ÇÖZÜM NOTU

SOC INSIGHTS

SecOps verimliliğini artırmak için çok miktarda olay, ağ, ekosistem ve DNS istihbarat verisini eyleme geçirilebilir içgörülere dönüştürmek için yapay zeka odaklı analizler uygulayın

SECOPS VERİMLİLİĞİNİN ÖNÜNDEKİ ENGELLER

Günümüzde işletme veya kamu kuruluşlarının diğer işlevlerinde olduğu gibi, modern SOC mevcut kaynaklarla daha fazlasını yapmak için mücadele etmektedir. SANS 2023 SOC Anketine[1] göre, SOC yeteneklerinden tam olarak yararlanmanın önündeki en önemli 10 SOC engelinin %80'i üç alanda toplanmaktadır:

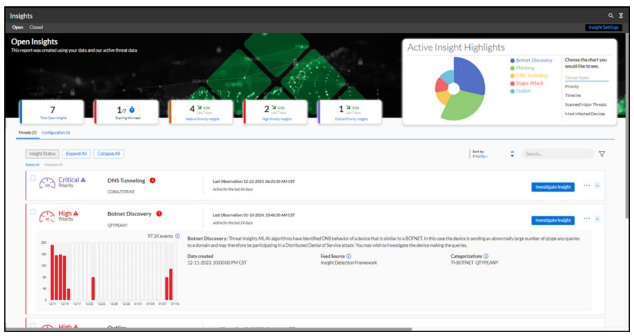
- Uyarıları anlama ve bunlarla başa çıkma
- Araçlar arasında sınırlı entegrasyon veya otomasyon
- Mevcut personel ve becerilerle temel görevleri yerine getirme

Ancak en trajik istatistik, tüm bu engellerin on yılı aşkın bir süredir SOC'yi zorluyor olması olabilir. Kötü amaçlı yazılım sıralamalarına ve diğer temel filtrelere dayalı olarak olayların otomatik önceliklendirilmesinden elde edilen aşamalı iyileştirmeler, SOC analistinin dikkatini gerektirebilecek uyarıların ve diğer olayların büyümesine ayak uyduramadı. Dolayısıyla işler daha da kötüye gitti.

AI-DRIVEN SOC INSIGHTS

Modern kalıcı tehditler, tek bir saldırıda bile yer alan çok sayıda pen-test, istimar, şifreleme ve diğer araçları barındırmak ve dağıtmak için esnek saldırgan altyapısına ve dinamik C2 sistemlerine bağlıdır. Bu durum onları DNS'e son derece bağımlı hale getirmekte ve savunucuların bu tehditleri algılamak ve engellemek için yararlanabileceği önemli bir zayıflığı vurgulamaktadır.

DNS, protokol, platform, işletim sistemi, uygulama ve hatta konumdan bağımsız olarak meşru ve kötü niyetli etkinlikleri görür. Bu benzersiz görünürlük sayesinde, NSA Siber Güvenlik Direktörlüğüne bağlı bir pilot program, DNS güvenliğinin malware saldırılarını %92 oranında azaltabileceğini ortaya koymuştur[2]!



Şekil 1: SOC Insights Özet sayfası analistlere en önemli konulara tek tıkla erişim sağlar.

GERÇEKLER VE RAKAMLAR

- SOC analistlerinin %60'ı **iş yüklerinin arttığını** ve %65'i önümüzdeki yıl içinde **iş değiştirebileceğini** söyledi[4].
- Ankete katılanların %55'i kritik uyarıların haftalık, hatta günlük bazda sıkça gözden kaçtığını söyledi[5].
- Analistlerin %64'ü **manuel çalışmanın zamanlarının yarısından fazlasını tükettiğini söyledi**[6].
- Yanlış yapılandırma, **hatayla ilgili ihlallerde en önemli 3 faktörden biri**[3].
- Tam SOC kullanımının önündeki **en önemli 10 engel den 8'i** uyarılar, araç entegrasyonu ve beceri eksikliklerini içeriyor[1]
- CEO'ların %77'si **kilit beceriler konusunda endişeli**[7].
- **Kötü amaçlı yazılım ve C2 faaliyetlerinin %92'si doğru** DNS istihbaratı ve görünürlüğü ile DNS katmanında kontrol edilebilir[2].

