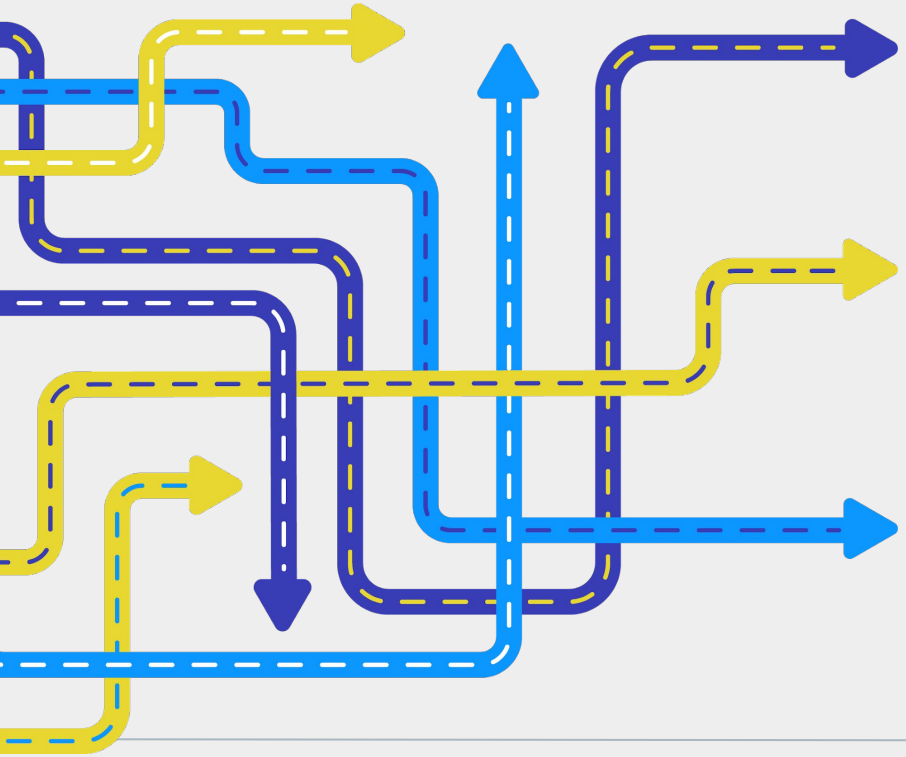
Introduction to InfoSec Certifications

Cybersecurity

Certification Prep Day 1

Class Objectives

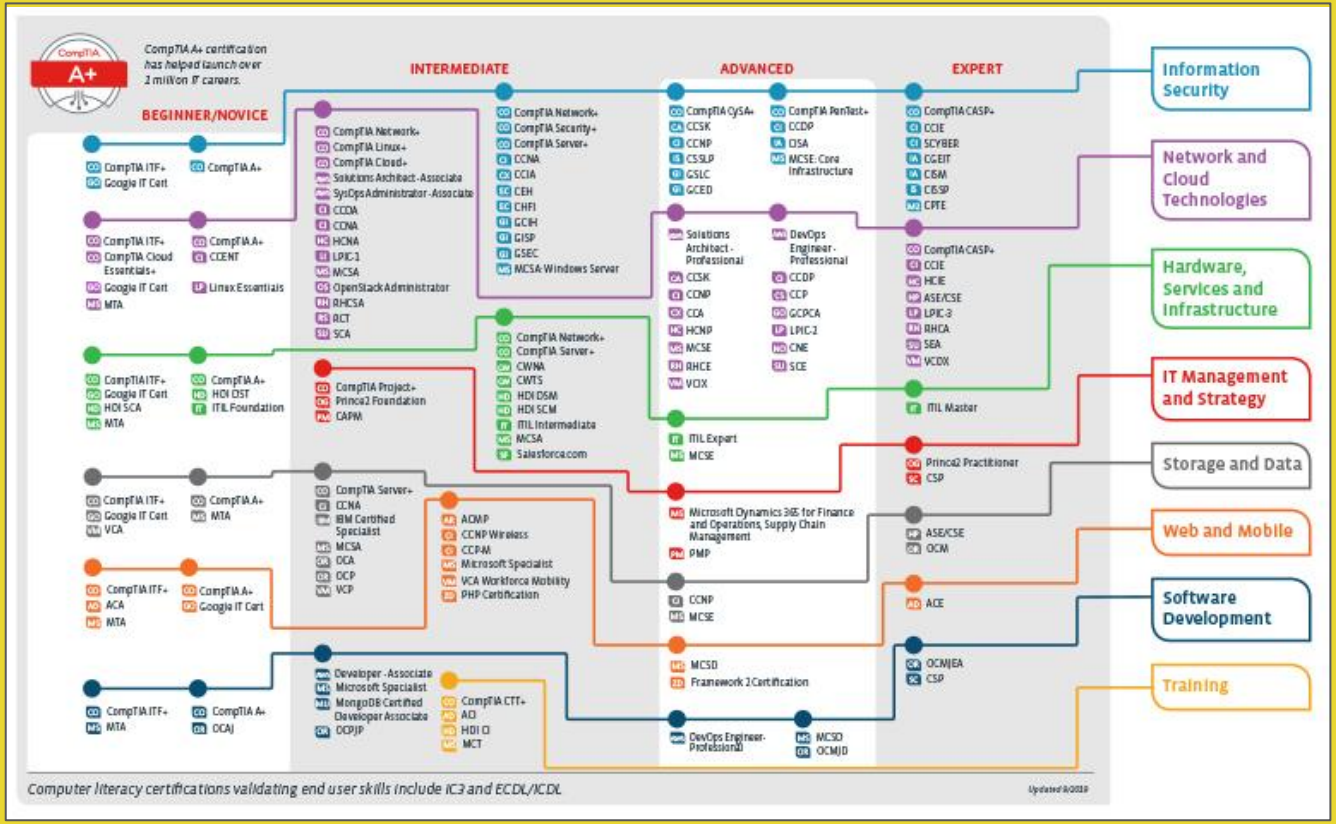
By the end of class, you will be able to:



