Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Devenir ingénieur certifié en sécurité Cloud (C|CSE)

Date et durée

Code formation : CCSE
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

C|CSE : Certified Cloud Security Engineer

Description

À l'ère du tout numérique, les services cloud présentent **de nombreux avantages pour les entreprises**, mais ils comportent également des risques en matière de sécurité. Les cybercriminels ciblent de plus en plus ces services en raison du volume important de données qui y sont stockées et traitées. Par conséquent, **la sécurité du cloud computing** est désormais une priorité majeure pour les organisations. En effet, les vulnérabilités dans ce type de solutions peuvent entrainer la divulgation, le vol ou la perte de données sensibles, amenant des coûts financiers élevés et un préjudice moral.
Notre **formation d'ingénieur certifié en sécurité cloud** (C|CSE) est un programme complet sur la sécurité des services cloud, développé par des ingénieurs spécialisés dans ce domaine. Elle couvre la sécurité des données, la sécurité des applications, la maintenance, les tests de pénétration, la gestion du risque, la réponse aux incidents et bien plus.
Destiné principalement aux professionnels de la cybersécurité, les cours offre une approche holistique dans **la sécurité des plateformes AWS, Azure et Google Cloud**, ainsi que pour des architectures privées et hybrides. Par ailleurs, elle permet d'acquérir des compétences pratiques et de passer l'examen C|CSE (312-40) afin de décrocher la **certification Certified Cloud Security Engineer** (en savoir plus dans l'onglet certification).

Objectifs

A l'issue de la **formation Cloud Security Engineer**, vous atteindrez les objectifs suivants :

- planifier, implémenter et gérer la sécurité des plateformes cloud pour une entreprise ;
- accéder à des ressources dans le cloud en utilisant la gestion des identités et des accès (IAM) ;
- évaluer et contrôler l'architecture d'un réseau cloud organisationnel en effectuant les opérations de contrôle de sécurité prévues par le fournisseur de services ;
- évaluer les techniques de stockage dans le cloud et ce qui peut compromettre les données qui y sont stockées ;
- protéger des données du cloud contre des attaques ;
- implémenter et gérer la sécurité du cloud sur AWS, Azure et Google Cloud ;
- connaitre le modèle de responsabilité partagée pour chaque fournisseur de services ;
- évaluer les divers standards de sécurité du cloud, les programmes de conformité et les fonctionnalités disponibles avec AWS, Azure et Google Cloud ;
- effectuer des audits de sécurité cloud pour chacun des fournisseurs de services ;
- implémenter les systèmes de détection et de réponse aux menaces proposés par Azure, AWS et Google Cloud pour identifier les menaces qui pèsent sur les services cloud d'une entreprise ;
- évaluer et atténuer les risques de sécurité, les menaces et les vulnérabilités sur une infrastructure cloud ;

- adopter les bonnes pratiques pour sécuriser les composants d'une infrastructure cloud (réseau, stockage, virtualisation et gestion) ;
- sécurisé des applications cloud d'entreprise en prenant en compte le cycle de développement de sécurité des APIs et en implémentant des contrôles de sécurité supplémentaires.
- créer et implémenter un cadre de gestion de la relation client, un plan de réponse aux incidents et un plan de continuité de l'activité pour chaque service cloud ;
- utiliser les services et les outils de sécurité de Azure, AWS et Google Cloud afin de sécuriser l'environnement cloud d'une entreprise ;
- connaitre les aspects juridiques du cloud afin de protéger efficacement une entreprise ;
- implémenter des contrôles opérationnels et des normes pour créer, exploiter, gérer et maintenir une infrastructure cloud ;
- connaitre et implémenter la sécurité pour les environnements cloud privés, multi-locataires et hybrides ;
- réussir l'examen C|CSE (312-40) et obtenir la certification Certified Cloud Security Engineer.

Oo2 est accrédité par EC-Council pour dispenser la formation C|CSE. Ce statut garantit la prestation d'un formateur agréé, des supports de cours officiels et des examens de certifications organisés en fin de formation.

Points forts

Une formation animée par un formateur expert en sécurité cloud et accrédité par le EC-Council, + de 50 labs complexes et la passage de l'examen Certified Cloud Security Engineer compris dans notre offre.

Certification

En suivant notre formation C|CSE, vous pourrez **passer à tout moment l'examen Certified Cloud Security Engineer** de notre partenaire certificateur EC-Council. Cet examen, disponible en ligne et en anglais, consiste à **répondre à un QCM de 125 questions** pendant une durée maximum de 4 heures. Pour décrocher le certification de Certified Cloud Security Engineer, vous devez **obtenir un score entre 60 et 70 % de bonnes réponses**.
Cette titre professionnel démontre ainsi que vous possédez des compétences et des connaissances nécessaires pour **protéger efficacement des environnements cloud** contre de possibles cyberattaques.

