BLUEMARK ACADEMY

CISSP (Certified Information Systems Security Professional) Eğitimi

Süre: 5 Gün · **Eğitim türü:** Sanal Sınıf / Online

Açıklama

Certified Information Systems Security Professional (CISSP), bilgi güvenliği alanında dünya genelinde en yaygın ve en prestijli sertifikasyonlardan biri olarak kabul edilmektedir. CISSP, bir bilgi güvenliği uzmanının; bir organizasyonun genel güvenlik duruşunu etkin şekilde tasarlama, mühendisliğini yapma ve yönetme konularında sahip olduğu derin teknik ve yönetsel bilgi ile deneyimi doğrular.

CISSP bilgi birikimi kapsamında ele alınan konu başlıklarının genişliği, sertifikanın bilgi güvenliği alanındaki tüm disiplinler için güncel ve geçerli olmasını sağlar. CISSP sertifikasını başarıyla alan adaylar, aşağıdaki sekiz temel alanda (domain) yetkinlik sahibidir:

- Güvenlik ve Risk Yönetimi
- Varlık Güvenliği
- Güvenlik Mimarisi ve Mühendisliği
- İletişim ve Ağ Güvenliği
- Kimlik ve Erişim Yönetimi (IAM)
- Güvenlik Değerlendirmesi ve Testleri
- Güvenlik Operasyonları
- Yazılım Geliştirme Güvenliği

Bu CISSP eğitimi, bilgi güvenliği alanında çalışan deneyimli profesyonellerin; kurumsal bilgi güvenliği yönetimi, risk ve uyum süreçleri, güvenlik mimarileri ve operasyonel güvenlik konularında bütüncül ve stratejik bir bakış açısı kazanmasını amaçlamaktadır. Eğitim, ISC2 tarafından belirlenen CISSP Common Body of Knowledge (CBK) yapısı ile birebir uyumlu olarak tasarlanmış olup, katılımcıların CISSP sertifikasyon sınavına etkin ve sistematik şekilde hazırlanmasını hedefler. Teknik bilgi ile yönetsel bakış açısını birlikte ele alan bu program, sınav başarısının yanı sıra katılımcıların kurumlarında bilgi güvenliği süreçlerine doğrudan değer katabilecek yetkinlikler kazanmasını sağlar.

Kimler Katılmalı?

- Bilgi Güvenliği Yöneticileri
- Siber Güvenlik Uzmanları
- IT Risk, Uyum ve Denetim Profesyonelleri
- Güvenlik Mimarı ve Kıdemli Sistem Yöneticileri

Eğitim İçeriği

Domain 1 – Security & Risk Management (Güvenlik ve Risk Yönetimi)

- Mesleki etik ilkelerini anlama, uygulama ve teşvik etme
    - ISC2 Mesleki Etik Kuralları
    - Kurumsal etik kuralları
- Güvenlik kavramlarını anlama ve uygulama
    - Gizlilik, Bütünlük, Erişilebilirlik
    - Kimlik doğrulama, inkâr edilemezlik
    - Bilgi Güvenliğinin 5 Temel Unsuru
- Güvenlik yönetişimi ilkelerini değerlendirme ve uygulama
- Bilgi güvenliğini bütüncül olarak etkileyen yasal, düzenleyici ve uyum gereksinimlerini anlama
- Soruşturma türlerine ilişkin gereksinimleri anlama
    - İdari
    - Cezai
    - Hukuki
    - Düzenleyici
    - Endüstri standartları
- Güvenlik politika, standart, prosedür ve rehberlerinin geliştirilmesi, dokümante edilmesi ve uygulanması
- İş Sürekliliği gereksinimlerinin belirlenmesi, analiz edilmesi ve uygulanması
    - İş Etki Analizi (BIA)
    - Dış bağımlılıklar
- Güvenlik fonksiyonunun iş stratejisi ile hizalanması
- Kurumsal süreçler ve roller
- Güvenlik kontrol çerçeveleri
    - ISO
    - NIST
    - COBIT
    - SABSA
    - PCI

    - FedRAMP
- Due care / due diligence kavramları
- Siber suçlar ve veri ihlalleri
- Lisanslama ve fikri mülkiyet
- Veri gizliliği ve kişisel veriler
    - GDPR
    - CCPA
    - Kişisel Verilerin Korunması mevzuatları
- Personel güvenliği politika ve süreçleri
    - İşe alım
    - Görev değişikliği
    - İşten ayrılma
- Risk yönetimi kavramları
    - Tehdit ve zafiyet tanımlama
    - Risk analizi ve değerlendirme
    - Risk yanıtı ve risk azaltma
- Tehdit modelleme yaklaşımları
- Tedarik zinciri risk yönetimi
- Güvenlik farkındalık, eğitim ve bilinçlendirme programları
    - Sosyal mühendislik
    - Oltalama (phishing)
    - Güvenlik elçileri
    - Oyunlaştırma

