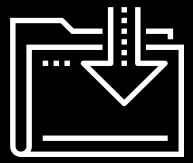
Career Prep and Certifications

Cybersecurity

Prep Week Day 1



Class Objectives

By the end of class, you will be able to:

- Understand the importance of career and job-search preparation.
- Understand the value of certifications in your job search and career development.
- Map out certification roadmaps based on your specific experience level and field of interest.
- Use CompTIA's CertMaster tool to begin preparing for the Security+ exam.
- Understand performance-based questions (PBQs) and how to answer them.


WELCOME

This week, you'll learn and apply job hunting skills that will help position you to land interviews and job offers.

This Week

Day 1:

We will:

- Begin by discussing Career Prep Week.
- Cover certifications, with a focus on Security+, and some strategies for taking certification tests.

Day 2:

We will:

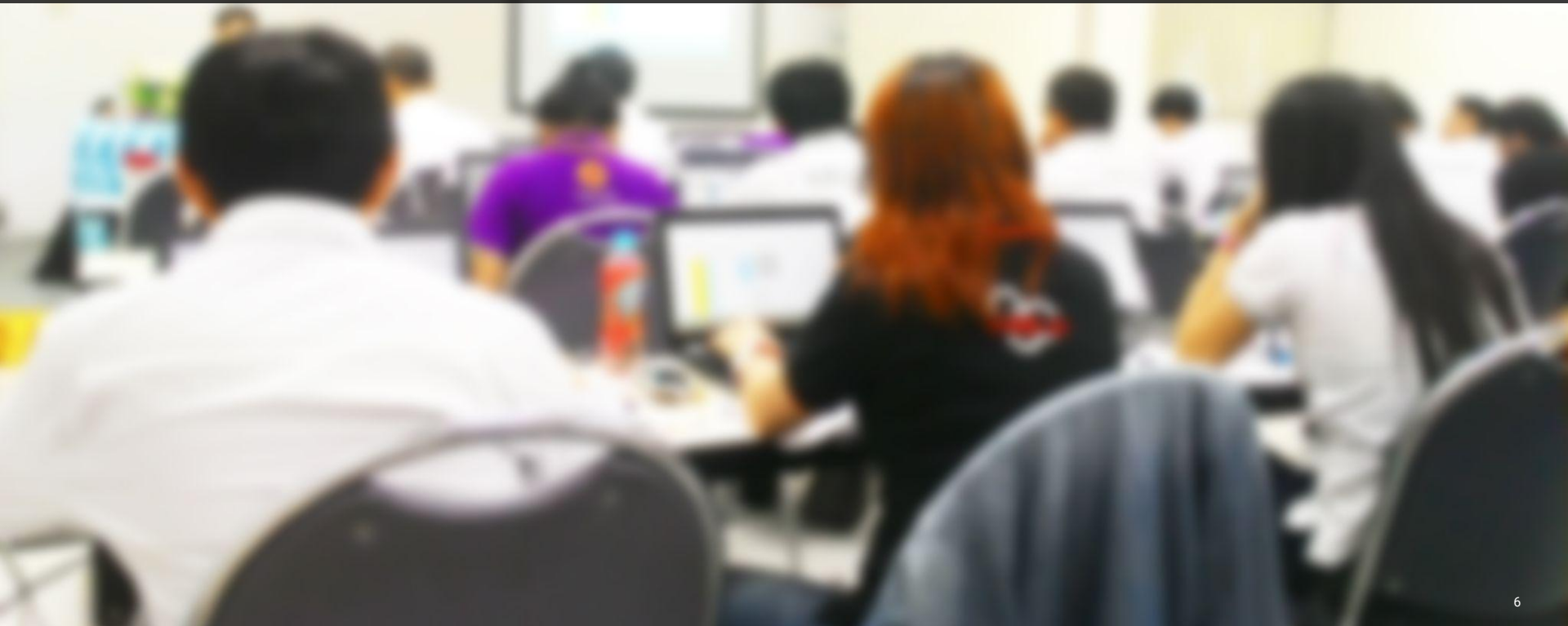
- Cover the Security+ domains, job searching, and career development methods.

Day 3:

We will:

- Focus on mock interviews.

An important first step to landing a job or furthering your career is demonstrating that you can perform the tasks that your job requires. A good way to do this is to pass a **certification exam**.



Certifications by the Numbers

As of April 2020…

This Week

We will also dive deeper into Security+.

This course comes with a voucher for the Security + exam. Therefore, we will spend the most time on this certification.

We will cover:

- Test preparation tips
- The CompTIA CertMaster study tool
- Performance-based questions (PBQs)
- Domains on the exam that are not covered in this course's curriculum

(comptia.org)

Information Security Certifications

Information Security Certifications

Certifications can give candidates an advantage when applying to their first cybersecurity jobs.

Certifications also provide the following benefits to all InfoSec professionals:

01 Further education

02 Networking

03 Career advancement

Information Security Certifications

01

Education

Individuals learn new skills while preparing for a certification, even before the certification is formally awarded. While achieving credentials is often the objective, the material learned while studying for the exam is also valuable to job performance.

Information Security Certifications

02

Networking

Many certifications have national and local organizations that host meetings, conferences, seminars, and social events. These events can provide opportunities to network with peers in your field.

