Kaspersky Next XDR Expert

Daha büyük, daha iyi,
daha hızlı ve daha fazla

kaspersky

Oyun değiştirici mi yoksa derde deva mı?

XDR: Genişletilmiş Algılama ve Müdahale

XDR, pek çok insanın telaffuz ettiği bir kısaltmadır. Ancak görece yeni tüm teknolojiler gibi herkes tam ne olduğunu veya işletmeler için ne yapabileceğini bilmiyor. Şurası kesin gibi. XDR, reaktif yaklaşımdan proaktif stratejiye geçişi kapsıyor. Çünkü 'bekle ve gör' taktiği siber güvenlikte pek işe yaramıyor. XDR'ı üründen çok strateji olarak görmek akıllıca bir yaklaşım olur.

XDR sadece derde deva arayan son teknoloji trendi mi, yoksa potansiyel bir oyun değiştirici mi? Dertler kuşkusuz ki ortada, küresel yetenek azlığı, aşırı çalışan IT güvenlik personeli, hiç durulmayan bir tehdit manzarasından tutun da aşırı yüklenmeye, dağınık araçlara, zayıf tehdit istihbaratına ve genişleyen saldırı yüzeyine kadar çeşit çeşit dert. IDC, XDR'ın "harici tehdit istihbaratı tedarikçisi olmasının yanısıra SIEM, EDR, SOAR, ağ istihbaratı ve tehdit analitiği platformlarının satışlarını etkileyen bir yenilikçi güç"[1] olacağını belirtiyor ve Forrester, farklılaştırılmış XDR teknolojisinin "kısa vadeli olarak uç nokta tespiti ve müdahalesini (EDR) geçeceğine ve uzun vadede SIEM'i devralacağına"[2] inanıyor.

XDR kimin için?

XDR, gelişmiş güvenlik yapısı olan ve alt yapısında neler olduğuyla ilgili tam ve anlamlı bir görüntü sunan tek bir platforma ihtiyaç duyan kuruluşlar içindir.

XDR ezber bozan bir güç olacak - IDC

Daha fazla cihaz, daha fazla uygulama, daha fazla ağ trafiği, daha fazla veri, daha fazla tehdit...

XDR kim içindir ve hangi zorlukları çözebilir?

XDR, gelişmiş güvenlik yapısı olan ve alt yapısında neler olduğuyla ilgili tam ve anlamlı bir görüntü sunan tek bir platforma ihtiyaç duyan kuruluşlar içindir.

Bu kuruluşların karşılaştığı siber güvenlik zorlukları sürekli olup iyi yapılandırılmıştır. ESG Araştırması IT ve siber güvenlik profesyonelleriyle anket yaptı[3] 100 ve daha fazla çalışanın olduğu kuruluşlarda, %80'den fazlası da bir dizi dikey sektördedir. Temel bulgulardan bazıları şunlardır:

SOC teknolojilerinin operasyonel ihtiyaçlarına yanıt verme zorlukları

SOC teknolojilerinin, veri hattının ölçeklenebilirliği, yük dengeleme işleme motorları, depolama kapasitesi eklemek vb. gibi operasyonel ihtiyaçlarına yetişme zorlukları nedeniyle güvenlik operasyonlarını yönetmek son iki yılda daha önce hiç olmadığı kadar zor hale geldi.

1 Kaynak: IDC Global Güvenlik Ürünleri Analizi: Güç Noktasından Güçlü Ürüne, XDR Şu Anda Nerede? 2022

2 Kaynak: Forrester, Genişletilmiş Algılama ve Müdahale (XDR) - Eski ve Yeni Arasındaki Mücadele, Allie Mellen, Baş Analist, 2021

3 Kaynak: ESG Araştırması Raporu, SOC Modernizasyonu ve XDR'ın Rolü, 2022

Büyüyen ve genel olarak sürekli değişen saldırı yüzeyi ve tehdit manzarası

Daha fazla cihaz, daha fazla uygulama, daha fazla ağ trafiği, daha fazla veri, daha fazla tehdit. Tehdit manzarası sabit durmuyor ve yeni araçlar çoğaldıkça siber tehditlerin sayısı ve karmaşıklığı durmadan artmaya devam ediyor. Ayrıca, bilgisayar korsanları için giriş engeli de her zamankinden az. Spektrumun bir tarafında, karanlık ağda ucuza satılan tehditleri alan düşük becerili kimseler, diğer tarafta yüksek becerilere sahip olup sabırla karmaşık saldırılar oluşturan korsanlar. İç tehditleri ve tedarik zinciri zayıflıklarını unutmayın.

