Szkolenie: CompTIA
CompTIA CASP+ Prep Course

CompTIA Authorized Partner DELIVERY PARTNER

DOSTĘPNE TERMINY

2022-08-29 | 5 dni | Kraków / Wirtualna sala
2022-08-29 | 5 dni | Warszawa / Virtual Classroom
2022-09-26 | 5 dni | Kraków / Virtual Classroom
2022-09-26 | 5 dni | Warszawa / Wirtualna sala

Cel szkolenia:

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

CASP+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program.

Each participant in an authorized training CompTIA CASP+ Prep Course held in Compendium CE will receive a free CAS-004 CompTIA CASP+ Certification Exam vouchers.

Who Should Attend

- Security Architect
- Senior Security Engineer
- SOC Manager
- Security Analyst

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Plan szkolenia:

- Security Architecture
  - Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network
  - Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design
  - Given a scenario, integrate software applications securely into an enterprise architecture
  - Given a scenario, implement data security techniques for securing enterprise architecture
  - Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls
  - Given a set of requirements, implement secure cloud and virtualization solutions
  - Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements
  - Explain the impact of emerging technologies on enterprise security and privacy
- Security Operations
  - Given a scenario, perform threat management activities
  - Given a scenario, analyze indicators of compromise and formulate an appropriate response
  - Given a scenario, perform vulnerability management activities
  - Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools
  - Given a scenario, analyze vulnerabilities and recommend risk mitigations
  - Given a scenario, use processes to reduce risk
  - Given an incident, implement the appropriate response
  - Explain the importance of forensic concepts
  - Given a scenario, use forensic analysis tools
- Security Engineering and Cryptography
  - Given a scenario, apply secure configurations to enterprise mobility
  - Given a scenario, configure and implement endpoint security controls
  - Explain security considerations impacting specific sectors and operational technologies
  - Explain how cloud technology adoption impacts organizational security
  - Given a business requirement, implement the appropriate PKI solution
  - Given a business requirement, implement the appropriate cryptographic protocols and algorithms
  - Given a scenario, troubleshoot issues with cryptographic implementations
- Governance, Risk, and Compliance
  - Given a set of requirements, apply the appropriate risk strategies

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Explain the importance of managing and mitigating vendor risk
- Explain compliance frameworks and legal considerations, and their organizational impact
- Explain the importance of business continuity and disaster recovery concepts

Wymagania:

- Suggested a minimum of ten years of general hands-on IT experience, with at least five of those years being broad hands-on IT security experience
- Network+, Security+, CySA+, Cloud+, and PenTest+ or equivalent certifications/knowledge

Poziom trudności

Certyfikaty:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the CompTIA CASP+ certification exam, which is available through the Pearson VUE test centers.

Each participant in an authorized training CompTIA CASP+ Prep Course held in Compendium CE will receive a free CAS-004 CompTIA CASP+ Certification Exam vouchers.

Prowadzący:

Autoryzowany trener CompTIA.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001