kaspersky GELECEĞİ YAKALAYIN

XDR - SIEM - SOAR

Çok fazla kısaltma olması kafanızı mı karıştırdı? Bu harflerin ardında nelerin yattığına birlikte bakalım...

Giriş

SIEM, SOAR, MDR, EDR, EPP, XDR... Siber güvenlikle ilgili kısaltmalarla dolu bir ormanda şaşkına dönmüş ve kaybolmuş mu hissediyorsunuz? Bu oldukça anlaşılabilir bir durum. Bu yüzden önemli kısaltmalardan üç tanesi arasındaki farkları anlamanız için bu faydalı kılavuzu hazırladık: SIEM, SOAR ve XDR. Peki bu kısaltmaların hikâyesi nedir? Bu kafa karıştırıcı ve birbirine benzeyen terimleri sektörde nasıl ortaya çıktı? Hepsi farklı bir anlama mı geliyor yoksa sadece pazarlama numaraları mı? Benzerlikleri ve farklılıkları nelerdir? Birbirlerini tamamlayabilirler mi yoksa birbirleriyle rekabet hâlindeler mi?

Gelin, bütün bu sorulara birlikte cevap bulalım! Bilgiden dövülmüş kılıçlarımızı alalım, kısaltmalar ve terimler ormanından geçelim ve bu konuyu bir açıklığa kavuşturalım!

SIEM

Güvenlik bilgileri ve olay yönetimi (SIEM), güvenlik olayları yönetimi (SEM) ve güvenlik bilgileri yönetimini (SIM) tek bir platformda birleştiren çeşitli araç ve hizmetlerdir. SIEM; denetim, uyumluluk ve şüpheli faaliyetlere yönelik kural tabanlı korelasyon eşleştirme de dâhil çeşitli kullanım senaryoları için BT altyapısından günlük verilerini toplar, biriktirir, analiz eder ve saklar.

SIEM nasıl çalışır?

İlk SIEM hizmetleri, uyumluluk bildirme amacıyla uç noktalar, uygulamalar ve ağ cihazları dâhil bir kuruluşun BT altyapısındaki günlükleri ve olayları toplama ve saklama amacıyla ilk olarak 2005 yılında geliştirildi. SIEM; bu veri kümesinde korelasyonlar gerçekleştirir, şüpheli davranışa işaret edebilecek desen veya olayları arar ve güvenlik operasyonları merkezi (SOC) için bir uyarı oluşturur. Güvenlik analistleri, kısa bir süre sonra bu uyarıları uyumluluk ve denetim amaçlarının yanı sıra ekosistemdeki kötü amaçlı faaliyetlerin ilerlemesini daha önleyici bir şekilde belirlemek ve durdurmak için kullanabileceklerini fark ettiler.

SIEM sınırlamaları

Sorun, SIEM hizmetlerinin vakaları tespit etmek ve onlara müdahale etmek gibi belirli amaçlara yönelik olarak tasarlanmamasından kaynaklanıyordu. Bu özellikleri, birkaç nedenden ötürü kullanımlarını biraz zor bir hâle getirdi:

- Çok fazla uyarı olması — SIEM tarafından sağlanan devasa veri kümesinin manuel olarak filtrelenmesi, işlenmesi ve analiz edilmesi gerekir; bu da yüksek tempolu bir tehdit ortamında saldırıları engellemeye çalışan güvenlik analistleri için uygun değildir.

- Bağlam olmaması — Güvenlik analistleri; yeni, karmaşık ve çok yönlü saldırılarla başa çıkmak için SIEM'nin sağladığı bağlantısız veri akışlarından çok kuruluşun tehdit ortamının bağlama uygun hale getirilmiş ve tutarlı bir resmine ihtiyaç duyarlar.

- Çok pasif olması — Şüpheli işlemleri engelleme, dosyaları karantinaya alma ve diğer müdahale yetenekleri SIEM'nin yetkileri dışındadır; özünde pasif ve analitik bir araçtır.

Güvenlik uzmanları, SIEM'nin üzerine ek araçlar ekleyerek veya makine öğrenimi ve davranışsal analiz eklentileri ile yeni nesiller geliştirerek bu sorunları çözmeye çalıştılar. Ancak daha kaliteli uyarılar sağlayıp daha hızlı ve otomatik hâle getirilmiş süreçleri kolaylaştıran bir araca olan talep devam etti.

