Siber Güvenlik Stratejisi

XDR

El Kitabı

Giriş

Bulut bilişim, Nesnelerin İnterneti (IoT) ve dijital dönüşüm gibi trendlerin hızla benimsenmesi, şirketlerin hassas verileri için riski artırdıkça, kritik verilerin güvenliğini sağlamanın zorluğu her geçen yıl daha da artıyor. Aynı zamanda, tehdit aktörleri, her zamankinden daha karmaşık saldırıların gücünü ve ölçeğini genişletmek için bu aynı teknoloji trendlerinin çoğundan yararlanır.

Güvenlik ekipleri, ortaya çıktıkları anda yeni tehditlere yanıt vermek için araçlar dağıttı, süreçler uyguladı ve personel tuttu, ancak sayıları ve silahları yetersiz. Ancak sürekli olarak yeni yeteneklerin mevcut sistemlere eklenmesi, çok fazla kıt zaman, enerji ve kullanım becerisi gerektiren, zayıf bir şekilde entegre edilmiş bir araç karmaşası yaratır. Bulut ve uzaktan çalışma gibi hızla değişen eğilimlere ve ortamlara uyum sağlamayan statik süreçler hızla eskimiş ve etkisiz hale gelir. Ve güvenlik analistleri, hiç bitmeyen bir güvenlik uyarıları tufanını tetiklemek gibi neredeyse imkansız bir görevle görevlendirilir, ancak genellikle sınırlı eğitim ve eşit derecede sınırlı araçlar alırlar. Çok fazla uyarı ve çok az bağlamın birleşimi, güvenlik ekiplerinin görünürlüğünü ve kontrolünü kaybetmesine neden olur. Sonuçta, şirket sonuç olarak daha da fazla risk altında olur.

Genişletilmiş algılama ve yanıt (XDR), bu karmaşıklığa bir yanıt olarak ortaya çıkmıştır. XDR, altyapının yalnızca bir yönü yerine, bir şirketin altyapısındaki (ağ, uç nokta, bulut ve kimlik dahil) tüm tehdit vektörlerinde birlikte çalışan bir tehdit algılama, araştırma ve yanıt çözümleri kategorisidir. XDR araçları, tasarımı doğrudan mimariye entegre ederek, güvenlik ekiplerinin çalışma şeklini optimize eden tehdit öngörüleri ve öneriler sunar.

Bu kitap hakkında

XDR güvenlik çözümleri kategorisini ve bunun şirketiniz için ne anlama geldiğini öğrenmenize yardımcı olur. Bu kitap, aşağıdakileri araştıran beş bölümden oluşmaktadır:

- Tehditler, sınırlamalar ve zorluklar dahil olmak üzere, tespit ve müdahalenin mevcut durumu (Bölüm 1)
- XDR nedir ve ne değildir (Bölüm 2)

XDR, saldırıları durdurmak için saldırı yaşam döngüsünü nasıl kırar Bölüm 3)

Farklı XDR kullanım örnekleri (Bölüm 4)

Sahip olunması gereken XDR yetenekleri ve özellikleri (Bölüm 5)

Her bölüm kendi başına duracak şekilde yazılmıştır, bu nedenle ilginizi çeken bir konu görürseniz, o bölüme atlamaktan çekinmeyin. Bu kitabı size uygun olan herhangi bir sırayla okuyabilirsiniz (tersine ya da tersten okumanızı tavsiye etmem).

Varsayımlar

Çoğu varsayımın yararsızlıklarından kurtulduğu söylendi, ancak yine de birkaç şeyi varsayıyorum!

Temel olarak, güvenlik stratejisinin etkinliğini, özellikle de algılama ve yanıt yeteneklerini geliştirmenin daha iyi bir yolunu arayan bir kuruluşta çalıştığınızı varsayıyorum. Belki de bir bilgi güvenliği şefi (CISO), baş bilgi yetkilisi (CIO) veya baş teknoloji yetkilisi (CTO) veya bir Başkan Yardımcısı veya güvenlik müdürü gibi bir BT yöneticisisiniz. Ya da belki bir ağ veya güvenlik mimarı veya mühendisisiniz. Bu nedenle, bu kitap, modern güvenlik operasyonları kavramları ve teknolojileri hakkında genel bir anlayışa sahip teknik okuyucular için yazılmıştır.

Bu varsayımlardan herhangi biri sizi tanımlıyorsa, bu kitap tam size göre! Bu varsayımlardan hiçbiri sizi tanımlamıyorsa, yine de okumaya devam edin - XDR mutlaka bilinmesi gereken bir teknolojidir ve ekibiniz XDR'de X uzmanı olduğunuz için size teşekkür edecektir!