Information Security Certifications

03

Career advancement

Information security certifications can also place more established professionals in a stronger position to obtain a promotion.

Types of InfoSec Certification

Types of InfoSec Certifications

We can break certifications into three categories:

Beginner information security certifications

The first certifications that individuals new to the field should obtain.

Advanced information security certifications

Should be obtained after working in the industry for several years.

Specialized information security certifications

Focus on a specific domain and should be obtained after working in the industry for several years.

Beginner Certifications

- Typically do not have minimum work requirements or prerequisite courses.
- Typically broad in the subjects that they cover.

Examples include: Security+, CEH, and GSEC

Advanced Certifications

- Often focus on security management.
- Typically have minimum work requirements and prerequisite courses.

Examples include: CISM and CISSP

Specialized Certifications

- Typically have minimum work requirements and prerequisite courses.
- Specific in the subjects that they cover.

GIAC Certified Forensic Examiner (GCFE) is specific to forensics professionals.

Offensive Security Certified Professional (OSCP) and **PenTest+** are specific to penetration testers.

Specialized Certifications

Specialized certifications can be vendor or non-vendor specific.

Non-vendor specific

OSCP is a **non-vendor specific** penetration testing certification.

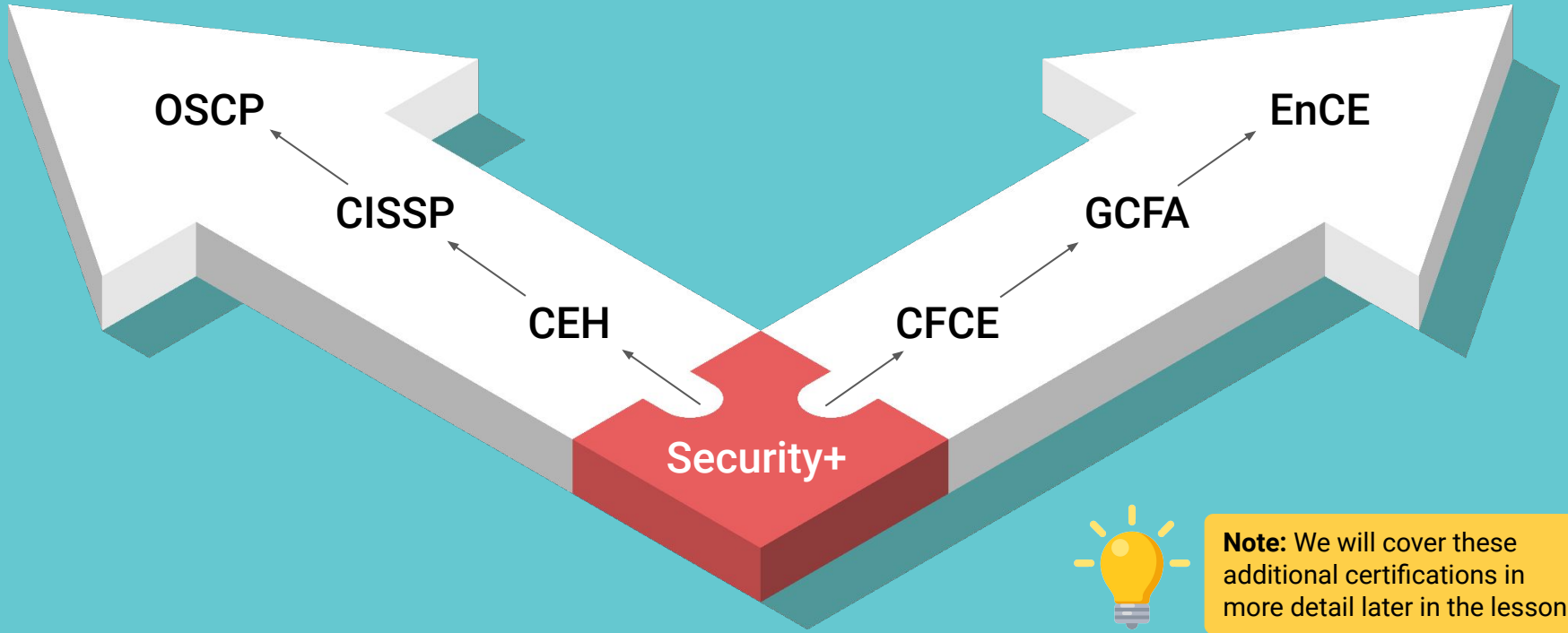
Vendor specific

Cisco Certified Network Associate (CCNA) is a **vendor-specific certification** for Cisco products.

