CISSP (Certified Information Systems Security Professional) Eğitimi

Süre: 5 Gün

Kurumsal CISSP Eğitimi Hakkında

Deneyimli bilgi güvenliği ekipleri için 5 günlük CISSP eğitim programı

CISSP (Certified Information Systems Security Professional) Eğitimi, bilgi güvenliği alanında çalışan profesyonellerin güvenliği teknik ve yönetsel boyutlarıyla birlikte değerlendirmesine odaklanır. Program; kurumsal risk yönetimi, varlıkların korunması, güvenlik mimarisi, ağ güvenliği, kimlik yönetimi, güvenlik operasyonları ve güvenli yazılım geliştirme konularını kapsar.

Eğitim içeriği, CISSP bilgi birikiminin sekiz alanı etrafında yapılandırılmıştır. Katılımcılar bir kurumun güvenlik yaklaşımını tasarlarken politika, süreç, teknoloji ve insan unsurlarının nasıl birlikte ele alınacağını inceler. Program aynı zamanda CISSP sertifikasyon sınavındaki konu başlıklarına sistematik biçimde hazırlanmayı amaçlar.

Eğitim sonunda katılımcılar:

- Kurumsal bilgi güvenliği ve risk yönetimi kararlarını daha geniş bir çerçevede değerlendirebilir.
- Bilgi varlıklarını sınıflandırma ve yaşam döngüleri boyunca koruma yaklaşımlarını açıklayabilir.
- Güvenlik mimarisi, ağ güvenliği ve kimlik yönetimi kontrolleri arasındaki ilişkiyi yorumlayabilir.
- Güvenlik değerlendirmesi, olay müdahalesi ve iş sürekliliği süreçlerini birlikte ele alabilir.
- Güvenli yazılım geliştirme yaşam döngüsündeki temel riskleri ve kontrolleri inceleyebilir.
- CISSP sınavının kapsadığı sekiz güvenlik alanındaki bilgilerini gözden geçirebilir.

CISSP Eğitimi İçeriği

Alan 1: Güvenlik ve Risk Yönetimi (Security & Risk Management)

- ISC2 mesleki etik kuralları ve kurumsal etik ilkeleri
- Gizlilik, bütünlük ve erişilebilirlik; kimlik doğrulama ve inkâr edilemezlik

- Güvenlik yönetişimi ve güvenlik fonksiyonunun iş stratejisiyle uyumu
- Yasal, düzenleyici ve kurumsal uyum gereksinimleri
- İdari, cezai, hukuki ve düzenleyici soruşturmalara ilişkin gereksinimler
- Güvenlik politika, standart, prosedür ve rehberlerinin hazırlanması
- İş sürekliliği gereksinimleri, iş etki analizi (BIA) ve dış bağımlılıklar
- Kurumsal güvenlik rolleri ve ISO, NIST, COBIT, SABSA, PCI ve FedRAMP gibi kontrol çerçeveleri
- Due care ve due diligence kavramları
- Siber suçlar, veri ihlalleri, lisanslama ve fikri mülkiyet
- GDPR, CCPA ve kişisel verilerin korunmasına ilişkin gereksinimler
- İşe alım, görev değişikliği ve işten ayrılma süreçlerinde personel güvenliği
- Tehdit ve zafiyetlerin belirlenmesi; risk analizi, risk yanıtı ve risk azaltma
- Tehdit modelleme ve tedarik zinciri risk yönetimi
- Sosyal mühendislik, oltalama ve güvenlik farkındalığı programları

Alan 2: Varlık Güvenliği (Asset Security)

- Bilgi ve varlıkların tanımlanması, envanteri ve sınıflandırılması
- Bilginin işlenmesine yönelik güvenlik gereksinimleri
- Veri yaşam döngüsü: toplama, saklama, kullanım, arşivleme ve imha
- Saklama süreleri ile kullanım ve destek ömrü sonu kavramları
- Veri güvenliği kontrolleri ve uyum gereksinimleri
- Bilgi ve varlık sahipliği; sahip, sorumlu, işleyen ve kullanıcı rolleri
- Kullanımda, aktarımda ve saklama hâlindeki verinin korunması
- DRM, DLP ve CASB gibi veri koruma yöntemleri

