PICUS

ÜRÜN BROŞÜRÜ

BÜTÜNCÜL GÜVENLİK DOĞRULAMA PLATFORMU

Tespit Kuralı Doğrulaması

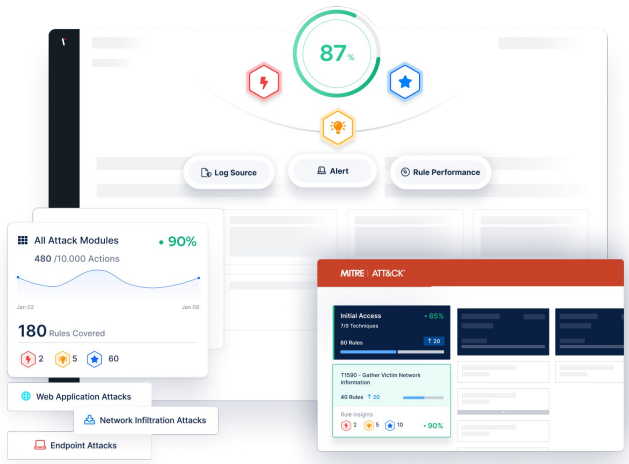
TESPİT KURALLARINIZIN ETKİNLİĞİNİ DOĞRULAYIN

SIEM çözümleri, güvenlik ekiplerinin siber saldırıları bir kurumun iş süreçlerini önemli ölçüde etkilemeden önce tespit ve müdahale etmesine yardımcı olarak modern SOC/SOME süreçlerinin temeline yerleşmiştir. Son yıllarda, güvenlik ekiplerinin uğraşmak zorunda olduğu alarmların, logların ve yeni tehditlerin sayısı katlanarak artmıştır. Bunun nedeni, kurumların gittikçe daha fazla veri toplaması ve sürekli olarak yeni ve sofistike tehditlerin ortaya çıkmasıdır. Zaman ve kaynak kısıtları nedeniyle, SOC mühendisleri mevcut kuralları yönetmek, yenilerini geliştirmek ve test etmek için mücadele etmektedir.

Güvenlik uyarılarını gerçek zamanlı olarak işleyen ve birden çok kaynaktan gelen verileri analiz eden SIEM çözümleri, kurumsal güvenlik için kritiktir. Kurumların SIEM sistemlerinin katma değerini en üst düzeye çıkarmasını engelleyen sorunların neler olduğu sorusuna en sık verilen yanıtlar, personel eksikliği (%41)* ve çok fazla yanlış pozitif (%37)* olmuştur.

* Cybersecurity Insights 2022 SIEM Raporu

Tespit Kuralı Doğrulaması çözümü ile güvenlik ekipleri, tespit kurallarının performansı ve hijyeniyle ilgili sorunları hızlı bir şekilde belirleyebilmenin yanı sıra tespit ve müdahale yeteneklerini optimize etmeye yardımcı olacak önerileri de elde edebilmektedir.



PICUS TESPİT KURALI DOĞRULAMASI

Picus Tespit Kuralı Doğrulaması, tespit kurallarının performansını optimize etmek için gereken eforu azaltmanın yanı sıra tehdit tespit ve müdahale yeteneklerini artırır.

TESPİT KURALI DOĞRULAMASI, TESPİT KURALLARINI NASIL GÜÇLENDİRİR?

SOC Etkinliğini En Üst Düzeye Çıkarın

SOC ekibinin doğru kuralların uygulandığına ve kritik güvenlik olayları için alarmların tetiklendiğine olan güvenini en üst düzeye çıkarın.

En Önemli Noktalara Odaklanın

Kurumunuz için kritik olan gerçek tehditlere dayalı tespit kapsamına yoğunlaşın ve SOC mühendislerinin asıl önemli olan işlere zaman ayırabilmelerini ve odaklanabilmeleri sağlayın.

Proaktif Kural Doğrulamayı Etkinleştirin

SIEM ve EDR tespit kurallarının tehdit kapsamı, doğruluğu ve performansı hakkında bilgi edinin ve SOC ekiplerinin proaktif kural doğrulaması gerçekleştirmesini sağlayın.

Tehdit Tespit ve Müdahalesini Optimize Edin

Tehdit tespit ve müdahale yeteneklerinin bütünsel bir görünürlüğünü elde edin ve MITRE ATT&CK Çerçevesinin operasyonel hale getirilmesini hızlandırın.

