Check Point Security Administration (CCSA) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Check Point Security Administration (CCSA) eğitimi, bir **Check Point Quantum Security Environment** ortamının yapılandırılması, yönetilmesi ve izlenmesi için gerekli temel kavramları, araçları ve yönetim süreçlerini öğretir.

Katılımcılar eğitim boyunca **Gaia Portal**, **Gaia Command Line Interface**, **SmartConsole** ve Check Point'in üç katmanlı mimarisi üzerinde uygulamalı çalışmalar gerçekleştirir. Eğitim; nesne yönetiminden güvenlik politikalarına, ordered ve inline layer yapılarından HTTPS Inspection, Identity Awareness, Application Control, URL Filtering ve Autonomous Threat Prevention gibi güvenlik özelliklerine kadar geniş bir içeriği kapsar.

Yönlendirmeli laboratuvarlar ve gerçek çalışma senaryoları sayesinde katılımcılar, bir Quantum ortamını güvenli şekilde yönetme, optimize etme, izleme ve sürdürme konusunda pratik deneyim kazanır.

Önkoşullar

Katılımcıların aşağıdaki alanlarda temel bilgi sahibi olmaları önerilir:

- Unix benzeri ve Windows işletim sistemleri
- İnternet teknolojilerinin temel kavramları
- Ağ teknolojileri
- Ağ güvenliği prensipleri
- Sistem yönetimi
- TCP/IP ağ yapısı

Kimler Katılmalı

Bu eğitim özellikle aşağıdaki roller için uygundur:

- Güvenlik yöneticileri
- Güvenlik mühendisleri
- Güvenlik analistleri
- Güvenlik danışmanları
- Güvenlik mimarları

Eğitim içeriği ayrıca NIST/NICE kapsamında yer alan **Implementation and Operation** ile **Protection and Defence** iş rolü kategorileriyle de uyumludur.

Check Point Security Administration (CCSA) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Neler Öğreneceksiniz

Eğitimin sonunda katılımcılar:

- Check Point üç katmanlı mimarisini ve bu mimarinin Quantum Security Environment içerisindeki rolünü açıklayabilecek,
- Gaia Portal, Gaia CLI ve temel SmartConsole ekranlarında etkin şekilde çalışabilecek,
- Yönetici hesapları, yetki profilleri ve eş zamanlı oturum kontrollerini oluşturup yönetebilecek,
- SmartConsole içerisinde fiziksel ve mantıksal nesneler oluşturarak güvenlik politikalarını destekleyebilecek,
- Kurumsal erişim gereksinimlerine uygun güvenlik politikaları oluşturabilecek, değiştirebilecek ve doğrulayabilecek,
- Trafik denetiminin doğruluğunu artırmak amacıyla ordered ve inline layer yapılarını uygulayıp test edebilecek,
- SmartConsole ve Gaia araçlarını kullanarak sistem performansını, logları, olayları ve platform durumunu izleyebilecek,
- Identity Awareness bileşenlerini yapılandırarak kullanıcı kimliğini güvenlik politikalarına dahil edebilecek,
- Şifreli trafiğin görünürlüğünü artırmak için HTTPS Inspection özelliğini etkinleştirip ayarlayabilecek,
- Application Control ve URL Filtering özelliklerini kullanarak uygulama ve web erişimini yönetebilecek,
- Autonomous Threat Prevention özelliğini etkinleştirip sonuçlarını doğrulayabilecektir.

Eğitim İçeriği

Quantum Security'ye Giriş

Bu bölümde Check Point Quantum ortamının temel mimarisi ve yönetim araçları tanıtılır.

- Check Point üç katmanlı mimarisine genel bakış
- Management, Log Server ve Gateway bileşenleri arasındaki etkileşim
- Temel SmartConsole ekranlarında gezinme
- Management Server, Log Server ve Gateway Cluster üzerinde Gaia erişimi ve inceleme

Laboratuvar Çalışmaları

- Management, Log Server ve Gateway sistemlerinde Gaia ortamını inceleme
- SmartConsole bağlantısı oluşturma
- Gateways & Servers ekranında gezinme
- Security Policies ekranlarını inceleme
- Logs & Events bölümünde çalışma
- Manage & Settings ekranlarını kullanma

Yönetici Hesaplarının Yönetimi

SmartConsole üzerindeki yönetici hesaplarının ve oturum yönetiminin çalışma mantığı ele alınır.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- SmartConsole administrator hesaplarının amacı
- Session management
- Eş zamanlı yönetim yetenekleri
- Yönetici profillerinin atanması

Laboratuvar Çalışmaları

- Yönetici hesapları oluşturma ve profiller atama
- Yönetici yetkilerini ve session kontrollerini test etme
- Eş zamanlı oturumları yönetme
- Başka bir yöneticinin oturumunu devralma

Nesne Yönetimi

SmartConsole içerisinde kullanılan nesnelerin yapısı ve güvenlik politikalarındaki rolü incelenir.

