CHECK POINT™

Horizon

# Horizon XDR/XPR
## Genişletilmiş Önleme ve Müdahale

## Önlemeye Odaklı Lider XDR/XPR Çözümü

Horizon XDR/XPR, ağlar, uç noktalar, mobil cihazlar, bulut ve e-posta dahil tüm ortamlardaki tehditleri önlemek için Check Point veya üçüncü taraf güvenlik çözümleriyle entegre çalışan bir güvenlik operasyonları platformudur.

Platform, BT ortamının herhangi bir bölümünde ortaya çıkan siber tehditleri anında engeller ve bunların kuruluşa veya diğer sistemlere yayılmasını önler.

XDR/XPR, tüm güvenlik altyapısı genelinde iş birliğine dayalı, yapay zekâ destekli korelasyon sayesinde kapsamlı tehdit önleme sağlar.

### Kapsamlı Tehdit Önleme

Tüm güvenlik altyapısında doğru saldırı önleme

### İş Birliğine Dayalı Tehdit ve Olay Korelasyonu

İş birliğine dayalı, akıllı yapay zekâ

### Birleşik Analitik

Saldırı davranışı, bağlam ve etkilerine ilişkin görünürlük sağlayarak güvenlik

OTD BİLİŞİM
GLOBAL VAD

# Ağlar, Uç Noktalar, Bulut ve E-posta Üzerindeki Bilinen ve Sıfırıncı Gün Saldırılarını Önleyin

XDR/XPR, siber savunmadaki son hattınızı temsil eder — birleşik güvenlik altyapınızda ek bir koruma katmanı sağlar. Horizon XDR/XPR, güvenlik ortamının farklı bölümlerinde birbirinden bağımsız gibi görünen olayları birleştirerek, kuruluşunuz için kritik tehditlere dönüşebilecek karmaşık saldırıları önler.

Platform, tehditlerin kuruluş içinde yayılmasını otomatik olarak durdurabilir ve SecOps kullanıcıları için ek adli analiz (forensics) sunarak olay doğrulamasını kolaylaştırır.

• Kapsamlı Tehdit Önleme
Check Point ve üçüncü taraf güvenlik çözümleriyle entegre biçimde çalışan, tüm güvenlik altyapısında otomatik ve doğru saldırı önleme sağlar.

• Akıllı Tehdit ve Olay Korelasyonu
Yapay zekâ ve tehdit istihbaratından güç alır; Check Point ve üçüncü taraf verilerini bağlamsal olarak ilişkilendirir.

• Birleşik Analitik
Saldırı davranışı, bağlam ve etkilerine dair görünürlük sunarak güvenlik duruşunu güçlendirir; saldırının kill chain içindeki konumunu anlamanızı sağlar.

# İş Birliğine Dayalı, Yapay Zekâ Tabanlı Korelasyon ile Güçlendirilmiş Önleme

Geniş kapsamlı görünürlük ve tehdit korelasyonu sayesinde platform, birden fazla veri kümesini ilişkilendirerek tehditleri tespit etme yeteneğine sahiptir. Saldırıların önlenmesinde kullanılan veri kaynakları şunları içerir:

• Ağlar, uç noktalar, mobil cihazlar, bulut ve e-posta arasında paylaşılır. Örneğin, e-postada tespit edilen şüpheli bir bağlantı (URL), mobil, uç nokta, bulut ve ağ sistemlerinde de otomatik olarak engellenir.

• Check Point'in 150.000 güvenlik ağ geçidi ve milyonlarca uç noktadan gelen IoC'ler (Indicators of Compromise) ile güçlendirilmiştir.

• CP<R> Tehdit Araştırma Ekibi: Yüzlerce uzman tehdit analistinden oluşan bu ekip, tersine mühendislik (reverse engineering) kullanarak yeni siber saldırı türlerini öngörür ve veri tabanına ekler; böylece gelecekteki saldırıların önüne geçilmesini sağlar.

• Potansiyel bir tehdidi işaret edebilecek anormal davranışları tanımlamak için kullanıcı ve sistem davranışlarını analiz eder.

• Üçüncü taraf güvenlik üreticilerinden sağlanan ek tehdit istihbaratını kullanarak genel tehdit tespitini zenginleştirir.

Horizon XDR/XPR, birbirinden bağımsız gibi görünen zararsız olayları ilişkilendirerek ustaca gizlenmiş önemli tehditleri ortaya çıkarma konusunda benzersiz bir yeteneğe sahiptir ve diğer çözümlerin tespit edemeyeceği tehditleri önceden engeller.

Horizon
XDR/XPR