- Explain 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.

Certifications by the Numbers

As of April 2020, there are 44 organizations that issue over 300 cybersecurity certifications, for 25 specializations and paths.



(certification.comptia.org)

While the amount of certifications, issuing organizations, and certification paths may seem overwhelming, this week we will navigate:

How certifications are beneficial to an infosec professional.

The difference between beginner, advanced, and specialized certifications.

The order in which certifications should be achieved.

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 with this certification.

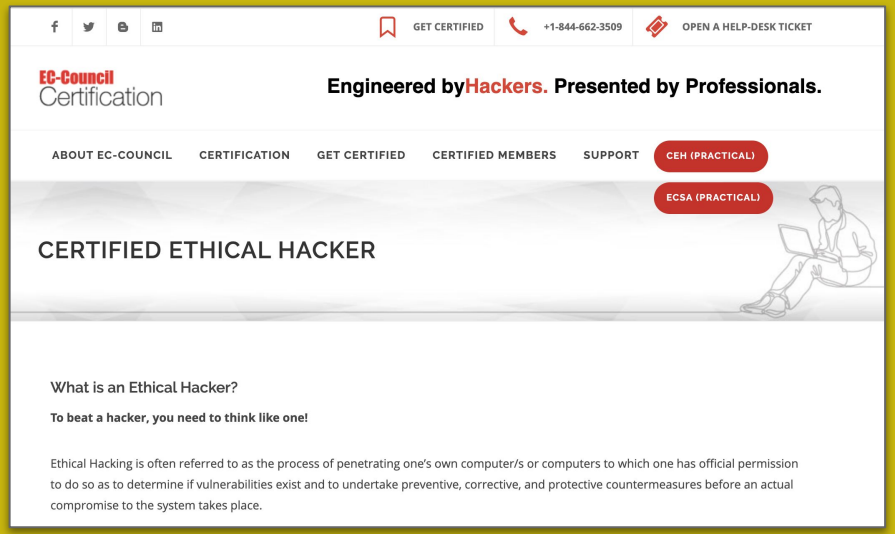
We will cover:

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

(comptia.org)

This Week

We will also briefly cover another beginner certification called **Certified Ethical Hacker** (CEH) and a popular advanced certification, **Certified Information Systems Security Professional** (CISSP).



(cert.eccouncil.org)

(isc2.org)

Benefits of InfoSec Certifications

Information Security Certifications

Certifications will give many new candidates an advantage when applying to their first cyber security jobs.

Certifications also provide the following benefits to all levels of infosec professionals:

01 Education

02 Networking

03 Career Advancement

Information Security Certifications

01

Education

Individuals will 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 during studying for the exam is also very 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.

Levels of InfoSec Certifications

Types of InfoSec Certifications

Certifications can be broken 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.

