Check Point Security Engineering (CCSE) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Check Point Security Engineering (CCSE) eğitimi, karmaşık **Check Point Quantum Security Environment** yapılarının kurulması, yönetilmesi ve izlenmesi konusunda ileri seviye bilgi ve uygulama deneyimi kazandırır.

Eğitim, temel Check Point yönetim yetkinliklerinin üzerine inşa edilir ve katılımcıları yüksek erişilebilirlik, gelişmiş politika yönetimi, dağıtık yapılarda güvenli bağlantı, yükseltme, taşıma ve kümeleme gibi daha ileri operasyonel konulara taşır.

Katılımcılar eğitim boyunca **Management High Availability**, gelişmiş ve dinamik politika bileşenleri, manuel NAT kuralları, site-to-site VPN, SmartEvent, Compliance Blade, gateway ve management server yükseltmeleri, veritabanı taşıma işlemleri ve **ElasticXL Cluster** kurulumu gibi konularda uygulamalı çalışmalar gerçekleştirir.

Yönlendirmeli laboratuvarlar ve yapılandırılmış uygulamalar sayesinde katılımcılar, yüksek performanslı, ölçeklenebilir ve dayanıklı Check Point güvenlik ortamlarını yönetmek için gereken ileri seviye operasyonel becerileri geliştirir.

Prerequisites

Katılımcıların aşağıdaki bilgi ve deneyime sahip olmaları beklenir:

- Unix benzeri ve Windows işletim sistemleri konusunda deneyim
- İnternet teknolojilerinin temelleri hakkında bilgi
- Ağ ve ağ güvenliği bilgisi
- Sistem yönetimi deneyimi
- TCP/IP ağ bilgisi
- Unix benzeri ortamlarda metin editörleriyle çalışma deneyimi
- Quantum Security Environment yönetiminde en az altı aylık uygulamalı deneyim

Gerekli hazırlık: Check Point Certified Security Administrator düzeyinde bilgi ve hazırlık.

Who Should Attend

Bu eğitim özellikle aşağıdaki profesyoneller için uygundur:

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

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

Check Point Security Engineering (CCSE) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Eğitimin sonunda katılımcılar:

- Dayanıklılık ve iş sürekliliğini artırmak için Management High Availability yapısını kurup yapılandırabilecek,
- Gelişmiş nesne türleri, dynamic object'ler ve manuel NAT kurallarıyla güvenlik politikalarını geliştirebilecek,
- Dağıtık ortamlarda management behind NAT yapılandırmasını uygulayıp doğrulayabilecek,
- Dahili olarak yönetilen gateway'ler ve gelişmiş kimlik doğrulama seçenekleriyle site-to-site VPN oluşturabilecek,
- VPN tunnel trafiğini analiz ederek link selection, ISP redundancy ve tunnel management özelliklerini uygulayabilecek,
- SmartEvent ve Compliance Blade gibi gelişmiş izleme araçlarını kullanarak event, alert, pattern ve uyumluluk verilerini analiz edebilecek,
- Security gateway'leri yükseltebilecek ve Central Deployment aracıyla hotfix kurabilecek,
- Dağıtık yapılarda gelişmiş management server yükseltmeleri ve database migration işlemleri gerçekleştirebilecek,
- Ölçeklenebilirlik ve yüksek erişilebilirliği artırmak amacıyla ElasticXL Cluster kurup yapılandırabilecek,
- Uygulamalı senaryolar aracılığıyla güvenlik duruşunu ve operasyonel performansı doğrulayabilecektir.

Outline

Management High Availability

Bu bölümde Check Point yönetim katmanında yüksek erişilebilirliğin amacı, yapısı ve uygulama gereksinimleri ele alınır.

- Management High Availability'ın amacı
- Temel bileşenler
- Kurulum ve devreye alma sırasında dikkate alınması gereken noktalar

Laboratuvar Çalışmaları

- Management High Availability kurulumu
- High Availability yapılandırması
- Failover davranışının doğrulanması
- Yüksek erişilebilirlik fonksiyonlarının test edilmesi

Gelişmiş Politika Yönetimi

Bu bölümde güvenlik politikalarının daha esnek ve dinamik hale getirilmesini sağlayan ileri seviye yapılandırmalar incelenir.

