GEORGIA CYBER CENTER

Security+ Prep Course (Online/Blended Learning)

Rolling Enrollment begins 1 June 2020

FY 2020 Course Dates:

Session 1- 1 June 2020 – 30 November 2020
Session 2- 1 July 2020 – 31 December 2020
Session 3- 1 August 2020 – 31 January 2021
Session 4- 1 September 2020 – 28 February 2021

Course Costs: $995

- Price includes shipping, tax, credit card processing and any applicable administrative fees.

General Information

Description

CompTIA Security+ tests core knowledge required in any cybersecurity role while focusing on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection. The Security+ Certification is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements for IAM level I and IAT level II.

Course Material Details

Material Included

The following materials are included with the cost of the course and provided directly to the student.

- CompTIA Security+ Student Guide (Print version)
- CompTIA CertMaster Lab Access (6 months access)
- CompTIA Security+ Exam Voucher
- CompTIA CertMaster Practice Exam
- CompTIA Official Security+ Training Slides
- 5 weeks live instruction, review and tutoring by training expert on curriculum
- 6 months access to Distance Learning Portal
  - ✓ Custom Instructor Recorded Lecture (20+ hours)
  - ✓ CompTIA course videos
  - ✓ Custom quizzes and activities for every chapter

Link for Enrollment

https://gacybercenter.pdx.catalog.canvaslms.com/courses/sec2020

Expectations and Goals

This course prepares the learner over a course of 5 weeks to pass the CompTIA Security+ Exam. Access for up to 6 months to all the online content allow individuals that need to continue to review the material ample time to prepare for the certification exam. Topics and objectives include:

- **THREATS, ATTACKS & VULNERABILITIES**

Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts

- **TECHNOLOGIES & TOOLS**

Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security

- **ARCHITECTURE & DESIGN**

Implement secure network architecture concepts and systems design

- **IDENTITY & ACCESS MANAGEMENT**

Install and configure identity and access services, as well as management controls

- **RISK MANAGEMENT**

Implement and summarize risk management best practices and the business impact

- **CRYPTOGRAPHY & PKI**

Install and configure wireless security settings and implement public key infrastructure

Course Schedule

Week	Topic (Includes lecture/video/student guide reading and associated labs)
Week 1	Ch. 1- Comparing and Contrasting Attacks Ch. 2- Comparing and Contrasting Security Controls Ch. 3- Assessing Security Posture with Software Tools Ch. 4- Explaining Basic Cryptography Concepts
Week 2	Ch. 5- Implementing a Public Key Infrastructure Ch. 6- Implementing Identity and Access Management Controls Ch. 7- Managing Access Services and Accounts Ch.8- Implementing a Secure Network Architecture
Week 3	Ch. 9- Installing and Configuring Security Appliances Ch. 10- Installing and Configuring Wireless and Physical Access Security Ch. 11- Deploying Secure Host, Mobile, and Embedded Systems Ch. 12- Implementing Secure Network Access Protocols
Week 4	Ch. 13- Implementing Secure Network Applications Ch. 14- Explaining Risk Management and Disaster Recovery Concepts Ch. 15- Summarizing Secure Application Development Concepts Ch. 16- Explaining Organizational Security Concepts
Week 5	Review/Summary of material Take Practice Exam Schedule Certification Exam through CompTIA