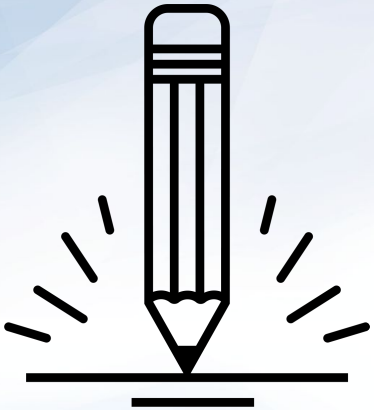
Certification Career Pathways

Certification Pathways

Penetration testers may follow this path:

Certification Pathways

Forensic investigators may follow this path:



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.

Beginner Certifications

While Security+ will likely be the first certification you'll work towards, 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 is generally focused 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.

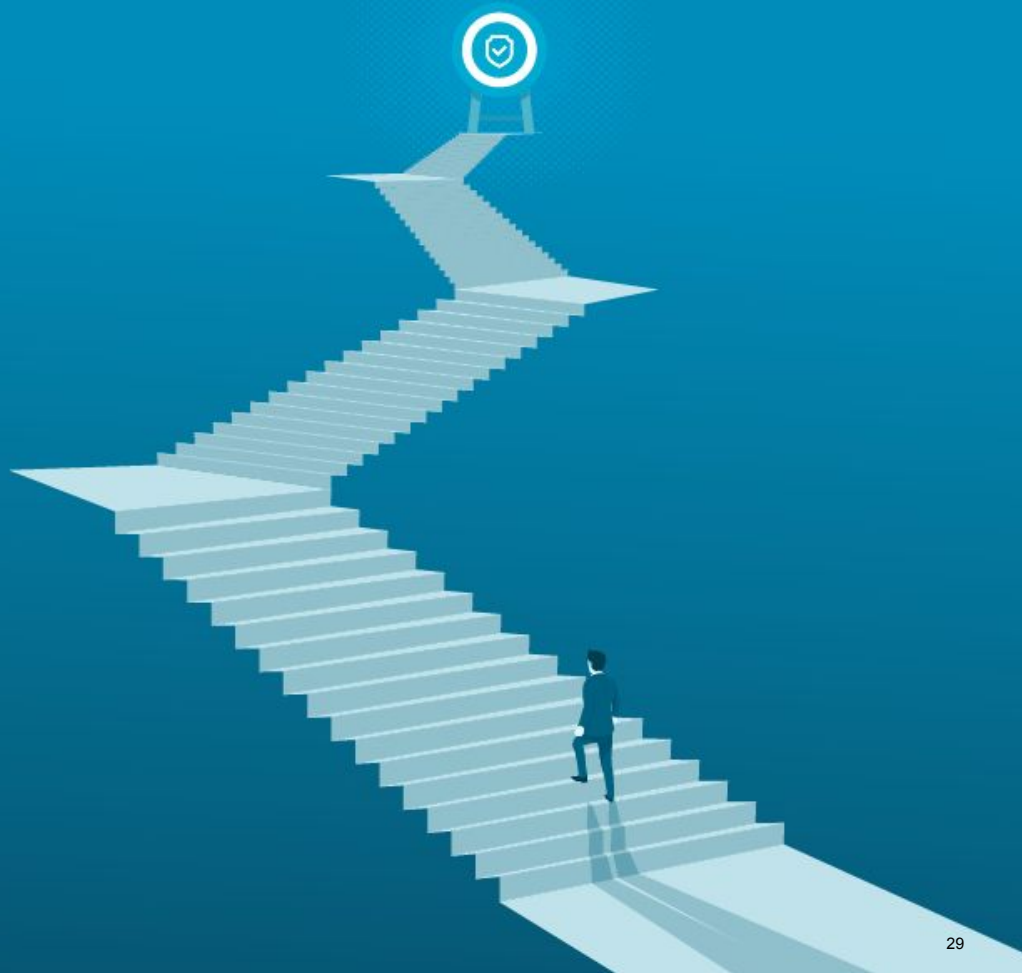
Systems Security Certified Professional (SSCP) is a certification offered by $(ISC)^2$ (“ISC squared”).

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

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

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 ISC2.

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

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.

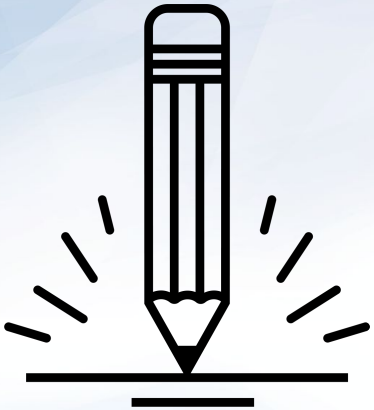
It is a practical exam consisting of two parts: a 24-hour penetration testing exam and a documentation report due 24 hours after the exam.