Certification Pathways

Penetration testers
may follow this path:

Forensic investigators
may follow this path:



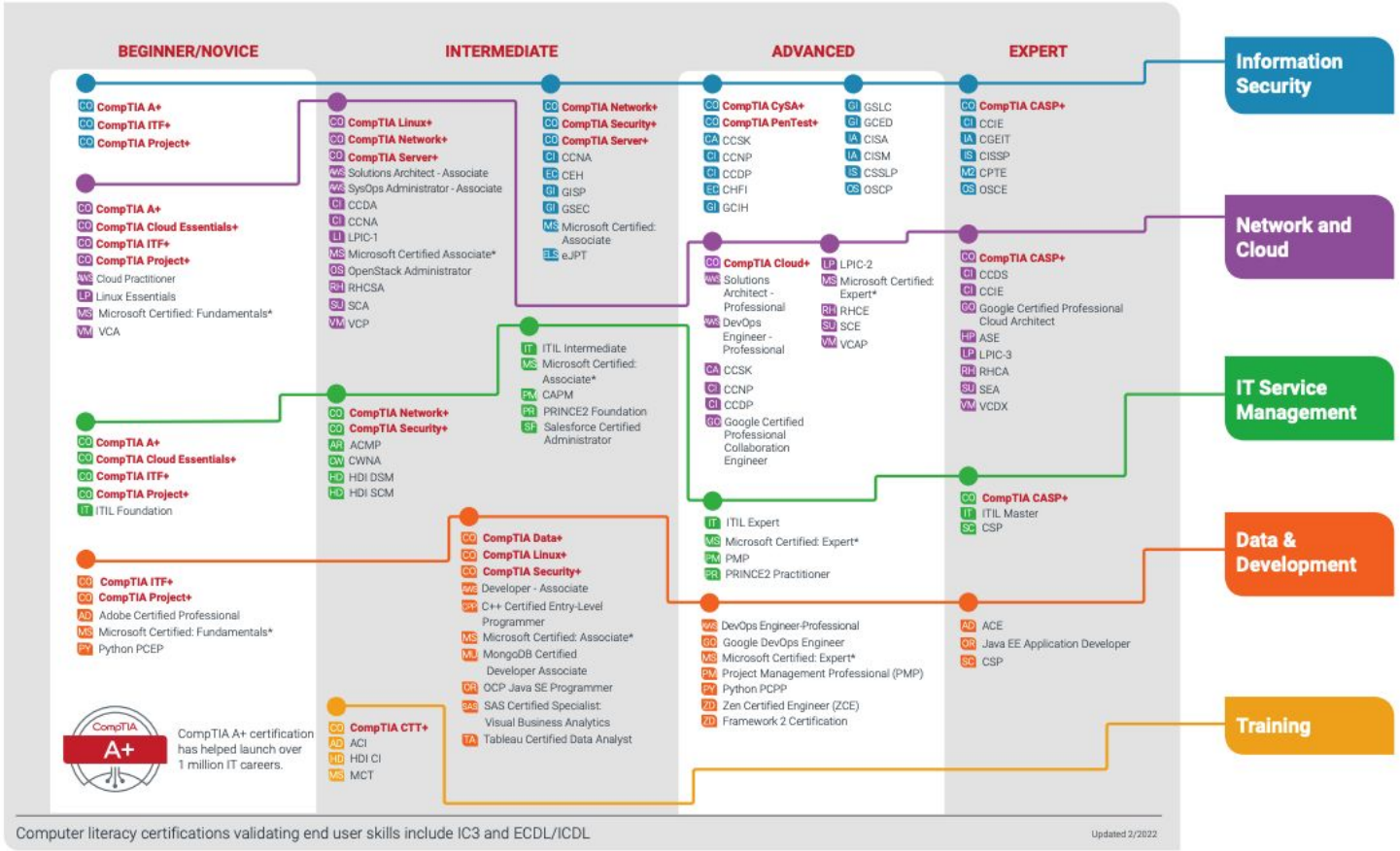
Note: We will cover these additional certifications in more detail later in the lesson.

IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at:
CompTIA.org/CertsRoadmap

CompTIA

Certifications validate expertise in your chosen career.



Microsoft provides three certification paths. Please visit Microsoft's webpage for a full list of their offerings: https://bit.ly/3tJYm8Z

Source: CompTIA

Activity: Certifications and Careers

In this activity, you will use job search websites to research InfoSec careers and certifications.

Suggested Time:

20 Minutes

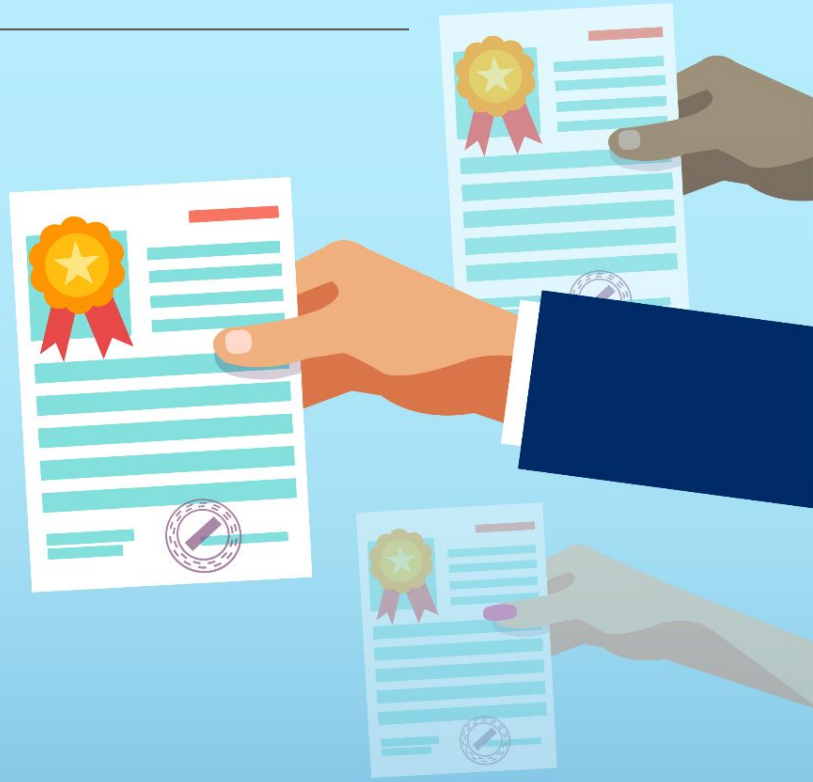
Time's Up! Let's Review.