SOAR

Güvenlik Yönetimi ve Otomatik Müdahale (SOAR) araçları, 2015 yılında SIEM sistemlerinde yukarıda belirtilen bazı kusurları gidermek için tasarlandı. SOAR platformları, yönetim sistemleri ve tehdit istihbaratı platformları da dâhil altyapı genelinde çeşitli kaynaklardan veriler alarak öncelik analizi sağlar. Güvenlik ekipleri, daha sonra SOAR platformunun API bağlantılı bir güvenlik araçları ekosistemi ile olan entegrasyonunu kullanarak gelen tehditlere karşı çok aşamalı ve çözümler arası otomatik müdahaleler yapılandırabilir.

SOAR nasıl çalışır?

Bu sefer kısaltmanın kendisi bu konuda oldukça faydalı! Nedenleri:
SOAR araçları Otomatikleştirir. Çoğunlukla olaylara müdahale süreçlerini otomatik hâle getirme kapasiteleri ile bilinseler de bu araçlar, aslında güvenlik açığı taraması, günlük analizi, kullanıcı erişimi yönetimi, tehdit saptaması ve çok daha fazlası dâhil çeşitli iş akışlarını otomatik hâle getirebilir.

Bu araçlar, bunu belirli olaylar tarafından tetiklenen ve sisteme belirli bir iş akışında hangi adımların uygulanması gerektiğini söyleyen önceden yapılandırılmış bir kurallar kümesi olan "kitapçıkları" kullanarak yaparlar. Çoğu SOAR çözümü, SOC ekiplerinin karşılaştığı en yaygın görevleri kapsayan yüzlerce kullanıma hazır kitapçıkla birlikte gelir. Ardından ekipler, sahip olabilecekleri daha belirli olan ve tekrarlayan süreçleri otomatik hâle getirmek için kendi kitapçıklarını yapılandırabilirler.

Araçların sonraki görevi Yönetmektir. Otomasyon tek bir iş akışı dâhilinde her bir görevin makine destekli olarak gerçekleştirilmesini ifade ederken yönetim, birden fazla farklı araç ve sürecin daha büyük bir iş akışında koordinasyonunu ve ilgili tüm verilerin birleştirilmiş ve eyleme dönüştürülebilir bilgiler elde etmek için tek bir platformda toplanmasını ifade eder.

SIEM ve SOAR arasındaki ilişki

Genelde SIEM, asistan-yönetici ilişkisine benzer bir şekilde SOAR araçlarıyla birlikte kullanılır: SIEM tüm günlükleri toplar, uyarılar bulmak için bu günlükleri ilişkilendirir ve bu bilgiyi SOAR'ye aktarır. SOAR de bu bilgileri müdahale eylemleri için kullanır.

SOAR sınırlamaları

Her şey kulağa hoş geliyor, değil mi? Ancak iş ortağı araçlarıyla entegre olan iyi yapılandırılmış bir SOAR platformunun bakımını yapmak için oldukça yetenekli ve ileri düzey bir SOC'nin sürekli olarak çalışması gerekir. Bu, mevcut siber güvenlik becerileri açığı dikkate alındığında şu anda birçok şirketin sahip olmadığı bir kaynak.

SOAR analistleri, bu tarz yetenek ve dikkat gerektiren bir bakım olmadan, platforma kesintisiz olarak eklenen çeşitli ve yalıtılmış araçların bir sonucu olarak çok fazla düşük öncelikli uyarı, hatalı tespit ve genel anlamda tutarsız veri kümeleri ile karşı karşıya kalabilirler. Bu da çalışırken tam olarak kaçındıkları bir durumdur.

XDR

XDR, şirket içi veya bulut tabanlı bir güvenlik çözümü olup genel anlamda iki kategoriye ayrılır: yerel ve hibrit. Yerel XDR, tek bir tedarikçiye ait birleşik bir araç paketiyken Hibrit XDR, ekosisteminize diğer üçüncü taraf çözümleri entegre eder. "XDR" kelimesi ilk olarak 2018'de kullanılmıştır ve bu kısaltmadaki "X", "eXtended" (genişletilmiş) kelimesini ifade etmektedir: XDR, BT altyapısının tamamında kapsamlı koruma sağlamak amacıyla e-posta, bulut ve ağ da dâhil birden fazla güvenlik katmanından veri toplayarak ve bu toplanan verileri ilişkilendirerek geleneksel uç nokta algılama, müdahale ve koruma araçlarının (EDR ve EPP) ötesine doğru "genişler".

Bu yüzden güvenlik ekiplerinin güvenlik ekosisteminin tamamını korumalarına yardımcı olmak için çeşitli araçları koordine edip makine öğrenimi ve otomasyonu kullanan tek bir platformdur... Biraz SOAR'ye benziyor sanki, değil mi? Ama aralarında bazı önemli farklılıklar var. Şimdi bu farklılıklara göz atalım...

XDR - SOAR: Aradaki fark nedir?