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: Advanced and Specialized Certifications

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

Suggested Time:
0:20

Time’s Up! Let’s Review.


Break

Security+ CertMaster

Introduction to Security+

What is a Security+?

According to **CompTIA**:

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

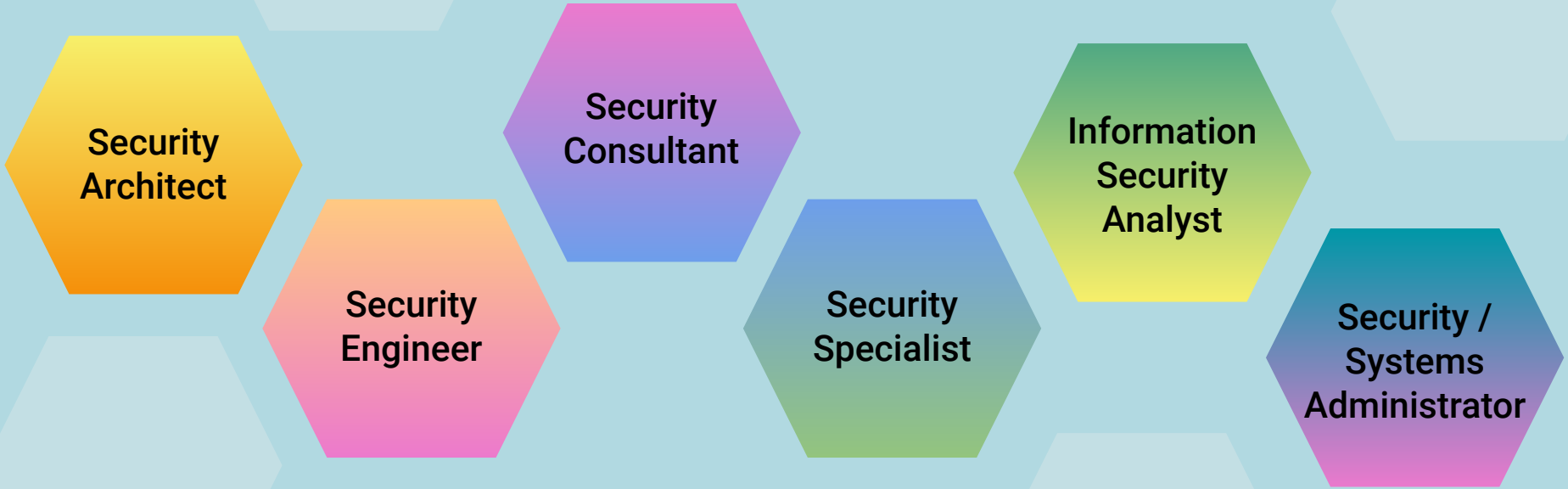
It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.

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

What are some jobs that may require the **Security+** certification?



As of June 2020, the average annual pay for an information security analyst in the United States is $99,944 a year.

Source: ZipRecruiter

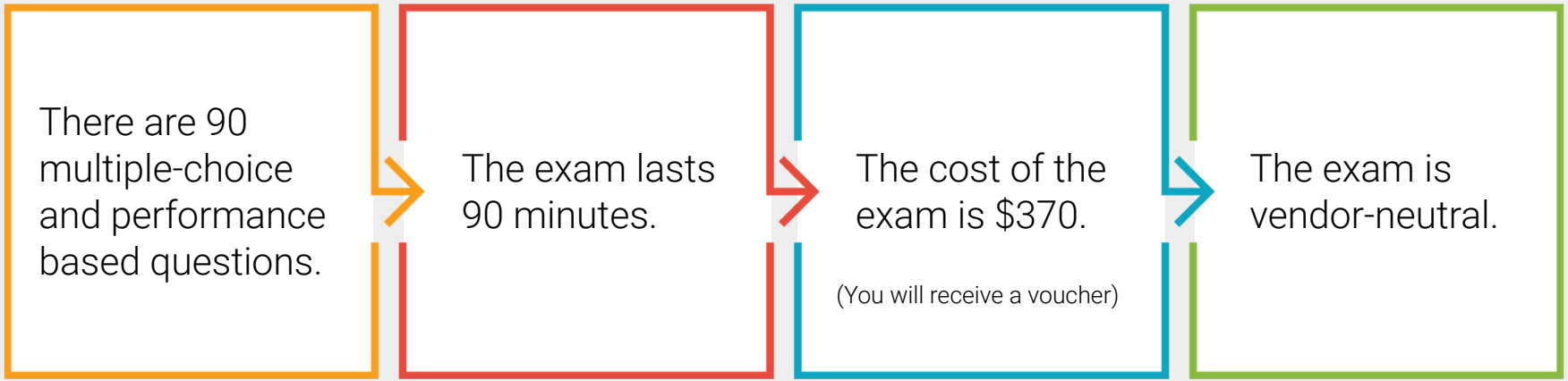
Introduction to Security+ Certification

What are some topics covered by Security+?