Questions?

Beginner Certifications

Beginner Certifications

While Security+ will likely be the first certification that you'll work toward, there are several other beginner InfoSec certifications that don't require experience and cover many domain areas.



Certified Ethical Hacker (CEH) is a certification offered by EC Council.

While the CEH generally focuses on penetration testing, it also covers a broad range of topics relevant to InfoSec professionals.

CEH also offers an advanced certification, CEH Practical, which tests individuals' skills with hands-on penetration testing tools.

GIAC Security Essentials (GSEC) is a certification offered by the Global Information Assurance Certification (GIAC).

GSEC covers a broad range of topics ranging from active defense to cryptography.

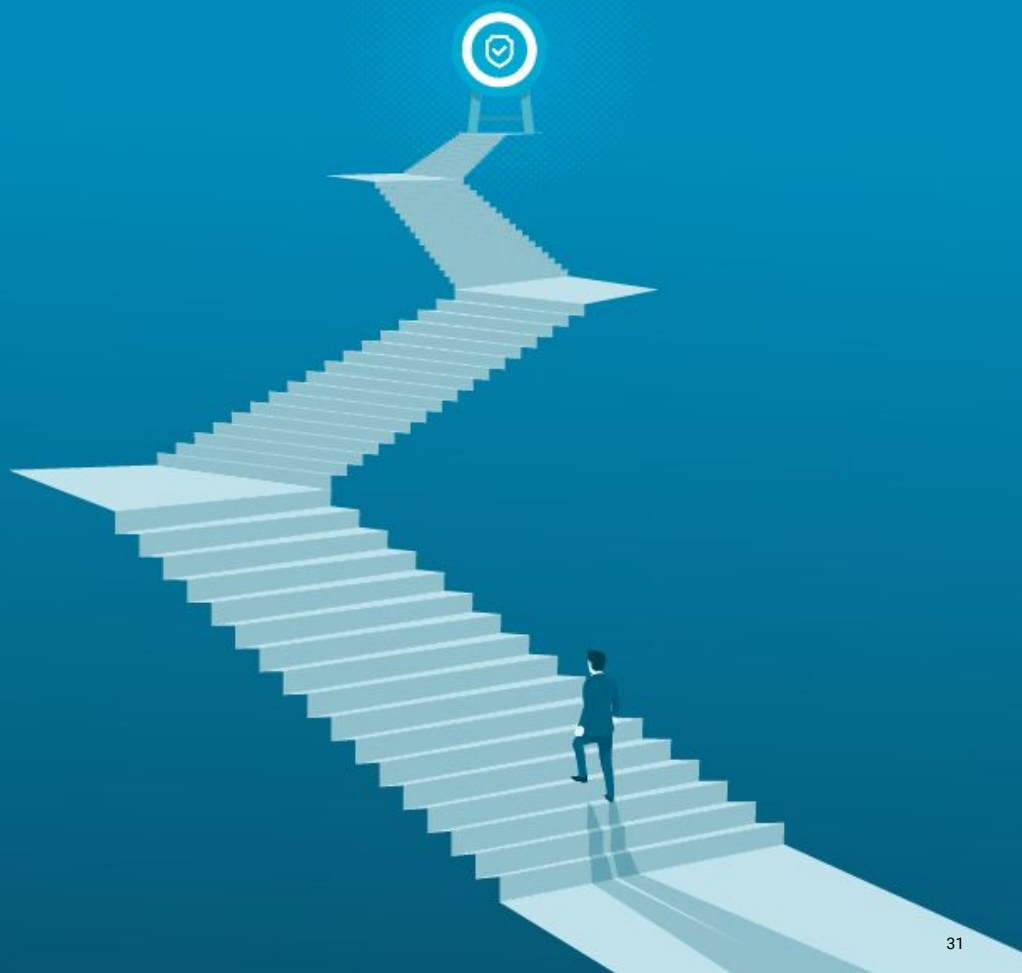
Systems Security Certified Professional (SSCP) is a certification offered by $(ISC)^2$ (“ISC squared”).

SSCP covers security best practices for setting up, monitoring, and administering IT infrastructure.

While SSCP is one of the entry-level certifications offered by $(ISC)^2$, one year of professional cybersecurity experience is recommended.

Advanced Certifications

Many cyber professionals advance their careers by obtaining advanced and specialized certifications.



Certified Information Systems Security Professional (CISSP) is an advanced certification offered by $(ISC)^2$.

It covers a wide variety of cybersecurity topics and is one of the most popular certifications in information security.

Certified Information Security Manager (CISM) is a certification offered by ISACA.

It covers information security management topics.

