This course supports the assessment for Security. The course covers 6 competencies and represents 4 competency units, and prepares for the CompTIA Security + (SY0-401) certification exam.

Introduction

Overview
How long do you think your business or organization would survive if your data was not secure? Computers can house social security numbers, financial data, educational records, health information, and even programs that control military weapons.

Long gone are the times when you only ensured that applications and systems were built to meet functional requirements. Security requirements are equally important, and existing systems are often overhauled to implement security measures. IT technology is constantly changing and so is the technology used by hackers and criminals. Security is a growing concern, and not just among IT professionals. Customers now consider how well an organization will protect their data when deciding with whom they will conduct business.

As an IT security professional, you are expected to implement techniques that secure networks and computers. Security attacks are on the rise and continue to be a concern for organizations worldwide. As a result, competent security professionals are in high demand. A career as an IT security professional will undoubtedly provide you with many opportunities in a variety of industries and organizational environments.

To be a competent security professional, you should know how to recognize and prevent security attacks, identify security needs for your organization, and understand encryption techniques. You should be able to effectively evaluate security risks and know how to leverage various access control models.

Watch the following video for an introduction to this course:

Note: To download this video, right-click the following link and choose "Save as...": download video.

Watch the following video for information on getting starting in this course:

Note: To download this video, right-click the following link and choose "Save as...": download video.

Competencies
This course provides guidance to help you demonstrate the following 6 competencies:

- Competency 419.2.1: Basic Security Concepts
The graduate identifies and discusses basic concepts of security and security threats, and recommends security procedures.

- **Competency 419.2.2: Access Control & Authentication Methods**
  The graduate recommends appropriate methods for controlling accessing data and information and for authenticating users and groups in gaining that access.

- **Competency 419.2.3: Security for Network Infrastructure**
  The graduate identifies security needs and recommends appropriate security practices for network infrastructure.

- **Competency 419.2.4: Encryption**
  The graduate identifies and explains the role of encryption in network security.

- **Competency 419.2.5: Security for Organizational Operations**
  The graduate explains and makes recommendations for appropriate security strategies and procedures for organizational operations.

- **Competency 419.2.6: Security Assessments & Audits**
  The graduate evaluates risks associated with network security and recommends monitoring strategies and methods.

**Course Instructor Assistance**

As you prepare to demonstrate competency in this subject, remember that course instructors stand ready to help you reach your educational goals. As subject matter experts, mentors enjoy and take pride in helping students become reflective learners, problem solvers, and critical thinkers. Course instructors are excited to hear from you and eager to work with you.

Successful students report that working with a course instructor is the key to their success. Course instructors are able to share tips on approaches, tools, and skills that can help you apply the content you're studying. They also provide guidance in assessment preparation strategies and troubleshoot areas of deficiency. Even if things don't work out on your first try, course instructors act as a support system to guide you through the revision process. You should expect to work with course instructors for the duration of your coursework, so you are welcome to contact them as soon as you begin. Course instructors are fully committed to your success!

**Preparing for Success**

The information in this section is provided to detail the resources available for you to use as you complete this course.

**Learning Resources**

The learning resources listed in this section are required to complete the activities in this course. For many resources, WGU has provided automatic access through the course. However, you may need to manually enroll in or independently acquire other resources. Read the full instructions provided to ensure that you have access to all of your resources in a timely manner.

*Note: If you decide to use other learning resources, particularly those found online, make certain that none qualify as a brain-dump. Using them can result in academic sanctions and loss of your certification.*
Note: Please see the full CompTIA Candidate Agreement.

Automatically Enrolled Resources

You will be automatically enrolled at the activity level for the following learning resources. Simply click on the links provided in the activities to access the learning materials.

You will access the following resource at the activity level within this course:

Your primary learning resource for this course is:

- uCertify

Launch Course

Your secondary learning resource for this course is:

The following Books24x7 e-texts will be used in this course:


Note: These e-texts are available to you as part of your program tuition and fees, but you may purchase hard copies at your own expense through a retailer of your choice. If you choose to do so, please use the ISBN listed to ensure that you receive the correct edition.

Pacing Guide

The pacing guide suggests a weekly structure to pace your completion of learning activities. It is provided as a suggestion and does not represent a mandatory schedule. Follow the pacing guide carefully to complete the course in the suggested timeframe.