Bu uyarılar, annenizin sizi uyardığı şeylere işaret ediyor. Muhtemelen hayır, ancak potansiyel olarak maliyetli veya sinir bozucu hatalardan kaçınmanıza yardımcı olacak pratik tavsiyeler sunuyorlar.

IN THIS CHAPTER

- » Seeing the urgent need for a better approach to security
- » Understanding the limitations of traditional detection and response tools
- » Addressing alert fatigue and the security skills gap

1. Bölüm

Tehdit Tespiti ve Müdahalesinin Mevcut Durumuna Bakmak

Bu bölümde, modern tehditlerin potansiyel olarak daha yıkıcı hale gelmek üzere nasıl evrimleştiğini açıklıyorum; neden önleme, tespit ve müdahaleye yönelik geleneksel yaklaşımlar yeterli değil?
hayali; ve alarm yorgunluğunun ve siber güvenlik becerileri eksikliğinin kuruluşunuz için riski nasıl artırdığını.

Modern Tehdit Manzarasını İncelemek

Son zamanlarda, veri ihlalleri ve fidye yazılımı saldırıları o kadar sık hale geldi ki, pratik olarak hava durumu, spor ve trafik ile birlikte kendi haber segmentlerini garanti altına alıyorlar. Ancak bu güvenlik olaylarının olağan olması, onları daha az tehlikeli yapmaz. Aktif bir tehdit aktörünün ortamınızda faaliyet gösterdiği her dakika muazzam bir hasar meydana gelir.

Ponemon Enstitüsü'ne göre, 2020'den 2021'e kadar bir veri ihlalinin ortalama maliyeti yüzde 10 artarak 4,24 milyon dolara yükseldi. Bu, son yedi yıldaki en büyük tek yıllık maliyet artışı oldu.

Tabii ki, bu gerçeği zaten biliyor ve yaşıyorsunuz ve veri kaybı oluşmadan önce tehditleri tespit etmek ve mümkün olduğunca hızlı ve etkili bir şekilde yanıt vermek için çok çalışıyorsunuz. Ancak bu, tehdit aktörleri tarafından kullanılan ve giderek daha gelişmiş taktikler, teknikler ve prosedürler (TTP'ler) karşısında zorlu bir mücadeledir. Saldırganlar artık dosya tabanlı kötü amaçlı yazılımlar

gibi geleneksel yöntemler kullanmadan neredeyse istedikleri zaman bir ortamı tehlikeye atabilir. Bunun yerine, yetkili sistem dosyalarını tehlikeye atan, bir cihazın kayıt defterine saldırılar ekleyen veya PowerShell gibi yardımcı programları kötü niyetli olarak kullanan yöntemler kullanacaklar. Yeni ve daha kaçan saldırı yöntemlerinin artması, tehdit önlemeye ek olarak algılama ve yanıt için yeni strateji ve taktiklere olan ihtiyacı artırdı.

Bir kuruluşun modern tehdit ortamının zirvesinde kalabilmesi, etkili araçlar ve yetenekli bir güvenlik analistlerinden oluşan bir ekip gerektirir. Ne yazık ki, uygun teknoloji ve vasıflı uzmanlar dengesine sahip olmak, kuraldan ziyade çoğu kuruluş için istisna olma eğilimindedir.

Geleneksel Teknolojilerin ve Yaklaşımların Sınırlılıklarının Farkına Varmak

Güvenlik ekipleriniz kuruluşunuza yönelik başarılı saldırıları önlemeye çalışırken, hiçbir ortamın tamamen güvenli olmadığı kaçınılmaz gerçekliğine hazırlanmanız gerekir. Sonunda, bir tehdit ortamınıza girecektir.

Güvenlik ekiplerinin tehditleri bulmasına yardımcı olmak için baş döndürücü bir dizi günlük kaydı, algılama ve yanıt aracı piyasaya çıktı. Bu araçların her birinin güçlü ve zayıf yönleri vardır ve bilinen dosya tabanlı kötü amaçlı yazılım olayları veya altyapının yalnızca bir bölümünü yenmek için tasarlanmış saldırılar gibi saldırılara karşı yararlı olabilir. Ancak bu araçların çoğu tek bir amaç için ayarlanmıştır ve hiçbiri karmaşık tehditleri tek başına ele almaya özellikle uygun değildir.