Specialized Certifications

Specialized Certifications

There are hundreds of specialized certifications available for those interested in mastering a specific cybersecurity domain.

Offensive Security Certified Pentester (OSCP) is a specialized pen testing certification offered by Offensive Security.

It is a practical exam consisting of two parts: a 24-hour penetration testing exam and a documentation report due 24 hours after the exam.

Certified Information Privacy Professional (CIPP) is a specialized privacy certification offered by IAPP.

It is considered the “gold standard” for those working in privacy.

EnCase Certified Examiner (EnCE) is a vendor-specific specialized certification for computer forensics professionals.

It is offered by OpenText and used by law enforcement.

Activity: Find a Certification Pathway

In this activity, you will research several advanced and specialized certifications.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

Countdown timer

15:00

(with alarm)

Introduction to Security+

What is the Security+ certification?

According to CompTIA:

Security+ is the first security certification IT professionals should earn.

It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.

Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills.

Cybersecurity professionals with Security+ know how to address security incidents—not just identify them.

Introduction to Security+ Certification

Some jobs that may require the **Security+** certification:

- Security architect
- Security engineer
- Security consultant
- Security specialist
- Security/systems administrator

Introduction to Security+ Certification

What topics does Security+ cover?

01 Attacks, Threats, and Vulnerabilities

02 Architecture and Design

03 Implementation

04 Operations and Incident Response

05 Governance, Risk, and Compliance

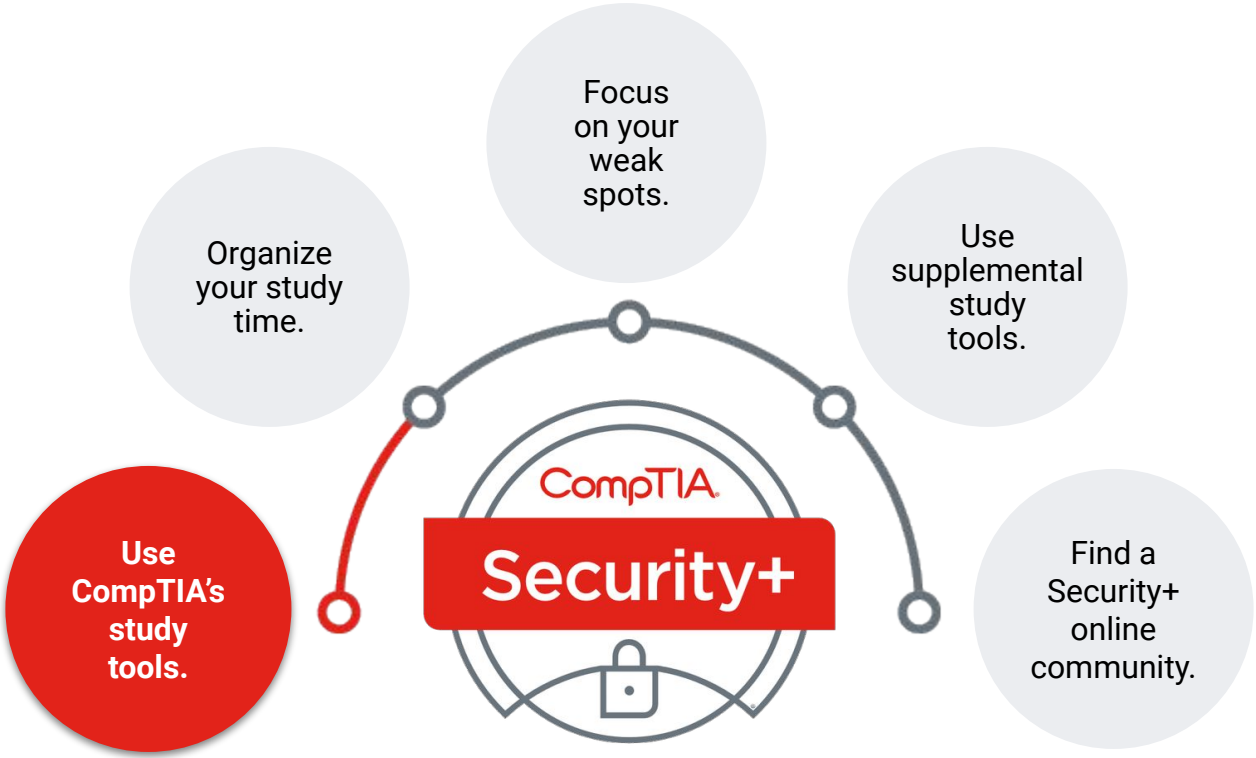
Security+ Specs

The Security+ certification is obtained by passing the CompTIA-administered Security+ exam.

- There are 90 multiple-choice and performance-based questions.
- The exam lasts 90 minutes.
- The cost of the exam is $392.
- The exam is vendor-neutral.

Preparation Tips

While there are many books, online resources, study guides, and apps available to help prepare for the exam, CompTIA provides the most up-to-date resources for exam prep.

