Live Online Training (LOT)
Course Catalog

Virtual Campus

3500 Lacey Road, Suite 100

Downers Grove IL 60515

Website: www.comptia.org

Email: comptiavirtualtraining@comptia.org

Telephone: 866-835-8020

Version 2.0, Effective date: 02/20/2024

Table of Contents

History

The Computing Technology Industry Association (CompTIA) has long been a leading voice and advocate for the global information technology ecosystem through education, training, certifications, philanthropy, and market research. In an effort to promote industry growth and further develop a highly skilled workforce with more opportunities for all, CompTIA is now offering Live Online Training ("LOT") programs for its vendor-neutral certifications direct to students. CompTIA is headquartered in Downers Grove, Illinois and operates a virtual campus for instruction.

Mission

CompTIA exists to unlock potential for companies seeking to grow their information technology business and for individuals seeking to establish or further their tech career.

CompTIA Live Online Training Board Members, Key Staff, and Faculty

Board Members:

Courtney Fong, CompTIA Chief Operating Officer
Brian Laffey, CompTIA Chief Financial Officer
Todd Thibodeaux, CompTIA Chief Executive Officer

Key Staff:

Steven Bejarano, Director, Faculty Academy
Margaret Casey, Senior Specialist, Program Delivery & Bursar
Blythe Girnus, Vice President, Training Delivery
Kathy Johnson, Specialist, Faculty and Resource Management
Jean Link, Specialist, Program Delivery & Registrar
Dave Moehle, Faculty Lead
Guy Mor, Senior Director, Program Delivery

Faculty:

See Addendum 1 for a list of institutional faculty and program(s) taught

Location and Hours of Operation

Downers Grove, Illinois Headquarters and Corporate Office

Location: CompTIA's headquarters and corporate office are located at 3500 Lacey Road, Suite 100, in the city of Downers Grove, IL 60515, on the ground floor of a thirteen-story high-rise building. The building is located near the I-88, the East-West Tollway, and 1-355, the North-South Tollway.

Hours of Operation: 8:30 AM to 4:30 PM Central Time (CT), Monday through Friday. Closed Saturdays, Sundays, and major holidays.

Phone number: Telephone: 866-835-8020

Online Campus

Online Instruction Hours

CompTIA Live Online Training (LOT) cohort sessions will be running from 9:00 AM to 8:00 PM CT, Monday through Friday. Closed Saturdays, Sundays, and major holidays. All LOT programs are held in Central time.

Phone number: Telephone: 866-835-8020

Facilities & Equipment

Online Campus

Each virtual online program session of CompTIA's LOT programs can accommodate up to 35 students and one (1) instructor.

Equipment

CompTIA's online campus does not provide computer equipment or internet access to students. Students will need access to the internet and a reliable laptop or desktop computer with a current web browser or a mobile device.

Disclosures

State Authorization

CompTIA is a private vocational institution that is approved by the Division of Private Business and Vocational Schools of the Illinois Board of Higher Education.

Accreditation

CompTIA is not accredited by an accrediting agency that is nationally recognized by the U.S. Department of Education.

2024 CompTIA Live Online Training Program Schedule and Holidays

CompTIA Holidays (No Class Scheduled)

Holiday	Date Observed
New Year's Day	1/1/2024
Martin Luther King Jr. Day	1/15/2024
President's Day	2/19/2024
Memorial Day	5/27/2024
Juneteenth	6/19/2024
Independence Day	7/4/2024
Labor Day	9/2/2024
Veteran's Day	11/11/2024
Thanksgiving Break	11/28/2024 – 11/29/2024
Holiday Break	12/23/2024 – 12/31/2024

CompTIA A+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA A+ LOT	1/08/2024	2/05/2024	M-F, 10:00 AM - 1:00 PM
CompTIA A+ LOT	1/08/2024	2/05/2024	M-F, 6:00 – 9:00 PM
CompTIA A+ LOT	1/16/2024	2/12/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	1/29/2024	2/26/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	1/29/2024	2/26/2024	M-F, 6:00 – 9:00 PM
CompTIA A+ LOT	2/26/2024	3/22/2024	M-F, 10:00 – 1:00 PM
CompTIA A+ LOT	3/11/2024	4/05/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	3/18/2024	4/12/2024	M-F, 1:00 – 4:00 PM
CompTIA A+ LOT	4/01/2024	4/26/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	4/08/2024	5/03/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	4/29/2024	5/24/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	5/06/2024	6/03/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	5/20/2024	6/18/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	6/03/2024	7/01/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	6/18/2024	7/16/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	7/01/2024	7/29/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	7/08/2024	8/02/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	7/29/2024	8/23/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	8/12/2024	9/09/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	9/03/2024	9/30/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	9/09/2024	10/04/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	9/23/2024	10/18/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	9/23/2024	10/21/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	9/30/2024	10/28/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	10/15/2024	11/12/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	10/28/2024	11/25/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	11/04/2024	12/04/2024	M-F, 5:00 – 8:00 PM
CompTIA A+ LOT	11/12/2024	12/11/2024	M-F, 10:00 AM – 1:00 PM
CompTIA A+ LOT	11/18/2024	12/17/2024	M-F, 5:00 – 8:00 PM

CompTIA Security+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA Security+ LOT	01/08/24	01/22/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	01/16/24	01/29/24	M-F, 8:00 – 11:00 AM
CompTIA Security+ LOT	01/22/24	02/02/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	01/22/24	02/02/24	M-F, 6:00 – 9:00 PM
CompTIA Security+ LOT	01/29/24	02/09/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	02/05/24	02/16/24	M-F, 10:00 – 1:00 PM
CompTIA Security+ LOT	02/12/24	02/26/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	02/20/24	03/04/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	02/26/24	03/08/24	M-F, 2:00 – 5:00 PM
CompTIA Security+ LOT	03/04/24	03/15/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	03/04/24	03/15/24	M-F, 6:00 – 9:00 PM
CompTIA Security+ LOT	03/11/24	03/22/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	03/18/24	03/29/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	03/25/24	04/05/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	04/01/24	04/12/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	04/08/24	04/19/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	04/15/24	04/26/24	M-F, 2:00 – 5:00 PM
CompTIA Security+ LOT	04/22/24	05/03/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	04/29/24	05/10/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	04/29/24	05/10/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	05/06/24	05/17/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	05/13/24	05/24/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	05/20/24	06/03/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	05/28/24	06/10/24	M-F, 2:00 – 5:00 PM
CompTIA Security+ LOT	06/03/24	06/14/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	06/10/24	06/24/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	06/18/24	07/01/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	07/01/24	07/15/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	07/01/24	07/15/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	07/08/24	07/19/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	07/15/24	07/26/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	07/22/24	08/02/24	M-F, 2:00 – 5:00 PM
CompTIA Security+ LOT	07/29/24	08/09/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	07/29/24	08/09/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	08/05/24	08/16/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	08/05/24	08/16/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	08/12/24	08/23/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	08/12/24	08/23/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	08/19/24	08/30/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	08/19/24	08/30/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	08/26/24	09/09/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	09/03/24	09/16/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	09/03/24	09/16/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	09/09/24	09/20/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	09/09/24	09/20/24	M-F, 2:00 – 5:00 PM
CompTIA Security+ LOT	09/16/24	09/27/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	09/16/24	09/27/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	09/23/24	10/04/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	09/30/24	10/11/24	M-F, 10:00 AM – 1:00 PM

CompTIA Security+ LOT	10/07/24	10/21/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	10/07/24	10/21/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	10/15/24	10/28/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	10/15/24	10/28/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	10/21/24	11/01/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	10/28/24	11/08/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	10/28/24	11/08/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	11/04/24	11/18/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	11/12/24	11/25/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	11/18/24	12/03/24	M-F, 2:00 – 5:00 PM
CompTIA Security+ LOT	11/25/24	12/10/24	M-F, 10:00 AM – 1:00 PM
CompTIA Security+ LOT	11/25/24	12/10/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	12/02/24	12/13/24	M-F, 5:00 – 8:00 PM
CompTIA Security+ LOT	12/06/24	12/19/24	M-F, 10:00 AM – 1:00 PM

CompTIA Network+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA Network+ LOT	01/08/24	01/22/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	01/22/24	02/02/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	02/05/24	02/16/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	02/20/24	03/04/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	03/04/24	03/15/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	03/18/24	03/29/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	04/08/24	04/19/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	04/15/24	04/26/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	04/29/24	05/10/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	05/13/24	05/24/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	06/03/24	06/14/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	06/18/24	07/01/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	07/01/24	07/15/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	07/15/24	07/26/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	08/05/24	08/16/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	08/12/24	08/23/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	09/03/24	09/16/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	09/16/24	09/27/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	09/30/24	10/11/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	10/15/24	10/28/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	10/28/24	11/08/24	M-F, 5:00 – 8:00 PM
CompTIA Network+ LOT	11/04/24	11/18/24	M-F, 10:00 AM – 1:00 PM
CompTIA Network+ LOT	12/02/24	12/13/24	M-F, 5:00 – 8:00 PM

CompTIA Data+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA Data+ LOT	02/20/24	03/04/24	M-F, 10:00 AM – 1:00 PM
CompTIA Data+ LOT	03/25/24	04/05/24	M-F, 10:00 AM – 1:00 PM
CompTIA Data+ LOT	05/06/24	05/17/24	M-F, 10:00 AM – 1:00 PM
CompTIA Data+ LOT	06/03/24	06/14/24	M-F, 5:00 – 8:00 PM
CompTIA Data+ LOT	07/29/24	08/09/24	M-F, 5:00 – 8:00 PM
CompTIA Data+ LOT	09/16/24	09/27/24	M-F, 10:00 AM – 1:00 PM

CompTIA PenTest+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA PenTest+ LOT	04/01/24	04/12/24	M-F, 5:00 – 8:00 PM
CompTIA PenTest+ LOT	05/13/24	05/24/24	M-F, 10:00 AM – 1:00 PM
CompTIA PenTest+ LOT	07/08/24	07/19/24	M-F, 10:00 AM – 1:00 PM
CompTIA PenTest+ LOT	09/09/24	09/20/24	M-F, 10:00 AM – 1:00 PM
CompTIA PenTest+ LOT	10/15/24	10/28/24	M-F, 10:00 AM – 1:00 PM
CompTIA PenTest+ LOT	11/04/24	11/18/24	M-F, 10:00 AM – 1:00 PM
CompTIA PenTest+ LOT	11/25/24	12/10/24	M-F, 5:00 – 8:00 PM

CompTIA CySA+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA CySA+ LOT	01/22/24	02/02/24	M-F, 5:00 – 8:00 PM
CompTIA CySA+ LOT	01/29/24	02/09/24	M-F, 10:00 AM – 1:00 PM
CompTIA CySA+ LOT	02/26/24	03/08/24	M-F, 5:00 – 8:00 PM
CompTIA CySA+ LOT	03/18/24	03/29/24	M-F, 10:00 AM – 1:00 PM
CompTIA CySA+ LOT	04/22/24	05/03/24	M-F, 10:00 AM – 1:00 PM
CompTIA CySA+ LOT	05/13/24	05/24/24	M-F, 5:00 – 8:00 PM
CompTIA CySA+ LOT	06/10/24	06/24/24	M-F, 10:00 AM – 1:00 PM
CompTIA CySA+ LOT	07/15/24	07/26/24	M-F, 5:00 – 8:00 PM
CompTIA CySA+ LOT	08/05/24	08/16/24	M-F, 10:00 AM – 1:00 PM
CompTIA CySA+ LOT	09/09/24	09/20/24	M-F, 5:00 – 8:00 PM
CompTIA CySA+ LOT	10/15/24	10/28/24	M-F, 10:00 AM – 1:00 PM
CompTIA CySA+ LOT	11/04/24	11/18/24	M-F, 10:00 AM – 1:00 PM
CompTIA CySA+ LOT	12/02/24	12/13/24	M-F, 10:00 AM – 1:00 PM

CompTIA Project+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA Project+ LOT	01/16/24	01/29/24	M-F, 10:00 AM – 1:00 PM
CompTIA Project+ LOT	04/08/24	04/19/24	M-F, 5:00 PM – 8:00 PM
CompTIA Project+ LOT	07/08/24	07/19/24	M-F, 5:00 PM – 8:00 PM
CompTIA Project+ LOT	07/15/24	07/26/24	M-F, 5:00 PM – 8:00 PM
CompTIA Project+ LOT	09/09/24	09/20/24	M-F, 10:00 AM – 1:00 PM
CompTIA Project+ LOT	10/07/24	10/21/24	M-F, 10:00 AM – 1:00 PM
CompTIA Project+ LOT	11/04/24	11/18/24	M-F, 5:00 PM – 8:00 PM

CompTIA Linux+ Live Online Training (LOT) Program

Program	Start Date	End Date	Times
CompTIA Linux+ LOT	03/04/24	03/15/24	M-F, 5:00 PM – 8:00 PM
CompTIA Linux+ LOT	09/23/24	10/04/24	M-F, 10:00 AM – 1:00 PM
CompTIA Linux+ LOT	10/07/24	10/21/24	M-F, 5:00 PM – 8:00 PM
CompTIA Linux+ LOT	10/21/24	11/01/24	M-F, 10:00 AM – 1:00 PM
CompTIA Linux+ LOT	11/04/24	11/18/24	M-F, 5:00 PM – 8:00 PM
CompTIA Linux+ LOT	11/25/24	12/10/24	M-F, 10:00 AM – 1:00 PM
CompTIA Linux+ LOT	12/06/24	12/19/24	M-F, 5:00 PM – 8:00 PM

CompTIA A+ Live Online Training Program

Program Description

The CompTIA A+ certification is the industry standard for establishing a career in IT and the preferred qualifying credential for technical support and IT operational roles. Candidates are better prepared to troubleshoot and problem solve, and technicians better understand a wide variety of issues ranging from networking and operating systems to mobile devices and security. The CompTIA A+ certification supports the ability to connect users to the data they need to do their jobs regardless of the devices being used.

The CompTIA A+ Live Online Training program consists of 60 clock hours of instruction over four (4) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA A+ certification examinations (CompTIA A+ 220-1101 "Core 1" and CompTIA A+ 220-1102 "Core 2").

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA A+ examinations; students receive this certification from a third party through an examination process. The cost of the program includes twenty (20) days of instructor-led online training, CertMaster Practice for CompTIA A+ Core 1 and Core 2, CertMaster Labs for CompTIA A+ Core 2, CertMaster Learn for instructor-led training for CompTIA A+, a CompTIA A+ 220-1101 Core 1 examination voucher, a CompTIA A+ 220-1102 Core 2 examination voucher, and one (1) examination retake voucher for each examination.

This program prepares students for a Computer User Support Specialist or equivalent entry-level IT help desk role (CIP Code 11.1006, "Computer Support Specialist"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA A+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA A+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA A+ Live Online Training program does not provide computer equipment or internet access. Students will need access to the internet and a reliable laptop or desktop computer, or mobile device. Webcams are not required.

Learning Resources for Program Content

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA A+ throughout this program.

CompTIA A+ Live Online Training Program Outline (Syllabus)

Day	Lessons	Activities
1	**Lesson 1: Installing Motherboards and Connectors** • Explain cable types and connectors • Install and configure motherboards • Explain legacy cable types	• Class Introductions • Code of Conduct • Review CertMaster Learn, Labs and Practice resources • Virtual WorkBench Lab: Upgrading/ Installing GPU and Daisy-Chain Monitors • Virtual Workbench Lab: Install a Motherboard
2	**Lesson 2: Installing System Devices** • Install and configure power supplies and cooling • Select and install storage devices • Install and configure system memory • Install and configure CPUs	• Review Activity: Power Supplies and Cooling • Virtual Workbench Lab: Install Power Supplies and Cooling • Review Activity: Storage Devices • Virtual Workbench Lab: Install and Configure SSD Storage • Review Activity: System Memory • Virtual Workbench Lab: Install RAM • Review Activity: CPUs • Virtual Workbench Lab: Install a CPU and Cooler
3	**Lesson 3: Troubleshooting PC Hardware** • Apply troubleshooting methodology • Configure BIOS/UEFI • Troubleshoot power and disk issues • Troubleshoot system and display issues	• Troubleshooting Methodology Review • BIOS and UEFI Review • Power and Disk Issues Review • System and Display Issues Review
4	**Lesson 4: Comparing Local Networking Hardware** • Compare network types • Compare networking hardware • Explain network cable types • Compare wireless networking types	• Assisted Lab: Explore the VM Lab Environment
5	**Lesson 5: Configuring Network Addressing and Internet Connections** • Compare internet connection types • Use basic TCP/IP concepts • Compare protocols and ports	• Internet Connection Review • Basic TCP/IP Concepts Review • Assisted Lab: Configure a SOHO Router

	• Compare network configuration concepts	
6	**Lesson 6: Supporting Network Services** • Summarize services provided by networked hosts • Compare internet and embedded appliances • Troubleshoot networks	• Assisted Lab: Compare Protocols and Ports Review • Internet and Embedded Appliances Review • Network Troubleshooting Review • Assisted Lab: Troubleshoot a Network Scenario #1 • Troubleshoot a network issue in a simulated network topology • Assisted Lab: Troubleshoot a Network Scenario #2 • Troubleshoot a problem on a home router network • APPLIED Lab: Troubleshoot a Network Scenario #3 • APPLIED Lab: Troubleshoot a Network Scenario #4 • Work independently to diagnose and remediate issues with a home router network
7	**Lesson 7: Summarizing Virtualization and Cloud Concepts** • Summarize client-side virtualization • Summarize cloud concepts	• Client-Side Virtualization Review • Cloud Concepts Review
8	**Lesson 8: Supporting Mobile Devices** • Set up mobile devices and peripherals • Configure mobile device apps • Install and configure laptop hardware • Troubleshoot mobile device issues	• Mobile Devices and Peripheral Review • Virtual Workbench Lab: Configure Laptop Dock and External Peripherals • Mobile Device Apps Review • Laptop Hardware Review • Virtual Workbench Lab: Add Expansion SSD in a Laptop • Virtual Workbench Lab: Update Laptop RAM
9	**Lesson 9: Supporting Print Devices** • Deploy printer and multifunction devices • Replace print device consumables • Troubleshoot print device issues	• Printer and Malfunction Review • Assisted Lab: Deploy a printer • Print Device Consumables Review
10	**Lesson 10: Configuring Windows** • Configure Windows user settings • Configure Windows system settings	• Window User Review • Assisted Lab: Explore the VM Lab Environment