Alan 3: Güvenlik Mimarisi ve Mühendisliği (Security Architecture & Engineering)

- Güvenli tasarım prensipleri ve mühendislik süreçleri
- Bell-LaPadula, Biba ve Star Model gibi güvenlik modelleri
- Sistem güvenlik gereksinimlerine göre kontrol seçimi
- Bellek koruma, TPM ve şifreleme gibi güvenlik yetenekleri
- Güvenlik mimarilerindeki zafiyetlerin değerlendirilmesi
- Simetrik ve asimetrik şifreleme, PKI, anahtar yönetimi ve dijital imzalar
- Tehdit modelleme, en az yetki ve savunmada derinlik
- Zero Trust ve Privacy by Design yaklaşımları
- Veri merkezi, sunucu odası, yangın önleme, enerji ve HVAC kapsamında fiziksel güvenlik
- Bilgi sistemlerinin analizden kullanım ömrü sonuna kadar güvenli yönetimi

Alan 4: İletişim ve Ağ Güvenliği (Communication & Network Security)

- Ağ mimarilerinde güvenli tasarım ve ağ bileşenlerinin korunması
- OSI, TCP/IP, IPv4 ve IPv6 temelleri
- IPSec, TLS ve SSH ile güvenli iletişim
- VLAN, VPN ve mikro segmentasyon ile ağların ayrılması
- Wi-Fi, Bluetooth ve mobil ağ güvenliği
- SDN, VPC ve CDN yaklaşımları
- Ağ izleme, uç nokta güvenliği ve uzaktan erişim

Alan 5: Kimlik ve Erişim Yönetimi (Identity & Access Management)

- Fiziksel ve mantıksal erişim kontrolleri
- Kimlik doğrulama ve yetkilendirme stratejileri
- Federatif kimlik yönetimi
- RBAC, ABAC, MAC ve DAC yetkilendirme modelleri
- Çok faktörlü kimlik doğrulama (MFA), tek oturum açma (SSO) ve parola kasaları
- Kimlik yaşam döngüsü, hesap açma ve erişimi sonlandırma süreçleri
- Ayrıcalıklı hesapların yönetimi

Alan 6: Güvenlik Değerlendirmesi ve Testi (Security Assessment & Testing)

- Güvenlik değerlendirmesi ve denetim stratejileri
- Güvenlik kontrollerinin test edilmesi
- Zafiyet taramaları ve penetrasyon testleri
- Log ve kod incelemeleri
- Uyum kontrolleri
- Bulguların raporlanması ve iyileştirme çalışmalarının takibi

Alan 7: Güvenlik Operasyonları (Security Operations)

- Güvenlik olaylarının yönetimi
- Loglama, izleme, SIEM ve IDPS
- Tehdit istihbaratı ve olay müdahalesi
- Felaket kurtarma ve iş sürekliliği
- Fiziksel güvenlik ve personel güvenliği

Alan 8: Yazılım Geliştirme Güvenliği (Software Development Security)

- Güvenli Yazılım Geliştirme Yaşam Döngüsü (SDLC)
- Agile, DevOps ve DevSecOps yaklaşımlarının güvenlikle ilişkisi
- Güvenli kodlama prensipleri
- SAST, DAST ve IAST uygulama güvenliği testleri
- Açık kaynak ve üçüncü taraf yazılım riskleri

Kurumsal CISSP Eğitimine Kimler Katılmalı?

Program; bilgi güvenliği yöneticileri, siber güvenlik uzmanları, BT risk, uyum ve denetim profesyonelleri, güvenlik mimarları ve kıdemli sistem yöneticileri için uygundur. Eğitim, güvenlik kararlarını kurum genelinde ortak bir çerçevede ele almak isteyen deneyimli ekipler tarafından değerlendirilebilir.

Yazılım ekiplerinin güvenli geliştirme uygulamalarına ayrıca odaklanması gerekiyorsa Güvenli Yazılım Geliştirme Eğitimi de incelenebilir.

Eğitim Katılım Ön Koşulları

Bu eğitim için bilgi güvenliği veya BT alanında **en az 5 yıl deneyim** belirtilmektedir. ISC2 tarafından uygulanan CISSP sertifikasyon deneyimi koşulları ayrıca değerlendirilmelidir.