ESG Research, kuruluşların yüzde 66'sının tehdit algılamalarının ve yanıt etkinliğinin, birden fazla bağımsız nokta aracına dayandığı için sınırlı olduğunu hissettiğini buldu.

Aşağıdaki bölümlerde, güvenlik ekipleri tarafından kullanılan daha yaygın günlük kaydı, algılama ve yanıt araçlarından bazılarına daha yakından bakacağım ve sizi bunların zorlukları ve sınırlamaları hakkında bilgilendireceğim.

Uç nokta algılama ve yanıt

Uç nokta algılama ve yanıt (EDR), uç nokta cihazlarındaki tehditleri tespit etmek ve araştırmak için kullanılan bir araç kategorisidir. EDR araçları tipik olarak algılama, analiz, araştırma ve yanıt yetenekleri sağlar.

EDR ilk olarak 2 013'te, kötü amaçlı yazılımları tersine mühendislik yapmak ve bir tehdit aktörünün güvenliği ihlal edilmiş bir cihazda tam olarak ne yaptığını

anlamak için çok ayrıntılı uç nokta telemetrisi gerektiren adli soruşturmalara yardımcı olmak için ortaya çıktı.

EDR araçları, şüpheli etkinlik aramak için uç nokta aracıları tarafından oluşturulan olayları izler. EDR araçlarının oluşturduğu uyarılar, güvenlik operasyonları analistlerinin olayları tanımlamasına, araştırmasına ve düzeltmesine yardımcı olur. EDR araçları ayrıca şüpheli etkinlikle ilgili telemetri verilerini toplar ve verileri ilişkili olaylardan elde edilen diğer bağlamsal bilgilerle zenginleştirebilir. Bu işlevler aracılığıyla EDR, olay müdahale ekipleri için yanıt sürelerinin kısaltılmasında etkilidir.

Ancak, yalnızca uç noktaya odaklanması nedeniyle EDR tek başına kurumsal tehdit algılaması sağlayamaz. Yönlendiriciler, anahtarlar, sunucular, Nesnelerin İnterneti (IoT) cihazları, kendi cihazını getir (BYOD) ve endüstriyel kontrol sistemi (ICS) gibi ağ ve ağ bağlantılı cihazlara aracılar yüklemeden cihazların ağ trafiğine ilişkin görünürlük sağlamaz.) — ve iş yükleri, bulut ağları ve hizmet olarak platform (PaaS) teklifleri gibi bulut kaynakları.

Uç nokta koruma platformu

Uç nokta koruma platformu (EPP), dosya tabanlı kötü amaçlı yazılım saldırılarını önlemek ve kötü amaçlı etkinliği tespit etmek için uç nokta cihazlarına yüklenen bir yazılım aracısıdır . EPP, geleneksel ana bilgisayar tabanlı antivirüs ve kötü amaçlı yazılımdan koruma çözümlerinin evrimidir ve genellikle bir uç noktada ilk savunma hattı olarak kabul edilir.

EPP çözümlerinde algılama yetenekleri değişiklik gösterir, ancak çoğu, aşağıdakiler de dahil olmak üzere bazı algılama ve önleme tekniklerinin bir kombinasyonunu kullanır:

- Statik uzlaşma göstergeleri (IOC'ler; yani imza tabanlı algılama)

  Beyaz listeye alma (izin verme) veya *kara listeye alma* (engelleme) uygulamaları, Tekdüzen Kaynak Konum Belirleyicileri (URL'ler), bağlantı noktaları ve adresler

  Davranış analizi ve makine öğrenimi

  Yürütülebilir dosyalar gibi şüpheli tehditleri patlatmak (veya test etmek) için korumalı alan

Bir EPP çözümü, faaliyet verilerinin sürekli olarak izlenmesini ve toplanmasını sağlamak için bulut tarafından yönetilmelidir ve bunun yanı sıra uç noktanın kurumsal ağda mı yoksa uzaktan mı kullanıldığına bakılmaksızın uzaktan iyileştirme eylemleri gerçekleştirme yeteneği olmalıdır. Ek olarak, EPP çözümleri bulut veri desteklidir. Başka bir deyişle, uç nokta aracısının bilinen tüm IOC'lerin yerel bir veritabanını tutması gerekmez; bunun yerine uç nokta aracısı, sınıflandıramadığı nesnelerle ilgili en son kararları bulmak ve gerçek

zamanlı tehdit istihbaratından yararlanmak için bir bulut kaynağını kontrol edebilir.