11	**Lesson 11: Managing Windows** • Use management consoles • Use performance and troubleshooting tools • Use command-line tools	• Assisted Lab: Manage User Settings in Windows • Performance and Troubleshooting Review • Assisted Lab: Use Task Manager • Assisted Lab: Monitor Performance and Event Logs • Command-line Tools Review • Assisted Lab: Use Command-line Tools • APPLIED Lab: Support Windows 10
12	**Lesson 12: Identifying OS Types and Features** • Explain OS types • Compare Windows editions	• OS Types Review • Windows Edition Reviews • Assisted Lab: Perform Windows 10 Installation
13	**Lesson 13: Installing and Troubleshooting Operating Systems** • Perform OS installations and upgrades • Install and configure applications • Troubleshoot Windows OS problems	• Review Activity: OS Installations and Upgrades • Assisted Lab: Perform Windows 10 Installation • Complete Windows setup and configure an account password • Assisted Lab: Perform Ubuntu Linux Installation • Use a product disc to install Ubuntu Linux • Review Activity: Install and Configure Applications • Assisted Lab: Install and Configure an application • Install an office productivity suite with custom options • Review Activity: Windows OS Problems • Assisted Lab: Troubleshoot Systems and Services • Troubleshoot issues with a pair of Windows computers • Assisted Lab: Troubleshoot a Windows OS Issue • Troubleshoot an issue with a Windows computer that will not boot
14	**Lesson 14: Managing Windows Networking** • Configure Windows networking • Troubleshoot Windows networking • Configure Windows security settings	• Review Activity: Windows Networking • Review Activity: Windows Network Troubleshooting

	• Manage Windows shares	• Assisted Lab: Configure Windows Networking • Diagnose and remediate a network connectivity issue • Review Activity: Security Settings • Review Activity: Windows Shares • Assisted Lab: Configure Folder Sharing in a Workgroup • Configure and test a file share on a Windows host • Assisted Lab: Support Active Directory Networking • Join a computer to a domain and implement a logon script and folder redirection policy
15	**Lesson 15: Managing Linux and macOS** • Identify features of Linux • Identify features of macOS	• Review Activity: Features of Linux • Assisted Lab: Manage Linux Using Command-line Tools • Use the Samba file sharing software to create a shared folder on a Linux host and access it from Windows • Assisted Lab: Manage Files Using Linux Command-line Tools • Work at a Linux command-line to manage directories and files • Review Activity: Features of macOS • APPLIED Lab: Support and Troubleshoot Network Hosts • Work independently to diagnose and remediate a network connectivity issue
16	**Lesson 16: Configuring SOHO Network Security** • Explain attacks, threats, and vulnerabilities • Compare wireless security protocols • Configure SOHO router security • Summarize security measures	• Review Activity: Attacks, Threats, and Vulnerabilities • Review Activity: Wireless Security Protocols • Review Activity: SOHO Router Security • Assisted Lab: Configure SOHO Router Security • Configure a secure wireless network and apply a port forwarding configuration to a home router • Review Activity: Security Measures
17	**Lesson 17: Managing Security Settings** • Configure workstation security	• Review Activity: Workstation Security

	• Configure browser security • Troubleshoot workstation security issues	• Assisted Lab: Configure Workstation Security • Enforce security settings using Local Security Policy in the Windows operating system • Review Activity: Browser Security • Assisted Lab: Configure Browser Security • Configure privacy settings for Microsoft's Edge browser • Review Activity: Workstation Security Issues • Assisted Lab: Troubleshoot Security Issues Scenario #1 • Investigate and remediate a host where the security configuration has been compromised • Applied Lab: Troubleshoot Security Issues Scenario #2 • Work independently to investigate and remediate a host where the security configuration has been compromised
18	**Lesson 18: Supporting Mobile Software** • Configure mobile OS security • Troubleshoot mobile OS and app software • Troubleshoot mobile OS and app security	• Review Activity: Mobile OS Security • Review Activity: Troubleshooting
19	**Lesson 19: Using Support and Scripting Tools** • Use remote access technologies • Implement backup and recovery • Explain data handling best practices • Identify basics of scripting	• Review Activity: Remote Access Technologies • Assisted Lab: Use Remote Access Technologies • Use RDP and SSH to connect to Windows and Linux hosts over a network • Review Activity: Backup and Recovery • Assisted Lab: Implement Backup and Recovery • Configure Windows backup and use it to restore files • Review Activity: Data Handling Best Practices • Review Activity: Basics of Scripting • Assisted Lab: Implement a PowerShell Script

		• Develop a PowerShell script to automate creation on virtual machines • Assisted Lab: Implement a Bash Script • Develop a Bash script to automate gathering information from a Linux host
20	**Lesson 20: Implementing Operational Procedures** • Implement best practice documentation • Use proper communication techniques • Use common safety and environmental procedures **Practice Test**	• Review Activity: Best Practice Documentation • Assisted Lab: Manage a Support Ticket • Ensure that resolution of a support issue is fully documented in a ticketing system • Review Activity: Proper Communication Techniques • Review Activity: Safety and Environmental Procedures

CompTIA Security+ Live Online Training Program

Program Description

The CompTIA Security+ certification is a leading industry standard for beginning a career in computer and network security and a preferred credential for entry-level cybersecurity job roles. Candidates receive hands-on training for core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.

The CompTIA Security+ Live Online Training program consists of 30 clock hours of instruction over two (2) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA Security+ certification examination (CompTIA Security+ SY0-601).

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA Security+ examination; students receive this certification from a third party through an examination process. The cost of the program includes ten (10) days of instructor-led online training, CertMaster Learn for CompTIA Security+, CertMaster Labs for CompTIA Security+, and CertMaster Practice for instructor-led training for CompTIA Security+, a CompTIA Security+ examination voucher, and one (1) examination retake voucher.

This program prepares students for a Security Specialist or equivalent entry-level IT security role (CIP Code 11.1003, "Computer and Information Systems Security/Auditing/Information Assurance"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA Security+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA Security+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA Security+ Live Online Training program does not provide computer equipment, internet access, or required software for students. Students will need access to the internet and a reliable laptop or desktop computer, or mobile device. Webcams are not required.

Learning Resources for Program Content

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Security+ in this program.

CompTIA Security+ Live Online Training Program Outline (Syllabus)

Day	Lessons	Activities
1	**Class Introductions/Code of Conduct** Review CertMaster Learn, Labs and Practice **Lesson 1: Summarizing Fundamental Security Concepts** • Security Concepts • Security Controls **Lesson 2: Comparing Threat Types** • Threat Actors • Attack Surfaces	• Lessons 1 and 2 in CompTIA Learn and Labs • Review Activity: Security Concepts • Assisted Lab: Exploring the Lab Environment • Assisted Lab: Perform System Configuration Gap Analysis • Review Activity: Security Controls • Assisted Lab: Configuring Examples of Security Control Types • Review Activity: Threat Actors • Review Activity: Attack Surface • Assisted Lab: Finding Open Service Ports

2	**Lesson 2- Topic C** • Social Engineering **Lesson 3 - Explain Cryptographic Solutions** • Cryptographic algorithms • Public Key Infrastructure • Cryptographic solutions	• Homework – students complete Lessons 2 and 3 CertMaster Learn and Labs • Review Activity: Social Engineering • Assisted Lab: Using SET to Perform Social Engineering • Review Activity: Cryptographic Algorithms • Applied Lab: Using Storage Encryption • Review Activity: Public Key Infrastructure • Review Activity: Cryptographic Solutions • Assisted Lab: Using Hashing and Salting
3	**Lesson 4: Implement Identity and Access Management** • Authentication • Authorization • Identity Management **Lesson 5: Secure Enterprise Network Architecture** • Enterprise Network Architecture • Network Security Appliances	• Complete lessons 4 and 5 in CertMaster Learn and Labs as homework • Review Activity: Authentication • Assisted Lab Managing Password Security • Review Activity: Access Management • Assisted Lab: Managing Permissions • Review Activity: Identity Management • Review Activity: Enterprise Network Architecture • Review Activity: Network Security Appliances
4	**Lesson 5 Continued – Topic C** • Secure Communications **Lesson 6: Secure Cloud Network Architecture** • Cloud Infrastructure • Embedded Systems and Zero Trust Architecture	• Complete CertMaster Lessons 5 and 6 in Learn and Labs • Review Activity: Virtual Private Networks • Assisted Lab: Setting up Remote Access • Assisted Lab: Using IPSec Tunneling • Review Activity: Cloud Infrastructure • Assisted Lab: Using Containers Assisted Lab: Using Virtualization • Review Activity: Embedded Systems and Zero Trust Architecture

5	**Lesson 7: Explain Resiliency and Site Security Concepts** • Asset Management • Redundancy Strategies Physical Security **Lesson 8: Explain Vulnerability Management** • Device and OS Vulnerabilities • Application and Cloud Vulnerabilities	• Complete CertMaster Lessons 7 and 8 in Learn and Labs • Review Activity: Asset Management • Applied Lab: Implement Backups Assisted Lab: Performing Drive Sanitization • Review Activity: Redundancy Strategies • Review Activity: Physical Security • Students complete lesson 8 in CertMaster Learn and Labs • Review Activity: Device and OS Vulnerabilities • Review Activity: Application and Cloud Vulnerabilities • Assisted Lab: Exploiting and Detecting SQLi
6	**Lesson 8 Continued – Topics C & D** • Vulnerability Identification Methods • Vulnerability Analysis and Remediation **Lesson 9: Evaluate Network Security Capabilities** • Network Security Baselines • Network Security Capability Enhancement •	• Students complete CertMaster Learn and Labs for lessons 8 and 9 • Review Activity: Vulnerability Identification Methods • Assisted Lab: Working with Threat Feeds • Review Activity: Vulnerability Analysis and Remediation • Assisted Lab: Performing Vulnerability Scans • Review Activity: Network Security Baselines • Assisted Lab: Understanding Security Baselines • Review Activity: Network Security Capability Enhancement • Applied Lab: Implementing a Firewall
7	**Lesson 10: Assess Endpoint Security Capabilities** • Implement Endpoint Security • Mobile Device Hardening **Lesson 11: Enhance Application Security Capabilities** • Application Protocol Security Baselines	• Students complete lessons 10 and 11 in CertMaster Learn and Labs • Review Activity: Endpoint Security • Assisted Lab: Using Group Policy Applied Lab: Hardening • Review Activity: Application Protocol Security Baselines • Assisted Lab: Performing DNS Filtering
8	**Lesson 11 – Continued Topic B**	• Students complete lessons 11 and 12 in CertMaster Learn and Labs. • Review Activity

	• Cloud and Web Application Security Concepts **Lesson 12: Explain Incident Response and Monitoring Concepts** • Incident Response • Digital Forensics • Data Sources • Alerting and Monitoring Tools	• Assisted Lab: Configuring System Monitoring • Review Activity: Incident Response • Review Activity: Digital Forensics • Review Activity: Data Sources • Applied Lab: Using Network Sniffers • Review Activity: Alerting and Monitoring Tools
9	**Lesson 13: Analyze Indicators of Malicious Activity** • Malware Attack Indicators • Physical and Network Attack Indicators Application Attack Indicators **Lesson 14: Summarize Security Governance Concepts** • Policies, Standards, and Procedures • Change Management Automation and Orchestration	• Students complete lessons 13 and 14 in CertMaster Learn and Labs • Review Activity: Malware Attack Indicators • Review Activity: Physical and Network Attack Indicators • Review Activity: Application Attack Indicators • Review Activity: Policies, Standards, and Procedures • Review Activity: Change Management • Review Activity: Automation and Orchestration • Assisted Lab: Use Cases of Automation and Scripting
10	**Management Processes** • Risk Management Processes and Concepts • Vendor Management Concepts • Audits and Assessments **Lesson 16: Summarize Data Protection and Compliance Concepts** • Data Classification and Compliance Personnel Policies	• CertMaster Learn and Labs • Review Activity: Risk Management Processes and Concepts • Review Activity: Vendor Management Concepts • Review Activity: Penetration Testing Concepts • Assisted Lab: Performing Reconnaissance Assisted Lab: Performing Penetration Testing • Review Activity: Data Classification and Compliance • Review Activity: Personnel Policies • Assisted Lab: Training and Awareness through Simulation Challenge Lab: Discovering Anomalous Behavior

CompTIA Network+ Live Online Training Program

Program Description

The CompTIA Network+ certification is a leading industry standard for establishing a career in network administration and a preferred credential for network troubleshooting and management. Candidates receive hands-on skills training to prepare them for working with both wired and wireless networks, and with emerging technologies such as unified communications, mobile, cloud, and virtualization technologies.

The CompTIA Network+ Live Online Training program consists of 30 clock hours of instruction over two (2) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA Network+ certification examination (CompTIA Network+ N10-008).

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA Network+ examination; students receive this certification from a third party through an examination process. The cost of the program includes ten (10) days of instructor-led online training, CertMaster Practice for CompTIA Network+, CertMaster Labs for CompTIA Network+, CertMaster Learn for instructor-led training for CompTIA Network+, a CompTIA Network+ examination voucher, and one (1) examination retake voucher.

This program prepares students for a Network Specialist or equivalent entry-level IT networking role (CIP Code 11.1001, "Network and System Administration/Administrator"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA Network+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA Network+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA Network+ Live Online Training program does not provide computer equipment, internet access, or required software for students. Students will need access to the internet and a reliable laptop or desktop computer, or mobile device. Webcams are not required.

Learning Resources for Program Content

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Network+ in this program.

CompTIA Network+ Live Online Training Program Outline (Syllabus)

Day	Lessons	Activities
1	**Lessons 1: Comparing OSI Model Network Functions** • Compare and contrast OSI model layers • Configure SOHO networks **Lesson 2: Deploying Ethernet Cabling** • Summarize Ethernet standards • Summarize copper cabling types • Summarize fiber optic cabling types • Deploy Ethernet cabling •	• Introductions, Canvas, and CertMaster Materials Tour • OSI Model Layers • Assisted Lab: Exploring the Lab Environment • SOHO Networks • Assisted Lab: Configure a SOHO Router • Ethernet Standards • Copper Cabling Types • Fiber Optic Cabling Types • Ethernet Cabling
2	**Lesson 3: Deploying Ethernet Switching** • Deploy networking devices • Explain network interfaces • Deploy common Ethernet switching features **Lesson 4: Troubleshooting Ethernet Networks** • Explain network troubleshooting methodology • Troubleshoot common cable connectivity issues	• Networking Devices • Network Interfaces • Assisted Lab: Capture Network Traffic • Common Ethernet Switching Features • Assisted Lab: Configure Interface Settings • Network Troubleshooting Methodology • Common Cable Connectivity Issues
3	**Lesson 5: Explaining IPv4 Addressing** • Explain IPv4 addressing schemes • Explain IPv4 forwarding • Configure IP networks and subnets **Lesson 6: Supporting IPv4 and IPv6 Networks** • Use appropriate tools to test IP configuration • Troubleshoot IP networks • Explain IPv6 addressing schemes	• IPv4 Addressing Schemes • Assisted Lab: Configure IPv4 Static Addressing • IPv4 Forwarding • Assisted Lab: Analyze ARP Traffic • Design an IP Subnet • Test IP Configuration

		• Assisted Lab: Use Tools to Test IP Configuration • Troubleshoot IP Networks • IPv6 Addressing Schemes • Assisted Lab: Configure IPv6 Static Addressing
4	**Lesson 7: Configuring and Troubleshooting Routers** • Compare and contrast routing concepts • Compare and contrast dynamic routing concepts • Install and troubleshoot routers **Lesson 8: Explaining Network Topologies and Types** • Explain network types and characteristics • Explain tiered switching architecture • Explain virtual LANs	• Routing Concepts • Assisted Lab: Configure Static Routing • Dynamic Routing Concepts • Design VLSM Subnets • Assisted Lab: Configure Dynamic Routing • Router Installation and Troubleshooting • Design a Branch Office Internetwork • Applied Lab: Troubleshoot IP Networks (Parts A and B) • Network Types and Characteristics • Tiered Switching Architecture • Virtual LANs
5	**Lesson 9: Explaining Transport Layer Protocols** • Compare and contrast transport protocols • Use appropriate tools to scan network ports **Lesson 10: Explaining Network Services** • Explain the use of network addressing services • Explain the use of name resolution services • Configure DNS services	• Transport Protocols • Port Scanning • Assisted Lab: Use Network Scanners • Network Addressing Services • Assisted Lab: Analyze a DHCP Server Configuration • Name Resolution Services • DNS Services • Assisted Lab: Analyze a DNS Server Configuration
6	**Lessons 11: Explaining Network Applications** • Explain the use of web, file/print, and database services	• Web, File/Print, and Database Services

	• Explain the use of email and voice services **Lesson 12: Ensuring Network Availability** • Explain the use of network management services • Use event management to ensure network availability • Use performance metrics to ensure network availability	• Use of Email and Voice Services • Assisted Lab: Analyze Application Security Configurations • Network Management Services • Assisted Lab: Configure Secure Access Channels • Event Management • Assisted Lab: Configure Syslog • Performance Metrics • Assisted Lab: Analyze Network Performance • Applied Lab: Verify Service and Application Configuration
7	**Lesson 13: Explaining Common Security Concepts** • Explain common security concepts • Explain authentication methods **Lesson 14: Supporting and Troubleshooting Secure Networks** • Compare and contrast security appliances • Troubleshoot service and security issues	• Common Security Concepts • Authentication Methods • Security Appliances • Assisted Lab: Configure a NAT Firewall • Service and Security Issues • Scenarios in Service and Security Issues
8	**Lesson 15: Deploying and Troubleshooting Wireless Networks** • Summarize wireless standards • Install wireless networks • Troubleshoot wireless networks • Configure and troubleshoot wireless security **Lesson 16: Comparing WAN Links and Remote Access Methods** • Explain WAN provider links • Compare and contrast remote access methods	• Wireless Standards • Wireless Network Installation • Wireless Network Troubleshooting • Wireless Security • WAN Provider Links • Remote Access Methods • Assisted Lab: Configure Remote Access
9	**Lesson 17: Explaining Organizational and Physical Security Concepts** • Explain organizational documentation and policies • Explain physical security methods	• Physical Security Methods • Internet of Things Devices

	• Compare and contrast Internet of Things devices **Lesson 18: Explaining Disaster Recovery and High Availability Concepts** • Explain disaster recovery concepts • Explain high availability concepts	• Disaster Recovery Concepts • Assisted Lab: Backup and Restore Network Device Configuration • High Availability Concepts
10	**Lesson 19: Applying Network Hardening Techniques** • Compare and contrast types of attacks • Apply network hardening techniques **Lesson 20: Summarizing Cloud and Datacenter Architecture** **Class Review**	• Types of Attacks • Assisted Lab: Analyze an On-path Attack • Network Hardening Techniques • Assisted Lab: Configure Port Security • Cloud Concepts • Virtualization and SAN Technologies • Datacenter Network Architecture • Applied Lab: Troubleshoot Service and Security Issues • **Practice Exam**

CompTIA CySA+ Live Online Training Program

Program Description

The CompTIA CySA+ certification is an IT workforce certification and an intermediate credential for security professionals. Candidates receive hands-on training for proactively capturing, monitoring, and responding to network traffic findings, as well as software and application security, automation, threat hunting, and IT regulatory compliance, which affects the daily work of security analysts.

The CompTIA CySA+ Live Online Training program consists of 30 clock hours of instruction over two (2) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA CySA+ certification examination (CompTIA CySA+ CS0-003).

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA CySA+ examination; students receive this certification from a third party through an examination process. The cost of the program includes ten (10) days of instructor-led online training, CertMaster Practice for CompTIA CySA+, CertMaster Labs for CompTIA CySA+, CertMaster Learn for instructor-led training for CompTIA CySA+, a CompTIA CySA+ examination voucher, and one (1) examination retake voucher.

