aci LEARNING | CollegePro

Purpose-built for your IT and Cybersecurity Program

A program-level lab solution for institutional adoption

CollegePro is designed to align hands-on learning with how IT and cybersecurity programs are structured.

With **100+ hands-on labs,** CollegePro provides a **shared, program-wide practical layer** that faculty can integrate across multiple courses each term—ensuring every course includes the most effective form of learning: **doing.**

What makes CollegePro different

Term-aligned by design

Each lab set aligns to a full academic term, supporting core skills and outcomes

Program-wide consistency

CollegePro creates a shared, hands-on foundation across courses and sections

Flexible for faculty

Labs are not locked to individual courses—faculty can select the labs that best align to their courses.

CollegePro is a standardized layer of hands-on practice that supports all courses in the first four semesters—easy to adopt, simple to integrate, and built to scale across programs.

Make hands-on labs a core part of your program—effortlessly

CollegePro aligns hands-on practice to core IT and cybersecurity concepts commonly taught in the first four terms, creating a consistent skills framework across your program.

With CollegePro, institutions gain:

- **Stronger alignment** across courses and sections
- **Improved learning continuity** across terms—without adding to instructor workload
- **Reduced inconsistency** in student skill attainment
- **Auto-grading** and **progress monitoring** to save time and improve outcomes
- **Job-ready students** with real-world experience —before graduation

CollegePro follows a clear instructional progression:

Foundations introduce core IT and security concepts, basic configuration, and essential technical literacy.

Infrastructure builds on this foundation with system administration, networking services, virtualization, storage, and cloud fundamentals.

Core Cyber Defense shifts focus to protecting and monitoring systems through firewalls, intrusion detection, endpoint security, and incident investigation

Advanced Security & Capstone Readiness emphasizes security operations, cloud security, threat analysis, and realistic, end-to-end investigation scenarios.

CollegePro delivers consistent, scalable, job-ready learning—while supporting faculty and simplifying program operations.

Foundations

This lab set introduces learners to core IT and cybersecurity fundamentals, building a strong baseline in computer hardware, operating systems, basic networking, and security concepts. Learners gain hands-on experience with PC configuration, OS installation and maintenance, data protection, and early network fundamentals.

The term also introduces basic scripting with Python, helping student develop problem-solving skills and technical confidence. By the end of Term 1, students have the foundational knowledge and practical skills needed to progress into more advanced IT and cybersecurity coursework.

Lab Title	Lab Set
Computer Hardware and Troubleshooting	Digital Literacy
Computer Software	Digital Literacy
Operating System Types and Features – Part 1	Digital Literacy
Operating System Types and Features – Part 2	Digital Literacy
Operating System Installations and Upgrades	CompTIA A+ 1202
Operating System Types and Filesystems	CompTIA A+ 1202
Documentation and Asset Management Best Practices	CompTIA A+ 1202
Basic Networking Concepts	CompTIA Tech+
Introduction to Networking – Part 1	Digital Literacy
Introduction to Networking – Part 2	Digital Literacy
Internet Security	Digital Literacy
Security Concept Fundamentals	CompTIA Security+
Identifying Security Vulnerabilities	CompTIA Security+
Network Security Concepts	CompTIA Network+
Data Security Concepts	CompTIA Server+
IP Subnetting & Loopback Interfaces	Network Fundamentals
Examining PC Hardware	PC Maintenance & Repair
Operating System Installations and Upgrades	CompTIA A+ 1202
Disk Maintenance and Data Recovery	PC Maintenance & Repair
Linux Backup & File Compression Concepts	CompTIA Linux+
Getting Started with Python: Your First Program	Scripting Fundamentals
Getting Started with Python: Command Line Execu-	Scripting Fundamentals
Working with For Loops	Intro to Programming using Python
Working with While Loops	Intro to Programming using Python
Reading Files	Intro to Programming using Python
Handling Exceptions	Intro to Programming using Python

Infrastructure

This lab set builds on foundational knowledge to focus on core infrastructure skills, including Linux administration, networking, virtualization, storage, backup, and cloud fundamentals. Students gain hands-on experience installing and managing Linux systems, configuring network services, and supporting resilient infrastructure environments.

Also introduced are virtualization and cloud platforms helping students understand how modern infrastructure is built, managed, and scaled. By the end of Term 2, students are prepared to support on-prem, virtualized, and cloud-based infrastructure in real-world IT environments.

Lab Title	Lab Set
CentOS Server Linux Installation	Linux Fundamentals
Ubuntu Desktop Linux Installation	Linux Fundamentals
Installing Packages & Shared Libraries on Linux	Linux Fundamentals
Configuring X Windows	Linux Server II System Admin
Linux Backup & File Compression Concepts	CompTIA Linux+
Disaster Recovery Concepts – Load Balancing	CompTIA Network+
Implementing Secure DHCP and DNS	Network Security Fundamentals
Server Operating Systems Installation Methods	CompTIA Server+
Server Virtualization Concept	CompTIA Server+
Introduction to Virtualization and Cloud Technologies	CompTIA Tech+
Server Virtualization Concepts	CompTIA Server+
Configuring and Verifying VLANs	Cisco Networking Devices
Configure and Verify Device Management	Virtualization
Detecting Virtualization	Virtualization
Manage Window Services	Windows Server Admin Fundamentals
Manage Backup & Restore	Windows Server
Storage Management Concepts	CompTIA Linux+
Managing Linux Shared Storage	CompTIA Linux+
Cloud Storage Concepts	CompTIA Cloud +
AWS Global Infrastructure Overview	AWS Cloud Practitioner
AWS Storage Services	AWS Cloud Practitioner
AWS Networking Services	AWS Cloud Practitioner
Working with Primitive Data Types	Intro to Programming Using Python
Working with If Statements	Intro to Programming Using Python
Reading Command Line Arguments	Intro to Programming Using Python

Core Cyber Defense

This lab set focuses on core defensive cybersecurity skills, covering how organizations protect systems, detect threats, and investigate incidents.