EPP, yalnızca önlemek veya kontrol etmek için tasarlanmıştır ve bu nedenle, modern saldırılara karşı savunmak için bilgi tespit etmeye veya toplamaya odaklanmaz. Çoğu EPP platformu, olayları araştırmak için gerekli müdahale yeteneklerinden de yoksundur . Sonuç olarak, EPP tek başına modern saldırıları durdurmak için gerekli özellikleri sağlamaz.

Güvenlik bilgileri ve olay yönetimi

Güvenlik bilgileri ve olay yönetimi (SIEM) yazılım araçları, çeşitli ağ cihazları ve uygulamaları tarafından oluşturulan güvenlik uyarılarının bildiriminin yanı sıra güvenlik olaylarının neredeyse gerçek zamanlı olarak toplanması, ilişkilendirilmesi ve analizini sağlar.

Birçok kuruluş, farklı güvenlik cihazlarından ve sunucu ortamlarından günlükleri toplamak için güvenlik bütçelerinin büyük bir bölümünü SIEM araçlarına ayırır. SIEM'ler başlangıçta uyumluluk raporlaması amacıyla günlük toplayıcılar olarak tasarlandı. Zamanla, kullanımları tehdit algılamaya kadar genişledi ve SIEM'ler artık birçok güvenlik operasyon merkezi (SOC) için merkezi uyarı deposu haline geldi.

Bir SIEM, uyarıları merkezileştirir ve günlük verilerini ayrıştırarak ve normalleştirerek toplar. Güvenlik ekipleri, günlük verilerini tek bir yerde görebilir, ancak genellikle anlamlı bir şekilde bir araya getirilmez ve bunları anlamlandırmakla görevlendirilen ön saflardaki analistler genellikle kullanamazlar.

uyarıları doğrulamak için daha zengin kaynak verileri içeren araçlar. Genel olarak, SIEM'ler, uç nokta verileri ve ağ verileri gibi temel veri kaynakları için analiz derinliğinden yoksundur ve kısmen bu kullanıma hazır bilgiden yoksun oldukları için dağıtılması, yapılandırılması ve bakımı zor olabilir.

Ağ algılama ve yanıt ile kullanıcı ve varlık davranışı analitiği

Ağ algılama ve yanıt (NDR) ve *kullanıcı ve varlık davranışı analitiği* (UEBA) araçları, SIEM'in bilinmeyen saldırıları tespit etmedeki zorluklarını ele almak için ortaya çıkan daha yeni bir güvenlik analitiği araçları sınıfını temsil eder. Bu araçlar, toplanan telemetriden bir etkinlik temel çizgisi geliştirmek için makine öğrenimini kullanır ve ardından kötü niyetli davranışı gösterebilecek atipik

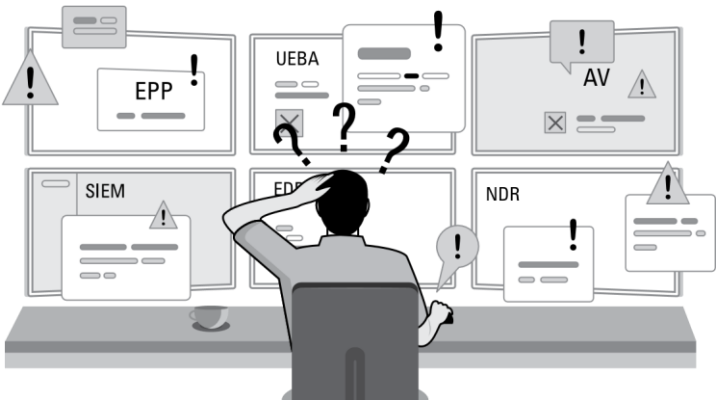
eylemleri arar. Bu teknolojiler, kuruluşların olağandışı trafik kalıplarını tanıyarak önceden bilinmeyen saldırıları belirlemesine olanak tanır.

Ancak, bu araçların da sınırlamaları vardır. Ağ tabanlı ürünler ağ ile sınırlıdır ve uç noktalarda toplanan süreç bilgileri gibi yerel olayları izleyemez veya izleyemez. NDR ayrıca çok sınırlı bir derinliğe sahiptir; EDR derin ve dar ise, NDR geniş ve sığdır.

Modern saldırıların karmaşıklığı, kötü amaçlı etkinliği belirlemek ve doğrulamak için birden çok veri kaynağının analizini gerektirir. Tek boyutlu araçlar üzerinde katman oluşturmak, güvenlik ekipleri için önemli maliyetler getirir, potansiyel kör noktalar oluşturur ve güvenlik analistlerinin konsollar arasında geçiş yapmak ve bir saldırıyı anlamlandırmak için çok fazla manuel çaba harcamasını gerektirir.

