Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CASP+ - CompTIA Advanced Security Practitioner

As of December, 2024 the CASP+ certification has been rebranded as SecurityX. Please find our SecurityX course page here.

Course Description

SecureNinja's CompTIA Advanced Security Practitioner (CASP+) training and certification boot camp in Washington, DC and San Diego, CA is like no other CASP+ accelerated immersion class available in the market today.

SecureNinja's Secure Ninja Team are widely known as the world's leading instructors for CompTIA exam preparation from whom you will not only receive the knowledge to pass the exam but come back to the job with real-world skills you can apply right away maximizing your training investment. You will benefit from their extensive knowledge base as they teach you proprietary tips and tricks for exam passing success.

The CompTIA Advanced Security Practitioner (CASP+) Certification is a vendor-neutral credential. The CASP+ exam is an internationally targeted validation of advanced-level security skills and knowledge. While there is no required prerequisite, the CASP+ certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus at the enterprise level.

The CASP+ exam will certify that the successful candidate has the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments. The candidate will apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies, translate business needs into security requirements, analyzes risk impact and respond to security incidents.

The CompTIA CASP+ exam is accredited by ANSI and shows compliance with the ISO 17024 standard. The exam also undergoes reviews and updates to exam objectives.

Topics Covered

- Enterprise Security
- Governance, Risk and Compliance (GRC)
- Research and Analysis and Assessment
- Integration of Computing, Communications and Business Disciplines
- Technical Integration of Enterprise Components

Successful Candidates Will

- Demonstrate competency in enterprise security, compliance standards, research and analysis and integration of computing, communications, and business disciplines.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Demonstrate proven knowledge of security concepts, tools, automation, and procedures to proactively guard against security threats at the enterprise level.
- Apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

Who Would Benefit

IT security professionals with a minimum of 10 years' experience in IT administration and at least 5 years of hands-on technical security experience.

- Information Systems Security
- Engineer
- Network Security Engineer
- Security Architect
- Security Consultant
- Security Assessor
- Security Manager or Information
- Assurance Manager (IAM)
- Security Analyst
- Information Systems Security
- Officer/Information Assurance
- Security Officer (ISSO/IASO)

Pre-Requisites

There are no required pre-requisites to attend; however, the CASP+ certification is intended to follow courses such as CompTIA Security+ or equivalent work experience in a technical field.

Course Outline

1. **Foundational Understanding:**

- Grasp core incident handling principles within information systems.
- Identify and analyze emerging computer security threats.
- Understand the incident response workflow and processes.

2. **Incident Classification and Response:**

- Classify and respond effectively to various security incidents like network threats, malicious code, and insider attacks.
- Develop strategies to mitigate and manage different incident types.
- Understand time and cost metrics and difficulties to resolve incidents.
- See examples of modern attacks and current approaches done to respond.

3. **Risk Assessment and Compliance:**

- Utilize risk assessment methodologies specific to incident handling.
- Understand the impact of laws, regulations, and policies on incident response.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

4. **Policy Development and Implementation:**

- Formulate and implement incident-handling policies based on industry standards.
- Ensure alignment and integration of policies within organizational frameworks.

5. **Team Roles, Reporting, and Recovery:**

- Define roles within incident response teams and establish effective reporting methods.
- Apply recovery techniques to restore systems and ensure business continuity post-incidents.

6. **Practical Proficiency:**

- Apply learned skills in simulated incident handling scenarios.
- Demonstrate proficiency in managing security incidents practically.

7. **Ethical Conduct:**

- Uphold ethical standards throughout incident handling procedures.
- Address ethical dilemmas that may arise during incident response.

Exams Details

- Number of Questions: Maximum of 90
- Question Types: Multiple-choice and performance-based
- Duration: 165 minutes
- Passing Score: Pass/fail only; no scaled score

Class Length

- 5 Days
- 40 Hours

Follow-on Courses

- CEH (Certified Ethical Hacker)
- CHFI (Certified Hacking Forensics Investigator)
- CISSP (Certified Information Systems Security Professional)