# IBM QRadar

IBM® QRadar®, güvenlik ekiplerinin olayları daha verimli şekilde yönetip yanıtlamasına yardımcı olmak için tasarlanmış tehdit tespit ve müdahale çözümüdür. Kurumsal ölçekli operasyonları destekler ve kuruluşların temel teknolojilerinde güvenlik duruşlarını güçlendirmelerini sağlar.

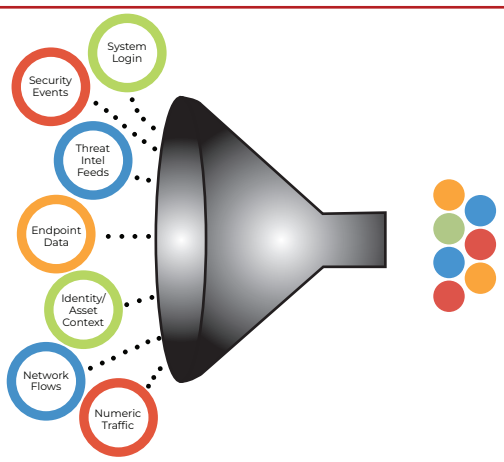
**2025 Veri İhlali Maliyet Raporu**
Saldırganlar yapay zekâyı hedef alıyor ve yapay zekâ ile ilgili veri ihlali yaşayan kuruluşların %97'sinde uygun erişim kontrolleri bulunmuyor.

## Özellikler

**Kullanıcı Davranış Analitiği**
IBM QRadar SIEM User Behavior Analytics (UBA), çalışanlarınız için davranış kalıplarını temel alan bir profil oluşturur. Böylece kuruluşunuza yönelik tehditleri daha etkili tespit edebilirsiniz. QRadar SIEM'deki mevcut verileri kullanarak kullanıcılar ve riskler hakkında yeni içgörüler üretir.

**Veri Toplama**
Sadece birkaç tıklamayla, veri toplayıcı telemetri verilerinin kolayca kurulmasını ve alınmasını sağlar. Pasif protokoller belirli portlardaki olayları dinlerken, aktif protokoller API'ler veya diğer iletişim yöntemleriyle harici telemetri kaynaklarına bağlanarak olayları toplar.

**Ağ Tespiti ve Müdahale (NDR)**
NDR, ağ aktivitelerini gerçek zamanlı analiz ederek güvenlik ekiplerinize destek olur. Derinlemesine ve kapsamlı görünürlüğü, kaliteli veri ve analitikle birleştirerek uygulanabilir içgörüler sunar ve etkili müdahaleyi mümkün kılar.




## IBM® QRadar® SIEM

Kuruluşların güvenliği tek merkezden yönetmesini sağlar: gerçek zamanlı tehdit tespiti, kolaylaştırılmış uyumluluk süreçleri ve düşen operasyonel maliyetlerle kontrolü elinize alın. QRadar SIEM, güvenlik ekiplerinizi olaylar büyümeden daha hızlı ve etkili yanıt vermeleri için güçlendirir.

- 14.000+ saat tasarruf – Tekrarlayan işler azalıyor, ekip kritik konulara odaklanıyor.
- %90 daha hızlı inceleme – Olaylara hızlı ve etkili yanıt.
- %60 daha az ihlal riski – Güvenlik seviyenizi yükseltin.
- 700+ entegrasyon – Tüm güvenlik ekosisteminiz tek noktada.

**Gelişmiş Tehdit Tespiti**
Gelişmiş tehditlere karşı koymak yoğun kaynak, zaman ve hassasiyet gerektirir. Tüm saldırı yolunu izleyerek tespit yetkinliklerinizi güçlendirin; ağır işi QRadar SIEM sizin için üstlensin.

**Tehdit Avcılığı**
Dağınık veri setlerini anlamlı bilgilere dönüştürün, analistlerinize neredeyse gerçek zamanlı tehdit avı yapmaları için kapsamlı içgörü sağlayın.

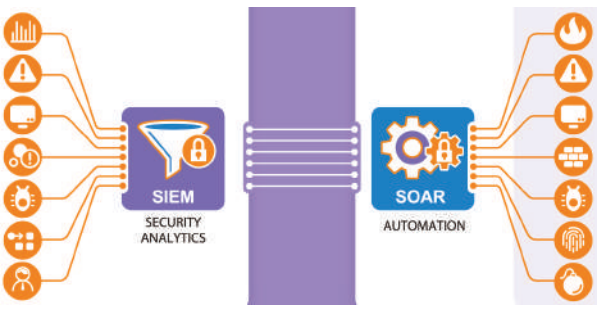
**Fidye Yazılımları**
Hızlı gelişen fidye yazılımı saldırıları daha hızlı yanıtlar gerektirir. Saldırganların hızlandığı ortamda, kurumların proaktif ve tehdit odaklı bir siber güvenli yaklaşımı benimsemesi şarttır.