Domain 2 – Asset Security (Varlık Güvenliği)

- Bilgi ve varlıkların tanımlanması ve sınıflandırılması
- Bilgi ve varlıkların işlenmesine yönelik gereksinimlerin belirlenmesi
- Bilgi ve varlıkların güvenli şekilde sağlanması
- Veri yaşam döngüsünün yönetilmesi
    - Toplama
    - Saklama
    - Kullanım
    - Arşivleme
    - İmha
- Varlık saklama süreleri
    - End of Life
    - End of Support
- Veri güvenliği kontrolleri ve uyum gereksinimleri

- Bilgi ve varlık sahipliği
- Varlık envanteri
- Veri rolleri
    - Sahip
    - Sorumlu
    - İşleyen
    - Kullanıcı
- Veri durumları
    - Kullanımda
    - Aktarımda
    - Dinlenir halde
- Veri koruma yöntemleri
    - DRM
    - DLP
    - CASB

Domain 3 – Security Architecture & Engineering (Güvenlik Mimarisi ve Mühendisliği)

- Güvenli tasarım prensipleriyle mühendislik süreçlerinin yönetilmesi
- Güvenlik modellerinin temel kavramları
    - Bell-LaPadula
    - Biba
    - Star Model
- Sistem güvenlik gereksinimlerine göre kontrol seçimi
- Bilgi sistemlerinin güvenlik yetenekleri
    - Bellek koruma
    - TPM
    - Şifreleme
- Güvenlik mimarilerindeki zafiyetlerin değerlendirilmesi
- Kriptografik çözümlerin seçimi ve yönetimi
    - Simetrik / Asimetrik
    - PKI
    - Anahtar yönetimi
    - Dijital imzalar
- Tehdit modelleme
- En az yetki
- Savunmada derinlik
- Zero Trust
- Privacy by Design

- Fiziksel ve tesis güvenliği tasarımı
    - Veri merkezleri
    - Sunucu odaları
    - Yangın önleme
    - Enerji ve HVAC
- Bilgi sistemleri yaşam döngüsü yönetimi
    - Analiz
    - Tasarım
    - Geliştirme
    - Dağıtım
    - İşletim
    - Emeklilik

Domain 4 – Communication & Network Security (İletişim ve Ağ Güvenliği)

- Ağ mimarilerinde güvenli tasarım prensipleri
- Ağ bileşenlerinin güvenliği
- Güvenli iletişim kanallarının uygulanması
    - OSI
    - TCP/IP
    - IPv4 / IPv6
    - IPSec
    - TLS
    - SSH
- Fiziksel ve mantıksal ağ segmentasyonu
    - VLAN
    - VPN
    - Mikro-segmentasyon
- Kablosuz ve mobil ağlar
    - Wi-Fi
    - Bluetooth
    - 4G / 5G
- SDN, VPC, CDN
- Ağ izleme ve yönetimi
- Uç nokta güvenliği
- Uzaktan erişim

Domain 5 – Identity & Access Management (IAM) – Kimlik ve Erişim Yönetimi

- Fiziksel ve mantıksal erişim kontrolü
- Kimlik doğrulama ve yetkilendirme stratejileri

- Federatif kimlik yönetimi
- Yetkilendirme mekanizmaları
    - RBAC
    - ABAC
    - MAC
    - DAC
- MFA, SSO, parola kasaları
- Kimlik yaşam döngüsü
    - Provisioning
    - Deprovisioning
- Ayrıcalıklı hesap yönetimi

Domain 6 – Security Assessment & Testing (Güvenlik Değerlendirmesi ve Testi)

- Güvenlik değerlendirme ve denetim stratejileri
- Kontrol testleri
    - Zafiyet taramaları
    - Penetrasyon testleri
- Log inceleme
- Kod inceleme
- Uyumluluk kontrolleri
- Bulguların raporlanması ve iyileştirme

Domain 7 – Security Operations (Güvenlik Operasyonları)

- Olay yönetimi
- Loglama ve izleme
- SIEM, IDPS
- Tehdit istihbaratı
- Olay müdahalesi
- Felaket kurtarma
- İş sürekliliği
- Fiziksel güvenlik
- Personel güvenliği

Domain 8 – Software Development Security (Yazılım Geliştirme Güvenliği)

- Güvenli Yazılım Geliştirme Yaşam Döngüsü (SDLC)
- Yazılım geliştirme metodolojileri
    - Agile
    - DevOps
    - DevSecOps

- Güvenli kodlama prensipleri
- Uygulama güvenliği testleri
    - SAST
    - DAST
    - IAST
- Açık kaynak ve üçüncü parti yazılım riskleri

Ön Koşullar

Bilgi güvenliği veya IT alanında en az 5 yıl deneyim