CERTIFIED SECURITY SPECIALIST (ECSS) EĞİTİMİ

5 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

Certified Security Specialist (ECSS) eğitimi, bilgi güvenliği alanında kapsamlı bir programdır. Profesyoneller için derin bilgi ve beceri kazandırır. Tehdit analizi, risk yönetimi ve sistem penetrasyonu bu programın odak noktalarıdır. Ayrıca ağ güvenliği ve bilgisayar adli tıbbı konuları da ele alıyoruz.

Certified Security Specialist (ECSS) eğitimi, geniş bir perspektif sunar. Güvenlik prensipleri ve stratejileri öğrenecekler. Güvenlik politikaları ve yönetimlerini inceliyoruz. Katılımcılar, bu temel bilgilerle bilgi güvenliği konusunda yetkin hale gelir.

Tehdit analizi, ECSS eğitiminin önemli bir parçasıdır. Katılımcılar, tehditleri tanımlama becerilerini geliştirir. Risk yönetimini de detaylı olarak işleyip risk değerlendirme tekniklerini uyguluyoruz. Stratejilerin nasıl uygulanacağını uygulamalı olarak yapıyoruz. Böylece, işletmeler güvenlik açıklarını tespit eder ve önler.

Sistem penetrasyonu, bu eğitimde dikkat çeken bir konudur. Katılımcılarımız güvenlik açıklarını tespit etmek için teknikleri öğrenecekler. Saldırılara karşı savunma mekanizmaları geliştirecekler. Nitekim ağ güvenliği de önemli bir konu. Güvenlik duvarları ve ağ izleme araçları kullanıp zafiyet tarama tekniklerini öğrenecekler.

Bunun yanında, bilgisayar adli tıbbı diğer bir önemli konudur. Dijital delil toplama teknikleri üzerinde duruyoruz, olay yanıtı becerileri geliştiriyoruz. Olayların nedenleri ve sonuçlarını analiz edip adli tıp prensiplerini öğreniyoruz.

ECSS, teorik ve pratik becerileri birleştirir. Bununla birlikte güncel araçlar ve teknolojiler kullanılır. Gerçek dünya senaryoları üzerinde çalışılır. Katılımcılar, teorik bilgilerini pratikte uygulama şansı bulur.

ECSS sertifikası, kariyer fırsatlarını artırır. Bilgi güvenliği alanında yeterliliği doğrular. İşverenler ve müşteriler tarafından itibar sağlar. Kariyer yapmak veya deneyim kazanmak isteyenlere avantajlar sunar.

Sonuç olarak, ECSS eğitimi kıymetlidir. Bilgi güvenliği konusunda bilgi ve aynı zamanda beceri sağlar. Güncel bilgilerle donatır ve pratik beceriler kazandırır. ECSS sertifikası, yetkinlikleri kanıtlar ve kariyer ilerlemesine yardımcı olur.

Neler Öğreneceksiniz?

Certified Security Specialist (E|CSS) eğitimi boyunca, katılımcılar aşağıdaki anahtar konuları ve daha fazlasını öğrenirler:

- Tehdit ve Risk Analizi: Farklı siber tehdit türlerini anlama ve bunlara karşı önlem almayı öğrenirsiniz. Tehdit modellerini anlama ve risk değerlendirmesi yapma becerileri edinirsiniz.
- Ağ Güvenliği: Ağ tehditlerini tanımlama ve yönetme, güvenlik duvarları ve IDS / IPS sistemleri hakkında bilgi edinme konularını öğrenirsiniz.

- Bilgi Sistemleri Güvenliği: Bilgi sistemlerinin ve uygulamaların güvenliğini sağlama stratejilerini öğrenirsiniz. Bu, veri güvenliği, veri şifreleme, kimlik doğrulama ve yetkilendirme sistemleri üzerine olabilir.
- Bilgisayar Forensikleri: Bilgisayar adli bilimler ve olaylara yanıt verme konularında bilgi edinirsiniz. Bu, olay tespiti, olaya yanıt verme, adli veri toplama ve analiz etme, ve adli raporlama gibi konuları içerir.
- Sistem ve Uygulama Penetrasyon Testi: Etkin saldırı teknikleri, sızma testi yöntemleri ve araçları hakkında bilgi edinirsiniz. Ayrıca, bulguları raporlama ve güvenlik açıklarını düzeltme yöntemlerini öğrenirsiniz.
- Güvenlik Politikaları ve Yönetimi: Bilgi güvenliği yönetimi, güvenlik politikaları, prosedürler ve süreçler hakkında bilgi edinirsiniz. Ayrıca, yasal ve düzenleyici gereklilikler, etik konular ve uyum konularını öğrenirsiniz.

E|CSS eğitimi, siber güvenlik alanında kapsamlı bir anlayış sağlar ve katılımcılara, bilgi sistemlerinin güvenliğini sağlama ve siber tehditlere karşı koruma becerileri kazandırır.