Student gain hands-on experience with network and host-based security, endpoint protection, secure configuration, and scripting, while building awareness of common attack techniques.

These labs also introduce digital forensics and log analysis, helping students understand how security teams investigate and respond to real-world events. By the end of Term 3, students are applying practical defense skills that align with real security operations and cyber defense roles.

Lab Title	Lab Set
Config. a Windows-Based Firewall to Allow Incoming Traffic	Net. Sec. Fundamentals
Configuring a Linux-Based Firewall to Allow Incoming and Outgoing Traffic	Network Security Fundamentals
Implementing Secure DHCP and DNS	Network Security Fundamentals
Intrusion Detection Using Snort	Network Security Fundamentals
Host-Based Firewalls	Network Security Fundamentals
Configuring RADIUS	Network Security Fundamentals
Configuring a Virtual Private Network with PPTP	Network Security Fundamentals
Configuring a Virtual Private Network with OpenVPN	Network Security Fundamentals
Closing Security Hole	Network Security Fundamentals
Configuring Endpoint Security	Cybersecurity Fundamentals
Administering and Deploying Endpoint Protection	Security Fundamentals
Understand Password Policies	Security Fundamentals
Understand Audit Policies	Security Fundamentals
HTML Injection (HTMLi)	PenTesting
HTML Injection Vulnerability and Mitigation	PenTesting
IDS, Syslog, and NTP	PenTesting
Incident Response Procedures and Forensic Analysis	PenTesting
Network Security-Firewalls	MS Azure
Analyzing Output from Network Security Monitoring Tools	MS Azure
Config. Access Control Lists on Linux-Based Firewalls	Network Security Fundamentals
Writing Custom Rules	Network Security Fundamentals
SIEM Configuration and Attack Analysis	SOC Analyst
Tracking the Threat Landscape	SOC Analyst
Vulnerability Management: Scan, Prioritize, Remediate	SOC Analyst
Analyst Use Case Walkthrough	LogRhythm – Analyst Fundamentals

Advanced Security & Capstone Readiness

This lab set focuses on advanced security operations, cloud security, and applied investigation, preparing students for SOC roles and real-world incident response environments.

Students gain hands-on experience securing and monitoring enterprise networks and cloud platforms, configuring VPNs, closing security gaps, and applying security controls across AWS and cloud environments.

The term emphasizes security monitoring, threat detection, and investigation, with labs covering SIEM configuration, threat landscape analysis, vulnerability management, and analyst-led use case investigations. Students also perform advanced forensic analysis, malware investigation, and attack recreation, culminating in capstone-style challenges that simulate real security incidents.

Lab Title	Lab Set
Configuring a Virtual Private Network with PPTP	Network Security Fundamentals
Configuring a Virtual Private Network with OpenVPN	Network Security Fundamentals
Configuring Site-to-Branch VPNs	Network Security Fundamentals
Closing Network Security Holes	Network Security Fundamentals
Cloud Security Monitoring Techniques	CompTIA Cloud+
Implementing Cloud Security Controls	CompTIA Cloud+
AWS Security & Compliance Concepts	AWS Cloud Practitioner
AWS Security Services	AWS Cloud Practitioner
AWS Deployment Methods	AWS Cloud Practitioner
AWS Virtual Networking Components	AWS Fundamentals
AWS Computing Services	AWS Could Practitioner
Cloud Security Monitoring Techniques	CompTIA Cloud+
SIEM Configuration and Attack Analysis	SOC Analyst
Tracking the Threat Landscape	SOC Analyst
Vulnerability Management: Scan, Prioritize, Remediate	SOC Analyst
Analyst Use Case Walkthrough	LogRhythm – Analyst Fundamentals
Complete Use Case Investigation	LogRhythm – Analyst Fundamentals
Ransomware Injection Detection and Analysis	LogRhythm – Analyst Fundamentals
Botnet Detection and Threat Identification	LogRhythm – Analyst Fundamentals
Acceptable Use Policy Compliance Monitoring	LogRhythm – Analyst Fundamentals
Digital Forensics Analysis and Validation	Computer Forensics & Investigations
Memory Analysis	Digital Forensics
Host-Based Forensics Challenge	Cyber Challenge Range
Malware Analysis in Windows	Cyber Challenge Range
Recreating an Attack	Cyber Challenge Range

aci LEARNING | CollegePro

Make it your own

Every institution serves a unique student population and regional workforce. CollegePro can be customized to tailor term-aligned lab sets to emphasize the skills and competencies that matter most—while maintaining a common foundation across the program.

CollegePro balances program-level standardization with the flexibility institutions need to support diverse programs, faculty approaches, and student populations.

Labs for every core course

CollegePro is built on a robust library of hands-on labs and complete lab sets designed to align directly to high-frequency, high-impact courses.

Institutions can confidently standardize on a single lab partner, knowing there is coverage for every core skill across IT, cybersecurity, and data foundations.