CompTIA®

Cybersecurity: A vital element of every IT job

Information security is a major concern of every organization around the world. With the continually rising threat of cyber attacks, organizations of all sizes seek ways to ensure the security of their systems.

Having knowledgeable and skilled IT staff is a vital element to building and maintaining secure systems.

CompTIA certifications help ensure your IT staff has the validated skills necessary to protect your organization.

While rising in popularity, CompTIA Security+ isn't the only CompTIA certification that covers this essential IT need.

Cybersecurity knowledge and skills are key components embedded throughout the wide range of CompTIA certifications.

% OF OBJECTIVES COVERING SECURITY	
CompTIA Security+	100%
CompTIA Cybersecurity Analyst+	100%
CompTIA CASP	100%
CompTIA IT Fundamentals	30%
CompTIA A+	28%
CompTIA Network+	37%
CompTIA Mobility+	36%
CompTIA Server+	33%
CompTIA Cloud+	20%

In 2015, large U.S. organizations had an average total cyber-security cost of **$15 million.**

Average time to contain a cyber attack is **46 days**.

Companies that invest in adequate resources and employ certified staff save **$1.5 million annually** in cyber crime costs.

Every IT professional, regardless of their job role, needs to be at the top of their game when it comes to cybersecurity.

For more information about the security domains covered in CompTIA certifications, visit: Certification.CompTIA.org

CompTIA CYBERSECURITY CERTIFICATION PORTFOLIO

The following CompTIA vendor-neutral certifications ensure your IT staff has the validated skills necessary to protect your organization.

CERTIFICATION	RELEVANCE TO CYBERSECURITY	COMPETENCIES
CompTIA IT Fundamentals	CompTIA IT Fundamentals introduces individuals to the exciting world of Information Technology. The certification covers the essential IT skills and knowledge needed by entry-level IT professionals.	• Identify common programs and their purpose • Understand basic security threats • Use security best practices • Use web-browsing best practices
CompTIA A+	All cyber investigations, forensics, and cyber law enforcement activities rely on a fundamental understanding of computer hardware, networks, and systems. CompTIA A+ certification validates that fundamental understanding and skills.	• Identify cybersecurity threats • Configure operating system security • Understand security best practices • Troubleshoot common security issues
CompTIA Network+	In our increasingly interconnected world, secure digital networks are essential. CompTIA Network+ certification prepares IT professionals to build, manage, and protect the critical asset that is the data network.	• Understand networking services and applications • Use appropriate network monitoring tools • Understand network security vulnerabilities and remedies
CompTIA Security+	CompTIA Security+ certification is 100% focused on Cybersecurity. It covers the foundational principles for network and operation security, threats and vulnerabilities, access control and identity management and cryptography.	• Understand network security • Identify and mitigate security threats • Understand application, data, and host security issues • Implement access control and identity management
CompTIA Cybersecurity Analyst+	CompTIA Cybersecurity Analyst+ applies behavioral analytics to the IT security market to improve the overall state of IT security. Analytics have been successfully integrated in the business intelligence, retail and financial services industries for decades. Analytics are now applied to IT security to detect and mitigate threats.	• Configure and use threat detection tools • Perform data analysis • Interpret results to identify vulnerabilities, threats and risk to an organization.
CompTIA CASP	The CompTIA Advanced Security Practitioner certification is the first mastery level certification exam by CompTIA. It validates abilities in enterprise security such as requirements, risk management, incident response, and critical thinking.	• Conceptualize, engineer, integrate and implement secure solutions across complex environments • Translate business needs into security requirements, analyze risk impact, and respond to security incidents
CompTIA Mobility+	The CompTIA Mobility+ certification covers the knowledge and skills required to understand mobile device management, capabilities of various mobile devices, and security aspects of wireless mobile devices.	• Implement mobile device operations • Identify encryption methods for securing mobile environments • Explain risks, threats and mitigation strategies of mobile ecosystems
CompTIA Server+	The CompTIA Server+ certification exam covers server hardware, software, storage, disaster recovery and troubleshooting. One third of the Server+ exam content is Cybersecurity related.	• Install and configure server operating systems • Understand physical security methods and concepts • Implement data security methods and secure storage disposal techniques
CompTIA Cloud+	The CompTIA Cloud+ certification validates the knowledge and best practices required of IT practitioners working in cloud computing environments, who must understand and deliver cloud infrastructure and security.	• Understand various cloud delivery models and services • Understand network and storage security concepts, tools, and best practices • Understand various encryption

For a complete list of CompTIA certification exam objectives, visit: Certification.CompTIA.org