Güvenliği yönetmek için çok sayıda manuel işlem gerekli

Toplanıp işlenecek daha fazla güvenlik verisi varken bunları manuel olarak işlemek yetersiz kalıyor. Bu durum, ölçeklendirmeyi etkileyen harika bir rüzgar yaratırken doğrudan insan müdahalesine fazlaca yaslanmayı gerektirdiği gibi genel olarak tehditlerle uğraşmayı zorlaştırır.

Algılama kurallarını geliştirme yetersizliği

Zaman, kaynak ve beceri azlığından algılama kurallarını geliştirme, güvenlik kontrollerini ayarlama ve tehditleri tanımlama ve hızlıca yanıt vermede yetersizlik. Kuruluşlarda her zaman gerekli güvenlik analitiği ve işlemlerini yürütecek becerileri taşıyan kişiler veya personel bulunmaz. Bu da hemen başka bir plana geçmeyi gerekli kılar...

Global ölçekte gerçek yetenek eksikliği

Global siber güvenlik iş gücü bugün tüm zamanların en yüksek rakamına denk düşen 4,7 milyon profesyonelden oluşuyorken, hala doldurulmayı bekleyen 3,4 milyon açık vardır ve bu açık henüz dolmamıştır. Bu uçurum iş gücüne kıyasla iki kat büyümekte olup yılda %26,2 artıyor.[4]

[4] Kaynak: (ISC)², Siber Güvenlik İş Gücü Çalışması, 2022

Mevcut araçlar

gelişmiş tehditleri algılama ve araştırmada genellikle zorlanır ayrıca bunları kullanmak ve yönetmek için özel beceriler gereklidir.

Amaca uygun olmayan araçlar

Araçların kendisi sorunun parçası haline gelince bir şeyler yapılması gerekir. Mevcut araçlar genellikle gelişmiş tehditleri algılayıp araştırmakta zorlandığı gibi ayrıca bunları kullanıp yönetmek için de özel yetenekler gereklidir. Araştırma[5] gösteriyor ki mevcut araçlar uyarıları ilişkilendirmekte sık sık yetersiz kalmakta ve IT güvenlik ekibi ayrı ayrı verileri ele alan çok sayıda birbirinden kopuk, tek tek araçla mücadele halindedir. Bu yetersiz, zahmetli, sorunlu ve pahalıdır. Başka bir zorluk da mevcut araçların genişleyen saldırı yüzeyiyle ilgilenecek ölçeğe geçememesi ayrıca bulut algılamada ve müdahale becerilerinde büyük boşluklar olmasıdır.[6]

CISO'nun stresli görünmesine şaşırmalı mı?

İyi haber şu ki, SecOps'u iyileştirmek bir öncelik olup finanse ediliyor. Kuruluşların %88'i bu yıl daha fazla harcama yapacak, %66'sı araç konsolidasyonunun bir öncelik olduğunu ayrıca modern uygulama geliştirme ve kullanım hızının yeni beceriler gerektirecek şekilde arttığını söylüyor.[7]

%88

oranında kuruluş SecOps'unu iyileştirmek için daha fazla harcama yapacak

%66

oranında kuruluş araç konsolidasyonunu öncelik olarak görüyor

XDR ne yapar

XDR bu zorlukları şu şekilde göğüsleyebilir.

XDR gelişmiş tehditleri daha iyi algılar

XDR'ın tehdit algılama becerileri uç noktalar, ağlar ve bulut ortamlarını kapsar. Makine öğrenmesi algoritmalarını ve davranışsal analitiği zararlı yazılım, fidye yazılımı ve gelişmiş kalıcı tehditleri (APT'ler) içeren karmaşık tehditleri tanımlamak için kullanır.

Otomatik müdahale ve iyileştirme işlemleri

XDR müdahale ve iyileştirme işlemlerini otomatize ederken kuruluşların tehditleri hızlıca ele almasını sağlayarak potansiyel hasarı en aza indirir. Güvenliği ihlal edilmiş uç noktaları otomatik olarak karantinaya alabilir, kötü amaçlı işlemleri engelleyebilir ve güvenlik açıklarını düzeltebilir, böylece harcanan emek ve yanıt süresini azaltabilir.