- Gelişmiş nesne türleriyle güvenlik politikalarının geliştirilmesi
- Gateway-updatable policy'ler için dynamic object oluşturulması

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- NAT kurallarının manuel olarak tanımlanması
- Dağıtık yapılarda management behind NAT yapılandırması

Laboratuvar Çalışmaları

- Updatable object kullanımı
- Server object'leri için NAT yapılandırması
- Network object'leri için NAT yapılandırması
- Branch office bağlantıları için management behind NAT kurulumu

Site-to-Site VPN

Dağıtık ağlar arasında güvenli iletişim kurulmasına yönelik site-to-site VPN yapıları ele alınır.

- Site-to-site VPN kavramları ve deployment modelleri
- VPN community yapıları
- VPN trafik akışının analizi
- Pre-shared key tabanlı kimlik doğrulama
- Certificate tabanlı kimlik doğrulama
- Link selection
- ISP redundancy
- Tunnel management davranışları

Laboratuvar Çalışması

- Dahili olarak yönetilen security gateway'ler kullanarak site-to-site VPN yapılandırılması

Gelişmiş Güvenlik İzleme

Bu bölümde olayların, uyarıların ve güvenlik davranışlarının daha ayrıntılı analiz edilmesini sağlayan Check Point araçları ele alınır.

- SmartEvent'in amacı ve yetenekleri
- Compliance Blade fonksiyonları
- Event analizi
- Alert yapılandırması
- Pattern monitoring
- Uyumluluk raporlaması

Laboratuvar Çalışmaları

- SmartEvent Server yapılandırılması
- Event ve alert tanımlarının oluşturulması
- SmartEvent raporlarının çalıştırılması
- Compliance Blade'in etkinleştirilmesi
- Best practice ayarlarının ve uyarıların incelenmesi
- Regulatory compliance score değerlerinin doğrulanması

Yükseltmeler

Check Point ortamlarında desteklenen yükseltme yöntemleri ve süreçleri ele alınır.

- Desteklenen upgrade yöntemleri
- Upgrade workflow'larının değerlendirilmesi

Laboratuvar Çalışmaları

- Bir security gateway'in yükseltilmesi
- Central Deployment aracıyla hotfix kurulması

Gelişmiş Yükseltme ve Migration İşlemleri

Bu bölümde management server yükseltmeleri ve veritabanı taşıma süreçleri incelenir.

- Management database export işlemi
- Management database import işlemi
- Yeni release veya appliance kullanılarak management server upgrade edilmesi

Laboratuvar Çalışmaları

- Dağıtık ortamda database migration içeren gelişmiş upgrade için hazırlık yapılması
- Primary Security Management Server import işleminin gerçekleştirilmesi

ElasticXL Cluster

Bu bölümde Check Point'in ölçeklenebilirlik ve yüksek erişilebilirlik ihtiyaçlarına yönelik ElasticXL Cluster yapısı ele alınır.

- ElasticXL Cluster'ın amacı
- Tasarım yaklaşımı
- Deployment sırasında dikkate alınması gereken unsurlar
- Operasyonel çalışma davranışları

Laboratuvar Çalışması

- ElasticXL Security Gateway Cluster kurulumu

Sınavlar ve Değerlendirme

Bu eğitim, katılımcıları **Certification Exam 156-315.82** sınavına hazırlamaya yöneliktir.

Eğitim kapsamında ayrı bir resmî sınav uygulanmaz. Bunun yerine katılımcılar, ileri seviye yönetim

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

yetkinliklerini geliştirmek ve doğrulamak amacıyla:

- Uygulamalı laboratuvar görevleri
- Yapılandırılmış egzersizler
- Gerçek çalışma senaryoları

üzerinde çalışır.

Uygulamalı Öğrenme

Eğitimin önemli bir bölümü ileri seviye laboratuvar çalışmalarından oluşur. Katılımcılar gerçek dünyaya yakın senaryolar üzerinden aşağıdaki alanlarda uygulama yapar:

- High Availability yönetimi
- Gelişmiş politika yapılandırması
- NAT
- Site-to-site VPN
- SmartEvent
- Compliance Blade
- Gateway upgrade
- Hotfix deployment
- Management server migration
- Database migration
- ElasticXL Cluster deployment

Eğitmenler uygulamalar boyunca katılımcılara yapılandırma, sorun giderme, doğrulama ve ileri seviye operasyonel kararlar konusunda rehberlik eder.