**Apex Program 10-week course description | 2023**

Apex Program prepares students with the knowledge and skills required to confidently take on the CompTIA A+ and Security+ certification exam series and pursue a career in cybersecurity. The 10-week program is designed for accessibility by IT professionals who’ve navigated BVI and veterans’ realities as a part of the cybersecurity workforce. Each week focuses on a core area of IT security and follows a defined course schedule.

Because all students learn differently, Apex Program takes a multi-format approach to instruction. Foundational cybersecurity topics are explored through informative lectures and video tutorials, then students are able to actively test their knowledge with hands-on labs and quizzes. At each step of a student’s journey with Apex Program, they have access to expert instructors for additional guidance and support.

\_\_

**Step-by-step Apex Program student journey**

All classes are offered virtually at a set time, with pre-set starting and ending dates following a traditional work week.

**Weeks 1-4:** Preparation for CompTIA A+ certification exam.

This 4-week course block prepares students for the CompTIA A+ Certification exam. It provides 2 weeks of lecture followed by 2 weeks of practice exams, quizzes, and video tutorials. Each week offers 20 hours of dedicated course experience, with homework designed to help students hone their understanding of core IT security concepts.

**1-2:** 20 hours of lecture, homework, and quizzes over 5 days.

**3-4:** 20 hours of test preparation including quizzes, practice exams, and other material.

**Weeks 5-8:** Preparation for CompTIA Security+ certification exam.

With a newfound understanding of the core IT security concepts required for the CompTIA A+ Certification, the student begins preparation for the CompTIA Security+ exam. They’ll receive 2 weeks of lecture followed by 2 weeks of practice exams, quizzes, and video tutorials. Each week offers 20 hours of dedicated course experience, with homework designed to help students hone their understanding of core IT security concepts.

**5-6:** 20 hours of lecture, homework, and quizzes over 5 days.

**7-8:** 20 hours of test preparation including quizzes, practice exams, and other material.

**Weeks 9-10:** Cyberanalysis & SIEM focus for the Security+ certification exam.

In the final two weeks of Apex Program, students get 50 hours of expert-guided, hands-on experience with a leading security information and event management (SIEM) software. Our interactive lab is designed to teach students how to put their fresh security analysis and response knowledge into action, including focused lessons on log assessment, security event management, and report preparation.

**9:** 30 hours of a hands on lab with security incident event management software.

**10:** 20 hours of hands-on event analysis, investigation, and reporting.

\_\_

**A partnership in pursuit of excellent: Apex Program + CompTIA**

**CompTIA A+**

The CompTIA A+ certification is an industry recognized credential, seen by organizations across the globe as a marker of IT skill and understanding. Today, the A+ certification appears in more IT job descriptions than any other credential, preparing professionals to build a career as an:

* Associate Network Engineer
* Data Support Technician
* Desktop Support Administrator
* Field Service Technician
* Help Desk Tech
* Service Desk Analyst
* Technical Support Specialist

With A+ certification training by Apex Program, you’ll learn how to support technologies core to a career in cybersecurity, including:

**Hardware:** Identifying, using, and connecting hardware components and devices, including the broad knowledge about different devices that is now necessary to support the remote workforce

**Operating systems:** Install and support Windows OS including command line & client support. System configuration imaging and troubleshooting for Mac OS, Chrome OS, Android and Linux OS.

**Software troubleshooting:** Troubleshoot PC and mobile device issues including common OS, malware and security issues.

**Networking:** Explain types of networks and connections including TCP/IP, WIFI and SOHO

**Network troubleshooting:** Troubleshoot real-world device and network issues quickly and efficiently

**Security:** Identify and protect against security vulnerabilities for devices and their network connections

**Mobile devices:** Install & configure laptops and other mobile devices and support applications to ensure connectivity for end- users

**Cloud computing and virtualization:** Compare & contrast cloud computing concepts & set up client-side virtualization

**Operational procedures:** Follow best practices for safety, environmental impacts, and communication and professionalism

**CompTIA Security+**

The CompTIA Security+ certification will ground you in knowledge and practice required of today’s intermediate-level cybersecurity roles. The Security+ certification is selected by more corporations and defense organizations than any other certification to validate core security skills and for fulfilling the DoD 8570 compliance. Security+ offers hands-on experience, incorporating best practices in analysis and troubleshooting so candidates are prepared to:

* Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
* Monitor and secure hybrid environments, including cloud, mobile, and IoT
* Operate with an awareness of applicable laws and policies so you can mitigate organizational risk, applying frameworks, policies, procedures, and controls
* Identify, analyze, and respond to security events and incidents using the appropriate response procedures, analyze potential indicators of compromise, and utilize basic digital forensics techniques

With Security+ certification training by Apex Program, you’ll also learn advanced skills that are key to applying behavioral analytics to networks and devices to identify and take on threats through continuous security monitoring in a Security Operations Center, including the ability to:

* Deliver proactive threat intelligence to support organizational security and perform vulnerability management activities
* Apply security solutions for infrastructure management, with the ability to explain hardware and software assurance best practices
* Analyze data as part of continuous security monitoring activities and implement configuration changes to improve security