
- Explain how endpoint vulnerabilities are assessed and managed.
- Select security controls based on risk assessment outcomes.
- Use incident response models and forensic techniques to investigate security incidents.

Equipment Requirements

Hands-on labs require computers capable of running virtualization software (VirtualBox or UTM) with at least 4GB of RAM and 20GB of free disk space. Labs that require more complex networking environments use the Packet Tracer network simulation tool. Other learning experiences require focused internet-based research and the completion of lab documents.

Optional Lab Equipment:

- Microsoft Windows host

Software:

- Oracle Virtual Box or UTM
- Lab virtual machine OVA file
- Packet Tracer 8.2.1 or higher

Course Outline

The first domain, Endpoint Security, introduces critical 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, students can identify common threats and mitigation techniques, use the concepts of threat, vulnerability, and risk, and gain experience analyzing common attacks, endpoint operation and security, and malware.

The second domain, Network Defense, introduces critical foundational concepts in cybersecurity, such as system and network defense, access control, firewalls, cloud security, applications of cryptography, network security data, and evaluating security alerts. By the end of the course, students can implement defensive measures and access control, configure a simulated firewall, use different types of network data, and evaluate security alerts.

The third domain, Cyber Threat Management, introduces critical foundational concepts in cybersecurity, such as ethics and governance, network security testing, threat intelligence, endpoint vulnerability assessment, risk management, and post-incident response. By the end of the course, learners will be prepared to participate in a wide range of threat management and incident response activities as a member of a cybersecurity operations team.

Listed below are the current set of modules and their associated competencies. Each module is an integrated learning unit consisting of content, activities, and assessments that target a specific set of competencies. The size of the module will depend on the depth of knowledge and skill needed to master the competency.

Table 1: Module Title and Objective

Module Title/Topic Title	Objective
Domain One: Endpoint Security	
Module 1: Cybersecurity Threats, Vulnerabilities, and Attacks	Explain how threat actors execute some of the most common types of cyber attacks.
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	Explain network security principles.
2.1 Current State of Affairs	Describe the current network security landscape.
2.2 Who is Attacking Our Network?	Explain how network threats have evolved.
Module 3: 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	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	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	Explain how devices and services are used to enhance network security.
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	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	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	Evaluate endpoint protection and the impacts of malware.
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.
Module 10: 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.
Domain Two: Network Defense	
Module 11: Understanding Defense	Explain approaches to network security defense.
11.1 Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
11.2 Cybersecurity Operations Management	Explain how an organization monitors cybersecurity threats.
11.3 Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.
Module 12: System and Network Defense	Implement some of the various aspects of system and network defense.
12.1 Physical Security	Explain how physical security measures are implemented to protect network equipment.
12.2 Application Security	Explain how to apply application security measures.
12.3 Network Hardening: Services and Protocols	Explain how to harden network services and protocols.
12.4 Network Hardening: Segmentation	Explain how network segmentation can help you harden the network.
12.5 Hardening Wireless and Mobile Devices	Configure wireless router hardening and security.
12.6 Cybersecurity Resilience	Explain physical security with IoT devices.
12.7 Embedded and Specialized Systems	Implement physical security with IoT devices.
Module 13: Access Control	Configure local and server-based access control.
13.1 Access Controls	Configure secure access on a host.
13.2 Access Control Concepts	Explain how access control protects network data.
13.3 Account Management	Explain the need for account management and access control strategies.
13.4 AAA usage and operation	Configure server-based authentication with TACACS+ and RADIUS.
Module 14: Access Control Lists	Implement access control lists (ACLs) to filter traffic and mitigate network attacks.
14.1 Introduction to Access Control Lists	Describe standard and extended IPv4 ACLs.
14.2 Wildcard Masking	Explain how ACLs use wildcard masks.
14.3 Configure ACLs	Explain how to configure ACLs.
14.4 Named Standard IPv4 ACL Syntax	Use sequence numbers to edit existing standard IPv4 ACLs
14.5 Implement ACLs	Implement ACLs.
14.6 Mitigate Attacks with ACLs	Use ACLs to mitigate common network attacks.

