

Get started with the certificate program

Introduction to cybersecurity

Core skills for cybersecurity professionals

Review: Welcome to the exciting world of cybersecurity

🕒

Video: Wrap-up

57 sec

📖

Reading: Glossary terms from week 1

10 min

🟢

Quiz: Weekly challenge 1

9 questions

🎉 Congratulations! You passed!

Grade received 88.88%

Latest Submission Grade 88.88%

Quiz • 45 min

To pass 80% or higher

Go to next item

📌

Submit your assignment

Due May 28, 11:59 PM +08

Attempts 3 every 24 hours

Try again

📌

Receive grade

To Pass 80% or higher

Your grade

88.88%

View Feedback

We keep your highest score

Review Learning Objectives

1. Fill in the blank: The purpose of ____ is to protect networks, devices, people, and data from unauthorized access or criminal exploitation.

1 / 1 point

👍 Like

👎 Dislike

📄 Report an issue

☒ cybersecurity

☐ change-management

☐ business continuity

☐ planning

🔍 Incorrect

Please review [the video about entry-level security analysts](#).

2. A security professional collaborates with information technology teams to deploy an application that helps identify risks and vulnerabilities. What does this scenario describe?

0 / 1 point

☐ Installing detection software

☐ Ethical hacking

☒ Conducting a security audit

☐ Upgrading network capacity

3. An employee receives an email that they believe to be legitimate. They click on a compromised link within the email. What type of internal threat does this scenario describe?

1 / 1 point

☐ Intentional

☒ Accidental

☐ Operational

☐ Abusive

👍 Correct

4. Fill in the blank: Identity theft is the act of stealing ____ to commit fraud while impersonating a victim.

1 / 1 point

☐ business records

☐ hardware

☒ personal information

☐ trade secrets

👍 Correct

5. Fill in the blank: An organization that is in regulatory compliance is likely to ____ fines.

1 / 1 point

☐ rectify

☒ avoid

☐ encounter

☐ incur

👍 Correct

6. An individual is in their first job as an entry-level security professional. They take training to learn more about the specific tools, procedures, and policies that are involved in their career. What does this scenario describe?

1 / 1 point

☐ Improving management capabilities

☐ Transferring capabilities from one career to another

☐ Understanding different perspectives

☒ Gaining new technical skills

👍 Correct

7. Fill in the blank: Security information and ____ management (SIEM) tools enable security professionals to identify and analyze threats, risks, and vulnerabilities.

1 / 1 point

☒ event

☐ enterprise

☐ emergency

☐ employer

👍 Correct

8. A security professional receives an alert about an unknown user accessing a system within their organization. They attempt to identify, analyze, and preserve the associated criminal evidence. What security task does this scenario describe?

1 / 1 point

☐ Resolving error messages

☐ Programming with code

☐ Software upgrades

☒ Computer forensics

👍 Correct

9. Which of the following statements accurately describe personally identifiable information (PII) and sensitive personally identifiable information (SPII)? Select all that apply.

1 / 1 point

☒ An example of PII is someone's date of birth.

👍 Correct

☒ Both PII and SPII are vulnerable to identity theft.

👍 Correct

☐ The theft of PII is often more damaging than the theft of SPII.

☒ An example of SPII is someone's financial information.

👍 Correct