Uç nokta koruma araçlarıyla entegre olur

EPP ile entegrasyon anahtar konudur. Ayrıca XDR uç nokta etkinliklerine derin içgörüler sağlamak için zengin uç nokta telemetrisini ve davranışsal analitiği güçlendirir. Şüpheli davranışı ve saldırı göstergelerini (IOA'lar) belirlemek için karmaşık tehditlerin erken teşhisini hızlandırarak gelişmiş makine öğrenmesi algoritmalarını devreye sokar.

[5] Kaynak: ESG Araştırması Raporu, SOC Modernizasyonu ve XDR'ın Rolü, Mayıs 2022

[6] Kaynak: ESG Araştırması Raporu, SOC Modernizasyonu ve XDR'ın Rolü, 2022

[7] Kaynak: ESG Araştırması Raporu, SOC Modernizasyonu ve XDR'ın Rolü, Mayıs 2022

XDR'ın EDR, MDR, SOAR ve SIEM ekosistemiyle uyumu

Yanıt genişletilmiş X'tedir. XDR, EDR'ın sunduğu becerileri karmaşık tehditleri çok sayıda altyapı düzeyi arasında proaktif olarak algılama ve otomatik olarak müdahale etme ve bu tehditleri savuşturma şeklinde genişletir.

Çözüm bütüncül bir yaklaşım

Çeşitli araçları ve güvenlik uygulamalarını entegre ederek ve uç noktalar, ağlar, bulutlar, web sunucuları, posta sunucuları vb. içindeki verileri izleyerek, XDR tehditleri tespit etmekten ve kaldırmaktan daha fazlasını yapar. Ayrıca XDR çapraz ürün etkileşimini otomatikleştirerek bilgi güvenliği yönetimini basitleştirir.

Forrester, çoğu örnekte XDR'ın güvenlik analitik platformlarını tamamen değiştirmeyeceğine inanır ve ekler, "XDR yol alıyor ve [biz] önümüzdeki beş yıl içinde güvenlik analitik platformlarının ve XDR'ın karşı karşıya gelmesini bekliyoruz".

SIEM tehdit algılamanın ötesinde kullanım alanlarına sahip olup SOAR'ın özelleştirilebilirliği faydalıdır ancak tehditleri tespit etme ve müdahale konusunda, XDR'ın gelişmiş korumasının ileri analitiği rakipsizdir.

Gerçek zamanlı görünürlük sağlar

XDR, kuruluşunuzun güvenlik yapısına gerçek zamanlı görünürlük katar. Devam eden tehditlere kapsamlı içgörü sağlamak ve şüpheli etkinlikleri tek bir konsolda birleştirmek üzere uç noktalar, sunucular, güvenlik duvarları ve bulut platformları gibi çeşitli kaynaklardan gelen verileri toplar ve analiz eder. Bunu tamamen proaktif hale getirir. Proaktif tehdit avcılığı ve daha hızlı olay müdahalesi. Bütünsel bir bakış güvenlik ekiplerinin şüpheli etkinlikleri ve potansiyel güvenlik olaylarını daha etkili bir şekilde tanımlamalarına yardımcı olur.

Veri ve tehdit istihbaratını kavramsallaştırır

Yüksek kaliteli tehdit istihbaratını ve kapsamlı tehdit istihbaratı veri tabanını güçlendirdiğinde XDR, tehditler ve saldırganlar hakkında son derece yararlı kavramsal bilgiler sağlar. Bu zenginleştirilmiş tehdit istihbaratı, araştırma uyarılarını ve olay işlemeyi basitleştirir ayrıca güvenlik ekiplerinin tehdit aktörlerinin taktiklerini, tekniklerini ve motivasyonlarını anlamalarına yardımcı olur. Böylece daha etkili olay müdahalesine ve proaktif savunma önlemlerine olanak sağlar.

Kolaylaştırılmış güvenlik operasyonlarını etkinleştirir

Doğru bir şekilde entegre edildiğinde, en iyi çözümler otomasyonun en iyi sonuçlarını elde etmek üzere mevcut altyapınıza sorunsuz bir şekilde uyarlanacak ve zaten kullanımda olan üçüncü taraf güvenlik çözümlerini değiştirmeniz gerekmeden tam görünürlük ve farkındalık sağlayacaktır. Güvenlik olaylarının ve kullanıcı davranışının kapsamlı bir görünümünü sağlamakla bütünlüğün uyumu destekleyeceğini unutmayın.