**Uyumluluk**
Ortamınıza uygun yasal düzenlemeler ve iç denetimlerle uyumluluğunuzu belgeleyin, kanıtlayın ve güvenle raporlayın.



IBM Gold Partner

isnet




## IBM QRadar SOAR

IBM QRadar SOAR platformu, güvenlik ekiplerinizin karar alma süreçlerini optimize etmek, güvenlik operasyon merkezi (SOC) verimliliğini artırmak ve olay müdahale süreçlerinizi akıllı otomasyon ve orkestrasyonla güçlendirmek için tasarlandı.

- Müşteri, olaylara müdahale süresinde yaklaşık %85 azalma sağladı.
- Bir müşterinin ortalama sorun giderme süresi sadece 5 dakika oldu.
- 180'den fazla yerleşik gizlilik regülasyonu desteği.

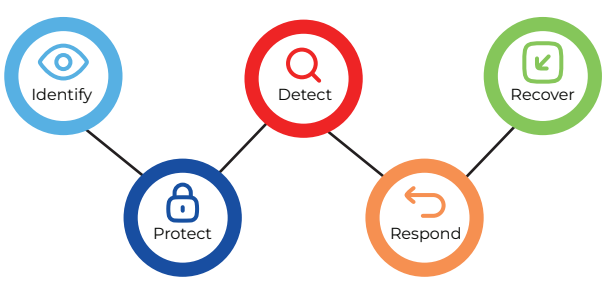
**Olaylara Daha Hızlı Yanıt Verin**
QRadar SOAR, korelasyon, veri zenginleştirme, inceleme ve vaka önceliklendirme için otomasyonu kullanır. Bu sayede bir müşteride olay yanıt süresi yaklaşık %85 kısaldı.

**Yanıt Süreçlerini Orkestre Edin ve Otomatikleştirin**
QRadar SOAR'un özelleştirilebilir vaka yönetimi yaklaşımı, geniş entegrasyon ekosistemi ve dinamik oyun kitaplarıyla mevcut yanıt iş akışlarınıza uyum sağlar.

**Daha Kolay Başlayın**
QRadar SOAR araçları, güvenlik analistlerinin yüksek öncelikli alarmlar için otomatik iş akışları ve yanıtlar oluşturmasını kolaylaştırır. Böylece gerçek olayları hızla tespit edip yanlış pozitifleri ortadan kaldırabilirler.

**Dinamik Oyun Kitaplarını Kullanın**
IBM QRadar SOAR Playbook Designer, sezgisel ve ödüllü arayüzü ile otomasyonu basitleştirir ve uygulama içi rehberlik sunar. Dinamik oyun kitapları, olay koşullarına uyum sağlar ve baştan başlamaya gerek bırakmaz.

---




## IBM QRadar EDR

Kötü niyetli ve otomatik siber aktivitelerin artışı, sıfır gün (zero-day) açıkları kullanarak yapılan fidye yazılımı saldırılarıyla kuruluşları zor durumda bırakıyor.

IBM QRadar EDR, daha kapsamlı bir uç nokta güvenliği yaklaşımı sunar:

- Akıllı otomasyon ile bilinen ve bilinmeyen uç nokta tehditlerini neredeyse gerçek zamanlı olarak giderir.
- Saldırıları görselleştiren storyboard'lar ile bilinçli karar almayı destekler.
- Analist yorgunluğunu azaltmak için uyarı yönetimini otomatikleştirir ve önemli tehditlere odaklanmayı sağlar.
- Gelişmiş sürekli öğrenen AI özellikleri ve kullanıcı dostu arayüzü ile ekibi güçlendirir ve iş sürekliliğini korur.

**Net Bir Görünürlük Elde Edin**
NanoOS teknolojisi sayesinde, uç noktalarda çalışan süreçler ve uygulamalar hakkında derinlemesine görünürlük sağlayarak tüm uç nokta ve tehdit aktiviteleri üzerinde tam kontrolü yeniden kazanın. Adversariler tarafından tespit edilmesi neredeyse imkansızdır.

**Yanıt Süreçlerinizi Otomatikleştirin**
Sürekli öğrenen AI'mız, daha önce görülmemiş tehditleri neredeyse gerçek zamanlı olarak tespit eder ve özerk şekilde yanıt verir. Hatta en deneyimsiz analistlere bile yönlendirilmiş müdahale ve otomatik uyarı yönetimi ile destek olur.

**Tepkisel'den Proaktif'e Geçin**
Kolayca oluşturulabilen tespit ve yanıt senaryolarıyla saldırganların önüne geçin; sonuçlar saniyeler içinde elde edilir ve pasif tehditlere saklanacak alan bırakmaz. Kullanıcı dostu senaryolar, uç nokta kesintisi olmadan tüm organizasyonda uygulanabilir.



IBM Gold Partner