Çok Fazla Uyarı, Çok Az Zaman ve Personel

Algılama ve önleme araçları, her gün binlerce uyarı üretir; bu, güvenlik ekiplerinin etkin bir şekilde idare etmek için görevlendirildiği hacmin çok ötesindedir. Bu uyarılar birçok bağlantısız kaynaktan gelir ve güvenlik analistlerini bulmacayı bir araya getirmeye bırakır (bkz. Şekil 1-1).



ŞEKİL 1-1: Silolanmış araçlar araştırmayı ve yanıtı yavaşlatır.

Potansiyel bir tehdidi analiz etmek genellikle birkaç adım gerektirir: **1. Olabilecekleri bir** araya getirmeye başlamak için mevcut günlük verilerini gözden geçirmek

2. Göstergelerin kötü amaçlı olduğunun bilinip bilinmediğini belirlemek için verileri tehdit istihbarat kaynaklarıyla manuel olarak karşılaştırma

3. Uyarının daha büyük bir saldırının parçası olup olmadığını belirlemek için IOC'leri kullanarak ilgili olayları aramak.

4. Sistemler, ana bilgisayarlar, varlıklar, kaynaklar, IP adresleri ve her uyarıyla ilişkili dosyalar dahil olmak üzere olay etrafında bağlam toplama.

5. Bir zaman çizelgesi oluşturma ve bir uyarının temel nedenini belirleme.

6. Uyarılara yönelik yeni bilgi bağlantılarının, çabaları koordine etmek için diğer ekip üyeleri tarafından işlenip işlenmediğini kontrol etme

7. Uyarının yükseltilmesi, atılması veya hızlı bir şekilde düzeltilmesi ve kapatılması gerekip gerekmediğini değerlendirme

Tüm bu adımların geleneksel bir SOC'de tamamlanması çok zaman alır ve birden fazla araç gerektirir - ve bu sadece triyajdır. Net sonuç, analistlerin yalnızca her gün karşılaştıkları “en yüksek öncelikli” uyarıları ele almak için zamanları olmasıdır; bu arada, endişe verici sayıda "düşük öncelikli" uyarı hiç ele alınmaz. Ve bir uyarıyı "yüksek" veya "düşük" olarak sınıflandırmak için uygun bağlam olmadan, SOC gerçekten önemli olanı kaçırıyor ve/veya gerçekten kritik olmayan sorunları takip ediyor olabilir.

SOC TAKIMI NE YAPAR?

Güvenlik operasyonları ekipleri büyük ve küçük bazı temel işlevleri paylaşır. Birçok SecOps ekibi ve SOC için geleneksel bir model, bu işlevleri deneyim düzeyine dayalı olarak katmanlı bir analist yapısına böler. İşte bu katmanların birincil sorumlulukları:

- **Kademe 1 — Triyaj:** Burası, güvenlik analisti saatlerinin çoğunluğunun tipik olarak harcandığı yerdir. Kademe 1 analistler genellikle en az deneyimli analistlerdir ve birincil işlevleri, şüpheli etkinlik için olay günlüklerini izlemektir. Bir şeyin daha fazla araştırılması gerektiğini düşündüklerinde, mümkün olduğu kadar çok kaynaktan kullanıcıyı, ana bilgisayarı, IP adresini ve ilgili tüm IOC'leri içeren bir olay biçiminde bir rapor halinde toplayabildikleri kadar çok bağlamı toplarlar ve durumu iletirler. Tier 2'ye olay.

- **2. Kademe — Soruşturma:** 2. Kademe analistler, tehdidin doğasını ve çevreye ne ölçüde sızdığını belirlemek için şüpheli etkinliği derinlemesine inceler; buna, temel nedeni belirlemek için sıralamayı ve olayları ilişkilendirmek için bir zaman çizelgesi oluşturmayı da içerir. Saldırının ne kadar ileri gittiğini anlamak için daha fazla araştırma yapmaları gerekiyor. Bu analistler daha sonra sorunu çözmek için bir yanıtı koordine eder. Bu, genellikle daha fazla analist deneyimi gerektiren daha yüksek etkili bir faaliyettir.

- **Kademe 3+ — Tehdit avcılığı:** Bunlar, karmaşık olay yanıtını destekleyen ve kalan zamanını algılama yazılımı tarafından şüpheli olarak tanımlanmamış tehditler için adli ve telemetri verilerini aramak için harcayan en deneyimli analistlerdir. Ortalama bir şirket, tehdit avlama faaliyetlerine en az zaman harcar çünkü Kademe 1 ve Kademe 2'nin faaliyetleri çok fazla analist kaynağı tüketir.

