

Certified Cloud Security Professional (CCSP) («CCSP3»)

Ziel dieses Kurses ist die Absolvierung der CCSP-Prüfung. Mit diesem Zertifikat erhöhen Sie Ihre Attraktivität für Arbeitgeber enorm. Sie helfen zudem mit, einen hohen Sicherheitsstandard für Cloud-Dienste zu garantieren und aufrechtzuerhalten.

Dauer: 3 Tage

Preis: 3'100.- zzgl. 8.1% MWST

Kursdokumente: Digicomp Kursunterlagen (Deutsch) und Begleitbuch «(ISC)² CCSP Certified Cloud Security Professional Official Study Guide 3rd Edition» (Englisch)

Inhalt

Für den Schutz von Cloud Services ist die persönliche Kompetenz jedes einzelnen Mitarbeiters wichtig. Dabei sind ethische Prinzipien und allgemeingültige Standards notwendig, um einen hohen Sicherheitsstandard zu erreichen und auch zu halten. (ISC)² und Cloud Security Alliance (CSA) haben gemeinsam ein Zertifikat für Cloud-Security-Spezialisten entwickelt.

Die Komplexität und das Risikoprofil von Cloud Computing erfordert neue Ansätze, um Cloud und hybride Umgebungen zu sichern – Legacy-Ansätze sind unzureichend. Es braucht erfahrene Profis mit den richtigen Cloud-Security-Kenntnissen und Fähigkeiten, um in diesem Bereich erfolgreich zu sein.

Das Certified Cloud Security Professional (CCSP) Credential soll gewährleisten, dass Cloud-Sicherheitsexperten die erforderlichen Kenntnisse, Fertigkeiten und Fähigkeiten in Cloud-Security-Design, -Implementierung, -Architektur, -Betrieb, -Kontrolle und -Einhaltung der regulatorischen Rahmenbedingungen aufbringen. CCSP steht für Informationssicherheits-Know-how in Cloud-Computing und zeigt Fachkompetenz in Cloud-Security-Architektur, -Design, -Betrieb und -Service-Orchestrierung.

Kursinhalte:

- Cloud-Computing-Konzepte: Definitionen, Rollen und Charakteristiken
- Design-Prinzipien, physische und logische Cloud-Infrastruktur
- Cloud-Referenzarchitekturen, -Servicemodelle und Deployment-Modelle
- Cloud-bezogene Sicherheitskonzepte; Verschlüsselung, Zugriffskontrolle, Netzwerksicherheit und Sicherheit von virtualisierten Umgebungen
- Cloud-Daten-Lifecycle, Speichertechnologien und Daten-Sicherheitsstrategien
- Data Discovery und Klassifikation, Datenschutz für Personendaten (Personally Identifiable Information PII), Data Rights Management, Datenaufbewahrung, -löschung und -archivierung
- Wiederherstellung und Notfallvorsorge
- Anwendungssicherheit, sichere Software-Entwicklung (Secure Development Lifecycle)
- Identity and Access Management
- Einhaltung von Regulatorien und Vorgaben (z.B. ITIL, ISO 27001), rechtliche Vorgaben, globale Datenschutzgesetze, Audit und Kontrolle, Outsourcing-Verträge

- Garantieren und Halten eines hohen Sicherheitsstandards für Cloud-Services
- Kennen der verschiedenen Cloud-Modelle bezüglich Servicemodelle und Architektur
- Vertieftes und praktisch anwendbares Verstehen der Sicherheit von Cloud-Services
- Kennen der globalen Anforderungen aus regulatorischer und gesetzlicher Sicht
- Umsetzen der Anforderungen in verschiedenen Cloud-Services (von globalen Anbietern bezogen oder selbst aufgebaut und angeboten)
- Verständliches Erläutern der Sicherheit von Software und Software-Entwicklung sowie Identity und Access-Management für eigene Services wie für Cloud-Services
- Analysieren von deren praktischen Anwendbarkeit
- Vorbereiten auf die Prüfung zum internationalen «CCSP»-Zertifikat

Zielpublikum

Alle, die sich auf die CCSP-Zertifizierung vorbereiten wollen, Security-Spezialisten mit bestehender **CISSP-Zertifizierung**, die ihre Kenntnisse im Bereich Cloud Security erweitern wollen sowie Security-Administratoren, Systemadministratoren und IT-Engineers im Bereich Cloud Computing

Anforderungen

Für die Zertifizierung zum CCSP müssen neben dem Bestehen der Prüfung folgende Voraussetzungen erfüllt sein: mind. fünf Jahre Praxiserfahrung in der Informationstechnologie (IT/ICT), 3 Jahre davon in Informationssicherheit sowie mindestens 1 Jahr davon in einem der sechs Arbeitsgebiete des CBK (Common Body of Knowledge). Bei vorhandener, gültiger CISSP-Zertifizierung werden keine zusätzlichen Praxisjahre benötigt. Die 6 CBKs sind:

- Architekturkonzepte und Design-Anforderungen (Architectural Concepts and Design Requirements)
- Cloud-Datensicherheit (Cloud Data Security)
- Cloud-Plattform und Infrastruktursicherheit (Cloud Platform and Infrastructure Security)
- Cloud-Anwendungssicherheit (Cloud Application Security)
- Betrieb (Operations)
- Recht/Gesetz und Compliance (Legal and Compliance)

Erfahrung im Bereich Telekommunikation, virtuelle Systeme und Netzwerke sind von Vorteil, gute Englischkenntnisse sind Bedingung. Weitere Informationen finden Sie unter der Website von ISC2.org (<https://isc2.org/ccsp-how-to-certify/default.aspx>)

- **Certified Information Systems Security Professional (CISSP) («SSP»)**

Zertifizierung

Die in diesem Kurs erlangte Fachkompetenz wird gemessen durch eine weltweit anerkannte Stelle. Das CCSP ist ein stand-alone Zertifikat, das bestehende Weiterbildungsprogramme ergänzt und ausbaut, einschliesslich (ISC)² **«Certified Information Systems Security Professional (CISSP)»** und dem CSA-Zertifikat «Cloud Security Knowledge (CCSK)».

Nicht im Preis inbegriffen sind die PearsonVUE-Prüfungsgebühren von ca. EUR 480.-. Wir empfehlen Ihnen nach dem Kurs eine zusätzliche Vorbereitungszeit, um sich optimal auf die Prüfung vorzubereiten. Sie können sich bei PearsonVUE online (<http://www.pearsonvue.com/isc2/>) für die CCSP-Prüfung anmelden. Die CCSP-Prüfung kann bei der Firma Helidux (<http://www.helidux.ch>) vor Ort absolviert werden.

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?



Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-security/cyber-security-defense/kurs-certified-cloud-security-professional-ccsp