- 1.0 Attacks, Threats, and Vulnerabilities
- 2.0 Architecture and Design
- 3.0 Implementation
- 4.0 Operations and Incident Response
- 5.0 Governance, Risk, and Compliance

Security+ Specs

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



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 explaining 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

01

Take care of yourself. Arrive early, well-rested, fed, hydrated, and relaxed.

02

Pay attention. Read each question and each answer twice before deciding on your answer. Always stay aware of how much time remains.

03

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.

(Source)

Security+ CertMaster

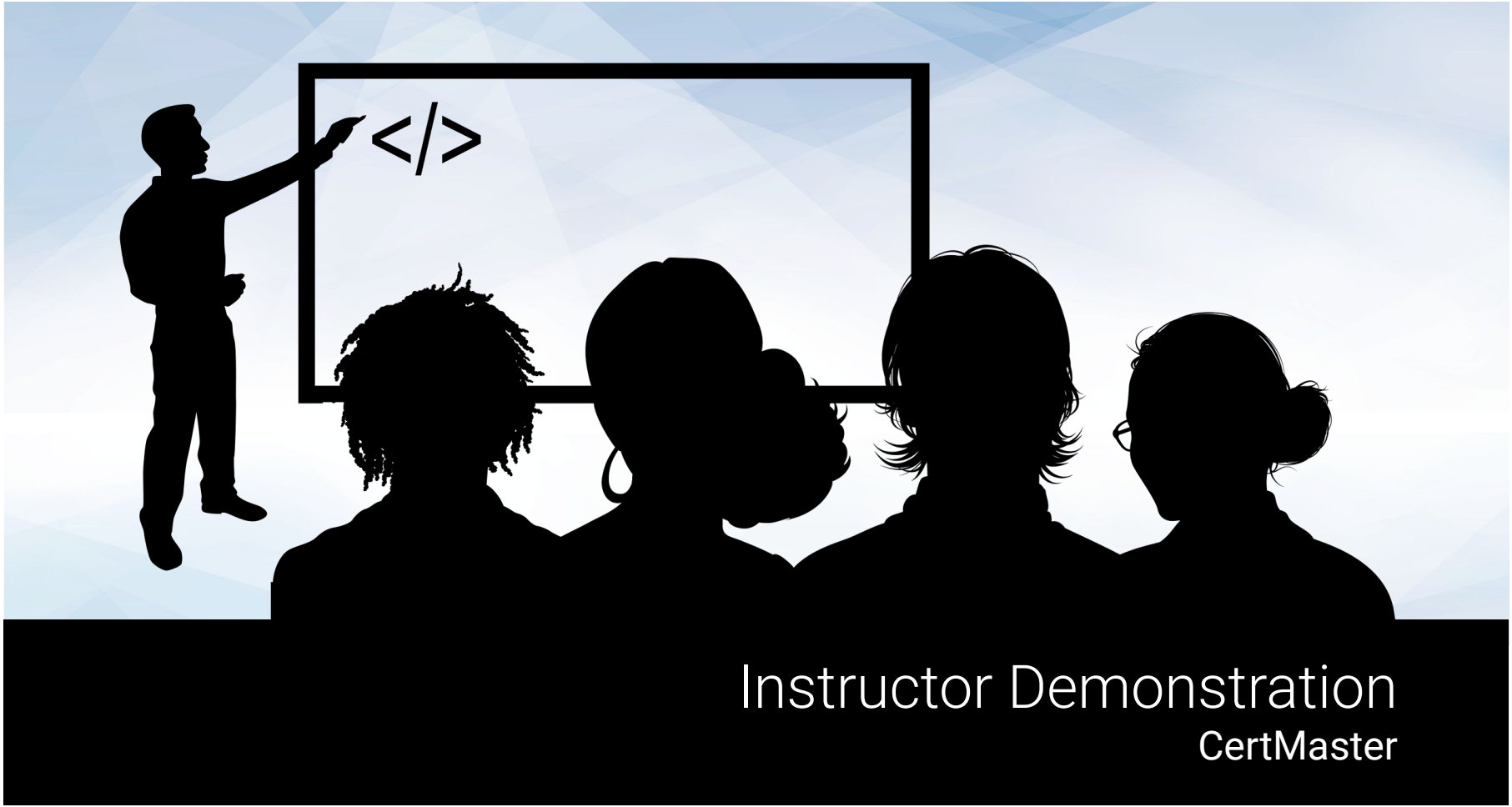
CertMaster Practice Tool

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

Per CompTIA, CertMaster Practice provides:

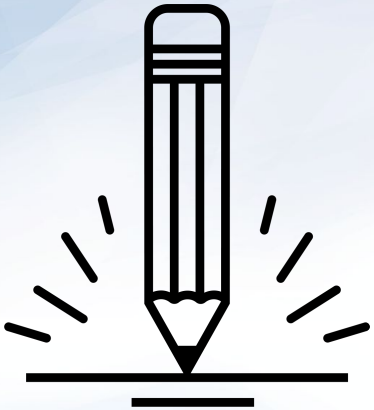
- Quick knowledge assessment.