14.7 IPv6 ACLs	Configure IPv6 ACLs using the CLI.
Module 15: Firewall Technologies	Explain how firewalls are implemented to provide network security.
15.1 Secure Networks with Firewalls	Explain how firewalls are used to help secure networks.
15.2 Firewalls in Network Design	Explain design considerations for implementing firewall technologies
Module 16: Zone-Based Policy Firewalls	Implement Zone-Based Policy Firewall using the CLI.
16.1 ZPF Overview	Explain how Zone-Based Policy Firewalls are used to help secure a network.
16.2 ZPF Operation	Explain the operation of a Zone-Based Policy Firewall.
16.3 Configure a ZPF	Configure a Zone-Based Policy Firewall with CLI.
Module 17: Cloud Security	Recommend cloud security requirements based on a given cloud scenario.
17.1 Virtualization and Cloud Computing	Describe ways to manage threats to the private and public cloud.
17.2 The Domains of Cloud Security	Explain the domains of cloud security.
17.3 Cloud Infrastructure Security	Explain mitigation of threats to the cloud platform infrastructure.
17.4 Cloud Application Security	Recommend cloud security applications.
17.5 Cloud Data Security	Explain how to secure cloud data.
17.6 Protecting VMs	Explain how to secure VM instances.
Module 18: Cryptography	Determine the cryptographic techniques that are required to ensure confidentiality, integrity, and authenticity.
18.1 Confidentiality	Determine the encryption algorithm to use according to requirements.
18.2 Obscuring Data	Use a technique to obscure data.
18.3 Integrity and Authenticity	Explain the role of cryptography in ensuring the integrity and authenticity of data.
18.4 Hashing	Explain how to use hashing tools.
18.5 Public Key Cryptography	Use a digital signature.
18.6 Authorities and the PKI Trust System	Use hashing to detect network interception.
18.7 Applications and Impacts of Cryptography	Explain how the use of cryptography affects cybersecurity operations.
Module 19: Technologies and Protocols	Explain how security technologies affect security monitoring.
19.1 Monitoring Common Protocols	Explain the behavior of common network protocols in the context of security monitoring.
19.2 Security Technologies	Explain how security technologies affect the ability to monitor common network protocols.
Module 20: Network Security Data	Use different types of logs and records to store information regarding hosts and the network.
20.1 Types of Security Data	Describe the types of data used in security monitoring.
20.2 End Device Logs	Describe the elements of an end device log file.
20.3 Network Logs	Use different types of services to gather network data.
Module 21: Evaluating Alerts	Explain the process of evaluating alerts.
21.1 Source of Alerts	Identify the structure of alerts.
21.2 Overview of Alert Evaluation	Explain how alerts are classified.
Domain Three: Cyber Threat Management	
Module 22: Governance and Compliance	Create documents and policies related to cybersecurity governance and compliance.
22.1 Governance	Create cybersecurity policy documents.
22.2 The Ethics of Cybersecurity	Create a personal code of ethical conduct.
22.3 IT Security Management Framework	Evaluate security controls.

Module 23: Network Security Testing	Use tools for network security testing.
23.1 Security Assessments	Use commands to gather network information and diagnose connectivity issues.
23.2 Network Security Testing Techniques	Describe the techniques used in network security testing.
23.3 Network Security Testing Tools	Describe the tools used in network security testing
23.4 Penetration Testing	Describe how an organization uses penetration testing to evaluate the security of the system.
Module 24: Threat Intelligence	Evaluate threat intelligence sources.
24.1 Information Sources	Evaluate information sources used to communicate emerging network security threats.
24.2 Threat Intelligence Services	Describe various threat intelligence services.
Module 25: Endpoint Vulnerability Assessment	Explain how endpoint vulnerabilities are assessed and managed.
25.1 Network and Server Profiling	Explain the value of network and server profiling.
25.2 Common Vulnerability Scoring System (CVSS)	Explain how CVSS reports are used to describe security vulnerabilities.
25.3 Secure Device Management	Explain how secure device management techniques are used to protect data and assets.
Module 26: Risk Management and Security Controls	Select security controls based on risk assessment outcomes.
26.1 Risk Management	Explain risk management.
26.2 Risk Assessment	Calculate risks.
26.3 Security Controls	Evaluate security controls according to organization characteristics.
Module 27: Digital Forensics and Incident Analysis and Response	Use incident response models and forensic techniques to investigate security incidents.
27.1 Evidence Handling and Attack Attribution	Explain the role of digital forensic processes.
27.2 The Cyber Kill Chain	Identify the steps in the Cyber Kill Chain.
27.3 The Diamond Model of Intrusion Analysis	Use the Diamond Model of Intrusion Analysis to classify intrusion events.
27.4 Incident Response	Apply the NIST 800-61r2 incident handling procedures to a given incident scenario.
27.5 Disaster Recovery	Use commands to back up files and restore network operations.