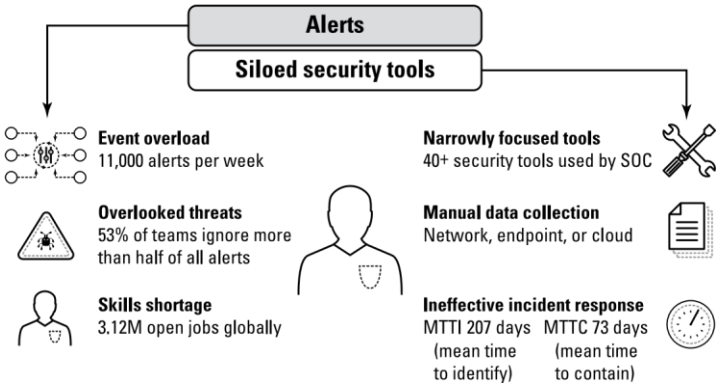
Bu model en yaygın olanı olsa da, mutlaka ideal değildir. Çoğu insan günlükleri tüm gün izlemeye pek uygun değildir. Uyarı yorgunluğu gerçektir ve bir SOC'deki sayısız sensör tarafından üretilen tüm gürültünün arasından tehditler süzülür. Bu görevi yerine getirmek için analistleri tutmak zor olabilir - araştırmalara anlamlı bir şekilde katkıda bulunmayı tercih ederler (ve eski araştırma süreçleri için gerekli teknik becerilere sahip olmadıkları için asla açıklanmayan yeni ve yenilikçi yaklaşımları olabilir). Kaynak saatlerinin çoğu tehditleri ortaya çıkarmak ve azaltmak için harcandığından, tehdit avlama ve süreç iyileştirme için çok az zaman harcanır.

Ayrıca, uyarı triyajından sorumlu güvenlik analistleri, bir saldırının kuruluşa sunduğu gerçek riski belirlemek için genellikle yetersiz bağlamla bırakılır. Bu

nedenle, uyarı daha fazla doğrulama için daha üst düzey bir gruba iletilir, daha fazla zaman, emek ve kaynak gerektirir ve her düzeyde verimsizlik yaratır.

Çoğu kuruluş, çok sayıda izleme çözümünden binlerce uyarı alır, ancak daha fazla gürültü ters etki yapar. Gelişmiş algılama, *daha fazla* uyarı ile ilgili değildir; daha *iyi*, daha uygulanabilir uyarılarla ilgilidir. Bu tür bir gelişmiş algılamaya ulaşmak, kullanımdaki tüm algılama teknolojilerinin entegrasyonunun yanı sıra ortamınızdaki saldırgan etkinliği bulmak ve doğrulamak için uç nokta, ağ ve bulut verilerini analiz eden karmaşık analitikleri gerektirir.

Tehdit tespiti için daha iyi ve daha kapsamlı araçlarla bile, uyarılarla ve olası olaylarla başa çıkmak, yetenekli müdahalecilerden daha fazla doğrulama ve önceliklendirme gerektirir. Ne yazık ki, bu güvenlik uygulayıcılarından yeterince yok ve bu önemli beceri açığı, kuruluşların saldırganlara ayak uydurma yeteneğini etkiliyor (bkz. Şekil 1-2).



ŞEKİL 1-2: Bir güvenlik analistinin birçok zorluğu.

Tehdit aktörleri, güvenlik açıklarını bulmak ve ortamınıza ilk erişim sağlamak için yüksek düzeyde otomatikleştirilmiş araçlar ve teknikler kullanır. Saldırganlar otomatik araç takımlarını daha hızlı ve daha uygun fiyata ölçeklendirebildikleri için bu, beceri boşluğunu daha da kötüleştirir.

kuruluşlar kalifiye güvenlik personeli ekleyebilir. Bu nedenle, yapabilecek araçları aramanız gerekir.

- Daha az deneyimli personelinizi daha etkin ve verimli hale getirin
- Karmaşık tehditlerin algılanmasını otomatikleştirin
- Araştırmaları basitleştirin
- Analistlerin becerilerini geliştirmelerine yardımcı olun

Uluslararası Bilgi Sistemleri Güvenlik Sertifikasyon Konsorsiyumu veya (ISC)[2], 2020 *Siber Güvenlik İş Gücü Çalışmasında,* dünya genelinde 3.12 milyon kalifiye siber güvenlik uzmanı sıkıntısı olduğunu bildiriyor. Cyberseek'e göre, bugün Amerika Birleşik Devletleri'nde 300.000'den fazla siber güvenlik iş ilanı var - bu sayının önümüzdeki yıllarda önemli ölçüde artması bekleniyor.

