Networking Academy

June 2021

Skills For All with Cisco Networking Academy

Cybersecurity Essentials 2.0
Scope and Sequence

Table of Contents

Target Audience

The Cybersecurity Essentials 2.0 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 Introduction to Cybersecurity, although learners should have a basic understanding using a laptop, smartphone, or tablet, and browsing the Internet.
While it is not required, it is recommended that learners complete Introduction of Cybersecurity.

Certification Alignment

There are currently no certifications aligned with this curse.

Course Description

Cybersecurity Essentials 2.0 includes:

- Eight modules comprised of key topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.
- 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 all levels.
- Assessments and practice activities focused on specific competencies are designed to increase retention and provide flexibility in the learning path.
- Multimedia learning tools, including paper-based labs, 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.
- Learners explore the basics of being safe online.
- Learners are introduced to different types of malware and attacks, and how organizations protect themselves against these attacks.
- Learners explore career options in cybersecurity.

Course Objectives

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

- Explain the basics of being safe online, including what cybersecurity is and its potential impact.
- Explain the most common cyber threats, attacks, and vulnerabilities.
- Explain how to protect yourself while online.
- Explain how organizations can protect their operations against these attacks
- Access a variety of information and resources to explore the different career options in cybersecurity.

Equipment Required

A laptop, smartphone, or tablet is necessary to access the course via the Internet.

Course Outline

Table 1 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	Explore the range of cybersecurity risks and threats that are ever-present in our world today.
1.1 Common Threats	Understand the most common cybersecurity threats.
1.2 Deception	Understand cybercriminal infiltration tactics.
1.3 Cyber Attacks	Explain common methods used by cybercriminals.
1.4 Wireless and Mobile Device Attacks	Explain common cybersecurity device threats.
1.5 Other Attacks	Explore other types of cyber attacks
Module 2: Cybersecurity P3 Principles, Practices and Processes	
2.1 The Three Dimensions	Understand the three principles of information security.
2.2 States of Data	Understand organizational data and why it must be protected.
2.3 Cybersecurity Countermeasures	Understand safeguards, training, and standards that can protect against cyberattacks.
2.4 Access Controls	Explain authentication, authorization, and accounting access methods.
2.5 Cryptography	Explain types of encryption and key management.

2.6 Hashing	Understand preventing attacks using hash algorithms and salting.
2.7 Obscuring Data	Explain using data masking and steganography to conceal information.
Module 3 System and Network Defenses	
3.0 System and Network Defenses	Explain how to protect systems and networks from today's threats.
3.1 Defending Systems and Devices	Explain how to secure your systems and devices
3.2 Application Security	Understand how to protect and security your applications
3.3 Network Hardening: Services and Protocols	Understand how to secure network services and protocols
3.4 Networking Hardening: Network Devices	Understand securing network devices
3.5 Networking Hardening: VPNs	Understand how to secure VPNs
3.6 Network Hardening: Segmentation	Explain how to use segmentation to security a network
3.7 Hardening Wireless and Mobile Devices	Understand securing wireless and mobile devices.
Module 4: Defending the Enterprise	
4.0 Defending the Enterprise	Understand how to support Guru to protect an organization.
4.1 Embedded and Specialized Systems	Explain how to secure embedded and specialized systems.
4.2 Virtualization and Cloud Computing	Understanding how to secure devices and network on the public cloud.
4.3 Account Management	Understand managing account permissions.
4.4 Cryptography in the Enterprise	Understand using cryptography to secure networks, devices, and data.
Module 5: Cybersecurity Operations	
5.0 Cybersecurity Operations	Understand managing cybersecurity operations
5.1 Defense in Depth	Understand the defense in depth approach.
5.2 Cybersecurity Operations Management	Ensure systems remain securely implemented and configured
5.3 Physical Security	Understand what physical measures can protect against cybercrime.
5.4 Security Assessments	Identify vulnerabilities and misconfigurations in security.
5.5 Cybersecurity Resilience	Design high availability systems and how to maintain them.
5.6 Penetration Testing Attack	Understand penetration testing attack frameworks for incident detection and response.

Module 6 Incident Response	
6.0 Incident Response	Support Guru to prepare for, detect, and investigate security incidents.
6.1 Incident Response Phases	Explain the incident response plans and processes.
6.2 Disaster Recovery	Implement disaster recovery and business continuity plans.
6.3 Digital Forensics	Investigate digital crime.
Module 7 Asset and Risk Management	
7.0 Asset and Risk Management	Become familiar with how risk assessments can be used to identify and analyze potential events that negatively impact assets.
7.1 Asset Management	Identify assets that need to be protected through the asset lifecycle stages.
7.2 Risk Management	Understand the risks and vulnerabilities that threaten an organization's assets.
7.3 Security Controls	Explain the types of controls to implement, reduce, and mitigate risk.
Module 8 Governance and Compliance	
8.0 Governance and Compliance	Explore the main goals of cybersecurity governance and compliance.
8.1 Governance	Understand an organization's approach to cybersecurity.
8.2 The Ethics of Cybersecurity	Become familiar with the code of responsible digital behavior.
8.3 IT Security Management Framework	Understand the ISO / IEC cybersecurity model

