Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

CCSP

Certified Cloud Security Professional (CCSP)

Durata: 5

Descrizione

(ISC)² e Cloud Security Alliance (CSA) hanno sviluppato e lanciato il Certified Cloud Security Professional (CCSP), progettata per garantire la sicurezza del cloud.
Un certificato CCSP ha le competenze e le conoscenze tecniche avanzate per progettare, gestire e proteggere dati, applicazioni e infrastrutture nel cloud utilizzando le migliori pratiche e procedure stabilite dagli esperti di sicurezza informatica di (ISC)². Un certificato CCSP, inoltre, applica le competenze in materia di sicurezza delle informazioni a un ambiente di cloud computing e ha ampie competenze in architettura cloud, progettazione, operazioni, sicurezza dei dati, rischio e conformità. La competenza del professionista certificato sarà misurata rispetto a un corpus di conoscenze riconosciuto a livello globale.

OverNet è Official Training Partner di (ISC)² dal 2023. Eroghiamo corsi ufficiali (ISC)², potrai usufruire di materiale didattico ufficiale e successivamente sostenere le certificazioni presso le sedi autorizzate.
OverNet fornisce la formazione ufficiale per quattro certificazioni (ISC)² incentrate su Cloud Security (CCSP), Information Security (CISSP), Software Security (CSSLP) e Systems Security (SSCP).

A chi è rivolto?

Professionisti esperti in sicurezza informatica e IT/TIC coinvolti nella transizione e nel mantenimento di soluzioni e servizi basati sul cloud. Il corso è rivolto a:

- Cloud Architect
- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Technology Officer (CTO)
- Engineer/Developer/Manager
- DevOps
- Enterprise Architect
- IT Contract Negotiator
- IT Risk and Compliance Manager
- Security Administrator
- Security Analyst
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect
- Systems Engineer

• SecOps

Prerequisiti

Il partecipante dovrebbe avere almeno cinque anni di esperienza professionale nel settore IT, di cui almeno tre nel campo della sicurezza delle informazioni e almeno uno nel campo del cloud computing.
Inoltre, dovrebbe già avere esperienza in ciascuno dei sei domini CBK:
- Concetti di architettura e requisiti di progettazione
- Sicurezza dei dati nel cloud
- Piattaforma cloud e sicurezza dell'infrastruttura
- Sicurezza delle applicazioni cloud
- Operazioni
- Legale e conformità

Contenuti

Domain 1: Architectural Concepts and Design Requirements
Understand cloud computing concepts
Describe cloud reference architecture
Understand security concepts relevant to could computing
Understand design principles of secure cloud computing
Identify trusted cloud services

Domain 2: Cloud Data Security
Understand Cloud Data Life Cycle
Design and Implement Cloud Data Storage Architectures
Understand and implement Data Discovery and Classification Technologies
Design and Implement Relevant Jurisdictional Data Protection for Personally Identifiable Information (PII)
Design and implement Data Rights Management
Plan and Implement Data Retention, Deletion, and Archival policies
Design and Implement Auditability, Traceability, and Accountability of Data Events

Domain 3: Cloud Platform Infrastructure Security
Comprehend Cloud Infrastructure Comp
Analyze Risks Associated to Cloud Infrastructure
Design and Plan Security Controls
Plans Disaster Recovery & Business Continuity Management

Domain 4: Cloud Application Security
Recognize Need for Training and Awareness in Application Security
Understand Cloud Software Assurance and Validation
Use Verified Secure Software
Comprehend the Software Development Life Cycle (SDLC) Process
Apply the Secure Software Development Life Cycle

Comprehend the Specifics of Cloud Application Architecture
Design Appropriate Identity and Access Management (IAM) Solutions

Domain 5: Operations
Support the Planning Process for the Data Center Design
Implement and Build Physical Infrastructure for Cloud Environment
Run Physical Infrastructure for Cloud Environment
Manage Physical Infrastructure for Cloud Environment
Build Logical Infrastructure for Cloud Environment
Run Logical Infrastructure for Cloud Environment
Manage Logical Infrastructure for Cloud Environment
Ensure Compliance with Regulations and Controls
Conduct Risk Assessment to Logical and Physical Infrastructure
Understand the Collection and Preservation of Digital Evidence
Manage Communications with Relevant Parties Domain

Domain 6: Legal and Compliance
Understand Legal Requirements and Unique Risks Within the Cloud Environment Module 2: Understand Privacy Issues, Including Jurisdictional Variances
Understand Audit Process, Methodologies, and Required Adaptions for a Cloud Environment
Understand Implication of Cloud to Enterprise Risk Management
Understand Outsourcing and Cloud Contract Design
Execute Vendor Management