Birçok şirket, algılama ve yanıt işlevlerini tamamen veya kısmen yönetilen güvenlik hizmeti sağlayıcılarına (MSSP'ler) veya yönetilen algılama ve yanıt (MDR) satıcılarına dış kaynak sağlamayı tercih eder. Bu işlevi dışarıdan temin etmek, özellikle daha küçük güvenlik bütçeleri olan ekipler veya kendi güvenliklerini yönetme arzusu veya kaynakları olmayan kuruluşlar için yaygındır (ve çoğu durumda en iyi uygulama olarak kabul edilir). Ancak, kapsamlı görünürlük ve kontrol isteyen kuruluşlar, sırf araçları yetersiz olduğu için güvenliklerini dış kaynaktan temin etmek zorunda kalmamalıdır. Teknoloji yığınının da dış kaynaklı bir güvenlik ekibi için aynı derecede önemli olduğunu belirtmekte fayda var; eski araçları kullanan satıcılar, kurum içi güvenlik ekiplerinin başına bela olan aynı verimsizliklerle boğuşacak.

Gerçekten ihtiyaç duyulan şey, toplam uyarı sayısını azaltırken aynı zamanda daha az deneyimli analistlerin tehditleri kendi başlarına verimli ve güvenli bir şekilde değerlendirmelerine olanak tanıyarak, yalnızca yüksek kaliteli uyarıların daha kıdemli analistlere iletilmesini sağlayan bir dizi teknolojidir.

IN THIS CHAPTER

- » Starting with ironclad threat prevention to reduce noise
- » Ensuring end-to-end visibility in your environment
- » Reducing manual investigations to accelerate and improve incident response
- » Maximizing the value of your security investments

2. Bölüm

XDR'yi tanımlama

Extended algılama ve yanıt (XDR), tehdit algılama ve yanıtlamaya yönelik yeni bir yaklaşımdır. *XDR* terimi , 2018, baş teknoloji sorumlusu (CTO) ve . Networks'ün kurucu ortağı Nir Zuk tarafından. XDR'yi oluşturmanın temel nedeni, saldırıları daha verimli bir şekilde durdurmak, önlenemeyen saldırgan tekniklerini ve taktiklerini tespit etmek ve güvenlik operasyonları merkezi (SOC) ekiplerinin inceleme gerektiren tehditlere daha iyi yanıt vermesine yardımcı olmaktı.

XDR'deki *X , genişletilmiş* anlamına gelir , ancak gerçekten herhangi bir veri kaynağını temsil eder, çünkü bir ortamın bileşenlerine ayrı ayrı bakmak verimli veya etkili değildir. XDR, tehdit algılama ve müdahaleye proaktif bir yaklaşım getirerek, günümüzün giderek karmaşıklaşan tehditlerini ele almak için analitik ve otomasyon uygularken tüm verilerinizde görünürlük sağlar.

Bu bölümde, XDR'nin ne olduğunu ve bir XDR çözümünün temel gereksinimlerini öğreneceksiniz.

Güçlü Tehdit Önlemenin Sağlanması

XDR'nin temeli sağlam tehdit önlemedir. Bir XDR çözümü, manuel doğrulama olmadan gerçek veya neredeyse gerçek zamanlı olarak otomatik olarak engellenebilecek tehditlerin yüzde 99'undan fazlasını doğru bir şekilde engellemelidir. Sınıfının en iyisi tehdit önleme ile ekibiniz, savunmanızı aşan her olası tehdidi araştırmak için zaman kaybetmek yerine daha karmaşık ve gizli saldırıları belirlemeye ve durdurmaya odaklanabilir.

Uç nokta tehditlerini yenmek için, bir saldırının her aşamasını algılayabilen ve engelleyebilen entegre yeni nesil antivirüs (NGAV) içeren sağlam bir çözüme ihtiyacınız var - ilk istismar ve kötü amaçlı yazılım kurulumundan kötü amaçlı yazılım çalıştıran bir tehdit aktörü tarafından yürütülen yasadışı eylemlere kadar. Her savunma katmanı, bir tehdit aktörünün kaçınma tekniklerini yenecek kadar akıllı olmalı ve en son tehditleri durdurmak için sürekli olarak uyum sağlamalıdır.

