

## CompTIA CASP + Eğitimi

### Eğitim Hakkında

CompTIA CASP + (CompTIA Advanced Security Practitioner) eğitimi, katılımcılara dayanıklı bir kuruluşu desteklemek için karmaşık ortamlarda güvenli çözümleri nasıl kavramsallaştıracaklarını, tasarlayacaklarını, entegre edeceklerini ve uygulayacaklarını öğretir.

### Neler Öğreneceksiniz

Tüm katılımcılar aşağıdakilerin nasıl yapıldığını öğreneceklerdir:

- Risk yönetimine vurgu yaparak kuruluşta BT yönetişimini desteklemeyi
- Kurumsal güvenliği desteklemek için işbirliği araçlarından ve teknolojisinden yararlanmayı
- İşletmeyi güvence altına almak için araştırma ve analizi kullanmayı
- Gelişmiş kimlik doğrulamayı ve yetkilendirme tekniklerini entegre etmeyi
- Kriptografik teknikleri, ana bilgisayarlar için güvenlik kontrollerini, mobil cihazlar için güvenlik kontrollerini uygulamayı, ağ güvenliğini uygulamayı ve sistemlerde ve yazılım geliştirme yaşam döngüsünde güvenlik uygulamayı
- Güvenli bir kurumsal mimaride ana makineleri, depolamayı, ağları, uygulamaları, sanal ortamları ve bulut teknolojilerini entegre etmeyi
- Güvenlik değerlendirmeleri yürütmeyi
- Güvenlik olaylarına yanıt vermeyi ve olaylardan kurtulmayı

### Eğitim İçeriği

#### Giriş

#### **BT Yönetişimini ve Risk Yönetimini Destekleme**

- BT Yönetişiminin ve Risk Yönetiminin Önemini Belirleyin
- Risk belirleme
- Riski azaltmak
- Belgeleri Risk Yönetimine Entegre Edin

#### **Güvenliği Desteklemek İçin İşbirliğinden Yararlanma**

- İş Birimlerinde İşbirliğini Kolaylaştırın
- Güvenli İletişim ve İşbirliği Çözümleri

#### **İşletmeyi Güvenceye Almak İçin Araştırma ve Analizi Kullanma**

- Sektör Trendlerini ve İşletme Üzerindeki Etkilerini Belirleyin
- İşletmeyi Güvenceye Almak İçin Senaryoları Analiz Edin

### **Gelişmiş Kimlik Doğrulama ve Yetkilendirme Tekniklerini Entegre Etme**

Kimlik Doğrulama ve Yetkilendirme Teknolojilerini Uygulama  
Gelişmiş Kimlik ve Erişim Yönetimini Uygulayın

### **Kriptografik Tekniklerin Uygulanması**

Şifreleme Tekniklerini Seçin  
Kriptografiyi Uygulama

### **Ana Bilgisayarlar için Güvenlik Kontrollerinin Uygulanması**

Ana Bilgisayar Donanım ve Yazılımını Seçin  
Harden Ana Bilgisayarları  
Sunucuları ve Masaüstlerini Sanallaştırın  
Önyükleme Yükleyicilerini Koruyun

### **Mobil Cihazlar için Güvenlik Kontrollerinin Uygulanması**

Mobil Cihaz Yönetimini Uygulayın  
Mobil Cihazlar için Güvenlik ve Gizlilik Endişelerini Ele Alın

### **Ağ Güvenliğinin Uygulanması**

Ağ Güvenliği Bileşenlerinin ve Cihazlarının Dağıtımını Planlayın  
Ağ Destekli Cihazların Dağıtımını Planlayın  
Gelişmiş Ağ Tasarımını Uygulayın  
Ağ Güvenliği Kontrollerini Uygulayın

### **Sistemler ve Yazılım Geliştirme Yaşam Döngüsünde Güvenliği Uygulama**

Teknoloji Yaşam Döngüsü boyunca Güvenliği Uygulayın  
Genel Uygulama Güvenlik Açıklarını Belirleyin  
Web Uygulaması Güvenlik Açıklarını Tanımlayın  
Uygulama Güvenliği Kontrollerini Uygulayın

### **Varlıkları Güvenli Kurumsal Mimariye Entegre Etme**

Standartları ve En İyi Uygulamaları Kurumsal Güvenlikte Entegre Edin  
Teknik Dağıtım Modellerini Seçin  
Bulutla Artırılmış Güvenlik Hizmetlerini Entegre Edin  
Kurumsal Altyapının Tasarımını Güvenli Hale Getirin  
Veri Güvenliğini Kurumsal Mimariye Entegre Edin  
Kurumsal Uygulamaları Güvenli Bir Mimaride Entegre Edin

### **Güvenlik Değerlendirmelerinin Yapılması**

Güvenlik Değerlendirme Yöntemlerini Seçin  
Uygun Araçlarla Güvenlik Değerlendirmeleri Gerçekleştirin

### **Olaylara Müdahale Etme ve Olaylardan Kurtulma**

Olay Müdahalesi ve Adli Soruşturmalar için Hazırlık  
Olaylara Müdahale ve Adli Analiz Yürütme