This program prepares students for a Security Analyst or equivalent intermediate-level IT security role (CIP Code 11.1003, "Computer and Information Systems Security/Auditing/Information Assurance"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA CySA+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA CySA+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA CySA+ Live Online Training program does not provide computer equipment, internet access, or required software for students. Students will need access to the internet and a reliable laptop or desktop computer, or mobile device. Webcams are not required.

Learning Resources for Program Content

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA CySA+ in this program.

CompTIA CySA+ Live Online Training Program Outline (Syllabus)

Day	Lessons	Activities
1	• Course Introduction • Lesson 01A: Understanding Cybersecurity Leadership Concepts • Lesson 01B: Exploring Control Types and Methods • Lesson 01C: Explaining Patch Management Concepts	• Assisted Lab: Exploring the Lab Environment • Assisted Lab: Configuring Controls
2	• Lesson 02A: Exploring Threat Actor Concepts • Lesson 02B: Identifying Active Threats • Lesson 02C: Exploring Threat-Hunting Concepts Assisted Lab: Performing Threat Hunting	• Assisted Lab: Reviewing IoC and Threat Intelligence Sources

3	• Lesson 03A: Reviewing System and Network Architecture Concepts • Lesson 03B: Exploring Identity and Access Management (IAM) • Maintaining Operational Visibility, Assisted Lab: Assess Time Synch Errors	• Applied LAB: Performing System Hardening • Assisted Lab: Configuring Centralized
4	• Lesson 04A: Exploring Leadership and Security Operations • Lesson 04B: Understanding Technology for Security Operations • Lesson 05A: Explaining Compliance Requirements • Lesson 05B: Understanding Vulnerability Scanning Methods	• Assisted Lab: Configuring Automation • Assisted Lab: Performing Asset Discovery, Assisted Lab: Performing Passive Scanning
5	• Lesson 05C: Exploring Special Considerations in Vulnerability Scanning • Lesson 06A: Understanding Vulnerability Scoring Concepts • Lesson 06B: Exploring Vulnerability Context Considerations • Lesson 07A: Explaining Effective Communication Concepts	• Assisted Lab: Performing Vulnerability Scanning • Assisted Lab: Establishing Context Awareness • Assisted Lab: Analyzing Vulnerability Scans
6	• Lesson 07B: Understanding Vulnerability Reporting Outcomes and Action Plans • Lesson 08A: Exploring Incident Response Planning • Lesson 08B: Performing Incident Response Activities	• Assisted Lab: Detecting Legacy Systems • Adaptive Lab: Performing Playbook Incident Response, • Applied Lab: Performing IoC Detection and Analysis • Applied Lab: Performing Post-Incident Forensic Analysis • Applied Lab: Collecting Forensic Evidence
7	• Lesson 09A: Understanding Incident Response Communication • Lesson 09B: Analyzing Incident Response Activities • Lesson 10A: Identifying Malicious Activity	• Assisted Lab: Performing Root Cause Analysis • Assisted Lab: Using File Analysis Techniques • Assisted Lab: Analyzing Potentially Malicious Files • Applied Lab: Using Network Sniffers
8	• 10B: Explaining Attack Methodology Frameworks • Lesson 10C: Explaining Techniques for Identifying Malicious Activity	• Applied Lab: Researching DNS and IP Reputation

	• Lesson 11A: Exploring Network Attack Indicators • Lesson 11B: Exploring Host Attack Indicators	
9	• Lesson 11C: Exploring Vulnerability Assessment Tools • Lesson 12A: Analyzing Web Vulnerabilities • Lesson 12B: Analyzing Cloud Vulnerabilities • Lesson 13A: Understanding Scripting Languages	• Assisted Lab: Using Nontraditional Vulnerability Scanning Tools • Applied Lab: Performing Web Vulnerability Scanning • Assisted Lab: Analyzing Cloud Vulnerabilities
10	• Lesson 13B: Identifying Malicious Activity Through Analysis • Lesson 14A: Explore Secure Software Development Practices • Lesson 14B: Recommending Controls to Mitigate Successful Application Attacks • Lesson 14C: Implementing Controls to Prevent Attacks,	• Assisted Lab: Exploiting Weak Cryptography • Assisted Lab: Performing Directory Traversal and Command Injection, • Assisted Lab: Performing XSS, • Assisted Lab: Performing LFI/RI • Assisted Lab: Performing SQLi • Assisted Lab: Performing CSRF • Assisted Lab: Performing Privilege Escalation • Applied Lab: Exploiting Security Misconfiguration

CompTIA Data+ Live Online Training Program

Program Description

The CompTIA Data+ certification is an industry standard for beginning a career in data analytics and a recognized credential for professionals tasked with developing and promoting data-driven business decision-making. Candidates receive hands-on training for mining, manipulating, and visualizing data, applying statistical methods to data, and analyzing complex datasets.

The CompTIA Data+ Live Online Training program consists of 30 clock hours of instruction over two (2) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA Data+ certification examination (CompTIA Data+ DA0-001).

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA Data+ examination; students receive this certification from a third party through an examination process. The cost of the program includes ten (10) days of instructor-led online training, CertMaster Practice for CompTIA Data+, CertMaster Labs for CompTIA Data+, CertMaster Learn for instructor-led training for CompTIA Data+, a CompTIA Data+ examination voucher, and one (1) examination retake voucher.

This program prepares students for a Data Analyst or equivalent entry-level IT data role (CIP Code 11.0301, "Data Processing and Data Processing Technology/Technician"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA Data+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA Data+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA Data+ Live Online Training program does not provide computer equipment, internet access, or required software for students. Students will need access to the internet and a reliable laptop or desktop computer, or mobile device. Webcams are not required.

Learning Resources (Content)

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Data+ in this program.

CompTIA Data+ Live Online Training Program Outline

Day	Lessons	Activities
1	• **Class Introductions/Code of Conduct** • **How to interact and engage with us exercise** • **Review CertMaster Learn, Labs and Practice** **Lesson 1: Identifying Basic Concepts of Data Schemas** • 01A Identify the Key Differences between Relational and Non- Relational Databases • 01B Identify the Way We Use Tables, Primary Keys, and Normalization	• Assisted Lab: Exploring the lab environment • Assisted Lab 1: Navigating and Understanding Database Design • Homework: Read Lesson 1 in CompTIA Learn and Labs
2	**Lesson 2: Understanding Different Data Systems** • 02A Describe Types of Data Processing and Storage Systems • 02B Explain How Data Changes **Lesson 3: Understanding Types and Characteristics of Data**	• Homework – students complete Lessons 2, 3, and 4 in CertMaster Learn and Labs • Building Basic SQL Statements • Assisted Lab 3: Working with Different File Formats

	• 03A Understand Types of Data • 03B Break Down the Field Data Types **Lesson 4: Comparing and Contrasting Different Data Structures, Formats, and Markup Languages** • 04A Differentiate between Structured Data and Unstructured Data • 04B Recognize Different File Formats	• Applied Lab 4: Understanding Data Structure and Types and Using Basic Statements
3	**Lesson 5: Explaining Data Integration and Collection Methods** • 05A Make Data Usable for Data Analysis and Reporting • 05B Explain API/Web Scraping and Other Collection Methods • 05C Collect and Use Public Data • 05D Use and Collect Survey Data **Lesson 6: Identifying Common Reasons for Cleansing and Profiling Data** • 06A Learn to Profile Data	• Homework – students complete Lessons 5 in CertMaster Learn and Labs • Find Public Data and do some profiling work for review.
4	**Lesson 6: Identifying Common Reasons for Cleansing and Profiling Data** • 06B Address Redundant and Duplicated Data • 06C Work with Missing Values • 06D Address Invalid Data • 06E Address Mismatched Data and Data Type Validation	• Review Profile Homework and class interactions • Assisted Lab 7: Addressing Redundant and Duplicated Data • Applied Lab 9: Preparing Data for Use • Homework – students complete Lessons 6 in CertMaster Learn and Labs
5	**Lesson 7: Executing Different Data Manipulation Techniques** • 07A Recode Data and Derived Variables • 07B Transpose and Append Data • 07C Query Data **Lesson 8: Explaining Common Techniques for Data Manipulation and Optimization** 08A Use Functions to Manipulate Data	• Homework – students complete Lessons 7-8 in CertMaster Learn and Labs • Assisted Lab 10: Recoding Data • Assisted Lab 11: Working with Queries and Join Types • Applied Lab 12: Building Queries and Transforming Data
6	**Lesson 9: Applying Descriptive Statistical Methods** • 09A Use Measures of Central Tendency • 09B Use Measures of Variability • 09C Use Frequencies and Percentages	• Students complete CertMaster Learn and Labs for lessons 9 and 10

	Lesson 10: Describing Key Analysis Techniques • 10A Get Started with Analysis • 10B Recognize Types of Analysis	• Review and Mark your confidence levels for lessons 1 through 9 in CertMaster. • Do some gamification is lessons covered.
7	**Lesson 11: Understanding the Use of Different Statistical Methods** • 11A Understand the Importance of Statistical Tests • 11B Break Down the Hypothesis Test • 11C Understand Tests and Methods to Determine Significance	• Students complete lessons 11 in CertMaster Learn and Labs • Applied Lab 15: Analyzing Data
8	**Lesson 12: Using the Appropriate Type of Visualization** • 12A Use Basic Visuals • 12B Build Advanced Visuals • 12C Build Maps with Geographical Data • 12D Use Visuals to Tell a Story **Lesson 13: Expressing Business Requirements in a Report Format** • 13A Develop Business Requirements for Reporting	• Students complete lessons 12 in CertMaster Learn and Labs.
9	**Lesson 13: Expressing Business Requirements in a Report** • 13D Prepare Reports or Dashboards • 13E Understand ways to filter data **Lesson 14: Designing Components for Reports and Dashboards** • 14A Design Elements for Reports/Dashboards • 14B Utilize Standard Elements **Lesson 15: Distinguishing Different Report Types** • 15A Differentiate between Static and Dynamic Report Types • 15B Determine the Uses for Ad-Hoc and Self-Service Reporting	• Students complete lessons 13, 14 and 15 in CertMaster Learn and Labs • Assisted Lab 19: Filtering Data • Assisted Lab 20: Designing Elements for Dashboards • Assisted Lab 21: Building an Ad Hoc Report • Applied Lab 22: Visualizing Data
10	**Lesson 16: Summarizing the Importance of Data Governance** • 16A Define Data Governance • 16B Understanding Agreements and Policies • 16C Understand Security Requirements	• **CertMaster Practice Exam**

	• 16D Understand Entity Relationship Requirements **Lesson 17: Applying Quality Control to Data** • 17A Applying quality control to data17B Understanding data quality, rules and metrics **Lesson 18: Explaining Master Data Management Concepts** • 18A Understanding Master Data Management • 18B Describe Master data Management Processes	

CompTIA PenTest+ Live Online Training Program

Program Description

The CompTIA PenTest+ certification is an IT workforce certification and an intermediate credential for security professionals. Candidates receive training on penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. In addition, the course provides hands-on training for planning and scoping a penetration testing engagement including vulnerability scanning, understanding legal and compliance requirements, analyzing results, and producing a written report with remediation techniques.

The CompTIA PenTest+ Live Online Training program consists of 30 clock hours of instruction over two (2) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA PenTest+ certification examination (CompTIA PenTest+ PT0-002).

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA PenTest+ examination; students receive this certification from a third party through an examination process. The cost of the program includes ten (10) days of instructor-led online training, CertMaster Practice for CompTIA PenTest+, CertMaster Labs for CompTIA PenTest+, CertMaster Learn for instructor-led training for CompTIA PenTest+, a CompTIA PenTest+ examination voucher, and one (1) examination retake voucher.

This program prepares students for a Security Penetration tester or equivalent intermediate-level IT security role (CIP Code 11.1003, "Computer and Information Systems Security/Auditing/Information Assurance"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA PenTest+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments.

Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA PenTest+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA PenTest+ Live Online Training program does not provide computer equipment, internet access, or required software for students. Students will need access to the internet and a reliable laptop or desktop computer, or mobile device. Webcams are not required.

Learning Resources for Program Content

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA PenTest+ in this program.

CompTIA PenTest+ Live Online Training Program Outline (Syllabus)

Day	Lessons	Activities
1	**Lesson 1: Scoping Organizational/Customer Requirements** • Compare and contrast governance, risk, and compliance reports • Explain the importance of scoping and organizational/customer requirements • Explain the importance of communication during the penetration testing process • Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity • Given a scenario, perform passive reconnaissance **Lesson 2: Defining the Rules of Engagement** • Compare and contrast governance, risk, and compliance reports	**Review Activity: Organizational PenTesting** • Explain the process of scoping and organizational requirements. • Outline the main steps of the structured PenTesting process • Describe the importance of communication during the penetration testing process. **Review Activity: Define Organizational PenTesting** • Describe the components of PCI DSS • List the main topics of GDPR • Discuss other privacy laws that govern the protection of data: • SHIELD, CCPA and HIPAA **Review Activity: Compare Standards and Methodologies** • Identify Pentesting Frameworks • List organizations have developed Pentest guidelines • Describe the key elements of MITRE ATT&CK

	• Explain the importance of scoping and organizational/customer requirements • Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.	• Compare and contrast CVE and CWE **Describe Ways to Maintain Professionalism** • List ways to assure the organization that the team has the appropriate experience and an excellent reputation. • Explain the importance of maintaining confidentiality. • Describe possible legal considerations that might be applicable during the PenTest process. **Assess Environmental Considerations** • Outline the importance of defining the Project Scope • Discuss activities related to gathering the requirements • Stress the importance of determining physical locations, and whether testing is on-site or off-site. • Explain how certain restrictions can influence PenTesting **Outline the Rules of Engagement** • Outline topics to cover when defining the restrictions • Review options when deciding on the type of assessment and selecting the strategy • Describe ways to validate the scope of the engagement **Prepare Legal Documents** • Review laws that require the confidentiality of data while testing • List some of the information included in the documentation that gives permission to attack • Discuss the importance of the Master Service Agreement • Describe what's included in a Statement of Work • Outline the components of a Service-Level Agreement

2	**Lesson 3: Footprinting and Gathering Intelligence** • Given a scenario, perform passive reconnaissance. • Given a scenario, perform active reconnaissance. • Given a scenario, analyze the results of a reconnaissance exercise. • Explain use cases of the following tools during the phases of a penetration test. **Lesson 4: Evaluating Human and Physical Vulnerabilities Intelligence** • Given a scenario, perform a social engineering or physical attack. • Explain use cases of the following tools during the phases of a penetration test.	**Discover the Target** • Outline ways footprinting and reconnaissance can reveal information about the target • List sites that can provide information on the company • Describe how public job boards can reveal information about the organization • Discuss how DNS information can provide additional information on the target **Gather Essential Data** • Explain the risks of using public source code repositories • List ways the team can use Google search engines to identify security w **Discover Open-Source Intelligence Tools** • Weaknesses in publicly available sources • Discuss ways the team can obtain older website information during reconnaissance • Describe how to search for images and interesting data **Compile Website Information** • Explain the value of enumerating a website • Describe why the team may be asked to examine the target's partners, consultants, and contractors' sites • Explain the significance of the robots.txt file • Describe the importance of testing the SSL/TLS certificate • Explain how the team can use the CT Framework • Compare the standard OCSP process with stapling the certificate • **Assisted Lab:** Exploring the Domain Tools: Nslookup, Dig and Whois **Discover Open-Source Intelligence Tools**

		• Recall how the team can use OSINT tools during the PenTest • Explain how the team can use Metagoofil and FOCA • List ways the Harvester can automate information gathering • Review how Recon-ng uses modules to customize a search • Outline the benefits of using Maltego to gather information on public resources. • Describe how Shodan can locate and index IoT devices **Assisted Lab:** Navigating Open-Source Intelligence Tools **Exploit the Human Psyche** • Outline what's involved when using social engineering • Explain some of the ways to deceive a victim • Compare and contrast phishing and pharming • Discuss why email is an ideal tool to use during social engineering. • Describe why Spearphishing is a better approach when launching a social engineering attack • List ways to use text or VoIP to target a victim • Explain how to bait, redirect and/or entice a victim • Outline how a watering hole attack works and how it can be used in a supply chain attack • Describe some of the different tactics such as impersonating, and imitating to get someone to do something • Discuss different tactics used to take advantage of human behavior **Assisted Lab:** Understanding Social Engineering Toolkit (SET)

		Summarize Physical Attacks • List some tasks the team will need to complete when assessing physical security • Describe some of the considerations involved when scaling fences and avoiding detection • Outline why the team may need to clone an RFID badge, and how this can be achieved • Explain what might happen if asset to be tested is behind a lock • Compare and contrast tailgating versus piggybacking • Describe the benefit of dumpster diving • Discuss ways to observe employees to learn actionable intel **Use Tools to Launch a Social Engineering Attack** • Discuss the features of the Social Engineering Toolkit • Explain what is required after selecting an option in SET • Outline what's involved when spoofing a phone call. • Describe what a malicious actor can do when spoofing a phone number. **APPLIED Lab:** Understanding Spear Phishing and Credentials Attack
3	**Lesson 5: Preparing the Vulnerability Scan** • Given a scenario, perform active reconnaissance • Given a scenario, perform vulnerability scanning. • Given a scenario, research attack vectors and perform wireless attacks. • Given a scenario, perform post-exploitation techniques. • Explain use cases of the following tools during the phases of a penetration test.	**Plan the Vulnerability Scan** • Outline the importance of identifying vulnerabilities • List the phases of a vulnerability • Describe what the team can discover when mapping the network • Explain some of the goals when scanning the network • Review what to consider prior to scanning the network **Detect Defenses** • Outline why it's important for the team to identify any devices such as load

	Lesson 6: Scanning Logical Vulnerabilities • Given a scenario, perform vulnerability scanning. • Given a scenario, perform active reconnaissance. • Given a scenario, analyze the results of a reconnaissance exercise. • Given a scenario, perform post-exploitation techniques. • Given a scenario, research attack vectors and perform wireless attacks. • Explain use cases of the following tools during the phases of a penetration test.	balancers, reverse proxies and firewalls during scanning • List ways the team can identify a web application firewall • Discuss reasons why specially crafted packets can slip past a firewall • Review ways the team can learn the details of a firewall • Compare methods to avoid AV detection • Describe how to use SET to create a malicious payload **Assisted Lab:** Exploring OpenVAS **Utilize Scanning Tools** • Compare how Censys and OpenVAS identify exposed systems • Explain why and how the team can craft packets • Discuss ways to test web server and the database • Describe how SQLmap can test for SQL injection flaws • Explain why you should check for SSL/TLS Vulnerabilities • List ways Nikto can test for vulnerabilities **Assisted Lab:** Using Web Scanners **Scan Identified Targets** • Compare discovery scans with port scans • Outline how full scan or TCP connect scan works • Discuss why you would operate a scan in stealth mode • Review what happens when scanning a web server and applications • Explain the significance of examining API requests • Compare vulnerability scanning methods and list the benefits of automating the scanning process **Evaluate Network Traffic**