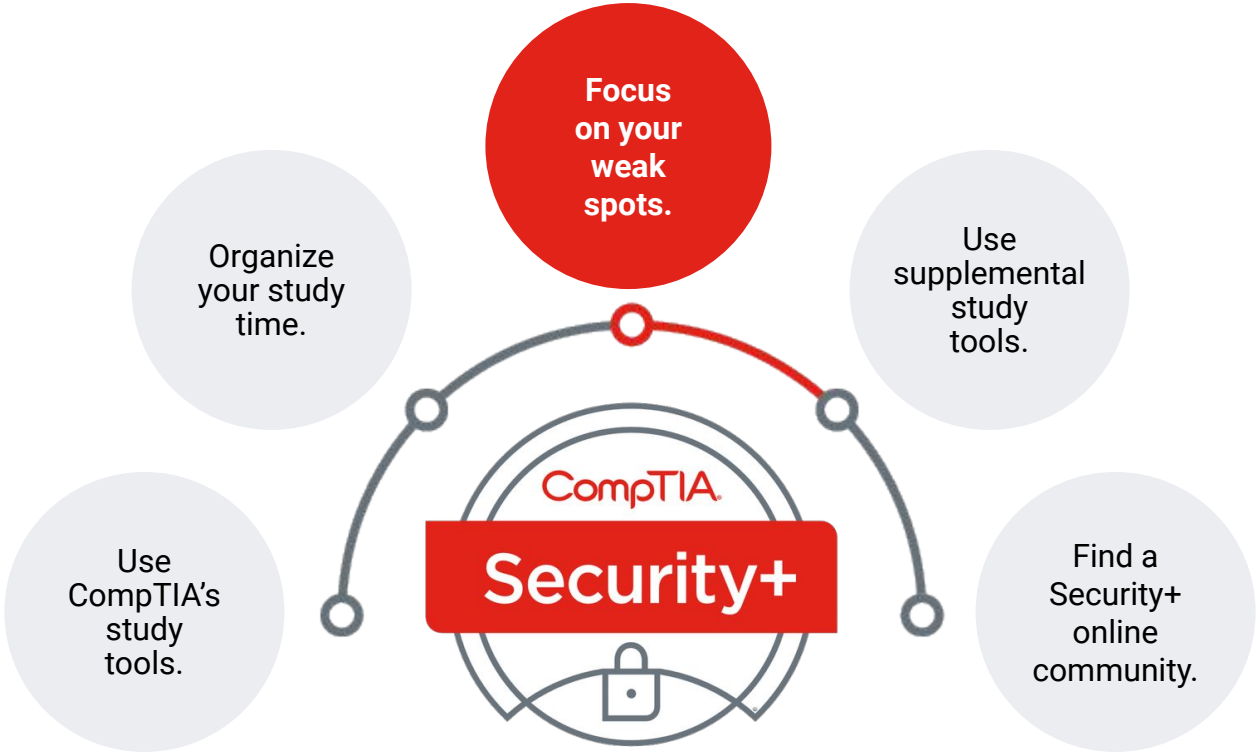


Preparation Tips

Design a structured study plan and stick with it. Block out at least several weeks to focus on studying for the exam.

Preparation Tips

Early on, attempt to determine which domains are the most challenging, and focus your studies there.



Preparation Tips

Create study guides and flashcards of common terms and acronyms. Find video content that explains confusing subjects.

Preparation Tips

There are many online blogs, forums (e.g., Reddit), and wiki pages dedicated to preparing for the Security+ exam.

Test-Taking Tips

Take care of yourself.

- Arrive early, well-rested, fed, hydrated, and relaxed.

Pay attention.

- Read each question and each answer twice before deciding on your answer.
- Look for keywords in the questions, such as “best,” “most,” or “least.”
- Always stay aware of how much time remains.

If you’re unsure of an answer, guess.

- Eliminate the answers you know are wrong, and select from the remaining answers.
- You’ll receive the same penalty for an incorrect answer as for an unanswered question, so always make a best guess.

Security+ CertMaster

CertMaster Practice Tool

As part of this boot camp, you will be provided with access to the **CertMaster Practice tool**.
Per CompTIA, CertMaster Practice comes with:

- Quick knowledge assessment.
- Adaptive learning that reinforces existing and new knowledge.
- Personalized feedback.
- Real-time learning analytics.

Instructor Demonstration

CertMaster

Activity: Security+ CertMaster

In this activity, you will utilize the Security+ CertMaster study trial to complete the sample test module.

Suggested Time:

10 Minutes

Begin Setting Up the Free Trial

Go to https://www.comptia.org/training/certmaster-practice/security

CertMaster Practice

CertMaster Practice is an intelligent online course that helps you learn fast and remember information long-term as you prepare for the exam. It quickly assesses what you know and then focuses on filling your knowledge gaps. It's a great addition to your exam prep plan and guides you to mastery of the curriculum.

Sign Up for Your Free Trial

Complete this form to register for the trial. Once you have registered, login to get started learning!

