Cybersecurity Essentials 1.1
Scope and Sequence

Last updated 22 August 2018

Target Audience

The *Cybersecurity Essentials 1.1* course is designed for students who are interested in pursuing more advanced studies the field of cybersecurity. This preparatory course provides with an overview of the cybersecurity field. The curriculum explores the characteristics of and tactics used by cyber criminals. It then delves into the technologies, products, and procedures cybersecurity professional use to combat cybercrime. The curriculum is appropriate for students at many education levels and types of institutions, including high schools, secondary schools, universities, colleges, career and technical schools, and community centers.

Prerequisites

For proper skill building, the students should be familiar with the content and skills described in the prerequisite course:

- Introduction to Cybersecurity 1.1

Target Certifications

There are no target certifications for this course

Curriculum Description

The course has many features to help students understand these concepts:

- Rich multimedia content, including interactive activities, videos, games, and quizzes, addresses a variety of learning styles and help stimulate learning and increase knowledge retention
- Hands-on labs and Packet Tracer simulation-based learning activities help students develop critical thinking and complex problem solving skills
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills
- Technical concepts are explained using language that works well for learners at all levels and embedded interactive activities break up reading of the content and help reinforce understanding
- The curriculum encourages students to consider additional IT education, but also emphasizes applied skills and hands-on experience

Cisco Packet Tracer activities are designed for use with Packet Tracer 6.3 or later.

Curriculum Objectives

Cybersecurity Essentials 1.1 covers foundation knowledge and essentials skills in all security domains in the cyber world - information security, systems security, network security, mobile security, physical security, ethics and laws, related technologies, defense and mitigation techniques use in protecting businesses.

Upon completion of the *Cybersecurity Essentials 1.1* course, students will be able to perform the following tasks:

- Describe the characteristics of criminals and experts in the cybersecurity world.
- Describe how the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.
- Describe the tactics, techniques and procedures used by cyber criminals.
- Describe how technologies, products and procedures are used to protect confidentiality.
- Describe how technologies, products and procedures are used to ensure integrity.
- Describe how technologies, products, and procedures provide high availability.
- Explain how cybersecurity professionals use technologies, processes and procedures to defend all components of the network.
- Explain the purpose of laws related to cybersecurity.

Minimum System Requirements

For the best learning experience, we recommend a typical class size of 12 to 15 students and a ratio of one Lab PC per student. At most, two students can share one Lab PC for the hands-on labs. Some lab activities require the student Lab PCs to be connected to a local network.

Lab PC Hardware Requirements

- Computer with a minimum of 2 GB of RAM and 8 GB of free disk space
- High speed Internet access to download Oracle VirtualBox and the virtual machine image file

Curriculum Overview

Cybersecurity Essentials 1.1 helps students:

- Understand the players in the cybersecurity world and the motivation of cyber criminals and cybersecurity specialists.
- Learn to identify security attacks, symptoms, processes, and countermeasures.
- Learn foundational knowledge in various security domains.
- Build skills in security management, controls, protection, and mitigation technologies.
- Learn security laws, ethics, and how to develop security policies.
- Learn the roles of different cybersecurity professionals and career options.

Course Outline

Table 1. Cybersecurity Essentials 1.1 Course Outline

Chapter/Section	Goals/Objectives
Chapter 1. Cybersecurity: A World of Experts and Criminals	**Describe the characteristics of criminals and experts in the cybersecurity world.**
1.1 The Cybersecurity World	Describe the common characteristics comprising the cybersecurity world
1.2 Cyber Criminals versus Cybersecurity Specialists	Differentiate the characteristics of cyber criminals and cybersecurity specialists.
1.3 Common Threats	Compare how cybersecurity threats affect individuals, businesses, and organizations.
1.4 Spreading Cybersecurity Threats	Describe the factors that lead to the spread and growth of cybercrime.
1.5 Creating More Experts	Describe the organizations and efforts committed to expanding the cybersecurity workforce.
Chapter 2. The Cybersecurity Cube	**Describe how the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.**
2.1 The Three Dimensions of the Cybersecurity Cube	Describe the three dimensions of the Cybersecurity Cube (McCumber Cube).
2.2 CIA Triad	Describe the principles of confidentiality, integrity, and availability.
2.3 States of Data	Differentiate the three states of data.
2.4 Cybersecurity Countermeasures	Compare the types of cybersecurity countermeasures.
2.5 IT Security Management Framework	Describe the ISO Cybersecurity Model
Chapter 3. Cybersecurity Threats, Vulnerabilities and Attacks	**Describe the tactics, techniques and procedures used by cyber criminals.**
3.1 Malware and Malicious Code	Differentiate the types of malware and malicious code.
3.2 Deception	Compare the different methods used in social engineering.
3.3 Attacks	Compare different types of cyberattacks.
Chapter 4. The Art of Protecting Secrets	**Describe how technologies, products and procedures are used to protect confidentiality.**
4.1 Cryptography	Explain how encryption techniques protect confidentiality.
4.2 Access Controls	Describe how access control techniques protect confidentiality.
4.3 Obscuring Data	Describe the concept of obscuring data.

Chapter 5. The Art of Ensuring Integrity	**Describe how technologies, products and procedures are used to ensure integrity.**
5.1 Types of Data Integrity Controls	Explain processes used to ensure integrity.
5.2 Digital Signatures	Explain the purpose digital signatures.
5.3 Certificates	Explain the purpose digital certificates.
5.4 Database Integrity Enforcement	Explain the need for database integrity enforcement.
Chapter 6. The Five Nines Concept	**Describe how technologies, products, and procedures provide high availability.**
6.1 High Availability	Explain the concept of high availability.
6.2 Measures to Improve Availability	Explain how high availability measures are used to improve availability.
6.3 Incident Response	Describe how an incident response plan improves high availability.
6.4 Disaster Recovery	Describe how disaster recovery planning plays an important role in implementing high availability.
Chapter 7. Protecting a Cybersecurity Domain	**Explain how cybersecurity professionals use technologies, processes and procedures to defend all components of the network.**
7.1 Defending Systems and Devices	Explain how processes and procedures protect systems.
7.2 Server Hardening	Explain how to protect servers on a network.
7.3 Network Hardening	Explain how to implement security measures to protect network devices.
7.4 Physical and Environmental Security	Explain how physical security measures are implemented to protect network equipment.
Chapter 8. Becoming a Cybersecurity Specialist	**Explain the purpose of laws related to cybersecurity.**
8.1 Cybersecurity Domains	Describe how cybersecurity domains are used within the CIA triad.
8.2 Understanding the Ethics of Working in Cybersecurity	Explain how ethics provide guidance.
8.3 Next Step	Explain how to take the next step to become a cybersecurity professional

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**