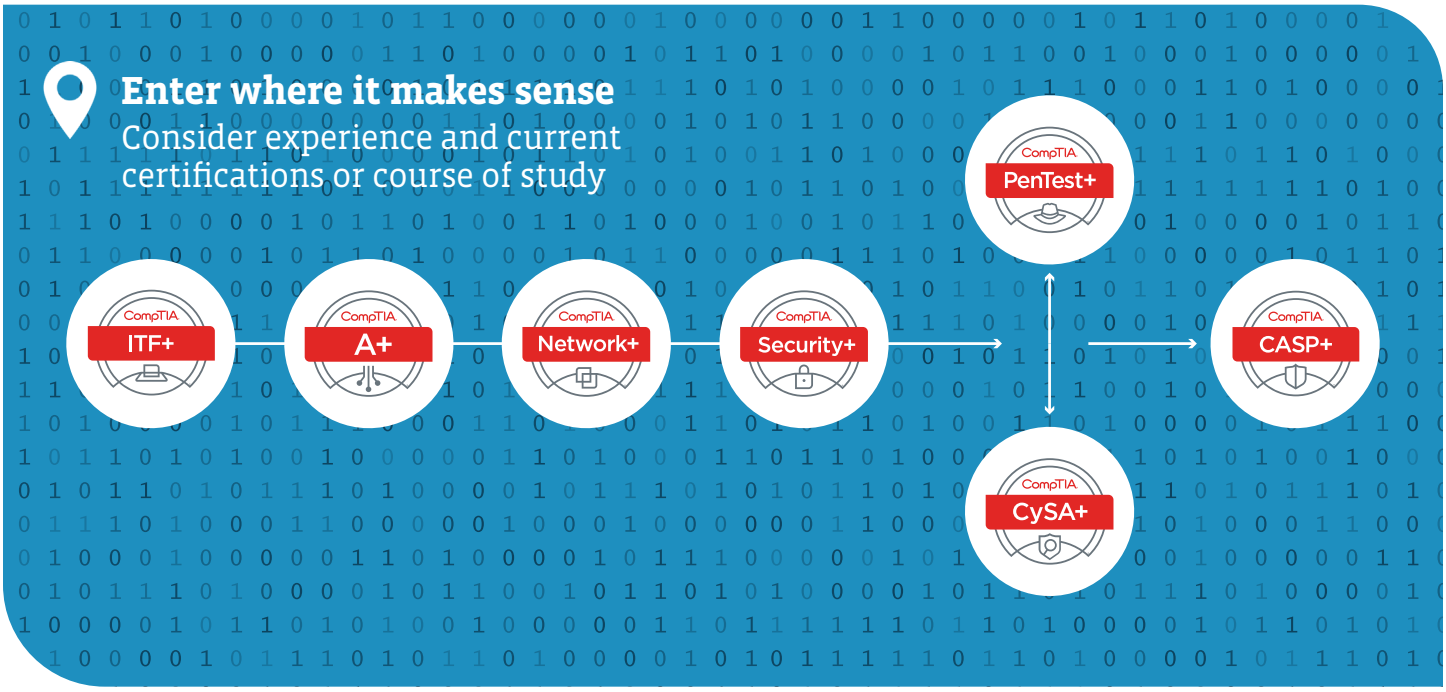
CompTIA

#secureIT

Introducing the CompTIA Cybersecurity Career Pathway

A vendor-neutral pathway for IT professionals to achieve cybersecurity mastery, from beginning to end



CompTIA IT Fundamentals is the beginning of the career pathway. It is for beginners who don't have **CompTIA A+** or six months of IT pro experience.

CompTIA A+ certification, which mirrors the skills of an IT pro with six months of experience, assesses the skills necessary to support IT infrastructures. An understanding of the most common hardware and software technologies used on the network is needed before earning **CompTIA Network+.**

CompTIA Network+, or the equivalent knowledge of nine months of networking experience, is an important recommended prerequisite to **CompTIA Security+.** IT pros must understand how the network functions before they can secure it; therefore, they need networking skills first.