Week 1

- Take the uCertify Pre-Assessment
- Read and take the quiz Lesson 1 – Measuring and Weighing Risk
- Read and take the quiz Lesson 2 – Monitoring and Diagnosing Networks
- Do lab section 1 and 2

Week 2

- Read and take the quiz Lesson 3 – Understanding Devices and Infrastructure
- Read and take the quiz Lesson 4 – Access Control, Authentication, and Authorization
- Do lab section 3 and 4

Week 3

- Read and take the quiz Lesson 5 – Protecting Wireless Networks
• Read and take the quiz Lesson 6 – Securing the Cloud
• Do lab section 5 and 6

Week 4

• Read and take the quiz Lesson 7 – Host, Data, and Application Security
• Read and take the quiz Lesson 8 – Cryptography
• Do lab section 7 and 8

Week 5

• Read and take the quiz Lesson 9 – Malware, Vulnerabilities, and Threats
• Read and take the quiz Lesson 10 – Social Engineering and other Foes
• Do lab section 9 and 10

Week 6

• Read and take the quiz Lesson 11 – Security Administration
• Read and take the quiz Lesson 12 – Disaster Recovery and Incident Response
• Do lab section 11 and 12

Week 7

• Review study materials in the e-text
• Make sure all labs and quizzes are completed in test mode scoring 90% or better
• Take any 3 of Practice Tests A through E in test mode scoring 90% or better
• Make sure all lab times are at 2 to 3 minutes each to prepare you for the simulation questions

Week 8

• Complete the uCertify post assessment with 90% or higher score
• Complete First Attempt Checklist

Note: This pacing guide does not replace the course. Please continue to refer to the course for a comprehensive list of the resources and activities.

uCertify Information

The following information pertains to uCertify and what will be covered in this course. Sections referenced correspond directly to the section in uCertify where the information is covered.

uCertify

The uCertify learning resource (CompTIA Security+) for this course contains the following:

• Pre-Assessment
• Chapters & Lessons
The uCertify Chapters & Lessons are constructed in a manner to build off previous lessons, so it is not recommended that you complete the sections out of order.

It is essential to read the materials prior to attempting the simulations to ensure you have a full and applicable understanding of the concepts and competencies required for successful completion of the practice exams.

Note: It is strongly recommended that you continue to attempt lab simulations until you can easily complete the tasks scoring 100% and pass practice exams with no less than 90% to maximize your chances of successfully passing the actual examination associated with this course.

This topic addresses the following competencies:

- **Competency 419.2.1: Basic Security Concepts**
  The graduate identifies and discusses basic concepts of security and security threats, and recommends security procedures.
- **Competency 419.2.2: Access Control & Authentication Methods**
  The graduate recommends appropriate methods for controlling accessing data and information and for authenticating users and groups in gaining that access.
- **Competency 419.2.3: Security for Network Infrastructure**
  The graduate identifies security needs and recommends appropriate security practices for network infrastructure.
- **Competency 419.2.4: Encryption**
  The graduate identifies and explains the role of encryption in network security.
- **Competency 419.2.5: Security for Organizational Operations**
  The graduate explains and makes recommendations for appropriate security strategies and procedures for organizational operations.
- **Competency 419.2.6: Security Assessments & Audits**
  The graduate evaluates risks associated with network security and recommends monitoring strategies and methods.

The Preassessment

The Pre-Assessment identifies areas for improvement with a 15 question assessment before you begin the course. Your performance on this assessment will help guide you to the areas on which you need to focus the most attention.
When you take this preassessment you should understand the following:

- take this exam without any outside help
- it is likely that you will get many of these questions wrong or find the test difficult
- the results will help you understand what you need to learn after going through the course content

Review the results of your pre-assessment with your mentor.

**uCertify Modules**

Direct your attention to the CompTIA Security+ exam objective(s) associated with each chapter. This will help you pinpoint those chapters that require special attention based on the results of your pre-assessment.

*Note: Because you are to complete the activities for this course within the uCertify learning resource, the following list of modules has been provided to*

- orient you as you begin the course, and
- provide an overview of the content you will be studying.