		• Explain what information can be obtained when sniffing traffic • Describe how the team can use Nessus • Outline how and why the team might gather ARP traffic **Uncover Wireless Assets** • Describe why it's essential to test the security of the organization's WAPs • Explain how the team can use wardriving during the PenTest • Compare the different types of antennas
4	**Lesson 7: Analyzing Scanning Results** • Given a scenario, analyze the results of a reconnaissance exercise. • Given a scenario, perform vulnerability scanning. • Given a scenario, research attack vectors and perform wireless attacks **Lesson 8: Avoiding Detection and Covering Tracks** • Given a scenario, perform active reconnaissance. • Given a scenario, perform post-exploitation techniques. • Explain use cases of the following tools during the phases of a penetration test.	**Discover Nmap and NSE** • Outline reasons Nmap is the most widely used scanner today • Explain ways to throttle back the scanning process • Compare TCP and UDP scanning techniques • Discuss the variety of NSE scripting options **Assisted Lab:** Understanding Nmap Common Usage **Enumerate Network Hosts** • Outline what's involved when mapping the network • Explain the different scans Nmap uses during host discovery • List techniques the team can use to modify the intensity of a scan • Review options the team can use during host discovery • Describe ways to fingerprint the OS • Discuss methods Nmap uses to determine a target's OS **Assisted Lab:** Understanding Scan Output **Analyze Output from Scans** • List some of the questions the team will need to find out when examining network traffic

		• Describe some of methods used when testing • Discuss how Burp Suite can be used to test web applications **APPLIED Lab**: Using Scanning a Vulnerable System **Evade Detection** • List ways you can fly under the radar when scanning • Discuss how you can bypass a NAC device • Describe a Living off the Land attack • Outline how the team can erase or modify a whole log file or change certain items in a log • Discuss how and why you might alter timestamps • Explain why the team might erase or shred data **Assisted Lab:** Using ProxyChains **Use Steganography to Hide and Conceal** • Discuss Steganography, and list examples of some tools used to embed a message in a carrier file. • Describe how NTFS Alternate Data Streams can hide information • Outline how you can hide information in white space • Explain how Coagula and Sonic Visualizer can convert an image into music **Assisted Lab:** Navigating Steganography Tools **Establish a Covert Channel** • Define Data exfiltration and ways this can occur • Describe how using SSH can be a vulnerability • Compare features of Netcat and Ncat • Explain how the team can use WinRM and PSExec to provide remote management of a system • Outline what's involved in using a proxy

		Discuss ways the team can stay anonymous during port scanning
5	**Lesson 9: Exploiting the LAN and Cloud** • Given a scenario, perform active reconnaissance. • Given a scenario, perform post-exploitation techniques. • Given a scenario, research attack vectors and perform network attacks. • Explain use cases of the following tools during the phases of a penetration test. **Lesson 10: Testing Wireless Networks** • Given a scenario, research attack vectors and perform network attacks. • Explain use cases of the following tools during the phases of a penetration test	**Enumerating Hosts** • List some network services to enumerate and describe how the information can be useful to the team. • Outline shares found on either Microsoft or Linux/Unix hosts along with ways the team can enumerate the information • Discuss the resources and technology that the web server is using and how this can help the team choose more effective vectors • Explain why it might be beneficial to query AD for Information **Assisted Lab:** Demonstrating Enumeration Techniques **Attack LAN Protocols** • Explain how a VLAN hopping works • Describe an on-path attack • List some spoofing or cache poisoning attacks • Discuss the benefit of poisoning LLMNR and NBT-NS requests • Outline how to circumvent an authentication process using a hash • Review how chaining exploits lead to a more successful attack **Compare Exploit Tools** • Discuss how the team can use the Metasploit Framework (MSF) • List some of other tools used when working PenTesting on a LAN • Describe how the team can use Exploit DB **Assisted Lab**: Exploring the Basics of Metasploit **Discover Cloud Vulnerabilities** • Explain the importance of properly configuring cloud assets.

		• Review how to reduce risks when running applications. • Discuss cloud storage vulnerabilities • Outlining the different types of identities and account types • Describe potential risks when dealing with account management **Explore Cloud-Based Attacks** • Describe some of the attacks on cloud resources. • Review the goal of harvesting credentials • Discuss methods to achieve privilege escalation. • Explain the effect of a DOS attack and list some examples of attacks and tools used to launch the attack • List tools available to perform automated vulnerability scanning and PenTesting on cloud assets **APPLIED Lab**: Using VSFTP Manual and Metasploit **Discover Wireless Attacks** • Discuss why wireless transmissions are especially vulnerable • Ways used to encrypt data transmissions • Explain how a death attack works • Outline why someone would want to jam a Wi Fi signal • Discuss ways to crack a WPA password or WPS PIN **Explore Wireless Tools** • List steps to take prior to launching an attack on the WLAN • Review the tools in the Aircrack-ng suite of tools • Explain some of the features of Kismet • Discuss how the team can use Wifite2 during the PenTest • Outline some of the testing options when using Fern

		• Describe how EAPHammer can be used to launch an attack • Summarize some of the modules in MDK4 **Assisted Lab:** Monitoring with Aircrack-ng
6	**Lesson 11: Targeting Mobile Devices** • Given a scenario, research attack vectors and perform wireless attacks. • Explain common attacks and vulnerabilities against specialized systems. **Lesson 12: Attacking Specialized Systems** • Explain common attacks and vulnerabilities against specialized systems.	**Recognize Mobile Device Vulnerabilities** • Review approaches to mobile device implementation • Discuss methods used to control access • Explain some of the key elements of EMM • Compare Android and iPhone security considerations • List some of the threats to the business logic process **Launch Attacks on Mobile Devices** • Outline some of the threats designed to target a mobile device • Review Social Engineering techniques used on a mobile device • Discus the steps taken when launching a social engineering attack • Describe why spyware can be a serious attack • Compare Bluejacking and Bluesnarfing • Review how iOS and Android devices deal with malware • Explain ways to analyze malware **Outline Assessment Tools for Mobile Devices** • Discuss some of the testing frameworks used to minimize risk • Review some of the tools included in Kali Linux • Outline the benefits of the Mobile Security Framework • List key elements of the Mobile Security Testing Guide • Compare Frida and Objection when examining code • Describe ways Drozer, APKX tool. and APK Studio to examine code • Explain how Postman interacts and tests an HTTP API.

		Identify Attacks on the IoT • Outline some reasons IoT devices represent a vulnerable target • List some of the component weaknesses in IoT devices • Explain why IoT devices should be tested prior to deployment • Discuss how using BLE can lead to data leakage • Describe some attacks on IoT devices • Review how IoT protocols can represent a vulnerability **Assisted Lab:** Discovering IoT devices with Shodan **Recognize Other Vulnerable Systems** • Review the different types of data storage systems • Describe the significance of an industrial control system (ICS) • Compare SCADA with and IIoT system • Review ways misconfiguration can lead to data exposure • Explain how error messages can be a vulnerability • Outline why the team would use a fuzzer **Explain Virtual Machine Vulnerabilities** • Describe the elements of a virtual platform • Discuss the two levels securing a VM environment takes place • Explain why it's essential to avoid VM sprawl • Review reasons why it's important to protect the repositories monitor the containers • List the different classes of virtualized environment attacks • Outline how VM escape can occur and the danger of Hyperjacking
7	**Lesson 13: Web Application-Based Attacks** • Given a scenario, perform active reconnaissance.	**Recognize Web Vulnerabilities** • Outline the significance of the OWASP Top 10

	• Given a scenario, research attack vectors and perform application-based attacks. • Given a scenario, perform a social engineering or physical attack. • Explain common attacks and vulnerabilities against specialized systems. • Given a scenario, perform post-exploitation techniques. • Explain use cases of the following tools during the phases of a penetration test **Lesson 14: Performing System Hacking** • Given a scenario, perform post-exploitation techniques. • Given a scenario, research attack vectors and perform network attacks. • Explain use cases of the following tools during the phases of a penetration test. • Given a scenario, analyze script or code sample for use in a penetration test.	• List ways developers can inadvertently expose sensitive data • Review the consequences of improperly handling errors • Discuss what could happen when there is a lack of input validation • Explain why it's good practice to sign and verify code, scripts, and executables • Describe what happens in a race condition **Launch Session Attacks** • Compare the different forms of session hijacking • Provide an overview of Request Forgery Attacks • Discuss ways the team can escalate privilege • Outline why the team would need to upgrade a non-interactive shell • Explain why it's essential to identify and mitigate business logic flaws **Plan Injection Attacks** • Outline why the team should test for SQLi vulnerabilities • Review how to traverse files using invalid input • Discuss how injection attacks can compromise an app • Describe some of the types of XSS attacks • Explain why the team may need to adjust the PenTest if the customer is using a web proxy **Assisted Lab:** Using SQL Injection **Identify Tools** • Compare differences in web testing tools and list some examples • Discuss how Browser Exploit Framework (BeEF) can be used to test web browsers • Explain how the team will move through exploiting a browser with BeEF

		• Describe how BeEF displays information on hooked browsers **System Hacking** • Outline why the team should be familiar with .NET and .NET Framework • Describe the Windows PowerShell scripting language • Outline how the team can use the Empire Framework during PenTesting • Compare the Covenant and Mythic C2 Frameworks **Assisted Lab:** Using Reverse and Bind Shells **Use Remote Access Tools** • Explain how the team can use Netcat during the PenTest • Discuss how Ncat has additional functionality that is key to a penetration tester • Review ways SSH can allow the team to securely communicate during the PenTest **Analyze Exploit Code** • Describe methods the team can use to download files • Explain how scripting can be used to achieve remote access • Discuss why the team would enumerate users and assets • Review considerations when downloading exploitation code • Outline methods to break down a program to reveal more about how it functions • List components of a Software development Kit (SDK) **Assisted Lab:** Analyzing Exploit Code
8	**Lesson 15: Scripting and Software Development** • Explain the basic concepts of scripting and software development.	**Analyzing Scripts and Code Samples** • Discuss the benefits of automating tasks using scripting • List some elements of a well-written script

	• Given a scenario, analyze a script or code sample for use in a penetration test **Lesson 16: Leveraging the Attack: Pivot and Penetrate** • Given a scenario, research attack vectors and perform network attacks. • Given a scenario, perform post-exploitation techniques. • Explain use cases of the following tools during the phases of a penetration test.	• Describe tasks that can be achieved using the Bash shell • Outline how PowerShell can automate tasks • Explain why the team might use Python and Ruby scripting • Compare and contrast Perl and JavaScript **Assisted Lab:** Exploring Programming Shells **Create Logic Constructs** • Explain how variables are used and assigned • Describe the basics of logic and flow control • Compare the three Boolean operators AND, OR, and NOT. • Discuss how arithmetic and string operators are used • Review JSON fundamentals • List some Python data structure types • Explain the difference between CSV and Trees • Define components of Object-Oriented Programming **Assisted Lab:** Applying PenTest Automation **Automate Penetration Testing** • Outline when it would be efficient to use scripting when conducting the PenTest • Discuss how you can automate PenTesting with scripts. **Test Credentials** • Describe what activity occurs in an offline password attack • Outline how a Dictionary attack works • List ways the team can bypassing lock out limits • Discuss what's involved when using a brute force attack • Compare methods to attack Linux and Windows passwords

		• List some password-cracking tools • Review alternative methods to obtain credentials **Assisted Lab:** Exploring Password Attacks with john the Ripper and Hydra **Move Throughout the System** • Explain why the team will need to upgrade a restrictive shell • Outline what the team can achieve when moving laterally • Describe how the team can achieve lateral movement with remote access services • Discuss what can achieved when pivoting into other areas • Review ways to escalate privileges • Compare ways to gain control in a Windows and Linux environment **Maintain Persistence** • Outline some of the goals involved in maintaining persistence • Explain the concept of an Advanced Persistent Threat • Review ways the team can bypass restrictions • Discuss what can be accomplished with Backdoors and Trojans • Describe how remote access services can enable persistence. • Describe the concept of reverse and bind shells • Discuss the benefit of using a remote access daemon • Compare ways to schedule tasks and jobs in either Windows or Linux environments • List some guidelines when using persistence techniques
9	**Lesson 17: Communicating During the PenTesting Process**	**Define the Communication Path** • Explain why it's essential to have good communication with all stakeholders during the PenTest.

	• Explain the importance of communication during the penetration testing process **Lesson 18: Summarizing Report Components** • Compare and contrast the important components of written reports	• Describe reasons the team should take steps to ensure that the right people are informed and what information should be shared • Discuss the importance of maintaining communicating with the team's client counterparts • List a few key contacts involved in the PenTest process **Communication Triggers** • List some reasons to initiate communication during the PenTest • Discuss why the team must be able to prioritize findings as they occur. • Describe why it's essential to provide situational awareness • Review best practice if the team observes evidence of criminal activity • List reasons that can trigger a false positive • Explain reasons you might need to identify when results indicate a false lead on a vulnerability **Use Built-In Tools for Reporting** • Discuss some best practice on how best to present the findings of the PenTest • Discuss why the team might choose to use Dradis to provide details of the PenTest • Explain the benefit of creating reports with Nessus **Identify Report Audience** • Explain the importance of identifying the report audience when preparing the PenTest report • List some of the stakeholders involved in a PenTest **List Report Contents** • Outline what's included in the Executive Summary • Explain how to present the Scope Details

		• Review what's included in the methodology section • Discuss the significance of the attack narrative • Describe how best to present the findings • List ways the team can determine the client's risk appetite • Explain the concept of rating and prioritizing risks • Outline how a business impact analysis (BIA) factors into the PenTest • Compare how Metrics and Measures are used during the PenTest • Describe how the team can present remediation recommendations • List components in the final report sections **Define Best Practices for Reports** • Discuss different factors to consider when storing and distributing the PenTest reports • List some best practices for handling reports • Review reasons the team might take notes and grab screenshots • Describe the importance of providing ongoing documentation • Explain how the team can identify common themes/root causes • Outline how best to present the vulnerabilities identified • List examples of observations on details about the PenTest
10	**Lesson 19: Recommending Remediation** • Explain common attacks and vulnerabilities against specialized systems. • Given a scenario, analyze the findings and recommend the appropriate remediation within a report.	**Employ Technical Controls** • List some techniques used when hardening a system • Discuss reasons for sanitizing user input • Describe how Multifactor Authentication improves security • Explain why its recommended to encrypt passwords • Review when it may be necessary to remediate at the process-level

	Lesson 20: Performing Post-Report Delivery Activities • Explain post-report delivery activities.	• Explain the significance of Patch Management • Describe what's involved when employing Key Rotation • Outline why it's essential to secure digital certificates • Review what's involved in a secret management solution • Describe the importance of segmenting a network **Administrative and Operational Controls** • Describe why an organization should implement policies and procedures • Outline the importance of employing role-based access control and enforcing minimum password requirements • Explain why it's essential to include security in the SDLC • Describe some insecure coding practices that should be avoided • Review techniques for managing mobile devices • Discuss reasons it's important to factor in the people when designing security controls • List operational considerations when suggesting remediation guidelines **Physical Controls** • Describe methods to control access to buildings • Explain how biometric controls can be used to restrict access • Discuss best practices when using video surveillance **Post-Engagement Cleanup** • List some of the tasks that take place during cleanup • Discuss the importance of removing any shells on the target system • Explain some of the issues that might take place when deleting test credentials

		• Describe what's involved when removing tools used during the PenTest. • Review some best practices when destroying test data **Follow-Up Actions** • Discuss the importance of post-delivery activities • Review the process of confirming that testing is complete • Explain the significance of attestation of findings • Outline why the team should schedule a retest • Describe the significance of creating a learned report (LLR) **CertMaster Practice Exam**

CompTIA Project+ Live Online Training Program

Program Description

The CompTIA Project+ Live Online Training program introduces students to the knowledge and skills required to manage the project life cycle, coordinate small-to-medium-sized projects, establish a communication plan, manage resources and stakeholders, maintain project documentation and artifacts, and support the completion of larger projects within an information technology (IT) environment.

The CompTIA Project+ Live Online Training program consists of 30 clock hours of instruction over two (2) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA Project+ certification examination (CompTIA Project+ PK0-005).

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA Project+ examination; students receive this certification from a third party through an examination process. The cost of the program includes ten (10) days of instructor-led online training, CertMaster Practice for CompTIA Project+, CertMaster Labs for CompTIA Project+, CertMaster Learn for instructor-led training for CompTIA Project+, a CompTIA Project+ examination voucher, and one (1) examination retake voucher.

This program prepares students for an IT Project Manager or equivalent IT role (CIP Code 11.1005, "IT Project Manager"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA Project+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA Project+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA Project+ Live Online Training program does not provide computer equipment, internet access, or required software for students. Students will need access to the internet and a reliable laptop or desktop computer, or a mobile device. Webcams are not required.

Learning Resources for Program Content

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Project+ in this program.

CompTIA Project+ Live Online Training Program Outline (Syllabus)

Day	Lessons	Activities
1	**Lesson 1: Preparing for the Project** • 1a. Understand Project Management Basics • 1b. Develop the Business Case • 1c. Identify Key Project Characteristics	• CML Lesson 1: Study Materials • Assisted Lab: Matching Roles and Responsibilities • Project+ Skills Quiz: Lesson 1
2	**Lesson 2: Selecting the Project Framework** • 2a. Identify Project Methodologies • 2b. Compare Agile and Waterfall Projects	• CML Lesson 2: Study Materials • Assisted Lab: Choosing a Project Methodology – Waterfall vs. Agile • Project+ Skills Quiz: Lesson 2
3	**Lesson 3: Initiating the Project** • 3a. Build a Project Team • 3b. Prepare Project Initiation Documents **Lesson 4: Facilitating Effective Meetings** • 4a. Lead Effective Meetings • 4b. Use Project Management Tools • 4c. Create a Communication Plan	• CML Lesson 3: Study Materials • CML Lesson 3: PBQ – Build a Project Team • Assisted Lab: Complete a Project Charter • Project+ Skills Quiz: Lesson 3 • CML Lesson 4: Study Materials • CML Lesson 4: PBQ – Lead Effective Meetings • Assisted Lab: Create a Communication Plan

4	**Lesson 5: Implementing Solution Design** • 5a. Create a Solution Design Document • 5b. Evaluate IT Infrastructure Needs **Lesson 6: Managing Resources** • 6a. Describe the Resource Life Cycle • 6b. Conduct a Needs Assessment	• CML Lesson 5: Study Materials • CML Lesson 5: PBQ – Evaluate IT Infrastructure Needs • Applied Lab: Interpret Solution Requirements • Project+ Skills Quiz: Lessons 4 & 5 • CML Lesson 6: Study Materials • Assisted Lab: Assign Project Resources
5	**Lesson 7: Managing Risk** • 7a. Identify and Analyze Risk • 7b. Treat and Monitor Risk **Midterm Examination**	• CML Lesson 7: Study Materials • Assisted Lab: Analyze Risk • Project+ Skills Quiz: Lessons 6 & 7 • Project+ Practice Midterm Exam (practice only) • Project+ Midterm Exam (required)
6	**Lesson 8: Creating a Project Schedule** • 8a. Define Units of Work • 8b. Sequence the Activities **Lesson 9: Creating a Project Plan** • 9a. Refine the Timeline • 9b. Establish Project Baselines • 9c. Create a Quality Assurance Plan	• CML Lesson 9: Study Materials • CML Lesson 9: PBQ – Create a Quality Assurance Plan • Applied Lab: Identify the Critical Path • Project+ Skills Quiz: Lessons 8 & 9
7	**Lesson 10: Procuring Solutions** • 10a. Compare Procurement Options • 10b. Evaluate and Select Vendors **Lesson 11: Manage Project Execution** • 11a. Document Progress • 11b. Communicate Progress	• CML Lesson 10: Study Materials • CML Lesson 10: PBQ – Evaluate and Select Vendors • Assisted Lab: Compare Resource Procurement Options • Project+ Skills Quiz: Lesson 10 • CML Lesson 11: Study Materials • CML Lesson 11: PBQ – Document Progress • Applied Lab: Build a Backlog with Sprints • Project+ Skills Quiz: Lesson 11
8	**Lesson 12: Managing Issues and Changes** • 12a. Resolve Issues • 12b. Control Changes **Lesson 13: Managing Performance** • 13a. Measure Performance	• CML Lesson 12: Study Materials • CML Lesson 12: PBQ – Resolve Issues • Assisted Lab: Identify Issues • Project+ Skills Quiz: Lesson 12 • CML Lesson 13: Study Materials

	• 13b. Maintain the Project Schedule	• CML Lesson 13: PBQ – Maintain the Project Schedule • Assisted Lab: Measure Project Performance
9	**Lesson 14: Wrapping Up the Project** • 14a. Prepare for Project Closure • 14b. Close the Project	• CML Lesson 14: Study Materials • Applied Lab: Reconcile the Budget • Project+ Skills Quiz: Lessons 13 & 14
10	**Project+ Review** **Project+ Final Exam**	• CML Project+ Final Assessment (optional practice) • Project+ Practice Final Exam • Project+ Final Exam

CompTIA Linux+ Live Online Training Program

Program Description

The CompTIA Linux+ Live Online Training program prepares students to work in the Linux operating system to manage infrastructure and software systems, create and execute scripts, establish and maintain system security, and analyze and troubleshoot user, application, and hardware issues.