Bakım ve Optimizasyon İçin Gereken Eforu Azaltın

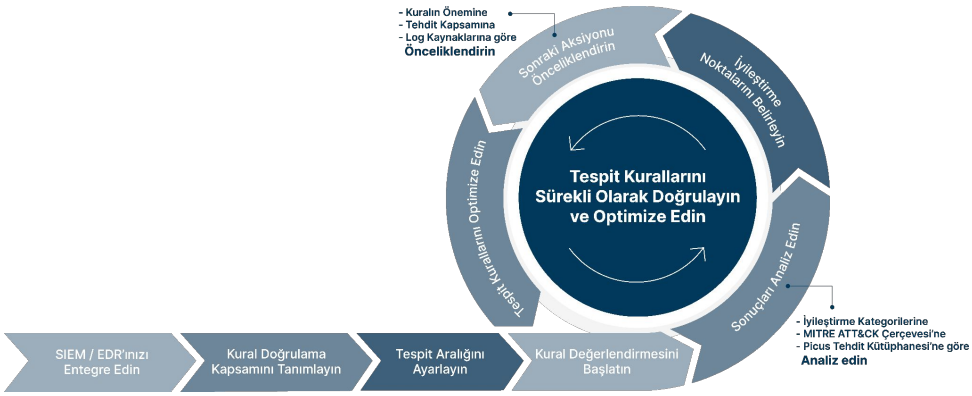
Yeni ortaya çıkan tehditler için tespit mühendisliği çabalarını saatlerden birkaç dakikaya düşürün.

Tespit Kurallarının Etkinliğini Doğrulayın

Log kapsamı, alarm sıklığı ve performans ölçümlerine dayalı olarak mevcut ve yeni kuralların etkinliğini doğrulayın.

EN MANTIKLI YOL
SÜREKLİ TESPİT KURALI DOĞRULAMASI

SOC ekipleri, gereksiz ve eski kurallar ile eksik ve belirsiz kural kullanımlarını belirlemek için proaktif bir alarm doğrulama sürecine ihtiyaç duyar. Bu süreç ayrıca, saldırganlar tarafından kullanılan yeni taktikleri, teknikleri ve prosedürleri ele almak için proaktif olarak yeni ve yüksek kaliteli tespit kuralları ekleyebilmelidir. Bu yöntem, alarm sayısını azaltmanın ve güvenlik analistlerinin sadece anlamlı alarmları almasını sağlamanın en mantıklı yoludur.



ÖNERİLEN EN İYİ UYGULAMALAR

✓ API bağlantısıyla bir değerlendirme kapsamı ve sürekli değerlendirme zamanlarını belirleyin. Sürekli değerlendirmelerin ilkini başlattıktan sonra, değerlendirmenin sonuçlarını inceleyin ve öneri kategorilerine göre kurallardaki iyileştirme önerilerini önceliklendirin ve kuralları iyileştirin. Bir sonraki değerlendirmede yapılan iyileştirmelerin etkilerini görün ve döngüyü tekrar edin.

✓ Yeni bir kural geliştirin ve bir sonraki otomatik değerlendirmede bu yeni kuralı analiz edin. Bu şekilde kuralla ilgili önerileri inceleyin ve gerekirse kuralı iyileştirin. Böylece yeni kuralın ilk günden itibaren daha iyi ve performanslı çalışmasını sağlayın ve kuralda ortaya çıkabilecek iyileştirme önerilerini sürekli değerlendirmelerle takip edin.

TESPİT KURALI DOĞRULAMASI GÜVENLİK ORTAKLIKLARI

splunk>

Düzenli olarak daha fazla güvenlik ortağı eklenmektedir.

NEDEN TESPİT KURALI DOĞRULAMASI?

- ✓ Farkındalık yaratan ve çözüm sağlayan çözüm
- ✓ Sorun yaratan değil, çözüm sağlayıcı teknoloji.
- ✓ Kurulumu, kullanımı ve yönetimi kolaydır.
- ✓ Yönetici gösterge panelleri ve raporları

TEMEL ÖZELLİKLER

✓ Tehdit tespit ve müdahale yeteneklerinin **bütünsel görünürlüğünü** sağlar.

✓ Tespit kuralları üzerinde Sabitleme Öğeleri, İyileştirme Noktaları ve Olumlu Noktalar hakkında bilgi sağlar.

✓ Kural için verilen iyileştirme önerilerinin korelasyonları ile kurallardaki iyileştirme noktalarını sürekli olarak tespit eder.

✓ Değerlendirme sonucu üzerinde filtreleme seçenekleri ile iyileştirilmesi gereken kuralları önceliklendirir.

✓ Yeni geliştirilen bir kuralın SIEM üzerindeki etkisini ortaya çıkarır.

✓ Sonuçları MITRE ATT&CK ile eşler.

✓ Kuralların tehdit kapsamını ölçer ve her gün güncellenen 20.000 aksiyondan oluşan 3.800'den fazla tehdit içeren kapsamlı bir Picus Tehdit Kütüphanesi ile boşlukları analiz eder.

> Sürekli ve proaktif tespit kuralı doğrulama süreçleri oluşturmak için tespit kurallarının bazının üstünde kalmak ve manuel tespit mühendisliği süreçlerini otomatikleştirmek için kullanımı kolay bir ürün.

Gartner peerinsights™

4.9 / 5*

*Ortalama puan (Ekim 2022)

Zaman bulamadığınız işleri otomatikleştirmenin tam zamanı!

www.picussecurity.com

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022 · CYBERTECH100 2022 The World's Most Innovative CyberTech Companies for Financial Services · GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022 · AICPA SOC 2

www.picussecurity.com

picussecurity