Açık bir şekilde XDR bekleneni sunar:
Kontrol, istikrar ve tüm diğer önemli özellikleri.
Diğer yandan tüm XDR teklifleri aynı değildir...
Size uygun olanı nasıl seçersiniz?

XDR tedarikçilerini ve çözümlerini karşılaştırırken dikkate alınması gereken 5 nokta

XDR bu zorlukları şu şekilde göğüsleyebilir.

1

XDR çözümünün kalitesi ile tedarikçinin EPP ve EDR'si arasındaki sinerjide doğrudan bağlantı var

Uç nokta düzeyinde karmaşık siber tehditlerin gelişmiş algılanması ve bunlara müdahale için EDR çözümü, XDR'ın temel bileşenidir. EDR aynı zamanda çok sayıda tehditle otomatik olarak baş edebilmek için güçlü bir Uç Nokta Koruması Platformu'na (EPP) ihtiyaç duyar. Uç nokta koruma özelliklerine dikkatlice bakmak ve her tür uç nokta (bilgisayar, dizüstü, sanal makineler, mobil cihazlar ve çeşitli işletim sistemleri) için destek olup olmadığını kontrol etmek önemlidir.

2

Güncel tehdit istihbaratı ve siber suçluların taktik ve tekniklerinin tam görünümü siber tehditlerle baş etmek için temel önemdedir

Bu roket bilimi değildir. Değerini hak eden her XDR çözümü bu iki beceriyi de sunacak olup ayrıca olay araştırması ve müdahalesini iyileştirmek ve hızlandırmak üzere ek bağlam içerecektir.

3

Bütünlük üçüncü taraf çözümlerle daha sürdürülebilir ve daha az maliyetlidir.

XDR çözümünün üçüncü taraflarla ne kadar iyi entegre olduğu tamamen başka bir kritik sorundur. Çünkü karşılıklı çalışabilirlik, satın alımı başından itibaren daha sürdürülebilir bir yatırım haline getirir. Bir dizi özgün entegrasyon seçeneği sunan XDR çözümü daha fazla veri kaynağı toplayacak ve alt yapınızda ne olduğuyla ilgili daha bütünlüklü bir tablo sunacaktır.

4

Bağımsız incelemeler, global tanınırlık ve bağımsız test sonuçları önemlidir

İşletmeniz için siber güvenlik gibi önemli bir şeylere yatırım yapıyorsanız bağımsız değerlendirmeleri es geçmeyin. Bağımsız test sonuçlarını isteyin. Forrester, IDC vb. kuruluşlardan uluslararası tanınırlığı kontrol edin. Çözümler global olarak mı uygulanıyor? Vaka çalışmalarını isteyin.

5

Yatırımınız gelecek kaygısından muaf mı?

Teknoloji yerinde durmuyor. Özellikle de XDR gibi nispeten henüz yeni bir teknolojide gelişmenin devam etmesi için tedarikçinin yol haritasının ne olduğunu öğrenmeniz gerekir.

Neden Kaspersky?

En çok test edilen. En çok ödül alan. Kaspersky koruması.

Kaspersky, güvenlik uzmanlığı konusunda güçlü bir kayıt sahibi olan küresel bir siber güvenlik şirketidir. Dünyanın dört bir yanındaki kuruluşları 25 yılı aşkın süredir koruyoruz ve bunun yanı sıra ürün ve hizmetlerimiz için sayısız ödül ve övgüye layık görüldük. 2013 ve 2022 yılları arasında Kaspersky ürünleri:

587

587 birincilik elde etti

685

ilk üçe girmeyi başardı

827

827 bağımsız test ve incelemeye katıldı

Kaspersky, 2023 yılında önde gelen küresel teknoloji araştırma ve danışmanlık firması ISG tarafından XDR çözümleri sektöründe Lider seçildi. ISG, 'liderleri' hem kapsamlı bir ürün ve hizmet yelpazesine sahip hem de yenilikçi güce ve rekabet istikrarına sahip şirketler olarak tanımlamaktadır.

Daha fazla bilgi edinin

Kaspersky Extended Detection and Response

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın