EC-Council Certified Cloud Security Engineer

Examen-ID: 312-40

Trainings-ID: CCSE

Prüfung: 312-40

Prüfung: 312-40

Zum Seminar →

Das nehmen Sie mit

Die Cloud-Technologie hat die IT-Landschaft verändert und wird dies auch in den kommenden Jahren tun. Der Certified Cloud Security Engineer (CCSE) von EC-Council ist ein herstellerneutraler Kurs, der sich auf Cloud-Sicherheitspraktiken, -Technologien, -Frameworks und -Prinzipien konzentriert, um eine ausgewogene Mischung aus theoretischen und praktischen Fähigkeiten zu vermitteln, die Sie benötigen, um ein Cloud-Sicherheitsexperte zu werden.

Der CCSE wurde mit Blick auf die Aufgaben im Bereich der Cloud-Sicherheit entwickelt und soll Ihnen helfen, die Herausforderungen von morgen zu meistern. Da sich die Cloud-Technologie weiterentwickelt, sollten auch Sie dies tun - lernen Sie die Fähigkeiten, die Sie jetzt brauchen, um die Technologie von morgen zu verteidigen.

Nach Abschluss des Kurses haben die Teilnehmer Kenntnisse zu folgenden Themen:

- Planen, Implementieren und Ausführen der Sicherheit von Cloud-Plattformen für ein Unternehmen.
- Sicherer Zugriff auf Cloud-Ressourcen durch Identitäts- und Zugriffsmanagement (IAM).
- Bewertung und Kontrolle der organisatorischen Cloud-Netzwerkarchitektur durch Integration verschiedener Sicherheitskontrollen, die der Dienstanbieter anbietet.
- Bewertung von Cloud-Speichertechniken und Bedrohungen für in der Cloud gespeicherte Daten und Verständnis dafür, wie Cloud-Daten vor Angriffen geschützt werden können.

- Implementierung und Verwaltung von Cloud-Sicherheit auf verschiedenen Cloud-Plattformen, wie AWS, Azure und GCP.
- Das Modell der geteilten Verantwortung des Dienstanbieters zu verstehen.
- Verschiedene Cloud-Sicherheitsstandards, Compliance-Programme und von AWS, Azure und GCP angebotene Funktionen bewerten und Sicherheitsaudits für Cloud Computing durchführen.
- Implementierung verschiedener von Azure, AWS und GCP angebotener Dienste zur Erkennung von Bedrohungen und zur Reaktion darauf, um Bedrohungen für die Cloud-Dienste eines Unternehmens zu identifizieren.
- Bewertung und Minderung von Sicherheitsrisiken, Bedrohungen und Schwachstellen in einer Cloud-Plattform.
- Integration von Best Practices zur Sicherung von Cloud-Infrastrukturkomponenten (Netzwerk, Speicherung und Virtualisierung sowie Verwaltung).
- Sicherung von Cloud-Anwendungen im Unternehmen durch Verständnis des sicheren Softwareentwicklungszyklus von Cloud-Anwendungen und durch Implementierung zusätzlicher Sicherheitskontrollen zur Verbesserung der Sicherheit von gehosteten Cloud-Anwendungen.
- Entwurf und Implementierung eines GRC-Frameworks, eines Reaktionsplans für Cloud-Vorfälle und eines Geschäftskontinuitätsplans für Cloud-Dienste.
- Nutzung der in Azure, AWS und GCP bereitgestellten Sicherheitsservices und -tools zur Sicherung der Cloud-Umgebung des Unternehmens.
- Verstehen der rechtlichen Implikationen im Zusammenhang mit Cloud Computing, um Organisationen zu schützen.
- Implementierung von Betriebskontrollen und Standards für Aufbau, Betrieb, Verwaltung und Wartung der Cloud-Infrastruktur.
- Verstehen und Implementieren von Sicherheit für private, mandantenfähige und hybride Cloud-Umgebungen.

Das nehmen Sie mit

Die Cloud-Technologie hat die IT-Landschaft verändert und wird dies auch in den kommenden Jahren tun. Der Certified Cloud Security Engineer (CCSE) von EC-Council ist ein herstellerneutraler Kurs, der sich auf Cloud-Sicherheitspraktiken, -Technologien, -Frameworks und -Prinzipien konzentriert, um eine ausgewogene Mischung aus theoretischen und praktischen Fähigkeiten zu vermitteln, die Sie benötigen, um ein Cloud-Sicherheitsexperte zu

werden.