First Name | Last Name

Company | Email

Create Password | Confirm Password

Select Country

CompTIA CertMaster Practice for Security+ SY0-701 Trial

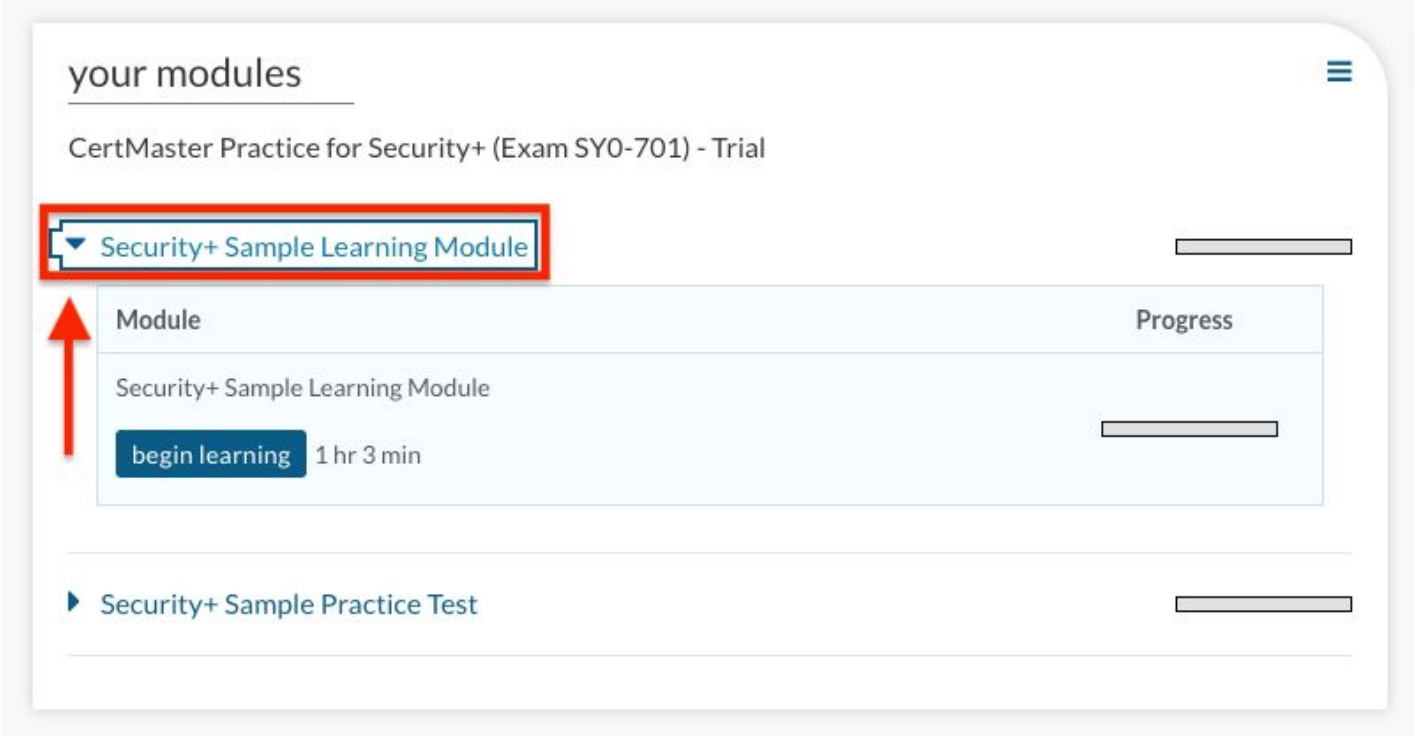
☐ I agree to the CompTIA CertMaster License Terms

☐ I agree to the Terms of Use & Privacy statement.

START YOUR FREE TRIAL NOW

Review the Learning Module

The free trial only has one module. The full CertMaster Tool will cover all domains of the exam.



Answering Questions

Double-click an answer to fill in the circle if you are certain that it is the correct answer.

QUESTION

As part of enhancing its data protection strategy, a corporation's IT manager aims to ensure defense-in-depth by integrating a technical control alongside existing managerial and operational controls. Which measure BEST exemplifies a technical security control according to the classification scheme?

ANSWER

- ○ Conducting employee cybersecurity training
- ○ Installing a building access control system
- ○ Implementing a risk identification tool
- ● I AM **SURE**
  Setting up a network intrusion detection system
- ○ I DON'T KNOW YET

submit

Answering Questions

If you are unsure of the answer, you can click multiple answers one time.

QUESTION

As part of enhancing its data protection strategy, a corporation's IT manager aims to ensure defense-in-depth by integrating a technical control alongside existing managerial and operational controls. Which measure BEST exemplifies a technical security control according to the classification scheme?

ANSWER

- Conducting employee cybersecurity training
- I AM **UNSURE**
  Installing a building access control system
- Implementing a risk identification tool
- I AM **UNSURE**
  Setting up a network intrusion detection system
- I DON'T KNOW YET

submit

Submitting Answers

The tool will let you know if any of your answers are correct.

QUESTION

As part of enhancing its data protection strategy, a corporation's IT manager aims to ensure defense-in-depth by integrating a technical control alongside existing managerial and operational controls. Which measure BEST exemplifies a technical security control according to the classification scheme?

ANSWER

- Conducting employee cybersecurity training
- YOU WERE **UNSURE** AND **1 IS CORRECT**
  Installing a building access control system
- Implementing a risk identification tool
- YOU WERE **UNSURE** AND **1 IS CORRECT**
  Setting up a network intrusion detection system
- I DON'T KNOW YET

next question

Reviewing Answers

The tool will let you know which answer is correct.

LEARN

QUESTION

REVIEWING 4 OF 4

As part of enhancing its data protection strategy, a corporation's IT manager aims to ensure defense-in-depth by integrating a technical control alongside existing managerial and operational controls. Which measure BEST exemplifies a technical security control according to the classification scheme?

