Cybersecurity Career Pathway Recommendation

Enter where it makes sense for you. Consider your experience and existing certifications or course of study.
<table>
<thead>
<tr>
<th>CERTIFICATION</th>
<th>RELEVANCE TO CYBERSECURITY</th>
<th>COMPETENCIES</th>
<th>JOB ROLES</th>
</tr>
</thead>
</table>
| 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 | • Sales Associate  
• Account Manager  
• Marketing Specialist  
• Customer Support |
| CompTIA A+ | All cyber investigations, forensics, and cyber law enforcement activities rely on a fundamental understanding of computer hardware, networks, and systems. CompTIA A+ proves you have the foundational IT knowledge and skills necessary to succeed. | • Identify cybersecurity threats  
• Configure operating system security  
• Understand security best practices  
• Troubleshoot common security issues | • Technical Support Specialist  
• Field Service Technician  
• IT Support Technician  
• IT Administrator |
| 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 | • Network Field Technician  
• Network Administrator  
• IS Consultant  
• Network Field Engineer |
| CompTIA Security+ | Certification is 100% focused on cybersecurity. The exam covers foundational principles for network and operation security, threats and vulnerabilities, access control and identity management and cryptography. More choose Security+ for DoD 8570 compliance than any other certification. | • 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 CSA+ | Seamlessly following Security+, CompTIA Cybersecurity Analyst (CSA+) applies behavioral analytics to greatly improve network threat visibility. As attackers have learned to evade traditional signature-based solutions, an analytics-driven cyber defense has become critical. | • 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 | CompTIA Advanced Security Practitioner (CASP) validates enterprise security abilities in requirements, risk management, incident response and critical thinking. CompTIA's first mastery level certification, CASP is the hands-on, performance-based, technical counterpart to the CISSP. | • 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 |

LEARN MORE:
CompTIA Cybersecurity Pathway
GovernmentSales@CompTIA.org
Certification.CompTIA.org