The CompTIA Linux+ Live Online Training program consists of 30 clock hours of instruction over two (2) weeks, taught through synchronous interactive distance learning. The focus of this program is to prepare students to take and pass the CompTIA Linux+ certification examination (CompTIA Linux+ XK0-005).

This single-course, postsecondary program teaches curriculum to students to prepare them to take the CompTIA Linux+ examination; students receive this certification from a third party through an examination process. The cost of the program includes ten (10) days of instructor-led online training, CertMaster Practice for CompTIA Linux+, CertMaster Labs for CompTIA Linux+, CertMaster Learn for instructor-led training for CompTIA Linux+, a CompTIA Linux+ examination voucher, and one (1) examination retake voucher.

This program prepares students for a System Administrator, Linux Administrator, or equivalent IT role (CIP Code 11.1001, System Administration/Administrator"). CompTIA does not offer job placement or other career services after successful completion of the program.

Completion Requirements

A Pass (P) final grade for the CompTIA Linux+ Live Online Training will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete the program are awarded a Certificate of Completion. Students can access and download a copy of their Certificate of Completion in CertMaster Learn.

Failure to Complete Program

Students who do not successfully complete the CompTIA Linux+ Live Online Training program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Equipment and Software

The CompTIA Linux+ Live Online Training program does not provide computer equipment, internet access, or required software for students. Students will need access to the internet and a reliable laptop or desktop computer, or a mobile device. Webcams are not required.

Learning Resources for Program Content

Students will have access to CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Linux+ in this program.

CompTIA Linux+ Live Online Training Program Outline (Syllabus)

Day	Lessons	Activities
1	**Lesson 1: Introducing Linux** • 1a. Identify Linux Characteristics • 1b. Understand Bash Interaction with Linux • 1c. Use Help in Linux • 1d. Identify the Linux Troubleshooting Methodology **Lesson 2: Administering Users and Groups** • 2a. Manage User Accounts • 2b. Manage Group Accounts • 2c. Configure Privilege Escalation • 2d. Troubleshoot User and Group Issues	• CML Lesson 1: Study Materials • CML Lesson 1: PBQ – Introducing Linux • Assisted Lab: Exploring the Lab Environment • Assisted Lab: Basic Linux Interaction • CML Lesson 2: Study Materials • Assisted Lab: Manage User Accounts • Assisted Lab: Manage Group Accounts • Assisted Lab: Configure and Troubleshoot Privilege Escalation • Linux+ Skills Quiz: Lessons 1 & 2
2	**Lesson 3: Configuring Permissions** • 3a. Configure Standard Linux Permissions • 3b. Configure Special Linux Permissions • 3c. Configure Access Control Lists **Lesson 4: Implementing File Management** • 4a. Understand the Linux File System • 4b. Use File Management Commands	• CML Lesson 3: Study Materials • Assisted Lab: Configure Standard Linux Permissions • Assisted Lab: Configure Access Control Lists • Assisted Lab: Troubleshoot Permissions • Applied Lab: Identity and Access Control • CML Lesson 4: Study Materials • CML Lesson 4: PBQ – Implementing File Management • Assisted Lab: Manage File Links • Assisted Lab: Use File Management Commands

	• 4c. Find File Locations	• Assisted Lab: Search for Files • Linux+ Skills Quiz: Lessons 3 & 4
3	**Lesson 5: Authoring Text Files** • 5a: Edit Text Files • 5b. Manage Text Files **Lesson 6: Managing Software** • 6a. Understand Software Management • 6b. Manage RPM Software Packages and Repositories • 6c. Manage Debian-based Software Packages and Repositories • 6d. Compile from Source Code • 6e. Acquire Software • 6f. Run Software in a Sandbox	• CML Lesson 5: Study Materials • CML Lesson 5: PBQ – Authoring Text Files • Assisted Lab: Edit Text Files • Assisted Lab: Backup, Restore, and Compress Files • CML Lesson 6: Study Materials • Assisted Lab: Manage RPM Packages • Assisted Lab: Manage DEB Packages • Assisted Lab: Compile a Program • Assisted Lab: Download Files from a Web Server
4	**Lesson 7: Administering Storage** • 7a. Understand Storage • 7b. Deploy Storage • 7c. Manage Other Storage Options • 7d. Troubleshoot Storage **Lesson 8: Managing Devices, Processes, Memory, and the Kernel** • 8a. Gather Hardware Information • 8b. Manage Processes • 8c. Manage Memory • 8d. Manage the Linux Kernel	• CML Lesson 7: Study Materials • CML Lesson 7: PBQ – Administering Storage • Assisted Lab: Deploy Storage and LVM • Linux Skills Quiz: Lessons 5, 6 & 7 • CML Lesson 8: Study Materials • Assisted Lab: Manage Processes
5	**Lesson 9: Managing Services** • 9a. Manage System Services • 9b. Configure Common System Service • 9c. Configure Localization Settings **Lessons 1-9 Midterm Examination**	• CML Lesson 9: Study Materials • Assisted Lab: Manage Services • Assisted Lab: Deploy Services • Linux+ Skills Quiz: Lessons 8 & 9 • Linux+ Practice Midterm Exam (practice only) • Linux+ Midterm Exam (required)
6	**Lesson 10: Configuring Network Settings** • 10a. Understand Network Fundamentals • 10b. Manage Network Settings • 10c. Configure Remote Administrative Access • 10d. Troubleshoot the Network **Lesson 11: Configuring Network Security** • 11a. Configure the Firewall	• CML Lesson 10: Study Materials • CML Lesson 10: PBQ – Configuring Network Settings • Assisted Lab: Configure Network Settings • Assisted Lab: Configure Remote Administration • Applied Lab: System Management • CML Lesson 11: Study Materials • Assisted Lab: Configure a Firewall

	• 11b. Monitor Network Traffic	• Assisted Lab: Intercept Network Traffic • Linux+ Skills Quiz: Lessons 10 & 11
7	**Lesson 12: Managing Linux Security** • 12a. Harden a Linux System • 12b. Manage Certificates • 12c. Understand Authentication • 12d. Configure SELinux or AppArmor **Lesson 13: Implementing Simple Scripts** • 13a. Understand Bash Scripting Basics • 13b. Use Shell Script Elements • 13c. Implement Scripts with Logical Controls	• CML Lesson 12: Study Materials • Assisted Lab: Harden a Linux System • Assisted Lab: Configure SELinux • Applied Lab: Security • Linux+ Skills Quiz: Lesson 12 • CML Lesson 13: Study Materials
8	**Lesson 14: Using Infrastructure as Code** • 14a. Understand Infrastructure as Code • 14b. Implement Orchestration • 14c. Manage Version Control with Git **Lesson 15: Managing Containers in Linux** • 15a. Understand Containers • 15b. Deploy Containers • 15c. Understand Virtualization Concepts	• CML Lesson 14: Study Materials • CML Lesson 14: PBQ – Using Infrastructure as Code • Assisted Lab: Configure a System with Ansible • Assisted Lab: Manage Version Control with Git • CML Lesson 15: Study Materials • CML Lesson 15: PBQ – Managing Containers in Linux • Assisted Lab: Deploy Containers • Linux+ Skills Quiz: Lessons 13, 14 & 15
9	Lesson 16: Installing Linux • 16a. The Linux Boot Process • 16b. Modify Boot Settings • 16c. Deploy Linux	• CML Lesson 16: Study Materials • CML Lesson 16: PBQ – Installing Linux • Assisted Lab: Deploy a Linux System • Linux+ Skills Quiz: Lesson 16
10	Linux+ Review Linux+ Final Exam	• CML Linux+ Final Assessment (optional practice) • Linux+ Practice Final Exam • Linux+ Final Exam

Admissions Requirements

Prospective CompTIA Live Online Training (LOT) students must meet the following enrollment or admissions requirements:

- Be at least 18 years of age[1]
- Able to speak, read/write, and understand the English language
- Access to the internet and a reliable laptop or desktop computer, or a mobile device

Language Requirements

The LOT programming at CompTIA is offered in the English language. CompTIA does not offer English as a Second Language (ESL). The student must be able to speak, read/write, and understand the English language to enroll in any LOT program. The student's signature on the enrollment agreement signifies that they attest to their ability to be able to speak, read/write, and understand the English language

Technical Requirements

CompTIA does not provide computer equipment, internet access, or software used over the course of its programming. Students will need access to the internet and a reliable laptop or desktop computer or a mobile device in order to connect to Canvas, Zoom, and the CertMaster products. Webcams are not required.

Special Needs Accommodations

Any prospective student who has a special need or accommodation request must submit an Accommodation Request Form, along with supporting documentation to CompTIA's secure portal for review. The Accommodation Request Form can be obtained here. For questions regarding an accommodation, please contact lpierce@comptia.org.

Non-discrimination Policy

CompTIA will not discriminate in any way (including with respect to the administration of its educational policies, admissions, policies, scholarship, grant and/or loan programs, and other school-administered programs) against any applicant on the basis of race, color, religion, sex (including pregnancy, childbirth, and related medical conditions, transgender status, and gender identity), national origin, age, disability, political affiliation, or belief, or, for beneficiaries, applicants, and participants only on the basis of either citizenship status or participation.

[1] Residents of Utah and Delaware must additionally either possess a high school diploma or a General Education Development (GED) certificate/diploma. Students must attest to meeting this requirement during the application process.

Application Procedure

Prospective students who are interested in enrolling in one of CompTIA's Live Online Training (LOT) programs must register for their program(s) of choice online by navigating to the CompTIA LOT website at https://www.comptia.org/training/classroom-training/online-instructor-led-training.

Enrollment Dates

CompTIA's LOT programming has ongoing enrollment throughout the year, and prospective students can apply anytime. Prospective students should refer to the CompTIA Live Online Training Program Schedule found on pages 7-10 of this course catalog for upcoming program cohorts.

CompTIA Live Online Training Program Costs

The total cost of CompTIA's Live Online Training (LOT) offerings will vary by program. See Fee Charts below for the total cost of each program, along with pricing breakdowns. The cost of each program includes access to program content (CertMaster Learn, CertMaster Labs, and CertMaster Practice), live instruction via interactive distance learning, and the cost of the certification examination voucher(s) and one (1) retake voucher per examination.

Program Content

The total price of any one of CompTIA's LOT programs includes access to CertMaster Learn, CertMaster Labs, and CertMaster Practice. CertMaster Learn is designed to help students acquire knowledge and study toward their certification exam, CompTIA Labs lets students solve real-world problems in a simulated environment, and CertMaster Practice reinforces prior knowledge and prepares students for their certification exam.

Certification Examination Vouchers

The total price of any one of CompTIA's eight (8) LOT program offerings includes the cost of a certification examination voucher and one (1) retake voucher per examination.

Equipment and Software

CompTIA does not provide computer equipment or internet access to students. Students will need access to a laptop or desktop computer with internet access or a mobile device.

Students enrolled in any of the CompTIA LOT programs will need access to a computer with internet access or a mobile device. These will be used to connect to Canvas, Zoom, and the CertMaster products. Webcams are not required. If the student does not already have access to this equipment and software, it is estimated that this will add $500.00 to the total cost of the program.

Application Fees and Administrative Costs for Withdrawal or Termination

CompTIA does not charge students a fee for application to or withdrawal or termination from the institution.

Service Charges

CompTIA does not have any additional service charges.

Tools and Lab Fees

CompTIA does not charge any fees for tools or labs.

Fee Chart – CompTIA A+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$3,999.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA A+)	Included
Examination Vouchers (CompTIA A+ 220-1101 and 220-1102 and retakes)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$3,999.00** (if equipment owned/available) **OR** **4,499.00** (if equipment NOT owned/available)

Fee Chart – CompTIA Security+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$2,499.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Security+)	Included
Examination Vouchers (CompTIA Security+ SY0-601 and retake)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$2,499.00** (if equipment owned or available) **OR** **$2,999.00** (if equipment NOT owned or available)

Fee Chart – CompTIA Network+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$2,299.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Network+)	Included
Examination Vouchers (CompTIA Network+ N10-008 and retake)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$2,299.00** (if equipment owned or available) **OR** **$2,799.00** (if equipment NOT owned or available)

Fee Chart – CompTIA CySA+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$2,499.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA CySA+)	Included
Examination Vouchers (CompTIA CySA+ CS0-003 and retake)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$2,499.00** (if equipment owned or available) **OR** **$2,999.00** (if equipment NOT owned or available)

Fee Chart – CompTIA Data+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$1,999.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice for CompTIA Data+)	Included
Examination Vouchers (CompTIA Data+ DA0-001 and retake)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$1,999.00** (if equipment owned or available) **OR** **$2,499.00** (if equipment NOT owned or available)

Fee Chart – CompTIA PenTest+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$2,499.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice) for CompTIA PenTest+)	Included
Examination Vouchers (CompTIA PenTest+ PT0-002 and retake)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$2,499.00** (if equipment owned or available) **OR** **$2,999.00** (if equipment NOT owned or available)

Fee Chart – CompTIA Project+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$2,299.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice) for CompTIA Project+)	Included
Examination Vouchers (CompTIA Project+ PK0-005 and retake)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$2,299.00** (if equipment owned or available) **OR** **$2,799.00** (if equipment NOT owned or available)

Fee Chart – CompTIA Linux+ Live Online Training Program

Fee Type	Fee Amount
Total Cost of Program	$2,299.00
Content/Learning Materials (CertMaster Learn, CertMaster Labs, and CertMaster Practice) for CompTIA Linux+)	Included
Examination Vouchers (CompTIA Linux+ XK0-005 and retake)	Included
Equipment	$500.00 (if not already owned or available)
Software	$0
Late Fee	$0
Registration Fee	$0
Withdrawal Fee	$0
Total	**$2,299.00** (if equipment owned or available) **OR** **$2,799.00** (if equipment NOT owned or available)

Program Payment

Students must pay for the cost of their chosen CompTIA LOT program upfront. Payments can be made online using a credit card (VISA, Mastercard, Discover, American Express) or PayPal. Students can also choose to pay monthly using Affirm. With Affirm, students can pay for the cost of the program with monthly payments over three, six, or twelve months. Rates are between 0–30% APR. A down payment may be required. Subject to eligibility check and approval. Payment options depend on your purchase amount. The estimated payment amount excludes taxes and shipping fees. Actual terms may vary. Payment options through Affirm are provided by these lending partners: affirm.com/lenders.

Attendance Policies

Program attendance is an essential part of the educational process at CompTIA, and students are expected to attend each Live Online Training (LOT) program classroom session on time in order to facilitate their academic success. Attendance will be monitored and recorded daily throughout the program.

Absences

Students are permitted up to two (2) absences while enrolled in CompTIA's two-week LOT programs. Students are permitted up to four (4) absences while enrolled in CompTIA's four-week LOT program.

CompTIA Program	Maximum Absences
CompTIA A+ Live Online Training	4
CompTIA Network+ Livre Online Training	2
CompTIA Security+ Live Online Training	2
CompTIA CySA+ Live Online Training	2
CompTIA PenTest+ Live Online Training	2
CompTIA Linux+ Live Online Training	2
CompTIA Project+ Live Online Training	2
CompTIA Data+ Live Online Training	2

Students are considered absent if they fail to log into the designated classroom for a scheduled class, if they fail to return to the designated classroom after a break, or if they leave the designated classroom at a time other than a break.

Tardiness/Early Departure/Class Cuts

Students are expected to be on time for each class session. Students will be considered tardy anytime they arrive late to the start of class or leave prior to the conclusion of class. Students will be considered tardy if they log into the designated classroom more than 15 minutes after the start of class or if they return to the designated classroom more than 10 minutes after the end of a break.

Acquiring three (3) tardies is equivalent to one (1) absence.

Tracking Attendance

Instructors will take attendance at the start of the class, upon return from each scheduled break, and at the end of the class.

Class Breaks

CompTIA provides for one (1) 10-minute break per 60 minutes of instruction time.

Make-up Work

There will be no assigned make-up work.

Leave of Absence

CompTIA does not allow students to take a leave of absence while enrolled in any programming.

Grading System

Grading for CompTIA's Live Online Training (LOT) programs is Pass/Fail. Students will engage in a variety of activities in their LOT program, including quizzes, labs, and midterm exams, that will be reviewed and graded to ensure that the students are progressing appropriately through the program. Students must achieve a cumulative score of 70% or higher on the graded assignments in order to successfully complete and pass the program.

A Pass (P) final grade for the LOT programming will be based on the successful completion of the program coursework with a cumulative score of 70% or higher on graded assignments. Students who successfully complete their program are awarded a Certificate of Completion. Students who do not successfully complete the program coursework with a cumulative score of 70% or higher will receive a Fail (F) grade.

Students who withdraw from a LOT program will receive a Withdraw (W) grade. Students who are dismissed from a LOT program (involuntary exit after drop date) will receive a Withdraw (W) grade.

Satisfactory Academic Progress (SAP) Policy

Satisfactory academic progress (SAP) will not be measured in CompTIA's LOT programming.

Progress Report Policy

Due to the short-term nature of CompTIA's programming, students will not be awarded progress reports.