- Adaptive learning that reinforces existing and new knowledge.
- Personalized feedback.
- Real-time learning analytics.

Now we will complete a walkthrough of the CertMaster tool and how to navigate the basic features.



Instructor Demonstration

CertMaster



Activity: Security+ CertMaster

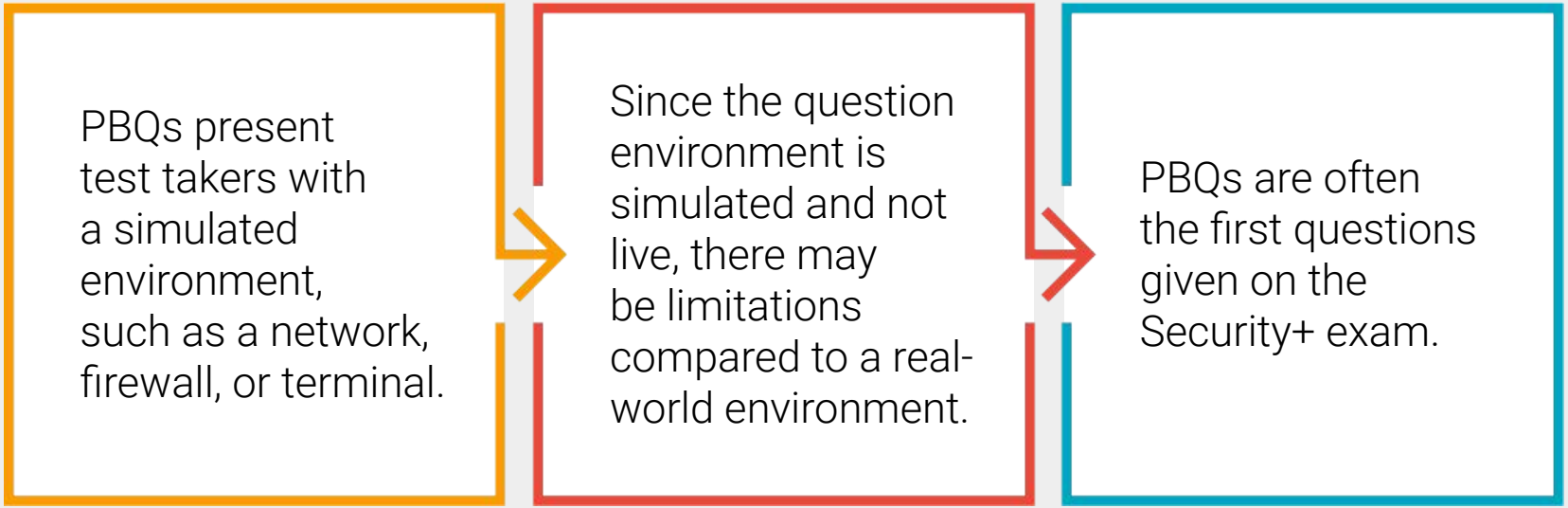
In this activity, you will access your Security+ CertMaster study tool and complete one module of 12 questions.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Performance Based Questions (PBQs)

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



Example Question: Performance-Based

Scenario: You are responsible for security at a small organization and have been tasked with implementing a security policy. Place the actions of organizing a security policy in their appropriate order. Note that there are five options, but you need to choose four.