Der CCSE wurde mit Blick auf die Aufgaben im Bereich der Cloud-Sicherheit entwickelt und soll Ihnen helfen, die Herausforderungen von morgen zu meistern. Da sich die Cloud-Technologie weiterentwickelt, sollten auch Sie dies tun - lernen Sie die Fähigkeiten, die Sie jetzt brauchen, um die Technologie von morgen zu verteidigen.

Nach Abschluss des Kurses haben die Teilnehmer Kenntnisse zu folgenden Themen:

- Planen, Implementieren und Ausführen der Sicherheit von Cloud-Plattformen für ein Unternehmen.
- Sicherer Zugriff auf Cloud-Ressourcen durch Identitäts- und Zugriffsmanagement (IAM).
- Bewertung und Kontrolle der organisatorischen Cloud-Netzwerkarchitektur durch Integration verschiedener Sicherheitskontrollen, die der Dienstanbieter anbietet.
- Bewertung von Cloud-Speichertechniken und Bedrohungen für in der Cloud gespeicherte Daten und Verständnis dafür, wie Cloud-Daten vor Angriffen geschützt werden können.
- Implementierung und Verwaltung von Cloud-Sicherheit auf verschiedenen Cloud-Plattformen, wie AWS, Azure und GCP.
- Das Modell der geteilten Verantwortung des Dienstanbieters zu verstehen.
- Verschiedene Cloud-Sicherheitsstandards, Compliance-Programme und von AWS, Azure und GCP angebotene Funktionen bewerten und Sicherheitsaudits für Cloud Computing durchführen.
- Implementierung verschiedener von Azure, AWS und GCP angebotener Dienste zur Erkennung von Bedrohungen und zur Reaktion darauf, um Bedrohungen für die Cloud-Dienste eines Unternehmens zu identifizieren.
- Bewertung und Minderung von Sicherheitsrisiken, Bedrohungen und Schwachstellen in einer Cloud-Plattform.
- Integration von Best Practices zur Sicherung von Cloud-Infrastrukturkomponenten (Netzwerk, Speicherung und Virtualisierung sowie Verwaltung).
- Sicherung von Cloud-Anwendungen im Unternehmen durch Verständnis des sicheren Softwareentwicklungszyklus von Cloud-Anwendungen und durch Implementierung zusätzlicher Sicherheitskontrollen zur Verbesserung der Sicherheit von gehosteten Cloud-Anwendungen.

- Entwurf und Implementierung eines GRC-Frameworks, eines Reaktionsplans für Cloud-Vorfälle und eines Geschäftskontinuitätsplans für Cloud-Dienste.
- Nutzung der in Azure, AWS und GCP bereitgestellten Sicherheitsservices und -tools zur Sicherung der Cloud-Umgebung des Unternehmens.
- Verstehen der rechtlichen Implikationen im Zusammenhang mit Cloud Computing, um Organisationen zu schützen.
- Implementierung von Betriebskontrollen und Standards für Aufbau, Betrieb, Verwaltung und Wartung der Cloud-Infrastruktur.
- Verstehen und Implementieren von Sicherheit für private, mandantenfähige und hybride Cloud-Umgebungen.

Zielgruppen

- Engineers für Netzwerksicherheit
- Cybersecurity-Analysten
- Analysten für Netzwerksicherheit
- Cloud-Administratoren und -Engineers
- Netzwerksicherheits-Administratoren
- Cloud-Analysten
- Cybersicherheits-Engineers
- Mitarbeiter im Bereich Netzwerk- und Cloud-Management und -Betrieb

Wichtige Informationen
Dieses Seminar bereitet auf die Prüfung 312-40 ECC Exam vor. Testfragen: 125 Testdauer: 4 Stunden Testform.
Das Examen ist im Kurspreis inkludiert!

Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis
27.01.2025–31.01.2025	5 Tage		Trainingspreis (Online)	€ 4.450,-
24.03.2025–28.03.2025	5 Tage		Trainingspreis (Vor Ort)	€ 4.450,-
24.03.2025–28.03.2025	5 Tage		Trainingspreis (Online)	€ 4.450,-