CERTIFIED CLOUD SECURITY ENGINEER (CCSE) EĞİTİMİ

5 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

Certified Cloud Security Engineer (C|CSE) eğitimi, bulut teknolojileri ve siber güvenlik alanında giderek artan bir talep olan bu kritik beceri setini kavramak ve uygulamak isteyen profesyoneller için hayati öneme sahiptir. Bulut bilişim, modern iş dünyasında bir devrim yaratmış olup, bu teknolojilerin güvenliği, gizliliği ve uyumluluğu daha da önemli hale gelmiştir.

Bir başka odak noktası, çok bulutlu stratejiler ve hibrit bulut sistemleridir. Birçok organizasyon, iş yüklerini ve verilerini farklı bulut sağlayıcılar arasında dağıtmayı tercih ediyor. C|CSE eğitimi, bu karmaşık yapıları güvence altına almak ve uyumlu bir şekilde yönetmek için gerekli araçları ve yöntemleri öğretir.

Bulut sağlayıcılarıyla ilişkiler ve sözleşmeler de bu eğitimin önemli bir parçasıdır. Organizasyonların, bulut sağlayıcılarıyla olan sözleşmelerinde güvenlik ve gizlilikle ilgili hususları nasıl ele alacaklarına dair rehberlik ve uygulamalar sağlar. Bu, işletmelerin ve kullanıcıların, verilerinin güvende olduğundan ve bulut sağlayıcısının güvenlik standartlarına uyduğundan emin olmasına yardımcı olur.

Güvenlik politikaları ve uyumluluk da bu eğitimde önemli bir rol oynar. Özellikle, GDPR, HIPAA gibi uluslararası ve yerel düzenlemelere uyumu sağlamak için bulut güvenliği politikalarının nasıl oluşturulacağını ve uygulanacağını kapsar. Bu, organizasyonların yasal gerekliliklere uygun hareket etmelerini ve potansiyel yaptırımlardan kaçınmalarını sağlar.

C|CSE eğitimi ayrıca olaya müdahale ve felaket kurtarma planlamasını da kapsar. Bulut ortamında güvenlik ihlallerine yanıt verme ve operasyon sürekliliğini öğretir. Bu, iş sürekliliği ve toparlanma stratejilerinin etkili bir şekilde planlanmasına ve uygulanmasına olanak tanır.

Ayrıca, bulut güvenliği alanında sertifikasyonlar ve sürekli eğitim de dahil olmak üzere kariyer gelişimi ve profesyonel ağ kurma fırsatları hakkında bilgi verir. Bu, katılımcıların bu dinamik alanın gerektirdiği sürekli değişen gerekliliklere uyum sağlamalarına yardımcı olur.

Sonuç olarak, Certified Cloud Security Engineer (C|CSE) eğitimi, bulut güvenliği alanında kapsamlı bir bilgi birikimi ve pratik beceriler sağlar. Bu, profesyonellerin bulut ortamlarını güvenli ve uyumlu bir şekilde yönetmelerine, aynı zamanda kariyerlerini bu hızla büyüyen ve hayati öneme sahip alanda ilerletmelerine yardımcı olur.

Neler Öğreneceksiniz?

Certified Cloud Security Engineer (C|CSE) eğitimi sırasında aşağıdaki konuları öğrenebilirsiniz:

- Bulut Güvenliği Temelleri: Bulut bilişimi ve bulut güvenliği kavramlarına genel bir bakış elde edersiniz. Bulut hizmet modelleri, dağıtım modelleri, güvenlik zorlukları ve bulut ortamında güvenlik ihtiyaçları hakkında bilgi sahibi olursunuz.
- Bulut Mimarisi ve Güvenlik: Bulut tabanlı altyapıların güvenli bir şekilde tasarlanması ve yönetilmesi için güvenlik mimarisi konularında bilgi edinirsiniz. Bulut güvenlik kontrolleri, ağ

güvenliği, veri güvenliği ve kimlik yönetimi gibi konulara odaklanarak güvenli bir bulut mimarisi oluşturmanın yöntemlerini öğrenirsiniz.