Step 1 _____ > Step 2 _____ > Step 3 _____ > Step 4 _____

Possible choices:

- Obtain support and commitment from management
- Analyze risks to security
- Secure budgeting
- Review, test, and update procedures
- Implement appropriate controls

Example Question: Performance-Based

Scenario: You are responsible for security at a small organization and have been tasked with implementing a security policy. Place the actions of organizing a security policy in their appropriate order. Note that there are five options, but you need to choose four.

Step 1 _____ > Step 2 _____ > Step 3 _____ > Step 4 _____

Step 1: Obtain support and commitment from management

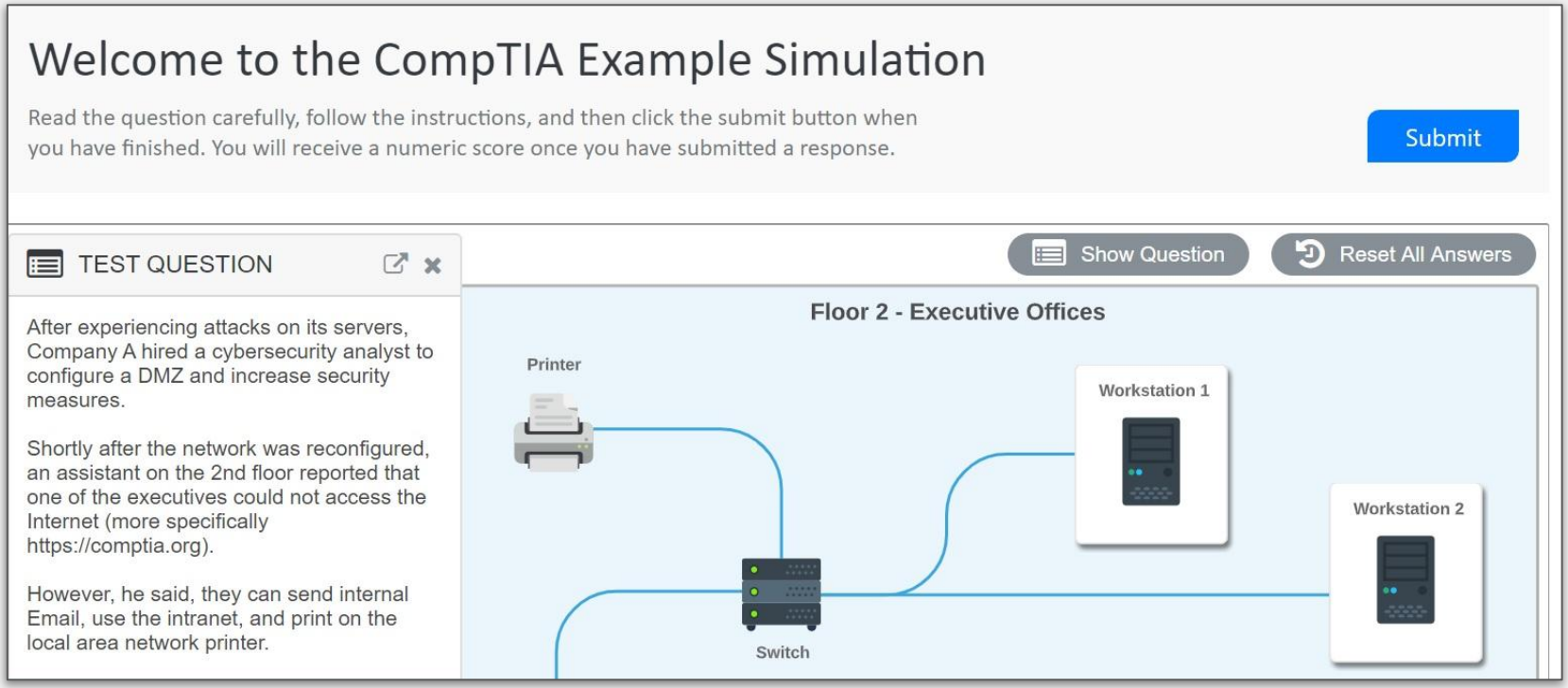
Step 2: Analyze risks to security

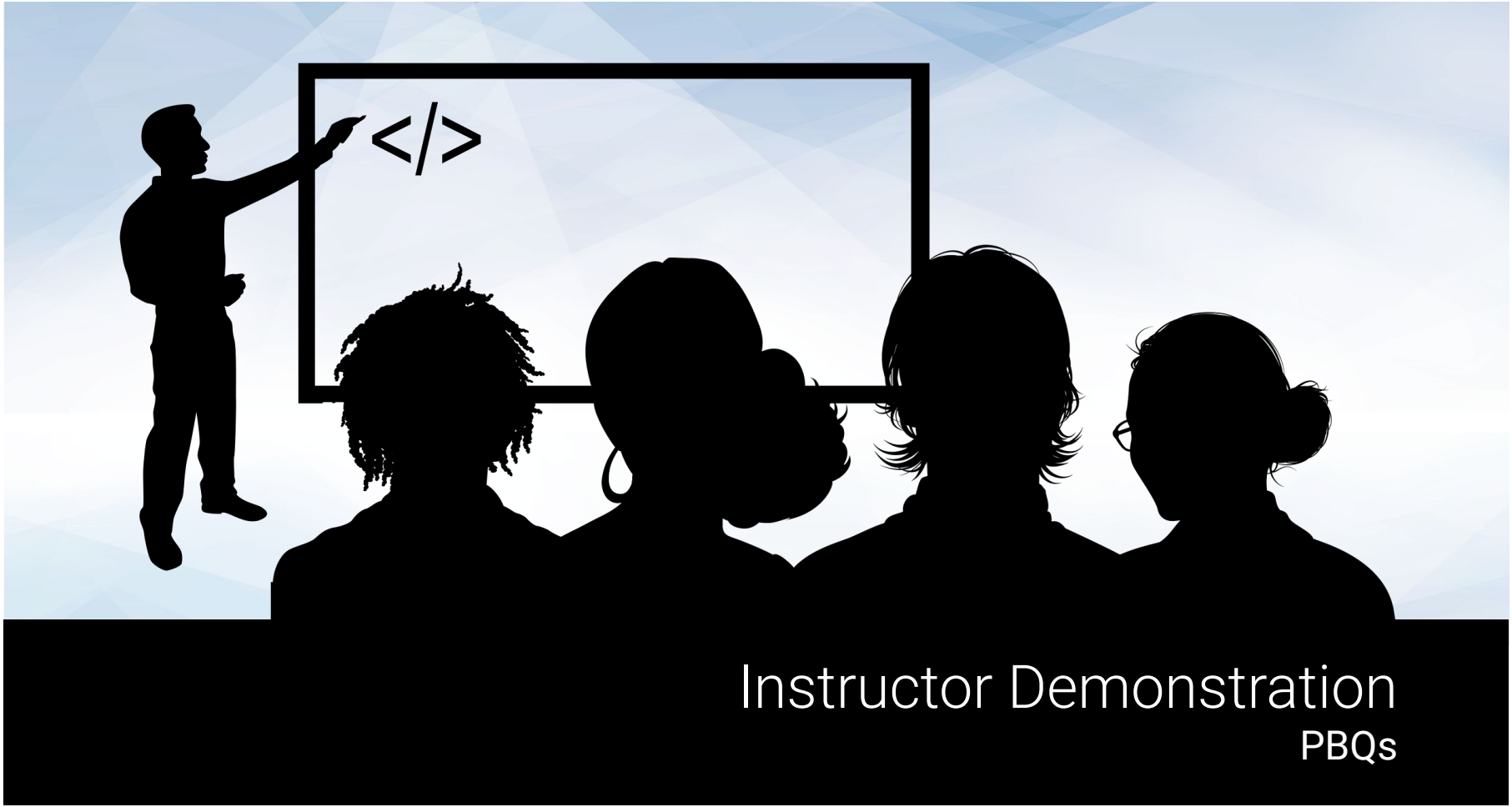
Step 3: Implement appropriate controls

Step 4: Review, test, and update procedures

PBQs

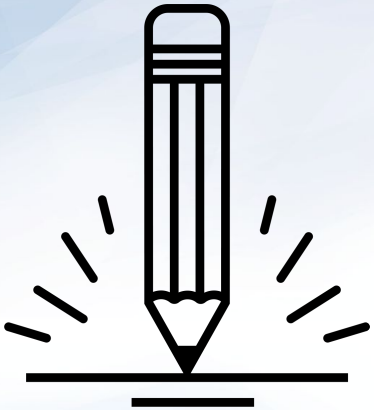
In the next guided tour, we will explore Security+ PBQ questions.





Instructor Demonstration

PBQs



Activity: Security+ PBQs

In this activity, you will work through several Security+ PBQ questions.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Next class, we'll dive deeper into the various domains and topics of the Security+ exam.


The End