Ön Koşullar

Certified Security Specialist (E|CSS) eğitimi için belirlenen belirgin ön koşullar genellikle eğitim sağlayıcıya göre değişir. Ancak, genel anlamda bu eğitim programına katılmak için aşağıdaki ön koşulların yerine getirilmesi beklenir:

- Bilgi Teknolojileri ve Ağ Bilgisi: Katılımcıların, temel bilgi teknolojisi ve ağ kavramlarına aşina olmaları beklenir. Bilgisayar sistemleri, işletim sistemleri, yazılım uygulamaları, ağ protokolleri ve cihazlar hakkında bilgi sahibi olmak önemlidir.
- Siber Güvenlik Temelleri: Katılımcıların, siber güvenlik temellerine aşina olmaları genellikle faydalıdır. Bu, siber tehditler, saldırı türleri ve güvenlik önlemleri hakkında temel bilgiyi içerebilir.
- Profesyonel Deneyim: Birçok program, belirli bir bilgi teknolojisi veya siber güvenlik alanında çalışma deneyimine sahip olmayı ön koşul olarak belirler. Bu, genellikle birkaç yıllık profesyonel deneyim anlamına gelir.
- İngilizce Dil Yetenekleri: E|CSS eğitimi genellikle İngilizce olarak verildiğinden, katılımcıların İngilizce okuma, yazma ve anlama yeteneklerine sahip olmaları genellikle önemlidir.

Bu ön koşullar, genellikle katılımcıların eğitim materyallerini anlamalarını ve eğitimden maksimum düzeyde yararlanmalarını sağlamak için belirlenmiştir. Her durumda, belirli bir eğitim programına başvurmadan önce belirli ön koşulların ne olduğunu kontrol etmek önemlidir

Kimler Katılmalı

Certified Security Specialist (E|CSS) eğitimi, aşağıdaki gruplardan bireyler için özellikle değerli olabilir:

- Bilgi Teknolojisi Profesyonelleri: Bilgi teknolojisi alanında çalışan profesyoneller, siber güvenlik konusundaki bilgilerini genişletmek ve derinleştirmek için bu eğitimi düşünebilirler. Bu, sistem yöneticileri, ağ yöneticileri, IT proje yöneticileri ve diğer IT rollerini içerebilir.
- Siber Güvenlik Profesyonelleri: Mevcut siber güvenlik profesyonelleri, becerilerini geliştirmek ve güncellemek için bu eğitimi kullanabilirler. Bu, güvenlik analistleri, güvenlik mühendisleri, sızma testi uzmanları ve diğer güvenlik rollerini içerebilir.
- Risk ve Uyumluluk Profesyonelleri: Risk ve uyumluluk profesyonelleri, siber güvenlik risklerini daha iyi anlamak ve yönetmek için E|CSS eğitimini kullanabilirler.
- Bilgi Güvenliği Yöneticileri: Bilgi güvenliği yöneticileri ve liderleri, bilgi güvenliği stratejilerini ve politikalarını yönetmek ve uygulamak için gereken becerileri geliştirebilirler.
- Bilgisayar Adli Tıp Uzmanları: Bilgisayar adli tıbbi uzmanları, adli tıbbi süreçlerini ve tekniklerini geliştirmek için bu eğitimi kullanabilirler.
- Kariyer Değişikliği Düşünenler: Bilgi teknolojisi veya başka bir alanda çalışan ancak siber güvenlik alanına geçmeyi düşünen bireyler için bu eğitim, yeni bir kariyer yoluna adım atmanın mükemmel bir yolu olabilir.

E|CSS eğitimi, güncel ve pratik siber güvenlik becerilerini geliştirmek ve bu alandaki profesyonel yeterliliklerini belgelemek isteyen herkese açıktır.

Outline

Network Defense Essentials

- Network Security Fundamentals
- Identification, Authentication, and Authorization
- Network Security Controls: Administrative Controls
- Network Security Controls: Physical Controls
- Network Security Controls: Technical Controls
- Virtualization and Cloud Computing
- Wireless Network Security
- Mobile Device Security
- IoT Device Security
- Cryptography and the Public Key Infrastructure
- Data Security
- Network Traffic Monitoring

Ethical Hacking Essentials

- Information Security Fundamentals
- Ethical Hacking Fundamentals

- Information Security Threats and Vulnerability Assessment
- Password Cracking Techniques and Countermeasures
- Social Engineering Techniques and Countermeasures
- Network Level Attacks and Countermeasures
- Web Application Attacks and Countermeasures
- Wireless Attacks and Countermeasures
- Mobile Attacks and Countermeasures
- IOT & OT Attacks and Countermeasures
- Cloud Computing Threats and Countermeasures
- Penetration Testing Fundamentals

Digital Forensics Essentials

- Computer Forensics Fundamentals
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Investigating Web Attacks
- Dark Web Forensics
- Investigating Email Crimes
- Malware Forensics