- Bulut Hizmetlerinde Güvenlik: Bulut ortamında kullanılan farklı hizmetlerin güvenliğini öğrenirsiniz. Platform hizmetleri, altyapı hizmetleri ve yazılım hizmetleri gibi bulut tabanlı hizmetlerin güvenliğini sağlama konularına odaklanırsınız. Ayrıca, bulut tabanlı güvenlik hizmetlerinin kullanımını ve yönetimini öğrenirsiniz.
- Bulut Tabanlı Uygulama Güvenliği: Bulut tabanlı uygulamaların güvenliğini sağlama konusunda bilgi ve becerilerinizi geliştirirsiniz. Uygulama katmanı güvenliği, güvenlik açıklarının tespiti, güvenli kodlama prensipleri, uygulama güvenlik testleri ve saldırı tespiti konularında uzmanlaşarak bulut tabanlı uygulamaları güvence altına almayı öğrenirsiniz.
- Bulut Güvenlik İzleme ve Olay Yönetimi: Bulut ortamında güvenlik olaylarını izleme, tespit etme ve yönetme becerilerinizi geliştirirsiniz. Güvenlik olaylarını izleme araçlarını kullanma, güvenlik olaylarına hızlı yanıt verme, log yönetimi ve olay yönetimi süreçlerini öğrenirsiniz.

C|CSE eğitimi, bulut güvenliği konusunda derinlemesine bilgi ve beceriler kazanmanızı sağlar. Bulut ortamında güvenliği sağlama, bulut hizmetlerini etkin bir şekilde yönetme ve bulut tabanlı uygulamaların güvenliğini güvence altına alma konularında uzmanlaşmanızı destekler. Bu eğitim sayesinde, organizasyonunuzun bulut ortamında güvenlik açıklarını azaltma ve verileri koruma yeteneklerinizi artırabilirsiniz.

Ön Koşullar

Certified Cloud Security Engineer (C|CSE) eğitimine katılmadan önce belirli bir ön koşul bulunmamaktadır. Bununla birlikte, aşağıdaki bilgi ve deneyimler, eğitimi daha iyi anlamanıza ve başarılı bir şekilde tamamlamanıza yardımcı olabilir:

- Bulut Temelleri: Bulut bilişimi ve bulut hizmet modelleri hakkında temel bir anlayışa sahip olmanız önerilir. İşletim modelleri (SaaS, PaaS, IaaS), bulut altyapıları ve temel bulut kavramları hakkında bilgi sahibi olmak, eğitim sürecini daha verimli hale getirebilir.
- Ağ ve Sistem Güvenliği: Ağ güvenliği ve sistem güvenliği konularında bir temel bilgiye sahip olmanız faydalı olacaktır. Ağ yapılandırması, güvenlik duvarları, ağ izleme araçları, saldırı tespit sistemleri ve temel sistem güvenliği prensipleri gibi konulara aşina olmak, bulut güvenliği eğitiminde size avantaj sağlayabilir.
- Güvenlik İlkeleri ve Standartları: Genel güvenlik ilkeleri ve standartlar hakkında bilgi sahibi olmak, bulut güvenliği konusunda anlayışınızı artırabilir. Örneğin, ISO 27001, NIST 800-53, CSA Security Guidance gibi güvenlik standartları ve çerçeveleri hakkında bilgi sahibi olmak faydalı olabilir.
- Bilgi Güvenliği: Bilgi güvenliği konularına aşina olmak, veri gizliliği, bütünlük, erişim kontrolü ve kimlik yönetimi gibi konulara dair bir anlayışa sahip olmanızı sağlar.

Bu ön bilgi ve deneyimler, C|CSE eğitimine katılmadan önce size avantaj sağlayabilir, ancak kesin bir ön koşul değildir. Eğitimi sağlayan kuruluşun belirlediği spesifik ön koşulları kontrol etmek önemlidir, çünkü gereksinimler farklı kuruluşlar arasında değişebilir. Eğitim sağlayıcının belirlediği ön koşulları karşıladığınızdan emin olmanız önerilir.

Kimler Katılmalı

Certified Cloud Security Engineer (C|CSE) eğitimi aşağıdaki profesyoneller için uygun olabilir:

