What is it?

CompTIA Advanced Security Practitioner (CASP+) is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise’s cybersecurity readiness.

Why is it different?

• **CASP+ is the only hands-on, performance-based certification for advanced practitioners** — not managers — at the advanced skill level of cybersecurity. While cybersecurity managers help identify what cybersecurity policies and frameworks could be implemented, CASP+ certified professionals figure out how to implement solutions within those policies and frameworks.

• **Unlike other certifications, CASP+ covers both security architecture and engineering** — CASP+ is the only certification on the market that qualifies technical leaders to assess cyber readiness within an enterprise, and design and implement the proper solutions to ensure the organization is ready for the next attack.

About the exam

CASP+ is an advanced-level cybersecurity certification covering technical skills in security architecture and senior security engineering in traditional, cloud, and hybrid environments, governance, risk, and compliance skills, assessing an enterprise’s cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions. Successful candidates will have the knowledge required to:

• Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise

• Use monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environment

• Apply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniques

• Consider the impact of governance, risk, and compliance requirements throughout the enterprise

---

### Exam Details

- **Exam #**: CAS-004
- **Release Date**: August 2021
- **Languages**: English
- **CE Required?**: Yes
- **Accreditation**: Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.
What's in this version?

Information security threats are on the rise globally. Organizations are increasingly concerned over the lack of adequately trained senior IT security staff’s ability to effectively lead and manage the overall cybersecurity resiliency against the next attack. Updates to CASP+ qualify advanced skills required of security architects and senior security engineers to effectively design, implement, and manage cybersecurity solutions on complex enterprise networks.

- **Security Architecture** – Expanded coverage to analyze security requirements in hybrid networks to work toward an enterprise-wide, zero trust security architecture with advanced secure cloud and virtualization solutions.

- **Security Operations** - Expanded emphasis on newer techniques addressing advanced threat management, vulnerability management, risk mitigation, incident response tactics, and digital forensics analysis.

- **Security Engineering and Cryptography** – Expanded to focus on advanced cybersecurity configurations for endpoint security controls, enterprise mobility, cloud/hybrid environments, and enterprise-wide PKI and cryptographic solutions.

- **Governance, Risk, and Compliance** - Expanded to support advanced techniques to prove an organization’s overall cybersecurity resiliency metric and compliance to regulations, such as CMMC, PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

How does CASP+ Compare to Alternatives?

<table>
<thead>
<tr>
<th>Certification</th>
<th>(ISC)² Certified Information Systems Security Professional (CISSP)</th>
<th>GIAC Certified Enterprise Defender (GCED)</th>
<th>ISACA Certified Information Security Manager (CISM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance-based Questions</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Exam Length</td>
<td>90 questions, 165 minutes</td>
<td>100-150 questions, 3 hours</td>
<td>115 questions, 3 hours</td>
</tr>
<tr>
<td>Experience Level</td>
<td>Advanced</td>
<td>Advanced</td>
<td>Advanced</td>
</tr>
<tr>
<td>Exam Focus</td>
<td>Cybersecurity Practitioner Skills, Architect &amp; Engineer</td>
<td>Cybersecurity Management Skills</td>
<td>Cybersecurity Practitioner Skills, Engineer</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>Recommend 10 years of IT administration, including 5 years hands-on, technical security experience.</td>
<td>Documented proof of minimum 5 years full-time IT work experience in two or more of the eight domains.</td>
<td>None. However, students should be aware of the technical level required for the certification.</td>
</tr>
<tr>
<td>Price</td>
<td>$466</td>
<td>$699</td>
<td>$1999 (requires the training bundle)</td>
</tr>
</tbody>
</table>

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage cybersecurity. Enter where appropriate for you. Consider your experience and existing certifications or course of study.

Top CASP+ Job Roles

- Security Architect
- Senior Security Engineer
- SOC Manager
- Security Analyst
- IT Cybersecurity Specialist/INFOSEC Specialist
- Cyber Risk Analyst
### Technical Areas Covered in the Certification