- SmartConsole nesnelerinin amacı ve çalışma biçimi
- Fiziksel ve mantıksal nesne türleri
- Nesnelerin güvenlik politikalarında kullanılması

Laboratuvar Çalışmaları

- Gateway ve Server nesnelerini görüntüleme ve değiştirme
- Network nesnelerini yönetme
- Service nesnelerini görüntüleme ve güncelleme

Güvenlik Politikalarının Yönetimi

Kurumsal erişim kontrollerinin oluşturulması ve yönetilmesi için kullanılan güvenlik politikaları ele alınır.

- Security Policy kavramı ve amacı
- Bir politika kuralının temel bileşenleri
- Politika yapılandırmasını ve yönetimini kolaylaştıran özellikler

Laboratuvar Çalışmaları

- Mevcut güvenlik politikasını doğrulama
- Policy Rule'ları değiştirme
- Standard Policy kurulumu
- Güvenlik kurallarının sonuçlarını test etme

Policy Layer Yapıları

Trafik denetimini daha esnek ve doğru hale getiren farklı policy layer yapıları incelenir.

- Ordered Policy Layer kavramı

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Layer yapılarının trafik denetimine etkisi
- DMZ Layer gibi inline layer yapıların oluşturulması

Laboratuvar Çalışmaları

- Ordered Layer ekleme
- Ordered Layer kurallarını yapılandırma ve devreye alma
- Policy Layer davranışını test etme
- Inline DMZ Layer oluşturma
- Inline layer sonuçlarını test etme

Güvenlik Operasyonlarının İzlenmesi

Check Point ortamında loglama, sistem durumu ve güvenlik bileşenlerinin izlenmesi ele alınır.

- Monitoring işlemlerinin amacı
- Log Server yapılandırması ve optimizasyonu
- Log sorgulama ve filtreleme
- Sistem durumu ve blade statülerinin izlenmesi

Laboratuvar Çalışmaları

- Log Management ayarlarını yapılandırma
- Rulebase görünümünü ve logging davranışlarını geliştirme
- Logları inceleme ve hedefli aramalar gerçekleştirme
- Monitoring Blade yapılandırması
- Sistem durumunu izleme

Identity Awareness

Kullanıcı kimliklerinin güvenlik politikalarına dahil edilmesini sağlayan Identity Awareness özelliği incelenir.

- Identity Awareness'ın amacı ve çalışma prensibi
- Temel bileşenler ve kimlik kaynakları
- Kullanıcı kimliğinin güvenlik politikasına entegre edilmesi

Laboratuvar Çalışmaları

- Güvenlik politikasını Identity Awareness için uyarlama
- Identity Collector yapılandırması
- User Access Role tanımlama
- Kimlik tabanlı erişimi test etme

HTTPS Inspection

Şifreli HTTPS trafiğinin güvenlik amacıyla denetlenmesi ele alınır.

- HTTPS Inspection'ın amacı
- Temel bileşenler
- Yapılandırma yaklaşımı

Laboratuvar Çalışmaları

- HTTPS Inspection özelliğini etkinleştirme
- Access Control kurallarını düzenleme
- Gateway sertifikasını dağıtma
- Inspection etkin durumdayken politika davranışını test etme ve analiz etme

Application Control ve URL Filtering

Uygulama ve web erişimlerinin merkezi güvenlik politikalarıyla yönetilmesi incelenir.

- Application Control özelliğinin amacı
- URL Filtering çalışma yapısı
- Temel yapılandırma akışı

Laboratuvar Çalışmaları

- Access Control Policy üzerinde gerekli değişiklikleri yapma
- Application ve URL Filtering kuralları oluşturma
- Mevcut kuralları değiştirme
- Kuralları test etme ve iyileştirme

Threat Prevention Temelleri

Quantum ortamında tehdit önleme yetenekleri ele alınır.

- Autonomous Threat Prevention'ın amacı
- Threat Prevention çözümünün temel bileşenleri

Laboratuvar Çalışmaları

- Autonomous Threat Prevention özelliğini etkinleştirme
- Threat Prevention sonuçlarını test etme

Sınavlar ve Değerlendirme

Bu eğitim, katılımcıları **Exam 156-215.82** sınavına hazırlamaya yöneliktir.

Eğitim sürecinin içerisinde ayrıca bir resmî sınav uygulanmaz. Bunun yerine katılımcılar, teorik bilgiyi pekiştirmek ve uygulama becerilerini geliştirmek amacıyla eğitim boyunca:

- Yapılandırılmış laboratuvar çalışmaları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Bilgi kontrolü aktiviteleri
- Uygulamalı doğrulama çalışmaları

gerçekleştirir.

Uygulamalı Öğrenme

Eğitimin önemli bir bölümü uygulamalı laboratuvar çalışmalarından oluşur. Katılımcılar Check Point ortamında doğrudan yapılandırma yaparak aşağıdaki konularda pratik deneyim kazanır:

- Gaia yönetimi
- SmartConsole kullanımı
- Güvenlik politikası yönetimi
- Identity Awareness
- HTTPS Inspection
- Application Control
- URL Filtering
- Autonomous Threat Prevention
- Loglama ve sistem izleme

Eğitmenler, laboratuvar çalışmaları sırasında katılımcılara yapılandırma, sorun giderme ve yapılan işlemlerin doğrulanması konularında destek sağlar.