- Bulut Güvenlik Mühendisleri: Bulut ortamlarında güvenlik stratejileri oluşturmak, güvenlik açıklarını tespit etmek ve çözümler geliştirmekle görevli mühendisler, C|CSE eğitimine katılarak bilgi ve becerilerini geliştirebilirler.
- Bulut Güvenlik Danışmanları: Müşterilere bulut güvenliği konusunda danışmanlık hizmeti veren profesyoneller, C|CSE eğitimi sayesinde güvenlik projelerinde etkin bir şekilde rol alabilir ve müşterilerine en iyi uygulamaları sunabilirler.
- Sistem ve Ağ Güvenlik Uzmanları: Bulut ortamlarında sistem ve ağ güvenliği alanında çalışan uzmanlar, C|CSE eğitimiyle bulut tabanlı güvenlik çözümleri hakkında derinlemesine bilgi sahibi olabilirler.
- Siber Güvenlik Yöneticileri: Organizasyonlarında bulut güvenliği stratejilerini yönetmekle görevli yöneticiler, C|CSE eğitimine katılarak bulut tabanlı güvenlik konusunda kapsamlı bir bilgi ve anlayış geliştirebilirler.
- Güvenlik Operasyon Merkezi (SOC) Personeli: SOC ekiplerinde çalışan güvenlik analistleri ve uzmanları, bulut ortamında güvenlik olaylarını yönetmek ve tehditleri tespit etmek için C|CSE eğitimi alabilirler.
- Bulut Altyapı Hizmet Sağlayıcıları: Bulut hizmeti sunan şirketlerde çalışan güvenlik ekipleri, müşterilerin verilerini ve hizmetlerini güvence altına almak için C|CSE eğitimini tercih edebilirler.

Yukarıda belirtilen gruplar, C|CSE eğitimine katılmak için uygun olabilecek örneklerdir. Bununla birlikte, bulut güvenliği konusunda ilgi ve motivasyona sahip olan herhangi bir profesyonel, bu eğitime katılarak bilgi ve becerilerini geliştirebilir. Bulut tabanlı güvenlik konularında çalışmak isteyen veya mevcut bilgi ve becerilerini güçlendirmek isteyen herkes, C|CSE eğitimine katılabilir.

Outline

Module 01: Introduction to Cloud Security

- In this module, you will be presented with the core concepts of cloud computing, cloud service models, and cloud-based threats and vulnerabilities. The module highlights service provider components, such as evaluation and the shared security responsibility model, that are essential to configuring a secure cloud environment and protecting organizational resources.

Module 02: Platform and Infrastructure Security in the Cloud

- This module explores the key components and technologies that form a cloud architecture and how to secure multi-tenant, virtualized, physical, and logical cloud components. This

module emonstrates confgurations and best practices for securing physical data centers and cloud nfrastructures using the tools and techniques provided by Azure, AWS, and GCP

Module 03: Application Security in the Cloud

- The focus of this module is securing cloud applications and explaining secure software development lifecycle changes. It explains the multiple services and tools for application security in Azure, AWS, and GCP.

Module 04: Data Security in the Cloud

- This module covers the basics of cloud data storage, its lifecycle, and various controls for protecting data at rest and data in transit in the cloud. It also addresses data storage features and the multiple services and tools used for securing data stored in Azure, AWS, and GCP.

Module 05: Operation Security in the Cloud

- This module encompasses the security controls essential to building, implementing, operating, managing, and maintaining physical and logical infrastructures for cloud environments and the required services, features, and tools for operational security provided by AWS, Azure, and GCP.

Module 06: Penetration Testing in the Cloud

- This module demonstrates how to implement comprehensive penetration testing to assess the security of an organization’s cloud infrastructure and reviews the required services and tools used to perform penetration testing in AWS, Azure, and GCP.

Module 07: Incident Detection and Response in the Cloud

- This module focuses on incident response (IR). It covers the IR lifecycle and the tools and techniques used to identify and respond to incidents; provides training on using SOAR technologies; and explores the IR capabilities provided by AWS, Azure, and GCP.

Module 08: Forensics Investigation in the Cloud

- This module covers the forensic investigation process in cloud computing, including various cloud forensic challenges and data collection methods. It also explains how to investigate security incidents using AWS, Azure, and GCP tools.

Module 09: Business Continuity and Disaster Recovery in the Cloud

- This module highlights the importance of business continuity and disaster recovery planning in IR. It covers the backup and recovery tools, services, and features provided by AWS, Azure, and GCP to monitor business continuity issues.

Module 10: Governance, Risk Management, and Compliance in the Cloud

- This module focuses on the various governance frameworks, models, and regulations (ISO/IEC 27017, HIPAA, and PCI DSS) and the design and implementation of governance frameworks in the cloud. It also addresses cloud compliance frameworks and elaborates on the AWS, Azure, and GCP governance modules.

Module 11: Standards, Policies, and Legal Issues in the Cloud

- This module discusses standards, policies, and legal issues associated with the cloud. It also covers the features, services, and tools needed for compliance and auditing in AWS, Azure, and GCP.