ISC2 Certified in Cybersecurity Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

ISC2 Certified in Cybersecurity (CC) resmi eğitimi, siber güvenlik alanına yeni adım atan katılımcılara temel bilgi ve kavramları kazandırmak amacıyla hazırlanmış giriş seviyesi bir programdır.

Eğitim; bilgi güvenliği prensipleri, risk yönetimi, erişim kontrolleri, ağ güvenliği, güvenlik operasyonları, olay müdahalesi, iş sürekliliği ve felaket kurtarma gibi temel konuları yapılandırılmış bir şekilde ele alır.

Daha önce siber güvenlik deneyimi olmayan veya çok sınırlı deneyime sahip katılımcılar için tasarlanan program, sektöre giriş yapmak ve daha ileri seviye sertifikalara hazırlanmak için sağlam bir temel oluşturur.

Canlı eğitmen anlatımı ile bireysel çalışma materyallerini bir araya getiren blended learning yaklaşımı sayesinde katılımcılar hem rehberli öğrenme hem de kendi hızlarında tekrar yapma imkânı bulur.

Program, **ISC2 Certified in Cybersecurity sınav kapsamıyla uyumludur** ve katılımcıların sertifikasyon sınavına daha hazırlıklı ve özgüvenli şekilde yaklaşmasına yardımcı olur.

Önkoşullar

Bu eğitime katılım için herhangi bir önceki deneyim veya teknik ön koşul bulunmamaktadır.

Kimler Katılmalı

Bu eğitim özellikle siber güvenlik kariyerine başlamak isteyen kişiler için uygundur.

Hedef kitle arasında:

- Siber güvenlik alanına geçmek isteyen IT profesyonelleri,
- Siber güvenlik bilgisini artırmak isteyen diğer teknik ekipler,
- Kariyer değişikliği yapmak isteyen profesyoneller,
- Üniversite ve yüksekokul öğrencileri,
- Yeni mezunlar,
- Siber güvenlik kariyer yollarını araştıran kişiler

yer alır.

ISC2 Certified in Cybersecurity Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Neler Öğreneceksiniz

Bu eğitimin sonunda katılımcılar:

- Temel siber güvenlik prensiplerini ve kavramlarını açıklayabilecek,
- Risk Management terminolojisini ve temel süreçlerini anlayabilecek,
- Security Controls türlerini tanımlayabilecek ve sınıflandırabilecek,
- Policies, Standards, Procedures, Regulations ve Laws arasındaki farkları açıklayabilecek,
- Siber güvenlikte Governance ve etik sorumlulukları anlayabilecek,
- Incident Response, Business Continuity ve Disaster Recovery kavramlarını açıklayabilecek,
- Access Control prensiplerini temel senaryolarda uygulayabilecek,
- Networking temellerini ve yaygın güvenlik tehditlerini anlayabilecek,
- Monitoring ve Encryption dahil temel Security Operations kavramlarını tanıyabilecek,
- Veri işleme ve sistem güvenliği için temel iyi uygulamaları belirleyebilecek.

Eğitim İçeriği

Modül 1 – Security Principles

- Information Assurance kavramları
- Temel güvenlik prensipleri
- Risk Management süreçleri
- Security Controls
- Governance unsurları
- Policy, Standard, Procedure, Regulation ve Law arasındaki farklar
- ISC2 Code of Ethics
- Siber güvenlikte etik sorumluluklar

Modül 2 – Business Continuity, Disaster Recovery ve Incident Response

- Incident Response süreçleri
- Güvenlik olaylarını tanıma ve müdahale yaklaşımı
- Business Continuity Planning
- Kritik iş süreçlerinin devamlılığı
- Disaster Recovery bileşenleri
- Sistem ve hizmetlerin geri kazanılması
- Olay sonrası toparlanma yaklaşımı

Modül 3 – Access Control Concepts

- Access Control temel prensipleri
- Access Control Models
- Kullanıcı ve kaynak erişim süreçleri
- Physical Access Controls
- Logical Access Controls
- Yetkilendirme ve erişim sınırlandırma yaklaşımları
- Temel erişim güvenliği senaryoları

Modül 4 – Network Security

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Networking fundamentals
- Temel ağ bileşenleri ve iletişim mantığı
- Common Threats
- Yaygın Attack Types
- Network Security Infrastructure
- Ağ trafiğini ve bağlantıları korumaya yönelik temel yaklaşımlar
- Güvenli ağ ortamının temel bileşenleri

Modül 5 – Security Operations

- Data Security best practices
- Verilerin güvenli şekilde işlenmesi ve korunması
- System Hardening teknikleri
- Security Policies and Procedures
- Monitoring kavramları
- Encryption'a giriş
- Security Awareness Training
- Güvenlik farkındalığı kültürünün desteklenmesi

Modül 6 – Sınav Hazırlığı ve Genel Tekrar

- ISC2 CC sertifikasyon gereksinimleri
- Sınav planlama ve kayıt süreci
- Sınav formatını anlama
- Sınav teknikleri ve stratejileri
- Tüm domainlerdeki temel kavramların gözden geçirilmesi
- Bilgi eksiklerinin belirlenmesi
- Sertifikasyon öncesi hazırlığın değerlendirilmesi

Uygulamalı Öğrenme

Bu eğitim, temel siber güvenlik bilgisinin yalnızca teorik olarak öğrenilmesini değil, gerçekçi durumlarda uygulanmasını da destekler.

Katılımcılar eğitim boyunca:

- Senaryo bazlı tartışmalara,
- Sınav konularıyla uyumlu practice questions çalışmalarına,
- Eğitmen liderliğinde temel kavram walkthrough'larına,
- Sertifikasyon sınavına yönelik guided review oturumlarına

katılır.

Bu yaklaşım, öğrenilen bilgilerin daha kalıcı olmasına ve temel güvenlik kavramlarının pratik senaryolarda nasıl kullanılacağının anlaşılmasına yardımcı olur.

Sınav ve Değerlendirmeler

Program, ISC2 Certified in Cybersecurity (CC) sınavına hazırlığı destekleyen yapılandırılmış değerlendirme faaliyetleri içerir.

- Resmi ISC2 Certified in Cybersecurity sınavı dahildir,
- Sınav Computer Adaptive Testing formatında uygulanır,

ISC2 Certified in Cybersecurity Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Sınav süresi yaklaşık 2 saattir,
- Sınavda 100–125 arasında soru bulunur,
- Sorular Multiple Choice ve Advanced Item Types formatlarında olabilir,
- Başarı için 1000 üzerinden 700 puan gerekir.

Eğitim sonunda katılımcılar, sertifikasyon sınavına ne kadar hazır olduklarını daha net değerlendirebilir ve siber güvenlikte giriş seviyesi rollere yönelik güçlü bir temel oluşturur.