Job Placement Assistance or Other Career Services

Because the LOT (Live Online Training) programs offered at CompTIA are only designed to prepare students to sit for certification examinations, the institution does not offer job placement assistance or other career services for students taking any of the programs listed in this catalog.

Student Conduct Policy

Students are expected to conduct themselves in a professional manner and to act, speak, and demonstrate respect to others while enrolled at CompTIA. Students are required to be aware of and abide by the following rules of conduct:

- Threatening, intimidating, or physically harming any CompTIA staff, affiliate, or fellow student will result in immediate termination from the program.
- Disorderly conduct is forbidden at CompTIA. This includes, but is not limited to, inappropriate, disrespectful, insulting and/or obscene language and lewd, indecent, or obscene conduct. Any **discrim**inating or derogatory remarks or behavior against CompTIA staff or another student in reference to religion, culture, race, sex, or sexual orientation are grounds for immediate termination from the program.
- Be friendly and respectful to your instructor, fellow participants, and CompTIA staff members. Students should conduct themselves in a professional manner. Students who are deemed disruptive, argumentative, or otherwise unprofessional may face disciplinary action, up to and including termination from the program.
- CompTIA does not condone cheating in any form or the use of outside study materials. Students enrolled in the program will be provided approved study materials. Materials that are not approved by CompTIA may not be correct or legal.
- CompTIA strictly prohibits the piracy of software and the violation of piracy and copyright laws. No student should attempt to copy, make available, or distribute copies of copyrighted material.
- CompTIA does not maintain a dress code/policy for its Live Online Training programming.

Student Probation, Suspension, or Dismissal

CompTIA reserves the right to dismiss students for activities detrimental to themselves, other students, instructors, and the school. CompTIA does not put students on probation or suspension if they do not act in accordance with institutional conduct policies. Individuals who fail to comply with the program policies will be dismissed from the program.

Student Readmission Policy

Students who have previously withdrawn or who do not earn a “Pass” grade in their chosen CompTIA Live Online Training (LOT) program may apply for readmission. Students who are dismissed from a CompTIA LOT program due to Student Conduct Policy violations will not be eligible to enroll in future program cohorts.

Cancellation and Refund Policy

CompTIA is compliant with the cancellation and refund policy for its home state of Illinois, as well as state-specific cancellation and refund policies for students who are residents of other states which require that CompTIA use their cancellation and refund policies, as applicable. These policies are all listed below.

Student's Right to Cancel (Illinois)

The student has the right to cancel the initial enrollment agreement until 24 hours before the first class starts.

Other Cancellations

1. **Rejection of Applicant:** If an applicant is rejected for enrollment by the institution, a full refund of all monies paid must be made to the applicant.
2. **Program Cancellation:** If an institution cancels a program subsequent to a student's enrollment, the institution must refund all monies paid.
3. **Cancellation Prior to the Start of Class or No-Show:** If an applicant accepted by the institution cancels prior to the start of scheduled classes or never attends class (no-show), the institution must refund all monies paid.

Enrollment Termination or Student Withdrawal After Start of Class

Students withdrawing through 50% of the length of their enrolled program will receive a refund of 50% of the total program cost. The refund policy will differ between some of the CompTIA LOT programs, as stated below.

CompTIA Network+, CompTIA Security+, CompTIA CySA+, CompTIA Data+, CompTIA PenTest+, CompTIA Project+, and CompTIA Linux+ LOT Programs

For the CompTIA LOT programs that are two (2) weeks in length, students have until the end of the first week of their program to receive a refund of 50% of the total cost of the program. Students will not receive a refund if they withdraw on/after the first day of the second week of these two-week programs.

CompTIA A+ LOT Program

For the CompTIA LOT program that is four (4) weeks in length, students who withdraw through the end of the first week of the program will receive a refund of 75% of the total program cost. Following the end of the first week, students have until the end of the second week of class to withdraw and receive a 50% refund of the total program cost. Students will not receive a refund if they withdraw on/after the first day of the third week of this four-week program.

Refund Dispersal

All refunds will be issued within 30 days of the determination of the withdrawal date. Refunds are issued back to the source from which payment was received.

Procedure for Program Withdrawal and Withdrawal Date

1. A student choosing to withdraw may provide notice to CompTIA. The notice should include the name of the program the student wishes to withdraw from, the reason for the withdrawal request, the student's full name, the student's telephone number, and the student's address.

   Although any mode of withdrawal will be recognized, students are strongly encouraged to submit their withdrawal notice via email at comptiavirtualtraining@comptia.org. Students can also submit their withdrawal notice via postal mail to: CompTIA, Attn: Blythe Girnus, Withdrawal Notice, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515.

2. All refunds will be issued to the source from which tuition payment was received within 30 days of the determination of the withdrawal date.

State-Specific Cancellation and Refund Policies

Certain states require the use of a state-specific cancellation and refund policy for residents of their respective states. Residents of the states listed below should refer to these cancellation and refund policies.

Illinois Residents

STUDENT'S RIGHT TO CANCEL

The student has the right to cancel the initial enrollment agreement until 5:00 pm CT of the 5th business day after the student has been admitted. If the right to cancel is not given to any prospective student at the time the agreement is signed, then the student has the right to cancel the agreement at any time and receive a refund on all monies paid to date within 30 days of cancellation. Cancellation should be submitted to the authorized official of the school in writing.

Texas Residents

Refund Policy for Program of 40 Hours or Less

1. Refund computations will be based on the period of enrollment computed on basis of course time (clock hours).
2. The effective date of termination for refund purposes will be the earliest of the following:
   a. the last date of attendance; or
   b. the date of receipt of written notice from the student.
3. If tuition and fees are collected in advance of entrance, and the student does not enter school, not more than $100 shall be retained by the school.
4. If the student fails to enter the program, withdraws, or is discontinued at any time before completion of the program, the student will be refunded the pro rata portion of tuition, fees, and

other charges that the number of class hours remaining in the program after the effective date of termination bears to the total number of class hours in the program.

5. A full refund of all tuition and fees is due in each of the following cases:
    a. an enrollee is not accepted by the school;
    b. if the program of instruction is discontinued by the school and this prevents the student from completing the program; or
    c. if the student's enrollment was procured as a result of any misrepresentation in advertising, promotional materials of the school, or misrepresentations by the owner or representatives of the school.

REFUND POLICY FOR STUDENTS CALLED TO ACTIVE MILITARY SERVICE

6. A student of the school or college who withdraws from the school or college as a result of the student being called to active duty in a military service of the United States or the Texas National Guard may elect one of the following options for each program in which the student is enrolled:
    a. if tuition and fees are collected in advance of the withdrawal, a pro rata refund of any tuition, fees, or other charges paid by the student for the program and a cancellation of any unpaid tuition, fees, or other charges owed by the student for the portion of the program the student does not complete following withdrawal;
    b. a grade of incomplete with the designation "withdrawn-military" for the courses in the program, other than courses for which the student has previously received a grade on the student's transcript, and the right to re-enroll in the program, or a substantially equivalent program if that program is no longer available, not later than the first anniversary of the date the student is discharged from active military duty without payment of additional tuition, fees, or other charges for the program other than any previously unpaid balance of the original tuition, fees, and charges for books for the program; or
    c. the assignment of an appropriate final grade or credit for the courses in the program, but only if the instructor or instructors of the program determine that the student has:
        i. satisfactorily completed at least 90 percent of the required coursework for the program; and
        ii. demonstrated sufficient mastery of the program material to receive credit for completing the program.
7. Refunds will be totally consummated within 60 days after the effective date of termination.

Cancellation and Refund Policy for Program of 40 Hours or More

Cancellation Policy

A full refund will be made to any student who cancels the enrollment contract within 72 hours (until midnight of the third day excluding Saturdays, Sundays, and legal holidays) after the enrollment contract is signed. A full refund ill also be made to any student who cancels enrollment within the student’s first three scheduled class days, except that the school may retain not more than $100 in any administrative fees charged, as well as items of extra expense that are necessary for the portion of the program attended and stated separately on the enrollment agreement.

Refund Policy

1. Refund computations will be based on scheduled course time of class attendance through the last date of attendance. Leaves of absence, suspensions and school holidays will not be counted as part of the scheduled class attendance.
2. The effective date of termination for refund purposes will be the earliest of the following:
    a. The last day of attendance, if the student is terminated by the school;
    b. The date of receipt of written notice from the student; or
    c. Ten school days following the last date of attendance.
3. If tuition and fees are collected in advance of entrance, and if after expiration of the 72-hour cancellation privilege the student does not enter school, not more than $100 in any administrative fees shall be retained by the school for the entire residence program or synchronous distance education course.
4. If a student enters a residence or synchronous distance education program and withdraws or is otherwise terminated after the cancellation period, the school or college may retain not more than $100 in any administrative fees charged for the entire program. The minimum refund of the remaining tuition and fees will be the pro rata portion of tuition, fees, and other charges that the number of hours remaining in the portion of the course or program for which the student has been charged after the effective date of termination bears to the total number of hours in the portion of the course or program for which the student has been charged, except that a student may not collect a refund if the student has completed 75 percent or more of the total number of hours in the portion of the program for which the student has been charged on the effective date of termination[2].
5. Refunds for items of extra expense to the student, such as books, tools, or other supplies are to be handled separately from refund of tuition and other academic fees. The student will not be required to purchase instructional supplies, books, and tools until such time as these materials are required. Once these materials are purchased, no refund will be made. For full refunds, the school can withhold costs for these types of items from the refund as long as they were necessary for the portion of the program attended and separately stated in the enrollment agreement. Any such items not required for the portion of the program attended must be included in the refund.
6. A student who withdraws for a reason unrelated to the student's academic status after the 75 percent completion mark and requests a grade at the time of withdrawal shall be given a grade of "incomplete" and permitted to re-enroll in the course or program during the 12-month period following the date the student withdrew without payment of additional tuition for that portion of the course or program.
7. A full refund of all tuition and fees is due and refundable in each of the following cases:
    a. An enrollee is not accepted by the school;
    b. If the course of instruction is discontinued by the school and this prevents the student from completing the course; or

[2] More simply, the refund is based on the precise number of course time hours the student has paid for, but not yet used, at the point of termination, up to the 75% completion mark, after which no refund is due. Form CSC-1040R provides the precise calculation.

c. If the student's enrolment was procured as a result of any misrepresentation in advertising promotional materials of the school, or representations by the owner or representatives of the school.

A full or partial refund may also be due in other circumstances of program deficiencies or violations of requirements for career schools and colleges.

REFUND POLICY FOR STUDENTS CALLED TO ACTIVE MILITARY SERVICE

8. A student of the school or college who withdraws from the school or college as a result of the student being called to active duty in a military service of the United States or the Texas National Guard may elect the following options for each program in which the student is enrolled:
    a. If tuition and fees are collected in advance of the withdrawal, a pro rata refund of any tuition, fees, or other charges paid by the student for the program and a cancellation of any unpaid tuition, fees, or other charges owed by the student for the portion of the program the student does not complete following withdrawal.
    b. A grade of incomplete with the designation "withdrawn-military" for the courses in the program, other than courses for which the student has previously received a grade on the student's transcript, and the right to re-enroll in the program, or a substantially equivalent program if that program is no longer available, not later than the first anniversary of the date the student is discharged from active military duty without payment of additional tuition, fees, or other charges for the program other than any previously unpaid balance of the original tuition, fees, and charges for books for the program; or
    c. The assignment of an appropriate final grade or credit for the courses in the program, but only if the instructor or instructors of the program determine that the student has:
        1. Satisfactorily completed at least 90 percent of the required course for the program; and
        2. Demonstrated sufficient master of the program material to receive credit for completion the program.
9. The payment of refunds will be totally completed such that the refund instrument has been negotiated or credited into the proper account(a), within 60 days after the effective date of termination.

Utah Residents

Refund Policy

1. CompTIA observes a three-business-day cooling-off period during which time the student may rescind the contract and receive a refund of all money paid. The cooling-off period may not end prior to midnight of the third business day after the latest of the following days:
    a. The day the student signs an enrollment agreement;
    b. The day the student pays the institution an initial deposit or first payment toward tuition and fees; or

c. The day that the student first visits the institution, if the program lasts more than 30 consecutive calendar days.

2. A student enrolled in a correspondence institution may withdraw from enrollment following the cooling-off period, prior to submission by the student of any lesson materials or prior to receipt of course materials, whichever comes first, and effective upon deposit of a written statement of withdrawal for delivery by mail or other means, and the institution shall be entitled to retain no more than $200 in tuition or fees as registration charges or an alternative amount that the institution can demonstrate to have been expended in preparation for that particular student's enrollment.
3. Students who desire a refund after the three-business-day cooling-off period or after a student enrolled in a correspondence institution has submitted lessons materials or been in receipt of course material will have their refunds calculated in the following manner:
    a. Refund amounts must be based on a student's last date of attendance (LDA). When determining the number of weeks completed by the student, the institution may consider a partial week the same as if a whole week were completed, provided the student was present at least one day during the scheduled week.
    b. During the first week of classes, tuition charges withheld must not exceed 10 percent (10%) of the stated tuition up to a maximum of $1,000.
    c. After the first week and through fifty percent (50%) of the period of financial obligation, tuition charges retained must not exceed a pro rata portion of tuition for the training period completed, plus ten percent (10%) of the unearned tuition for the period of training that was not completed, up to a maximum of $1,000. Institutions that do not retain any unearned tuition may assess an administrative fee associated with withdrawal or termination not to exceed $100.
    d. After fifty percent (50%) of the period of financial obligation is completed by the student, the institution may retain the full tuition for that period.
4. A pay-as-you learn payment schedule limits a student's prospective contractual obligation(s), at any one time, to the institution for tuition and fees to four months of training, plus registration or start up costs not to exceed $200 or an alternative amount the institution can demonstrate to have spent in undertaking a student's instruction.

Oklahoma Residents

Cancellation and Refund Policy

1. **Rejection:** An applicant rejected by the school shall be entitled to a refund of all monies paid minus any stated application fee, not to exceed $25.00.
2. **Three-day cancellation:** All monies paid by an applicant shall be refunded if requested within three days after signing an enrollment agreement and making an initial payment.
3. **Other cancellation:** An applicant subsequently requesting cancellation shall be entitled to a refund of all monies paid minus a registration fee of 15% of the contract price of the course, but in no event may the school retain more than $150.00.
4. **First week:** For a student terminating training after entering school and starting the course of training but within the first week, the tuition retained by the school shall not exceed 10% of the contract price of the course plus $150.00 but in no event more than $350.00. The Board may waive this requirement upon written request by the school if it feels the request is justified.

5. **After first week:** For a student terminating training after one week but within the first 25% of the course, the tuition retained by the school shall not exceed 25% of the contract price of the course plus $150.00.
6. **After 25%:** For a student terminating training after completing over 25% but within 50% of the course, the tuition retained by the school shall not exceed 50% of the contract price of the course plus $150.00.
7. **After 50%:** A student completing more than 50% of the course is not entitled to a refund of any tuition.
8. **Special cases:** In case of student prolonged illness or accident, death in the family, or other circumstances that make it impractical to complete the course, the school shall make a settlement which is reasonable and fair to both.
9. **Discontinued class:** If a class is discontinued by a school while students are still enrolled in that class, and the school is still offering training in other areas, all monies (student loan, grant, and etc.) paid the school for students enrolled in the class at the time it is discontinued shall be refunded to the entity legally entitled to the refund. A school shall have thirty (30) days to restart the class or pay the refund.

Minnesota Residents

Refund Policy for Programs That Are 40 Hours or Less

If your application is rejected, you will receive a full refund of all tuition, fees, and other charges. If your program is 40 hours or less and you withdrew from your program, your refund will be pro-rated by the number of hours attended and the length of the program. To receive a full refund of tuition, fees, and other charges, you must withdraw from your program before the scheduled start day of the program. You will receive written notice acknowledging your withdraw request within 10 business days after receipt of the notice and you will receive a refund of any tuition, fees, and other charges within 30 business days of receipt of your withdrawal. Any mailed notice is effective as of the date of the postmark if sent by mail or the day it has been hand-delivered to the school. Notice to withdraw may also be given by email, verbally to a school official (not just an instructor), or with a voicemail to a school official. Please submit this withdraw notice to comptiavirtualtraining@comptia.org.

Refund Policy for Programs Greater Than 40 Hours with a Written Contract or Enrollment Agreement

If your application is rejected, you will receive a full refund of all tuition, fees, and other charges. You will be entitled to a full refund of tuition, fees, and other charges if you give notice that you are canceling your contract within 5 business days after the contract or enrollment agreement is considered effective. A contract or enrollment agreement will be presumed to be effective on the date that the school notifies you that you have been accepted into the school and you have signed the contract or enrollment agreement. If the notification of acceptance into the school is sent by mail, then the effective day of being accepted is the postmark on the acceptance letter.

This five-day refund policy applies regardless of when the program starts. If you give notice more than 5 days after you signed the contract, but before the start of the program (or first lesson for an online distance education program), you will receive a refund of all tuition, fees, and other charges minus 15%, up to $50, of the total cost of the program. If you withdraw after the start of your program and it has been more than 5 days after you signed the contract, you will receive a pro-rated refund of the entire cost of

your program based on your last day of attendance. You will be provided a prorated tuition, fees, and other charges refund minus your initial application fees, up to $50, and minus the less or 25% of the total tuition or $100. Proration is based on whether your program is term-based or clock hours and how much of the program you have completed.

If your program is term-based, the completion rate is the number of calendar days from the first date of the program through your last documented date of attendance divided by the length of the program. The completion rate is calculated to the second decimal point (.XX).

If your program is clock-hour based, the completion rate is the number of clock hours you actually attended divided by the number of clock hours in the program. The completion rate is calculated to the second decimal point (.XX)

If you withdraw from your program after 75.00% of the program has completed, you are not entitled to a refund of tuition, fees, and other charges.

You will receive written notice acknowledging your withdraw request within 10 business days after receipt of the notice and you will receive a refund of any tuition, fees, and other charges within 30 business days of receipt of your withdrawal. Any mailed notice is effective as of the date of the postmark if sent by mail or the day it has been hand delivered to the school. Notice to withdraw may also be given by email or verbally, including a voicemail, to a school official (defined by school's Student Right to Cancel policy). Please submit this withdraw notice to comptiavirtualtraining@comptia.org.

If you do not withdraw in writing or contact the school about your absence and you have not attended your program or contact the school about your absence for 14 consecutive days, you will be considered to have withdrawn from the school as of your last date of attendance. Your school is responsible for sending you a written notice of cancellation if you are withdrawn for failing to attend to your last known address. The confirmation from the school must state that the school has withdrawn your enrollment, and if this action was not the student's intent, the student must contact the school.

California Residents

Students Right to Cancel (California)

The student has the right to cancel the initial enrollment agreement and obtain a refund of charges paid through attendance at the first class session, or the seventh day after enrollment, whichever is later.

Other Cancellations

The institution will refund all monies paid if an applicant is rejected for enrollment by the institution, if the institution cancels a program subsequent to a student's enrollment, or if an applicant accepted by the institution cancels prior to the start of scheduled classes or never attends class ("no-show").

Enrollment Termination or Student Withdrawal After Start of Class

Students withdrawing through 50% of the length of their enrolled program will receive a refund of 50% of the total program cost. The refund policy will differ between some of the CompTIA LOT programs, as stated below.