<table>
<thead>
<tr>
<th>Security Architecture</th>
<th>Security Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>25%</strong></td>
<td><strong>30%</strong></td>
</tr>
<tr>
<td>• Analyze security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network and to provide the appropriate authentication and authorization controls</td>
<td>• Given a scenario, perform threat management and vulnerability management activities and analyze those vulnerabilities to recommend risk mitigations</td>
</tr>
<tr>
<td>• Analyze organizational requirements to determine the proper infrastructure security design</td>
<td>• Use appropriate vulnerability assessment and penetration testing methods and tools</td>
</tr>
<tr>
<td>• Integrate software applications securely into an enterprise architecture</td>
<td>• Analyze indicators of compromise and formulate an appropriate response</td>
</tr>
<tr>
<td>• Implement data security techniques for securing enterprise architecture and implement secure cloud and virtualization solutions</td>
<td>• Given a scenario, use processes to reduce risk</td>
</tr>
<tr>
<td>• Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements</td>
<td>• Given an incident, implement the appropriate response</td>
</tr>
<tr>
<td></td>
<td>• Explain the importance of forensic concepts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Engineering and Cryptography</th>
<th>Governance, Risk and Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>26%</strong></td>
<td><strong>15%</strong></td>
</tr>
<tr>
<td>• Given a scenario, apply secure configurations to enterprise mobility or configure and implement endpoint security controls</td>
<td>• Given a set of requirements, apply appropriate risk strategies</td>
</tr>
<tr>
<td>• Explain security considerations impacting specific sectors and operational technologies</td>
<td>• Explain the importance of managing and mitigating vendor risk</td>
</tr>
<tr>
<td>• Explain how cloud technology adoption impacts organizational security</td>
<td>• Understand compliance frameworks and legal considerations, and their organizational impact</td>
</tr>
<tr>
<td>• Given a business requirement, implement appropriate PKI solution or implement appropriate cryptographic protocols and algorithms</td>
<td>• Explain the importance of business continuity and disaster recovery concepts</td>
</tr>
<tr>
<td>• Given a scenario, troubleshoot issues with cryptographic implementations</td>
<td></td>
</tr>
</tbody>
</table>
Organizations that have contributed to the development of CASP+

• AT&T Cybersecurity
• Lockheed Martin
• Exxon Mobil
• Archdiocese of Philadelphia
• RxSense
• SecureWorks
• U.S. Dept. of State
• U.S. Army

• U.S. Marine Corps
• U.S. Navy Center for Information Dominance
• East Tennessee State University
• Target Corp.
• General Dynamics IT (GDIT)
• Ricoh
• Splunk
• John Hopkins University Applied Physics Laboratory

Research and Statistics

Fastest-Growing Job Category

Growing Value

The U.S. Bureau of Labor Statistics predicts that advanced-level cybersecurity jobs will be among the fastest-growing job categories, with 5 percent overall growth between 2019 and 2029.¹ CASP+ is named as one of the top 10 certifications paying the highest premiums, earning IT professionals a 14 percent increase above base salary.²

Learn with CompTIA

Official CompTIA Content is the only study material exclusively developed by CompTIA for the CompTIA certification candidate; no other content library covers all exam objectives for all certifications. CompTIA learning products have been developed with our Official CompTIA Content to help you prepare for your CompTIA certification exams with confidence. Learners now have everything they need to learn the material and ensure they are prepared for the exam and their career.

Whether you are just starting to prepare and need comprehensive training with CertMaster Learn, want to apply your knowledge hands-on with CompTIA Labs, need a final review with CertMaster Practice, or need to renew your certification upon expiration with CertMaster CE, CompTIA’s online training tools have you covered.

What does it mean to be a “vendor-neutral” exam?

An extraordinarily high level of rigor is employed in developing CompTIA certifications. Each question created for a CompTIA exam undergoes multiple layers of quality assurance and thorough psychometric statistical validation, ensuring CompTIA exams are highly representative of knowledge, skills and abilities required of real job roles. This is why CompTIA certifications are a requirement for many professionals working in technology. Hiring managers and candidates alike can be confident that passing a CompTIA certification exam means competence on the job. This is also how CompTIA certifications earn the ANSI/ISO 17024 accreditation, the standard for personnel certification programs. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

What does it mean to be a “high stakes” exam?

An extraordinarily high level of rigor is employed in developing CompTIA certifications. Each question created for a CompTIA exam undergoes multiple layers of quality assurance and thorough psychometric statistical validation, ensuring CompTIA exams are highly representative of knowledge, skills and abilities required of real job roles. This is why CompTIA certifications are a requirement for many professionals working in technology. Hiring managers and candidates alike can be confident that passing a CompTIA certification exam means competence on the job. This is also how CompTIA certifications earn the ANSI/ISO 17024 accreditation, the standard for personnel certification programs. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

What is a Performance Certification?

CompTIA performance certifications validate the skills associated with a particular job or responsibility. They include simulations that require the test taker to demonstrate multi-step knowledge to complete a task. CompTIA has a higher ratio of these types of questions than any other IT certifying body.

2. Foote Partners, 10 IT certs paying the highest premiums today, 2020

© 2021 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA, Inc. CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners. Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. Printed in the U.S.

08447-Feb2021