1. XDR çözümleri, uç nokta verileri ve optimizasyonu ile bağlantılıdır: Bu, olay algılama ve müdahalenin merkezî bir tasarım özelliği olduğu ve onlara SOAR araçlarının normalde sahip olmadığı ileri düzey analiz yetenekleri sağladığı anlamına gelir. XDR araçları, bir kuruluşu sınırlarının ötesinde korumak amacıyla bilinmeyen tehditleri ve sıfır gün tehditlerini tespit etme ve güçlü yapay zekâ, makine öğrenimi algoritmaları ve tehdit istihbaratından faydalanma konusunda oldukça etkilidir. Buna karşın SOAR araçları, sadece olaylara müdahaleyi değil, altyapıdaki tüm süreçleri yönetip otomatik hâle getirebildiklerinden çok daha geniş bir kullanım senaryosu yelpazesi sunabilir.

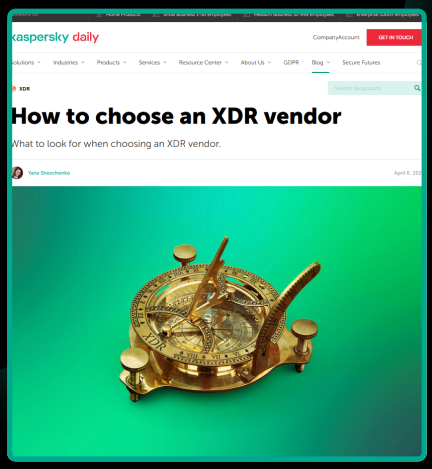
2. XDR, SOAR'nin daha basit versiyonu gibi düşünülebilir: gelen tehditlere ve uyarılara tek tıkla otomatik olarak müdahale imkânı sunan basitleştirilmiş bir arayüz. Bu, iyi yapılandırılmış bir SOAR platformunun karmaşıklığını muhafaza etmek için gerekli kaynaklara sahip olmayan bir kuruluş için çok daha uygun olabilir.

3. XDR, ürünler arası sorunsuz entegrasyon sağlar: XDR, tek bir tedarikçiye ait araçlarda veya üçüncü taraf ürünlerde olmasına bakılmaksızın sorunsuz birlikte kullanılabilirlik sağlama konusunda mükemmeldir. SOAR araçları, bünyesindeki farklı ve bağımsız araçların tamamını entegre etmede genelde zorluk yaşar. XDR, etkili ve hepsini kapsayan bir tehdit müdahalesi için bu uygulama gruplarını birbirinden ayırır.

Bir XDR tedarikçisi nasıl seçilir?

Birçok siber güvenlik tedarikçisi, kendi çözümleriyle XDR modasına ayak uydurmaya başladı. Aldığınız ürünün iyi olup olmadığını nasıl anlayabilirsiniz? Yardımcı rehberimize göz atın:

https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



O hâlde XDR, SIEM ve SOAR'nin yerini mi alacak?

XDR sürekli olarak geliştirilmekte olan nispeten yeni bir teknoloji olduğundan bu konuda henüz kesin bir yargıya varmak doğru değildir. Her çözüm diğerlerini tamamlayan avantajlar sunduğundan şu anda çoğu uzman, bütünleyici bir yaklaşım önermektedir:

- SIEM — SIEM'de günlük yönetimi, uyumluluk ve tehditle ilgili olmayan verilerin analizi gibi tehdit algılama kapsamının dışında kalan kullanım senaryoları vardır.
- SOAR — SOAR kitapçıklarındaki özelleştirilebilme işlevi, kuruluşların altyapısındaki süreçleri yönetme ve otomatik hâle getirme açısından son derece faydalıdır.
- XDR — Konu tehditleri algılama ve bunlara müdahale etmek olduğunda bir XDR çözümünün gelişmiş analizleri rakipsiz bir geliştirilmiş koruma sunar.

Uzmanlarınız için denenip test edilmiş ve uyarlanabilir bir çözüm mü arıyorsunuz? Buluta özel bir EDR çözümüne dayalı XDR olan Kaspersky Expert Security, kuruluşunuza bütün uç noktalarda ve ağda yapay zekâ tabanlı algılama ve otomatik müdahale mantığına yönelik iyileştirilmiş görünürlük ve işlevsellik sağlar ve çeşitli otomatik olay müdahale senaryoları sunar. Platformun algılama ve analize yönelik yerleşik gelişmiş teknolojisine dünya markası olmuş tehdit istihbaratı eşlik eder. Kaspersky XDR'nin birleştirilmiş mimarisi, tek bir web konsolundan merkezî yönetim sağlar. Daha fazla bilgi almak için lütfen https://go.kaspersky.com/TR_Expert.html adresini ziyaret edin.

www.kaspersky.com.tr