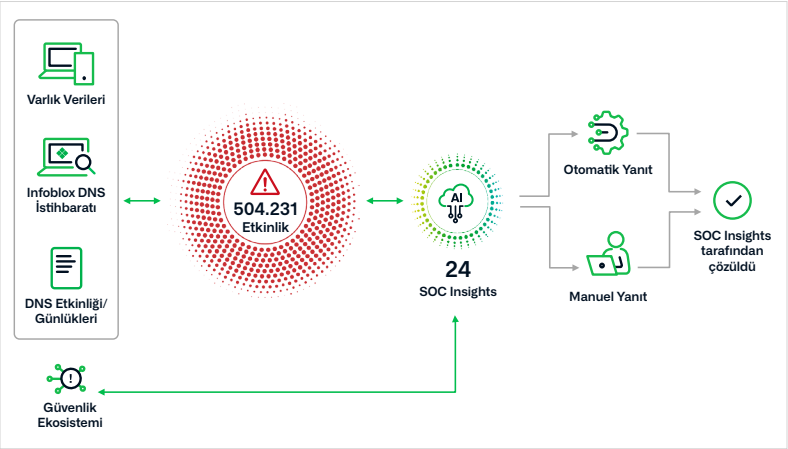
SOC Insights, benzersiz sunmak için Infoblox'un DNS Algılama ve Yanıt (DNSDR) çözümü BloxOne Threat Defense ile çalışarak diğer araçların gözden kaçırdığı bilinmeyen tehditleri algılamak, SOC verimliliğini artırmak ve mevcut güvenlik yatırımlarının genel yatırım getirisini iyileştirmek için benzersiz yapay zeka odaklı analitik sunar.

BİRDEN FAZLA SORUNU BİRÇOK BAKIŞ AÇISIYLA ÇÖZMEK

Olay sonrası veya ihlal araştırmaları genellikle yanlış yapılandırmalar, güvenlik aracı entegrasyonu zorlukları veya basit uyarı aşırı yüklenmesi nedeniyle kötü amaçlı etkinliğin erken göstergelerinin gözden kaçırıldığını ortaya çıkarır. SOC Insights, bu risklerin ele alınmasına yardımcı olmak için büyük miktarda veriye yapay zeka odaklı analitik uygular.

Güvenlik İçgörüleri

BloxOne Threat Defense 'Business Cloud' veya 'Advanced' için mevcut olan SOC Insights için Güvenlik eklentisi, büyük miktarda olay, ağ, ekosistem ve DNS görünürlüğü ve istihbaratını yönetilebilir bir dizi eyleme geçirilebilir güvenlik içgörüsüne dönüştürmek için yapay zeka kullanır.

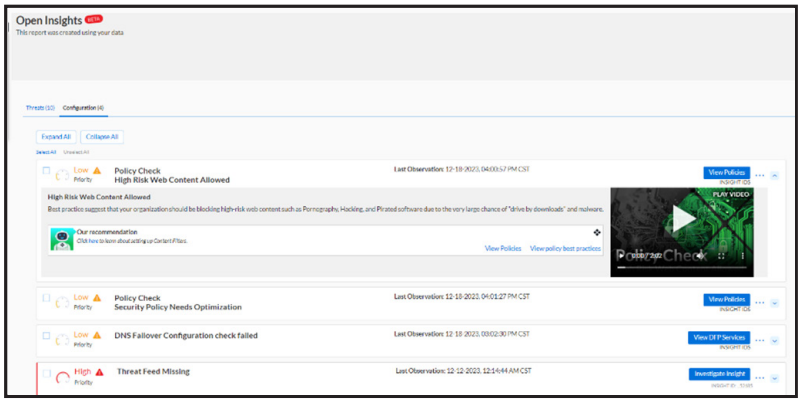


Şekil 2: SOC Insights'ın aşırı uyarı yükünü ortadan kaldırmasına, çok saydı olayı daha yönetilebilir, anlamlı ve eyleme dökülebilir içgörülere dönüştürmesini sağlayın.

- Zero Day DNS™
- Kalıcı Tehdit
- Aktif Tehdit Yayılması
- Büyük Saldırı
- Botnet Keşfi
- Aykırı İletişim
- Kimlik Avı
- Malware
- Açık DNS Çözücü
- DNS Tünelleme
- Veri Kaybı Etkinliği
- Hedefli Saldırı
- Aşırı DNS Hataları
- İzlenen Benzer Etki Alanı

Yapılandırma içgörüleri

SOC Insights'ın Yapılandırma özelliği, kullanıcıların mevcut en iyi uygulamalardan tam olarak yararlanmalarını ve yaygın hatalardan kaçınmalarını sağlamalarına yardımcı olmak için BloxOne Threat Defense 'Business Cloud' ve 'Advanced' ile birlikte sunulmaktadır. Hataların ve zayıflıkların giderilmesine yardımcı olmak için videoları ve diğer kılavuzları izleyin veya izin verilen istisnalar için gereksiz uyarıları devre dışı bırakın.



Şekil 3: Optimum savunma, araştırma ve müdahale yeteneklerini sağlamak için zayıf veya tehlikeli yapılandırma hatalarını proaktif olarak belirleyin.