Access the following uCertify resource:

**Launch Course**

Complete all of the modules within the following sections:

- 1. Measuring and Weighing Risk
- 2. Monitoring and Diagnosing Networks
- 3. Understanding Devices and Infrastructure
- 4. Access Control, Authentication, and Authorization
- 5. Protecting Wireless Networks
- 6. Securing the Cloud
- 7. Host, Data, and Application Security
- 8. Cryptography
- 9. Malware, Vulnerabilities, and Threats
- 10. Social Engineering and Other Foes
- 11. Security Administration
- 12. Disaster Recovery and Incident Response

Please remember to proceed through the activities in the specified order.

**E-Text Reading**

Read the sections of the following text as they correspond to uCertify:

- *CompTIA Security+ Study Guide: SYO-401*
Transcender Practice Exam

The Transcender practice exam will help you gauge how prepared you are for the CompTIA Security+ exam.

Transcender Practice Exam
Take the Transcender practice exam to determine your readiness for the CompTIA Security+ exam.

This topic addresses the following competencies:

- **Competency 419.2.1: Basic Security Concepts**
  The graduate identifies and discusses basic concepts of security and security threats, and recommends security procedures.

- **Competency 419.2.2: Access Control & Authentication Methods**
  The graduate recommends appropriate methods for controlling accessing data and information and for authenticating users and groups in gaining that access.

- **Competency 419.2.3: Security for Network Infrastructure**
  The graduate identifies security needs and recommends appropriate security practices for network infrastructure.

- **Competency 419.2.4: Encryption**
  The graduate identifies and explains the role of encryption in network security.

- **Competency 419.2.5: Security for Organizational Operations**
  The graduate explains and makes recommendations for appropriate security strategies and procedures for organizational operations.

- **Competency 419.2.6: Security Assessments & Audits**
  The graduate evaluates risks associated with network security and recommends monitoring strategies and methods.

Transcender Practice Exam

Use the Transcender practice exams to help you determine your readiness for the CompTIA Security+ exam:

- [CompTIA Practice Exam for SY0-401 CompCert: Security+](#)

Final Steps

Congratulations on completing the activities in this course! This course has prepared you to complete the assessments associated with this course. If you have not already been directed to complete the assessments, schedule and complete your assessments now.

**uCertify Practice Exams**
Take the "Practice Exams" at the end of the course. This will provide you with valuable feedback about
• your readiness to take the Certification Exam, and
• more specifically, questions you miss and what section you can refer back to in order to complete additional study.

It is recommended that you take and pass the Practice Exams with a score of 90% or higher before considering yourself ready for the assessment.

First Attempt Checklist
One of the many things that makes WGU unique is its competency based education model. If you know the material, all you have to do is prove it by passing the exam. If you can do this, you can accelerate the receipt of your degree.

To make sure you have the best chance possible to pass the exam on your first attempt, the following should be completed before you refer to take it:

1. Complete the uCertify course in its entirety. Make sure the quiz and exercise for each lesson is completed at 90% in Test Mode, plus the practice exams and post-assessment at 90% in Test Mode as well. Ensure all labs are completed also.
2. Spend at least 6–8 weeks studying.
3. Contact your course instructors for additional input and insight.

After completing the above sections and passing, please speak to your program mentor to have your voucher emailed to you.

This course of study supports the CompTIA Security+ 401 exam. Your voucher gives you access to several different exams. Please ensure you register for the correct version of the Security+ 401 exam. If you are unsure of how to register for the correct exam, please contact your mentor.

If the first attempt is failed, you will be required to get in contact with the course instructor to see what went wrong and how you can prepare to make sure your second attempt is a success. Once the course instructor feels you are ready to refer for the second attempt of the exam, he or she will approve your second exam referral.

Outside Vendor Assessment
You will complete the CompTIA Security+, 2014 Edition Exam:

• Exam ID: CompTIA Security+ 2014 Objectives (SY0-401 or educational code JK0-022) exam
• Number of Items: 90
• Passing score: at least 750 out of 900 points to be considered "passed."
• Time Limit: 90 minutes

Note: Your voucher will show JK0-022, which is how CompTIA codes vouchers from educational institutions. The exam is the same as the SY0-401.
Note: Please note that CompTIA exams are no longer available at Prometric testing centers. Please see the CompTIA KnowledgeBase if you have questions.

For directions on how to receive access to outside vendor assessments, see the “Accessing Objective and Outside Vendor Assessments” page.

Submitting Outside Vendor Assessment Scores

After completing an outside vendor assessment, follow the directions for submitting a score report on the “Following Outside Vendor Assessments” page.