ANSWER

YOU CHOSE 2

- Conducting employee cybersecurity training
- YOU WERE UNSURE AND INCORRECT
  Installing a building access control system
- Implementing a risk identification tool
- YOU WERE UNSURE AND CORRECT
  Setting up a network intrusion detection system
- I DON'T KNOW YET

Reviewing Answers

At the bottom of the answer page, it will explain why the answer is correct.

WHAT YOU NEED TO KNOW

Intrusion detection systems represent a technical control involving hardware and software systems specifically designed to monitor and control the network's security. Network intrusion detection systems are naturally automated and technical, making this the best example of a technical control in the options given.

Implementing a risk identification tool falls under the category of managerial controls. These types of controls oversee the information system.

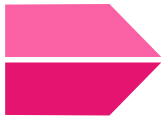
Time's Up! Let's Review.

Questions?

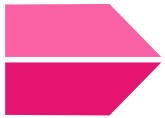
Security+ PBQ

Security+ PBQ

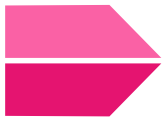
The Security+ exam has two types of questions: multiple choice and performance-based questions (PBQs).



PBQs present test takers with a simulated environment, such as a network, firewall, or terminal.



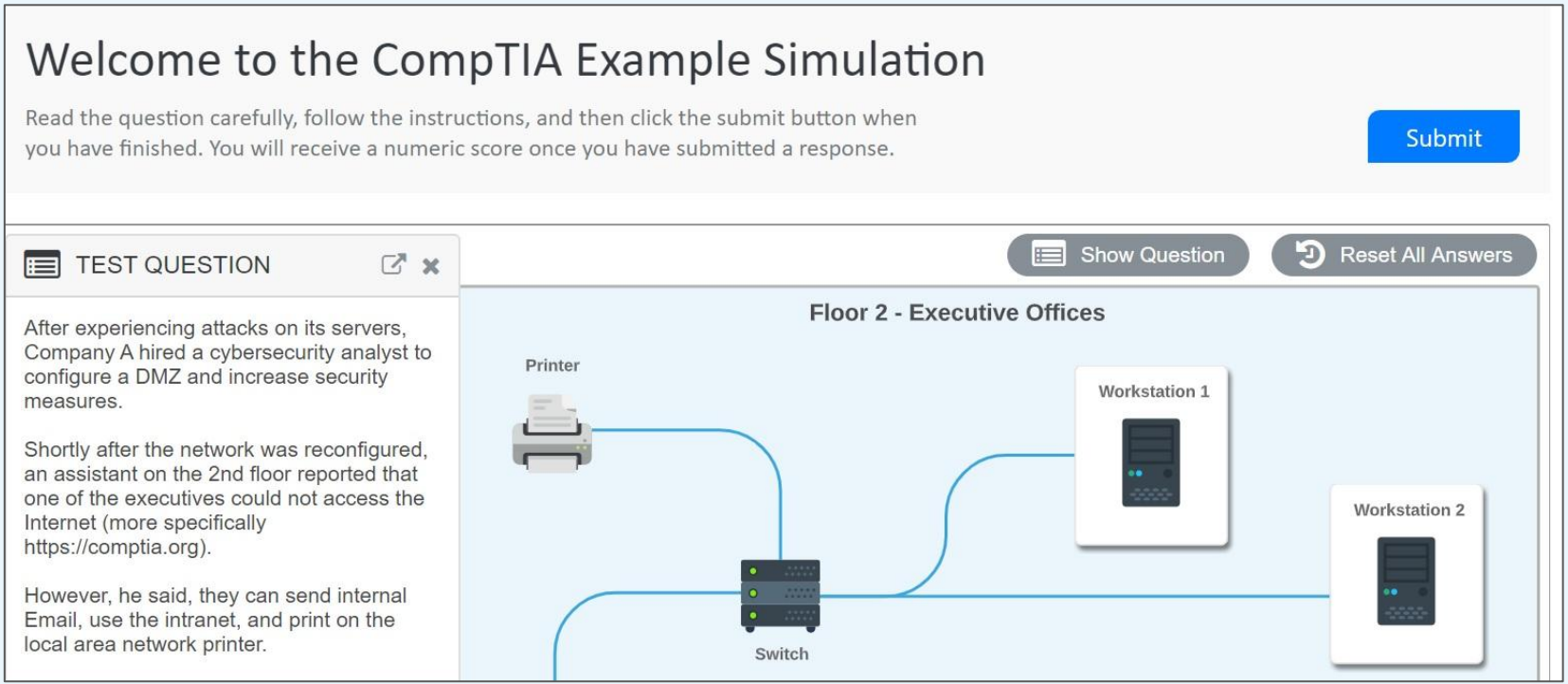
Since the question environment is simulated and not live, there may be some limitations compared to a real-world environment.



PBQs are often the first questions on the Security+ exam.

PBQs

In the next guided tour, we will explore Security+ PBQ questions.



https://simulation.comptia.org/

Instructor Demonstration

Security+ PBQs

Activity: Security+ PBQs

In this activity, you will work through several Security+ performance-based questions.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Next Class

We'll dive deeper into the various domains and topics of the Security+ exam.


The End