- DNS Tehdit Akışı Eksik
- VirusTotal Ücretsiz Anahtarı Eksik
- Güvenlik Politikasının Optimize Edilmesi Gerekiyor
- DNS Devralma Denetimi Hatası
- Feed İşlemi Uyuşmazlığı
- DFP Varlık Ayrıntılarını Gizleme
- Günlükleme Modunda Güvenlik Politikası
- Web İçerik Dosyalayıcıları KAPALI
- Yüksek Riskli Web İçeriğine İzin Verildi

OLUMLU BIR FINANSAL, OPERASYONEL VE IŞ ETKISI

Çoğu güvenlik aracı "kullanım kolaylığı" ve "daha az ihlalden" biraz daha fazlasını vaat edebilirken, SOC Insights, analist stresini ve devir oranını azaltmaktan genişleme, M&A ve diğer iş girişimlerinden kaynaklanan birçok güvenlik endişesini azaltmaya kadar çok daha fazlasını yapabilir. Örneğin:

- DNS'in doğası, yeni bir konumu veya iş ortağını aylar yerine dakikalar içinde ortak bir DNS altyapısında birleştirmeyi kolaylaştırır.
- Configuration Insights, hatayla ilgili ihlallerde bildirilen en önemli 3 faktörden biri olan "yanlış yapılandırma" nedeniyle ihlalleri veya veri kaybını azaltmaya yardımcı olmak için oldukça proaktiftir[3].
- "Malware", "Kimlik Avı", "Botnet" ve diğer "Büyük" veya "Yayılma" faaliyetlerinin otomatik korelasyonu, müdahale ekiplerinin aynı anda birçok tehdidi ele almasını sağlayarak verimliliklerini artırır.
- "Açıklar", "DNS Tünelleme" ve "Açık Çözümleyici" gibi içgörü kategorilerini ve BloxOne Threat Defense'ın benzersiz görünümünü ve uygulama görünürlüğü özelliklerini izleme yeteneği ile daha proaktif bir güvenlik duruşu sağlayın.
- Güvenlik ekosisteminin istihbarat entegrasyonu, yalnızca ham günlükler ve olaylar yerine eyleme geçirilebilir 'içgörüler' sunarak tüm güvenlik yığınının yatırım getirisini artırır.
- SOC Insights, ilgili verileri otomatik olarak toplar ve analistlerin sonuçlara daha hızlı ve güvenilir bir şekilde ulaşmak için bu verileri görmelerini ve değerlendirmelerini sağlar. Bu da daha düşük strese ve yetenekli ve deneyimli güvenlik profesyonellerinin daha fazla elde tutulmasına katkıda bulunur.

ŞAŞIRTICI SONUÇLAR

Müşteriler, BloxOne Threat Defense ile SOC Insights'ı kullanmanın aşağıdakiler de dahil olmak üzere büyük avantajlar sağladığını bildiriyor:

- EDR ve FW Uyarıları %50 oranında azaldı
- Aylık ortalama 500 SOC analist saati tasarrufu sağlandı
- Yıllık 400.000$ verimlilik tasarrufu sağlandı

SIEM, SOAR VE EKOSİSTEMİN DİĞER BÖLÜMLERİNİ İÇGÖRÜLER SAYESİNE DAHA ÇOK DEĞERLENDİRİN

SecOps, güvenlik ekosisteminde ham veri paylaşımının değerini ve sınırlarını bilir. Bu durum SIEM ve SOAR uzmanlığını çoğu kuruluş için en zorlu beceri setlerinden biri haline getirmiştir. SOC Insights, bu diğer araçların yükünü ortadan kaldırır ve ortaya çıkan içgörüleri güvenlik yığını genelinde paylaşarak diğer araçları daha etkili hale getirerek genel SecOps verimliliğini daha da yükseltir.

1 "SANS 2023 SOC Anketi", Haziran 2023, Chris Crowley, Barbara Filkins, John Pescatore

2 "NSA savunma müteahhitlerini güvence altına almak için pilot program başlattı", 18 Haziran 2020, Lauren C. Williams, NEXTGOV/FCW

3 "Verizon 2023 DBIR Raporu"

4 SOC Analistinin Sesi

5 Orca Security 2022 Bulut Güvenliği Uyarısı Yorgunluk Raporu

6 SOC Analistinin Sesi

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

infoblox.

Infoblox, benzersiz performans ve koruma sağlamak için ağ ve güvenliği birleştirir. Fortune 100 şirketleri ve gelişmekte olan yenilikçiler tarafından güvenilen firmamız, ağınıza kimin ve neyin bağlandığı üzerinde gerçek zamanlı görünürlük ve kontrol sağlıyor. Böylece kuruluşunuz daha hızlı harekete geçerek tehditleri daha çabuk durdurabilir.

Kurumsal Merkez
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Sürüm: 20240411v2