CompTIA Security+ covers network security, compliance and operation security, threats and vulnerabilities, risk management, plus application, data and host security. It mirrors two years of IT security experience, thus precedes **CompTIA PenTest+** or **CompTIA CySA+** which mirrors three to four years.

CompTIA PenTest is our newest certification and joins CySA+ at the intermediate-skills level. PenTest+ focuses on offense through penetration testing and vulnerability assessment. Depending on your course of study, PenTest+ and CySA+ can be taken in any order, but typically fills the gap between Security+ and CASP+.

CompTIA Cybersecurity Analyst (CySA+) focuses on defense and assesses the skills needed to apply behavioral analytics to the IT security environment. It fills the skills gap between Security+ and CASP+.

CompTIA Advanced Security Practitioner (CASP+) should be pursued by IT pros after **PenTest+** or **CySA+** to prove their mastery of hands on cybersecurity skills required at the 5- to 10-year experience level.

THE CompTIA CYBERSECURITY CAREER PATHWAY

IT pros can enter the CompTIA Cybersecurity Pathway at any point, depending on their IT experience, existing certifications, course of study, job needs, interests and the specific skills they are looking for. For example, if you have two years of IT security experience or equivalent knowledge, you can jump into the pathway at CompTIA Security+ to prove your knowledge. If you already have CompTIA Security+, you can go right into PenTest+ or CySA+. In general, the pathway follows a hierarchy of skills needed for IT security; each certification builds upon the skills from the previous one.

There are no required prerequisites for these CompTIA certifications, and they can be taken without IT experience. CompTIA certifications mirror the current job roles of IT professionals, so it makes sense to earn these certifications to gain the knowledge and hands-on skills currently being used in the workforce, whether you have job experience or not.

If you are an IT professional or an employer, you understand the value of on-the-job experience. IT certifications are a great place to start, but they are not a replacement. If you have CompTIA certifications and on-the-job experience, you have the best of both worlds.

CompTIA CYBERSECURITY CERTIFICATION PORTFOLIO

CERTIFICATION	COMPETENCIES	JOB ROLES
CompTIA ITF+	• Install software • Establish basic network connectivity • Identify/prevent basic security risks • Explain troubleshooting theory and preventative maintenance of devices	• Sales Associate • Account Manager • Marketing Specialist • Customer Support
CompTIA A+	• Identify cybersecurity threats • Confgure operating system security • Understand security best practices • Troubleshoot common security issues	• Technical Support Specialist • Field Service Technician • IT Support Technician • IT Administrator
CompTIA Network+	• Understand networking services and applications • Use appropriate network monitoring tools • Understand network security vulnerabilities and remedies	• Network Field Technician • Network Administrator • IS Consultant • Network Field Engineer
CompTIA Security+	• Understand network security • Identify and mitigate security threats • Understand application, data and host security issues • Implement access control and identity management	• Security Specialist • Security Consultant • Security Engineer • Security Administrator
CompTIA PenTest+	• Plan and scope an assessment • Understand legal and compliance requirements • Perform vulnerability scanning and penetration testing • Analyze data and effectively report and communicate results.	• Penetration Tester • Vulnerability Tester • Security Analyst (II) • Vulnerability Assessment Analyst
CompTIA CySA+	• Configure and use threat detection tools • Perform data analysis • Interpret results to identify vulnerabilities, threats and risk to an organization	• Security Analyst • Vulnerability Analyst • Cybersecurity Specialist • Security Engineer
CompTIA CASP+	• Conceptualize, engineer, integrate and implement secure solutions across complex environments • Translate business needs into security requirements, analyze risk impact and respond to security incidents	• Cybersecurity/IS Professional • Information Security Analyst • Security Architect • IT Specialist INFOSEC

CompTIA

Learn more at **Certification.CompTIA.org**

© 2018 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC, in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC, or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 06038-Dec2018