> **A noter :** *la certification professionnelle C|CSE est soumise à un processus de renouvellement et de maintien du niveau de compétence. Les exigences sont publiées sur la politique de formation continue de l'EC-Council (ECE).*

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Cloud Security Engineer** nécessite le prérequis suivant :

- avoir des connaissances de base en cybersécurité, sur les technologies du cloud et sur la gestion de la sécurité des réseaux.

Public

Cette formation s'adresse aux publics suivants :

- les professionnels IT expérimentés comme les ingénieurs Cloud, les administrateurs de sécurité réseau ou encore les analystes en cybersécurité ;
- toute autre professionnel de l'informatique chargée d'administrer un réseau ou une plateforme Cloud.

Cette formation s'adresse aux profils suivants

Administrateur réseaux - télécoms
Ingénieur réseaux - télécoms
Responsable sécurité informatique
Analyste cybersécurité

Programme

Module 01 : les bases de la sécurité dans le Cloud

Ce premier module décrit les concepts de base du cloud computing, les modèles de services cloud, ainsi que les menaces et les vulnérabilités qui y sont liées. Il vous présente également les modèles d'évaluation de la sécurité et le partage des responsabilités qui sont des éléments clés pour la mise en place d'un environnement cloud sécurisé et pour protéger les ressources d'une entreprise.

Module 02 : la sécurité des plateformes et de l'infrastructure du Cloud

Ce module décrit les principaux composants et technologies des architectures cloud et vous explique comment sécuriser les composantes cloud multi-locataires, virtualisées, physiques et logiques. Il vous présente aussi les configurations et les bonnes pratiques pour sécuriser des data centers physiques et des infrastructures cloud avec les outils et les techniques fournies par Azure, AWS et Google Cloud.

Module 03 : la sécurité des applications dans le Cloud

Ce module est axé sur la sécurisation des applications cloud et sur les modifications du cycle de vie du développement des APIs sécurisées. Il présente également les divers services et outils de sécurisation proposés par Azure, AWS et Google Cloud.

Module 04 : la sécurité des données dans le Cloud

Ce module décrit les bases du stockage de données dans le cloud, son cycle de vie et les divers contrôles qui permettent de protéger les données stockées en local et celles qui sont en transfert vers le cloud. Les fonctionnalités de stockage des données ainsi que les différents services et outils utilisés pour les sécuriser dans Azure, AWS et Google Cloud sont également abordés.

Module 05 : la sécurité des opérations dans le Cloud

Ce module couvre les contrôles de sécurité fondamentaux pour la création, la mise en œuvre, l'exploitation, la gestion et la maintenance des infrastructures physiques et logiques des environnements cloud. Il aborde également les services, les fonctionnalités et les outils fournis par AWS, Azure et Google Cloud pour assurer la sécurité des opérations.

Module 06 : le test de pénétration dans le Cloud

Ce module traite des tests de pénétration complets destinés à évaluer la sécurité de l'infrastructure cloud d'une entreprise et présente les services et outils utilisés pour effectuer des tests dans AWS, Azure et Google Cloud.

Module 07 : la détection et la réponse aux incidents dans le Cloud

Ce module est consacré au processus de réponse aux incidents. Il aborde le cycle de vie ainsi que les outils et les techniques utilisés pour identifier les incidents et y répondre efficacement. De plus, il permet de se familiariser avec l'utilisation des technologies SOAR et explique les solutions de réponse aux incidents proposées par AWS, Azure et Google Cloud.

Module 08 : l'investigation forensique dans le Cloud

Ce module explique le processus des investigations forensiques, telles que les défis et les méthodes de collecte de données. Il vous montre en outre la manière d'enquêter sur les incidents de sécurité avec les outils d'AWS, d'Azure et de Google Cloud.

Module 09 : la continuité des activités et la reprise après sinistre dans le Cloud

Ce module présente l'importance de la continuité des activités et de la planification de la reprise après sinistre. Il vous présente aussi les outils de sauvegarde et de récupération, les services et les fonctionnalités proposés par AWS, Azure et Google Cloud afin de contrôler les problèmes de continuité des activités.

Module 10 : la gouvernance, la gestion des risques et la conformité dans le Cloud

Ce module se focalise sur les référentiels de gouvernance et les normes (ISO/IEC 27017, HIPAA et PCI DSS) ainsi que de leurs implémentations dans le cloud. Il traite aussi des référentiels de conformité du cloud et approfondit la gouvernance sur AWS, Azure et Google Cloud.

Module 11 : les normes, les politiques et les aspects juridiques du Cloud

Ce dernier module traite des normes, des politiques et des obligations juridiques applicables à l'utilisation du Cloud. Il aborde également les fonctionnalités, les services, les outils de conformité et d'audit sur AWS, Azure et Google Cloud.