CompTIA Network+, CompTIA Security+, CompTIA CySA+, CompTIA Data+, CompTIA PenTest+, CompTIA Project+, and CompTIA Linux+ LOT Programs

For the CompTIA LOT programs that are two (2) weeks in length, students have until the end of the first week of their program to receive a refund of 50% of the total cost of the program. Students will not receive a refund if they withdraw on/after the first day of the second week of these two-week programs.

CompTIA A+ LOT Program

For the CompTIA LOT program that is four (4) weeks in length, students who withdraw through the end of the first week of the program will receive a refund of 75% of the total program cost. Following the end of the first week, students have until the end of the second week of class to withdraw and receive a 50% refund of the total program cost. Students will not receive a refund if they withdraw on/after the first day of the third week of this four-week program.

Delaware Residents

Cancellation Policy

In addition to the cancellation conditions listed on the Student's Right to Cancel on page 68, Delaware residents will receive a full refund of all monies paid if the enrollment of the student was procured as the result of any misrepresentation in advertising, promotional materials of the school or representations by the owner or representative of the school.

Refund Policy

Refund computations will be based on scheduled course time of class attendance through the last date of attendance.

1. Following the cancellation period, the minimum refund of the remaining tuition will be:
    a. After 0.01% enrollment time of the course, 80% of the remaining tuition.
    b. After 5% to 9.9% enrollment time of the course, 70% of the remaining tuition;
    c. After 10% to 14.9% enrollment time of the course, 60% of the remaining tuition;
    d. After 15% to 24.9% enrollment time of the course, 55% of the remaining tuition;
    e. After 25% to 49.9% enrollment time of the course, 30% of the remaining tuition;
    f. After 50% or more enrollment time of the course, the student may be considered obligated for the full tuition;
2. The effective date of termination for refund purposes will be the earliest of the following:
    a. The last day of attendance, if the student is terminated by the school;
    b. The date of receipt of written notice from the student; or
    c. Ten school days following the last date of attendance.

Louisiana Residents

Cancellation and Refund Policy

1. Three-Business-Day Cancellation. All monies paid by a student shall be refunded if requested within three business days after signing an enrollment agreement and making an initial payment.

2. Cancellation after the Three-Business-Day

   Cancellation Period but Before Commencement of Classes by the Student. If tuition or fees are collected in advance of entrance, and if the student does not begin classes, not more than a $150 registration fee shall be retained by the institution. Appropriate refunds shall be made within 30 days of the start of the quarter, term, or semester.

3. For programs less than 300 clock hours, the withdrawal after commencement of classes refund policy shall be:
   a. after a student has completed less than 15 percent of the program, the institution shall refund at least 80 percent of the tuition, less the registration fee, thereafter;
   b. after a student has completed less than one-fourth of the program, the institution shall refund at least 70 percent of the tuition, less the registration fee, thereafter;
   c. after a student has completed one-fourth, but less than one-half of the program, the institution shall refund at least 45 percent of the tuition, less the registration fee, thereafter;
   d. after a student has completed one-half or more of the program, the institution may retain 100 percent of the stated program price.
4. Any unused portion of the book fee will be refunded.

Arkansas Residents

Refund Policy

The refund shall be based on the cost and length of the program. All tuition beyond the current enrollment period shall be refunded when a student terminates.

- At completion of less than twenty-five percent (25%) of the program, the refunds shall be made on a pro rata basis.
- At completion of 25% but less than 50% of the program, the student shall be refunded not less than 50% of the tuition.
- At completion of 50% but less than 75% of the program, the student shall be refunded not less than 25% of the tuition.
- At completion of 75% or more of the program, no refund is due to the student.

Alabama Residents

Cancellation Policy

Students may cancel enrollment at any time complying with the notification procedures established by the school. Refunds of unearned prepaid tuition, fees, and other charges shall be made in the following manner within thirty (30) days of termination:

a.) If cancellation occurs within seventy-two (72) hours of enrollment date, all money paid by the prospective student shall be refunded.

b.) If cancellation occurs seventy-two (72) hours of enrollment date, but before classes begin or correspondence materials are delivered, a refund shall be made of all money paid except the registration fee.

c.) If cancellation occurs after classes begin or after shipment of correspondence materials, a pro rata refund will be made of all unearned prepaid tuition, fees, and charges for books and supplies not issued to the student. Once books and supplies are issued received by students, these become property of the students and refunds may be made only at the discretion of the private school.

d.) A full refund is due students whose contracted educational services are denied by the school as a result of economic or academic fraud as defined in the *Code of Alabama* §16-46-1(7) and (8) (1975).

Washington Residents

A student may request cancellation in any manner and upon such request for cancellation being received and recorded by the school demonstrating the last date of attendance and/or completion of a lesson.

An applicant may cancel up to five business days after signing the enrollment agreement. In the event of a dispute over timely notice, the burden to prove service rests on the student.

If a student cancels after the fifth calendar day (excluding Sundays and holidays) but before the school receives the first completed lesson, the school may keep only a registration fee of either fifty dollars or an amount equal to fifteen percent of the tuition, but no greater than a registration fee of one hundred and fifty dollars.

After the school receives the students first completed lesson and until the student completes half the total number of lessons in the program, the school is entitled to keep the registration fee and a percentage of the total tuition as described in the following table:

If the student completes this percentage of lessons:	**The school may keep this percentage of the tuition cost:**
0% through 10%	10%
11% through 25%	25%
26% through 50%	50%
More than 50%	100%

Other Policies

Credit for Previous Experience

CompTIA does not offer credit for previous education, training, work, or life experience (experiential credit) for its Live Online Training (LOT) programs.

Transfer of Credits

Graduates of CompTIA's certification examination preparation programs will not be issued academic credits that can be transferred to other academic institutions. CompTIA does not accept academic credits issued by other academic institutions. Because the programs at CompTIA are designed as one-course programs, the transferability of credits cannot be considered.

Transcripts

Students can access and print an unofficial copy of their transcript at any time by logging into the student portal. Students can request an official copy of their transcript by submitting a request to comptiavirtualtraining@comptia.org. Official transcripts cannot be emailed.

Program Cancellation

If any CompTIA LOT program cohort is cancelled, a full refund of tuition, fees, and other charges will be issued to the source from which the tuition payment was received.

Orientation

Students are required to complete orientation before starting their CompTIA training program. Instructions for completing the orientation will be provided in the program welcome email.

Confidentiality of Student Records

CompTIA complies with the Family Educational Rights and Privacy Act (FERPA) by protecting the confidentiality of personally identifiable educational records of students and former students.

The student has the following rights: the right to inspect and review their education records within 45 days of the day the school receives a request for access; the right to request an amendment of their education records that the student believes are inaccurate or misleading; the right to consent to disclosures of personally identifiable information (PII) contained in their education records except to the extent that FERPA authorizes disclosure without consent; and the right to file a complaint with the U.S. Department of Education concerning alleged failures by CompTIA to comply with the requirements of FERPA. A health and safety exception permits the disclosure of PII from a student's record to appropriate parties if knowledge of the information is necessary to protect the health or safety of the student or other individuals from an immediate threat.

Grievance Policy

Purpose:

To establish a fair and transparent process for raising, addressing, and resolving grievances raised by students enrolled in CompTIA's Live Online Training (LOT) programs ("CompTIA LOT Programs") in a timely and appropriate manner.

Scope:

This policy applies to all students enrolled in CompTIA LOT Programs.

Definitions:

Grievance: A formal expression of dissatisfaction or complaint regarding any aspect of CompTIA LOT Programs, including but not limited to course content, instructor performance, facilities, or administrative processes.

Process:

1. All grievances must be submitted in writing to the CompTIA Compliance Department at compliance@comptia.org within 30 days of the incident or issue that led to the grievance.
2. CompTIA's Compliance Department will acknowledge receipt of the grievance within five (5) business days and will initiate an investigation into the matter.
3. The Compliance Department will perform a fact investigation based on the grievance, which may include gathering relevant information and documentation, including statements from the student, the instructor, and any other relevant parties.
4. The Compliance Department will review the information and make a determination on the grievance within 30 days of receipt of the grievance. The Compliance Department will communicate such determination and any proposed resolution to the student in writing. If additional time is needed to make and/or communicate this determination, the Compliance Department will notify the student in writing.
5. If the student is not satisfied with CompTIA's initial determination, the student may appeal within 15 days of receiving the determination. An appeal must be made in writing, to compliance@comptia.org.
6. If applicable, within 30 days of receiving the appeal, CompTIA shall make a final and binding decision regarding the grievance, after taking into consideration the original grievance, all available facts, and any supplemental materials provided by the student in the appeal.

Confidentiality:

All information related to a grievance will be treated as confidential and will only be shared with those individuals directly involved in the grievance process. CompTIA will take all reasonable steps to protect the privacy of the student and any other individual(s) involved in the grievance process.

Non-Retaliation:

CompTIA prohibits retaliation against any student for filing a grievance or participating in the grievance process. Any student who believes they have been subjected to retaliation should contact compliance@comptia.org immediately.

Contact Information:

Students may contact CompTIA Compliance at compliance@comptia.org for assistance with the grievance process or to submit a grievance.

Illinois Complaint Procedure

If the complaint cannot be resolved after exhausting the institution's grievance procedure, the student may file a complaint with the Illinois Board of Higher Education, Division of Private Business and Vocational Schools. Student complaints must be submitted in writing to the Board (Section 85(i)(1) of the Act). Information about the complaint may be submitted online through the IBHE website (www.ibhe.org). Additional information regarding the complaint process can be obtained by contacting the Board at:

Illinois Board of Higher Education
Division of Private Business and Vocational Schools - 1 N. Old State Capitol Plaza, Suite 333, Springfield IL 62701-1377, Phone Number: (217) 782-2551 Fax Number: (217) 782-8548 Website: www.ibhe.org

Institutional Disclosure Information (Illinois Requirement)

All schools are required to make available, at a minimum, the following disclosure information clearly and conspicuously on their 1) internet website, 2) school catalog, and 3) as an addendum to their Enrollment Agreement:

- The number of students who were admitted in the program as of July 1 of that reporting period.
- The number of additional students who were admitted in the program during the next 12 months and classified in one of the following categories: new starts, re-enrollments, and transfers into the program from other programs at the school.
- The total number of students admitted in the program during the 12-month reporting period.
- The number of students enrolled in the program during the 12-month reporting period who: transferred out of the program and into another program at the school, completed or graduated from a program, withdrew from the school, and are still enrolled.
- The number of students enrolled in the program who were: placed in their field of study, placed in a related field, placed out of the field, not available for placement due to personal reasons, and not employed.
- The number of students who took a State licensing exam or professional certification exam, if any, during the reporting period, as well as the number who passed.
- The number of graduates who obtained employment in the field who did not use the school's placement assistance during the reporting period (pending reasonable efforts to obtain this information from graduates).
- The average starting salary for all school graduates employed during the reporting period (pending reasonable efforts to obtain this information from graduates).

NOTE from CompTIA: Information currently not available for the Live Online Training programs contained in this course catalog as they are new programs.

COMPLAINTS AGAINST THIS SCHOOL MAY BE REGISTERED WITH THE BOARD OF HIGHER EDUCATION

Complaints should be directed to:

Division of Private Business and Vocational Schools
1 N. Old State Capitol Plaza, Suite 333, Springfield IL 62701-1377
Phone Number: (217) 782-2551 Fax Number: (217) 782-8548 Website: www.ibhe.org

Addendum 1

Listing of CompTIA Faculty and Program(s) Taught

CompTIA A+ Live Online Training Program

- Alan Kuttner
- Annaliza Marks
- Barrett Busch
- Crystal Pendergrass
- Dan Davis
- Daniel Hughes
- David Harcyznski
- David Perry
- Eddie Horton
- Gray Church
- Herb Poland
- Jagger Coffey
- Jeffrey Mehl
- Jeremiah Minner
- Jerry Carillo
- John Sparks
- Joe Walsh
- Jon Weiss
- Leonard Nichols
- Noel Broman
- Peter Barron
- Ryan Bingham
- Steve O'Dell
- Tami Berner
- Thomas Moore-Pizon
- Tony Carlson

CompTIA Security+ Live Online Training Program

- Alan Kuttner
- Annaliza Marks
- Barrett Busch
- Brian Ford
- Bryan Durrance
- Crystal Pendergrass
- Dan Davis
- Daniel Hughes
- David Harczynski
- Dean Worster
- Eddie Horton
- Greg Childers
- Herb Poland

- Jagger Coffey
- Jeffrey (Billy) Book
- Jeffrey Mehl
- Jeremiah Minner
- Jerry Carillo
- Joe Walsh
- John Sparks
- Jon Weiss
- Jonathan Weiss
- Leonard Nichols
- Ryan Bingham
- Tami Berner
- Thomas Moore-Pizon
- Tony Carlson

CompTIA Network+ Live Online Training Program

- Alan Kuttner
- Annaliza Marks
- Dan Davis
- Daniel Hughes
- David Harczynski
- Eddie Horton
- Greg Childers
- Herb Poland
- Jagger Coffey
- Jeffrey (Billy) Book
- Jeffrey Mehl
- Jeremiah Minner
- Jerry Carillo
- Joe Walsh
- John Sparks
- Jon Weiss
- Leonard Nichols
- Ryan Bingham
- Thomas Moore-Pizon
- Tony Carlson

CompTIA Data+ Live Online Training Program

- Annaliza Marks
- Brian Ford
- Daniel Davis
- Daniel Hughes
- Gray Church
- Greg Childers
- Joe Walsh
- Jon Weiss

- Leonard Nichols
- Ryan Bingham

CompTIA CySA+: Live Online Training Program

- Brian Ford
- Daniel Davis
- Daniel Hughes
- David Perry
- Dean Worster
- Eddie Horton
- Greg Horton
- Herb Poland
- Jagger Coffey
- Jeffery (Billy) Book
- Jeffrey Mehl
- Jeremiah Minner
- Joe Walsh
- John Sparks
- Leonard Nichols
- Peter Barron
- Tami Berner
- Tony Carlson

CompTIA PenTest+ Live Online Training Program

- Barrett Busch
- Brianna Greenberg
- Daniel Davis
- Daniel Hughes
- Greg Childers
- Jeremiah Minner
- John Sparks
- Tami Berner

CompTIA Project+ Live Online Training Program

- Barrett Busch
- Daniel Davis
- Daniel Hughes
- Gray Church
- Greg Childers
- Leonard Nichols
- Thomas Moore-Pizon

CompTIA Linux+ Live Online Training Program

- Brian Ford
- Eddie Horton
- Jeremiah Minner
- Leonard Nichols
- Ryan Bingham

Addendum 2

Texas Requirements

Student Grievances

Unresolved grievances for Texas residents should be directed to the Texas Workforce Commission. Their contact information is as follows:

Texas Workforce Commission
Career Schools and Colleges, Room 226T
101 East 15th Street
Austin, Texas 78778-0001
Phone: 512-936-3100 Texasworkforce.org/careerschools

Key Staff and Faculty

A list of key staff and faculty of the institution, showing degrees held, and all specialized training related to the areas of instruction. Each individual's area of instruction should be indicated.

Chief School Officers

- **Courtney Fong**, B.S., MBA, JD – Chief Operations Officer
- **Brian Laffey**, M.S. – Chief Financial Officer, CompTIA
- **Todd Thibodeaux**, M.S., Economics – Chief Executive Officer

Chief School Administrators

- **Blythe Girnus**, M.S, Vice President, Training Delivery

Faculty Members

- **Alan Kuttner,** CompTIA A+, Cloud+, Network+, and Security+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, and CompTIA Security+ LOT programs)
- **Annaliza Marks,** M.S., B.S., Adult and Continuing Education, Business Administration; CompTIA A+, Network+, Security+, and Data+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA Data+ LOT programs)
- **Barrett Busch,** B.S., Cybersecurity and Information Assurance CompTIA A+, Network+, Project+, PenTest+, and Cloud Essentials certifications (programs taught CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Project+ LOT, and CompTIA PenTest+ LOT programs)
- **Brian Ford,** M.S., B.S., Information Assurance, Computer Science; CompTIA Security+, CySA+, Data+, CASP+, Linux+, and Cloud Essentials+ certifications (programs taught: CompTIA Security+ LOT, CompTIA CySA+ LOT, CompTIA Data+ LOT, and CompTIA Linux+ LOT programs)
- **Brianna Greenberg**, M.S., B.S., A.A.S, Information Technology, Networking and Computer Support; CompTIA Network+, PenTest+, and Cloud+ certifications (programs taught: CompTIA Network+ LOT and CompTIA PenTest+ LOT programs)
- **Bryan Durrance,** M.S., B.S., Computer Science, Computer Networks and Cybersecurity; CompTIA Security+ certification (programs taught: CompTIA Security+ LOT program)
- **Crystal Pendergrass,** B.S., Business Management; CompTIA A+, Security+, ITF+, and CTT+ certifications (programs taught: CompTIA A+ LOT and CompTIA Security+ LOT programs)

- **Daniel Davis,** B.S., Cybersecurity and Information Assurance; CompTIA A+, Network+, Security+, CySA+, PenTest+, Project+, CTT+, and CASP+, Cloud+, Data+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, CompTIA Data+ LOT, CompTIA PenTest+ LOT, and CompTIA Project+ LOT programs)
- **Daniel Hughes** GED; CompTIA A+, Network+, Security+, CASP+, Cloud Essentials+, CySA+, Data+, ITF+, PenTest+, Project+, and Server+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, CompTIA Data+ LOT, and CompTIA PenTest+ LOT, and CompTIA Project+ LOT programs)
- **David Harczyski,** B.S. Accounting; CompTIA A+, Network+, and Security+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, and CompTIA Security+ LOT programs)
- **David Perry,** CompTIA A+ and CySA+ certifications (programs taught: CompTIA A+ LOT, CompTIA and CompTIA CySA+ LOT programs)
- **Dean Worster**, M.S., B.S., Information Systems Management, Internetworking Technologies; CompTIA A+, CySA+, CASP, Cloud+ certifications (programs taught: CompTIA A+ LOT and CompTIA CySA+ LOT programs)
- **Eddie Horton,** Ph.D., M.Ed., B.S. Business, Network Security, and Information Management, Educational Technology, and Computer Information Systems and Information Engineering; CompTIA A+, Network+, Security+, Server+, CySA+, CASP, Cloud+, and Linux+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, and CompTIA Linux+ LOT programs)
- **Gray Church,** M.S., B.A. Software Engineering, Slavic Languages and Literature; CompTIA A+, Project+ and Data+ certifications (programs taught: CompTIA A+ LOT, CompTIA Data+ LOT, and CompTIA Project+ LOT programs)
- **Greg Childers,** B.A. Sociology; CompTIA A+, Network+, Security+, Project+, CySA+, CASP, Cloud+ Data+, and PenTest+ certifications (programs taught: CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, CompTIA Data+ LOT, CompTIA PenTest+ LOT, and CompTIA Project+ LOT programs)
- **Herb Poland**, A.A., Applied Science; CompTIA A+, Network+, Security+, CySA+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT programs)
- **Jagger Coffey,** M.S., Applied Engineering and Technology Management; CompTIA A+, Network+, Security+, and CySA+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, and CompTIA CySA+ LOT programs)
- **Jeffrey (Billy) Book**, B.S., A.A.S., Information Technology, Information Systems; CompTIA Network+, Security+, and CySA+ certifications (programs taught: CompTIA Network+ LOT, CompTIA Security+ LOT, and CompTIA CySA+ LOT programs)
- **Jeffrey Mehl,** MBA, B.S., B.S., Marketing/Operations Management, Information Technology, Business Administration; CompTIA A+, Network+, Security+, CySA+ and ITF+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA CySA+ and CompTIA Security+ LOT programs)
- **Jeremiah Minner,** MBA, B.S, Engineering Management; CompTIA A+, Network+, Security+, CySA+, PenTest+, Cloud+, Cloud Essentials, ITF+, Linux+, Server+, CASP+, and CTT+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, CompTIA PenTest+ LOT, and CompTIA Linux+ LOT programs)
- **Jerry Carillo,** CompTIA A+, Network+, and Security+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, and CompTIA Security+ LOT programs)

