Course 2 overview

Image update

Hello, and welcome to **Play It Safe: Manage Security Risks**, the second course in the Google Cybersecurity Certificate. You're on an exciting journey!

By the end of this course, you will develop a greater understanding of the eight Certified Information Systems Security Professional (CISSP) security domains, as well as specific security frameworks and controls. You'll also be introduced to how to use security tools and audits to help protect assets and data. These are key concepts in the cybersecurity field, and understanding them will help you keep organizations, and the people they serve, safe from threats, risks, and vulnerabilities.

Certificate program progress

The Google Cybersecurity Certificate program has eight courses. **Play It Safe: Manage Security Risks** is the second course.

Graphic illustration displays the titles of each of the eight courses, with course two highlighted.

1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.

2. **Play It Safe: Manage Security Risks** — *(current course)* Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.

3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks.

4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.

5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.

6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.

7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.

8.

Put It to Work: Prepare for Cybersecurity Jobs — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

Course 2 content

Each course of this certificate program is broken into weeks. You can complete courses at your own pace, but the weekly breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months.

What's to come? Here's a quick overview of the skills you'll learn in each week of this course.

Week 1: Security domains

You will gain understanding of the CISSP's eight security domains. Then, you'll learn about primary threats, risks, and vulnerabilities to business operations. In addition, you'll explore the National Institute of Standards and Technology's (NIST) Risk Management Framework and the steps of risk management.

Week 2: Security frameworks and controls

You will focus on security frameworks and controls, along with the core components of the confidentiality, integrity, and availability (CIA) triad. You'll learn about Open Web Application Security Project (OWASP) security principles and security audits.

Week 3: Introduction to cybersecurity tools

Five icons show the course followed by the four weeks sequentially from left to right with week 3 highlighted.

You will explore industry leading security information and event management (SIEM) tools that are used by security professionals to protect business operations. You'll learn how entry-level security analysts use SIEM dashboards as part of their every day work.

Week 4: Use playbooks to respond to incidents

Five icons show the course followed by the four weeks sequentially from left to right with week 4 highlighted.

You'll learn about the purposes and common uses of playbooks. You'll also explore how cybersecurity professionals use playbooks to respond to identified threats, risks, and vulnerabilities.

What to expect

Each course offers many types of learning opportunities:

- **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories.
- **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies.
- **Discussion prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the discussion forums**.**

- **Self-review activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example.

- **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course.

- **In-video quizzes** help you check your comprehension as you progress through each video.

- **Practice quizzes** allow you to check your understanding of key concepts and provide valuable feedback.

- **Graded quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score.

Tips for success

-

It is strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge.

- Participate in all learning opportunities to gain as much knowledge and experience as possible.

- If something is confusing, don't hesitate to replay a video, review a reading, or repeat a self-review activity.

- Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the Resources tab.

- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.

- Understand and follow the Coursera Code of Conduct to ensure that the learning community remains a welcoming, friendly, and supportive place for all members.

Revision #1
Created 2023-06-03 04:56:17 UTC by naruzkurai
Updated 2023-06-03 04:59:05 UTC by naruzkurai