- **Joe Walsh,** B.S., Information Systems; CompTIA A+, Network+, Security+, CySA+, Data+, ITF+, and CASP+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, and CompTIA Data+ LOT programs)
- **John Sparks,** B.S. Industrial Technology; CompTIA A+, Network+, Security+, PenTest+, CySA+, ITF+, Server+, and Cloud Essentials+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, and CompTIA PenTest+ LOT)
- **Jon Weiss,** M.A., B.S., B.A., Interdisciplinary Studies, Information Technology, Liberal Arts and Sciences; CompTIA A+, Network+, Security+, Data+, ITF+, and Cloud Essentials+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, and CompTIA Data+ LOT programs)
- **Jonathan Weiss,** M.S., B.A. Computer Science, Math, and Computer Science; CompTIA Security+ certification (programs taught: CompTIA Security LOT program)
- **Leonard Nichols,** M.S, B.A., Cybersecurity, Criminal Justice; CompTIA A+, Network+, Security+, CySA+, Data+, Project+, PenTest+, Server+, ITF+, Linux+, CASP, Cloud Essentials+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, CompTIA Data+ LOT, CompTIA PenTest+ LOT, and CompTIA Linux+ LOT programs)
- **Noel Broman,** Ph.D., M.S., B.S., Information Technology Management, Management Information Systems, Information Technology; CompTIA A+ certification (programs taught: CompTIA A+ LOT program)
- **Peter Barron,** B.A., Communications & Theological Studies; CompTIA A+ and CySA+ certifications (programs taught: CompTIA A+ LOT and CompTIA CySA+ LOT programs)
- **Ryan Bingham,** M.S., B.A. Technology Management, Philosophy; CompTIA A+, Network+, Security+, Data+, ITF+, and Linux+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, CompTIA Data+ LOT, and CompTIA Linux+ LOT programs)
- **Steve O'Dell,** Ph.D., MBA, M.S., B.S., B.S., Business, Forensic Science, Justice Science, Microbiology; CompTIA A+, Security+, ITF+, Cloud Essentials certifications (programs taught: CompTIA Security+ LOT and CompTIA CySA+ LOT programs)
- **Tami Berner,** B.S., Cybersecurity and Information Assurance; CompTIA A+, Network+, Security+, CySA+, Project+, PenTest+, ITF+, Mobility+, and Server+ certifications (programs taught: CompTIA A+ LOT, CompTIA Security+ LOT, CompTIA CySA+ LOT, and CompTIA PenTest+ LOT programs)
- **Thomas Moore-Pizon,** MBA, M.S., B.A., Library and Information Sciences, Computer Science, Mathematics; CompTIA A+, Network+, Security+, Project+, CTT+, and Server+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, CompTIA Security+ LOT, and CompTIA Project+ LOT programs)
- **Tony Carlson,** M.S., Network Security; CompTIA A+, Network+, Security+, CySA+, Server+, Cloud+, CTT+ certifications (programs taught: CompTIA A+ LOT, CompTIA Network+ LOT, and CompTIA Security+ LOT, and CompTIA CySA+ LOT programs)

True and Correct Statement

The information contained in this catalog is true and correct to the best of my knowledge.

_____

Todd Thibodeaux, Chief Executive Officer

Addendum 3

Kentucky Requirements

Existence of the Kentucky Student Protection Fund

Pursuant to KRS 165A.450, all licensed schools, resident and nonresident, shall be required to contribute to a student protection fund. The fund shall be used to reimburse eligible Kentucky students, to pay off debts, including refunds to students enrolled or on leave of absence by not being enrolled for one (1) academic year or less from the school at the time of the closing, incurred due to the closing of the school, discontinuance of a program, loss of license, or less of accreditation by a school or program.

Process for Filing a Claim Against the Kentucky Student Protection Fund

To file a claim against the Kentucky Student Protection Fund, each person filing must submit a signed and completed Form for Claims Against the Student Protection Fund, Form PE-38 and provide the requested information to the following address:

Kentucky Commission on Proprietary Education, 500 Mero Street, 4th Floor, Frankfort, Kentucky 40601
Forms may be located at http://www.kcpe.ky.gov/

Complaint Policy per School

Students must address their concerns about this School or any of its educational programs by following the grievance process outlined in the School's catalog. Schools are responsible for ensuring and documenting that all students have received a copy of the School's grievance procedures and for describing these procedures in the School's published catalog. If, as a student, you were not provided with this information, please inform School management. Students dissatisfied with this School's response to their complaint or who are not able to file a complaint with the School, can file a formal complaint with the Kentucky Commission on Proprietary Education, as well as other relevant agencies or accreditors, as applicable.

Filing a Complaint with the Kentucky Commission on Proprietary Education

To file a complaint with the Kentucky Commission on Proprietary Education, a complain shall be in writing and shall be filed on Form PE-24, Form to File a Complaint, accompanied, if applicable, by Form PE-25, Authorization for Release of Student Records. The form must be mailed to the following address:

Kentucky Commission on Proprietary Education, 500 Mero Street, 4th Floor, Frankfort, Kentucky 40601
Forms may be located at http://www.kcpe.ky.gov/

True and Correct Statement

This document is certified as true and correct in content and policy.

_____

Todd Thibodeaux, Chief Executive Officer
6/15/2023

Addendum 4

Utah Requirements

Disclaimers

a) REGISTERED UNDER THE UTAH POSTSECONDARY PROPRIETARY SCHOOL ACT (Title 13, Chapter 34, Utah Code).
b) Registration under the Utah Postsecondary Proprietary School Act does not mean that the State of Utah supervises, recommends, nor accredits the institution. It is the student's responsibility to determine whether credits, degrees, or certificates from the institution will transfer to other institutions or meet employers' training requirements. This may be done by calling the prospective school or employer.
c) The institution is not accredited by a regional or national accrediting agency recognized by the United States Department of Education.

Addendum 5

Oklahoma Requirements

Grievance Information

Students who are residents of Oklahoma and have a grievance against CompTIA Tech Career Academy are encouraged to follow the instructions provided in the institutional Grievance Policy. In the event that the student is not satisfied with the results of the deposition of their grievance, students can contact the Oklahoma Board of Private Vocational Schools. OBPVS's contact information is listed below.

3700 N. Classen Blvd., Ste. 250, Oklahoma City, OK 73118
Phone: (405) 528-3370

Addendum 6

Minnesota Requirements

Required Disclosure Statement

CompTIA is licensed as a private career school with the Minnesota Office of Higher Education pursuant to Minnesota Statutes, sections 136A.821 to 136A.832. Licensure is not an endorsement of the institution. Credits earned at the institution may not transfer to all other institutions.

Grievance Procedure

If the complaint cannot be resolved after exhausting the institution's grievance procedure, the student may file a complaint with the Minnesota Office of Higher Education. Additional information regarding the complaint process can be obtained by contacting the Board at:

Minnesota Office of Higher Education
1450 Energy Park Drive, Ste. 350
St. Paul, MN 55108
https://www.ohe.state.mn.us

Addendum 7

California Requirements

Required Disclosure Statements

CompTIA is licensed as a private institution that is approved to operate by the bureau. Approval to operate means compliance with state standards as set forth in the CEC and 5, CCR.

As a prospective student, you are encouraged to review this catalog prior to signing an enrollment agreement. You are also encouraged to review the School Performance Fact Sheet, which must be provided to you prior to signing an enrollment agreement.

Any questions a student may have regarding this catalog that have not been satisfactorily answered by the institution may be directed to:

The Bureau for Private Postsecondary Education
1747 N. Market Blvd. Ste 224
Sacramento, CA 95834
www.bppe.ca.gov
Telephone and Fax: (888) 370-7589 or by fax (916) 263-1897
(916) 574-8900 or by fax (916) 263-1897

A student or any member of the public may file a complaint about this institution with the Bureau for Private Postsecondary Education by calling (888) 350-7589 or by completing a complaint form, which can be obtained on the bureau's internet website (www.bppe.ca.gov)

Other California Disclosures

1. CompTIA has no pending petition in bankruptcy, is not operating as debtor in possession, has not filed a petition within the preceding five years, and has not had a petition in bankruptcy filed against it within the preceding five years that resulted in reorganization under Chapter 11 of the United States Bankruptcy Code (11 U.S.C. Sec. 1101 et seq.).
2. As a prospective student, you are encouraged to review this catalog prior to signing an enrollment agreement. You are also encouraged to review the School Performance Sheet, which must be provided to you prior to signing an enrollment agreement.
3. CompTIA does not offer financial assistance.

NOTICE CONCERNING TRANSFERABILITY OF CREDITS EARNED AT OUR INSTITUTION

Graduates of CompTIA's certification examination preparation programs will not be issued academic credits that can be transferred to other academic institutions. CompTIA does not accept academic credits issued by other academic institutions. Because the programs at CompTIA are designed as one-course programs, the transferability of credits cannot be considered.

California Resident Student Tuition Recovery Fund Disclosure

a. A qualifying institution shall include the following statement on both its enrollment agreement and school catalog:

> The State of California established the Student Tuition Recovery Fund (STRF) to relieve or mitigate economic loss suffered by a student in an educational program at a qualifying institution, who is or was a California resident while enrolled, or was enrolled in a residency program, if the student enrolled in the institution, prepaid tuition, and suffered an economic loss. Unless relieved of the obligation to do so, you must pay the state-imposed assessment for the STRF, or it must be paid on your behalf, if you are a student in an educational program, who is a California resident, or are enrolled in a residency program, and prepay all or part of your tuition.

You are not eligible for protection from the STRF and you are not required to pay the STRF assessment, if you are not a California resident, or are not enrolled in a residency program."

b. In addition to the statement required under subdivision (a) of this section, a qualifying institution shall include the following statement in its school catalog:

> It is important that you keep copies of your enrollment agreement, financial aid documents, receipts, or any other information that documents the amount paid to the school. Questions regarding the STRF may be directed to the Bureau for Private Postsecondary Education, 1747 North Market Blvd., Suite 225, Sacramento, California, 95834, (916) 574-8900 or (888) 370-7589.

To be eligible to STRF, you must be a California resident or enrolled in a residency program, prepaid tuition, paid or deemed to have paid the STRF assessment, and suffered an economic loss as a result of any of the following:

1. The institution, a location of the institution, or an educational program offered by the institution was closed or discontinued, and you did not choose to participate in a teach-out plan approved by the Bureau or did not complete a chosen teach-out plan approved by the Bureau.
2. You were enrolled at the institution or a location of the institution within the 120 day period before the closure of the institution of location of the institution, or were enrolled in an educational program within the 120 day period before the program was discontinued.
3. You were enrolled at an institution or a location of the institution more than 120 days before the closure of the institution or location of the institution, in an educational program offered by the institution as to which the Bureau determined there was a significant decline in the quality or value of the program more than 120 days before closure.
4. The institution has been ordered to pay a refund by the Bureau but has failed to do so.
5. The institution has failed to pay or reimburse load proceeds under a federal student loan program as required by law or has failed to pay or reimburse proceeds received by the institution in excess of tuition and other costs.
6. You have been awarded restitution, a refund, or other monetary award by an arbitrator or court, based on a violation of this chapter by an institution or representative of an institution, but have been unable to collect the award from the institution.
7. You sought legal counsel that resulted in the cancellation of one or more of your student loans and have an invoice for services rendered and evidence of the cancellation of the student loan or loans. To qualify for STRF reimbursement, the application must be received within four (4) years from the date of the action or event that made the student eligible for recovery from STRF.

A student whose loan is revived by a loan holder or debt collector after a period of noncollection may, at any time, file a written application for recovery from STRF for the debt that would have otherwise been eligible for recovery, If it has been more than four (4) years since the action or event that made the student eligible, the student must have filed a written application for recovery within the original four (4) year period, unless the period has been extended by another act of law. However, no claim can be paid to any student without a social security number or taxpayer identification number.

Addendum 8

Kansas Requirements

Grievance Procedure

If the complaint cannot be resolved after exhausting the institution's grievance procedure, the student may file a complaint with the Kansas Board of Regents. Additional information regarding the complaint process can be obtained by accessing the following website:

https://www.kansasregents.org/academic_affairs/private_out_of_state/complaint_process

CompTIA Instructor Qualifications

- **Alan Kuttner**: High School Diploma (Terryville High School)
- **Annaliza Marks**: M.S., B.S., Adult and Continuing Education, Business Administration (Marshall University)
- **Barrett Busch, B.**S., Cybersecurity and Information Assurance (Western Governors University)
- **Brian Ford:** M.S., B.S., Information Assurance, Computer Science (Norwich University)
- **Brianna Greenberg**, M.S., B.S., A.A.S, Information Technology, Networking and Computer Support (Middle Georgia State University)
- **Bryan Durrance:** M.S., B.S., Computer Science, Computer Networks and Cybersecurity (University of Maryland)
- **Crystal Pendergrass:** B.S., Business Management (Old Dominion University)
- **Daniel Davis**: B.S., Cybersecurity and Information Assurance (Western Governors University)
- **Daniel Hughes**: High School Diploma (Pickerington High School Central)
- **David Braun**: B.S., Computer Science (Parkwood University)
- **David Harczynski**: B.S. Accounting (Arizona State University)
- **David Perry**: High School Diploma (Putnam City North High School)
- **Dean Worster**, M.S., B.S., Information Systems Management, Internetworking Technologies (Walden University)
- **Eddie Horton**: Ph.D., M.Ed., B.S. Business, Network Security, and Information Management, Educational Technology, and Computer Information Systems and Information Engineering (Northcentral University)
- **Gray Church**: M.S., B.A. Software Engineering, Slavic Languages and Literature (University of St. Thomas)
- **Gregory Childers**: B.A. Sociology (University of Memphis)

- **Herbert Poland**: A.A., Applied Science (Community College of the Air Force)
- **Jagger Coffey**: M.S., Applied Engineering and Technology Management (Eastern Kentucky University)
- **Jeffrey (Billy) Book**, B.S., A.A.S., Information Technology, Information Systems (Community College of the Air Force)
- **Jeffrey Mehl**: MBA, B.S., B.S., Marketing/Operations Management, Information Technology, Business Administration (University of Arizona)
- **Jeremiah Minner**: MBA, B.S, Engineering Management (Old Dominion University)
- **Jerry Carrilo**, High School Diploma (South San Antonio High School)
- **Joe Walsh**: M.S., Information Systems (DeSales University)
- **John Sparks**: B.S. Industrial Technology (San Jose State University)
- **Jon Weiss**: M.A., B.S., B.A., Interdisciplinary Studies, Information Technology, Liberal Arts and Sciences (Western New Mexico University)
- **Jonathan Weiss**: M.S., B.A. Computer Science, Math and Computer Science (University of Pennsylvania)
- **Keith Stephens**: B.S., Cybersecurity and Information Assurance (Western Governors University)
- **Kenneth Proctor**: M.S., B.S., Cybersecurity and Information Assurance, Information Technology (Western Governors University)
- **Leonard Nichols**: M.S, B.A., Cybersecurity, Criminal Justice (American Military University)
- **Noel Broman**: Ph.D., M.S., B.S., Information Technology Management, Management Information Systems, Information Technology (Capella University)
- **Peter Barron**: B.A., Communications & Theological Studies (St. Louis University)
- **Ralph Moore**: MBA, M.S., MISM, B.S., Management and Leadership, Technical Management (Western Governors University)
- **Ryan Bingham**: M.S., B.A. Technology Management, Philosophy (Marist College)
- **Steven O'Dell**: Ph.D., MBA, M.S., B.S., B.S., Business, Forensic Science, Justice Science, Microbiology (University of the Cumberlands)
- **Tami Berner**: B.S., Cybersecurity and Information Assurance (Western Governors University)
- **Terry Deckard**: B.S., Computer Network Specialist (Bryan College)
- **Thomas Moore-Pizon**: MBA, M.S., B.A., Library and Information Sciences, Computer Science, Mathematics (University of South Florida)
- **Tony Carlson**: M.S., Network Security (American Intercontinental University)

Addendum 9

Louisiana Requirements

Required Disclosure Statement

CompTIA is licensed by the LA Board of Regents and adheres to the rules and regulations of the LA Proprietary Schools Advisory Commission.

Addendum 10

Arkansas Requirements

Student Complaint Process for Arkansas Students

If you wish to file a grievance about an institution of higher education that you have attended, please contact the office of Arkansas Division of Higher Education using the contact details below. It is recommended that you complete your institution's complaint process before submitting this form.

Arkansas Division of Higher Education
101 E. Capitol Ave., Suite 300
Little Rock, AR 72201
Tel. 501.371.2000
Website:
https://adhe.edu or https://adhe.edu/students-parents/student-grievance-form

Addendum 11

Florida Requirements

License Status and Information Request

Licensed by the Commission for Independent Education, Florida Department of Education. Additional information regarding this institution may be obtained by contacting the Commission at 325 West Gaines Street, Suite 1414, Tallahassee, FL 32399-0400, toll-free telephone number (888)224-6684.

Additional information regarding the institution, if licensed, may be obtained by contacting the Commission for Independent Education, Department of Education, 325 West Gaines Street, Suite 1414, Tallahassee, Florida 32399-0400, toll-free telephone number (888)224-6684.

Physical Facilities

Since CompTIA's training programs are delivered online, CompTIA's office space in Florida is for administrative purposes only. It is located at 401 East Jackson Street, Suite 3300, Tampa, FL 33602.

Addendum 12

Washington Requirements

Licensure Disclosure and Inquiry/Complaint Process

This school is licensed under Chapter 28C.10 RCW. Inquiries or complaints regarding this private vocational school may be made to the:

Workforce Board, 128 – 10th Ave. SW, Box 43105, Olympia, Washington 98504-3105
Web: wtb.wa.gov
Phone: 360-709-4600
E-Mail Address: pvsa@wtb.wa.gov

Transcript Disclosure

CompTIA keeps copies of all student transcripts indefinitely. Refer to page 79 of this course catalog for the procedure students must follow to request copies of their transcripts.

Student Dismissal Disclosure

WAC 490-105-042(8), “Nothing in the policy prevents the student from contacting the Workforce Board at 360-709-4600 at any time with a concern or complaint.”