Bir XDR çözümünde aşağıdaki NGAV özelliklerini arayın:

- Makine öğrenimi tabanlı yerel analiz ve tehdit önleme
- Çalışan süreçlerin dinamik analizi için davranış tabanlı tehdit önleme
- İstismar tekniği ile istismar önleme
- Dosya karmaları gibi tehdit istihbaratına dayalı bilinen tehdit önleme
- Analiz raporları ve minimum MB dosya boyutu desteği ile bulut tabanlı kötü amaçlı yazılım önleme hizmetiyle otomatik entegrasyon
- Hızla koruma sağlamak ve tehdit istihbaratını paylaşmak için sıfır gecikmeli imzalar
- Ters kabuk koruma özelliği
- Şeffaf tehdit algılama motoru güncellemeleri
- Güvenlik profilleri ve istisnalar
- Uç noktaların ad hoc ve zamanlanmış taraması
- Kötü amaçlı yazılımlara, fidye yazılımlarına ve dosyasız saldırılara karşı koruma
- Uç nokta koruması, algılama ve yanıt için tek hafif aracı

XDR çözümünüz ayrıca saldırı yüzeyinizi azaltmalı ve aşağıdakiler dahil uç nokta koruma özellikleriyle hassas verileri korumalıdır:

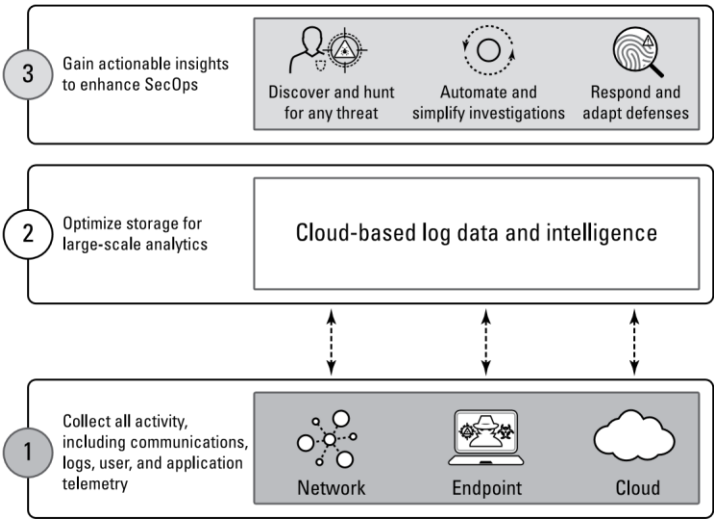
- ana güvenlik duvarı
- Disk şifreleme
- USB cihaz kontrolü
- Özelleştirilebilir önleme kuralları

Son olarak, XDR çözümünüz, güvenli uzaktan erişim, tehdit önleme ve URL filtreleme sağlamak için uç noktalar için bir ağ güvenlik istemcisi ile uyumlu olmalıdır.

Eksiksiz Görünürlük ve Tespit Sağlamak

Görünürlük ve algılama, tehdit azaltma için kritik öneme sahiptir. Bir tehdidi *göremiyorsanız* , onu tanımlayamaz veya araştıramazsınız ve kesinlikle durduramazsınız. Tehdit aktörleri, kalıcılık sağlamalarına ve değerli verileri ve fikri mülkiyeti sızdırmalarına olanak tanıyan devasa, çok yönlü saldırılar gerçekleştirmek için bulut ve makine öğreniminden yararlanır. Bu, XDR'nin aşağıdakiler dahil olmak üzere sağlam görünürlük ve algılama özelliklerine sahip olması gerektiği anlamına gelir:

Geniş görünürlük ve bağlamsal anlayış: Siled point ürünleri silo haline getirilmiş verilere yol açar - ve bu etkili değildir. Kendi ortamınızda en az tehdit aktörleri kadar çevik değilseniz, saldırılara karşı etkili bir şekilde savunma yapmayı umamazsınız. XDR, uç noktalarınızdan, ağlarınızdan ve bulut ortamlarınızdan telemetriyi entegre ederek ortamınızın tamamında görünürlük ve algılama özelliklerine sahip olmalıdır. Ayrıca, çeşitli olayların nasıl bağlantılı olduğunu ve belirli bir davranışın bağlama göre ne zaman şüpheli olduğunu (veya olmadığını) anlamak için bu veri kaynaklarını ilişkilendirebilmelidir (bkz. Şekil 2-1).



ŞEKİL 2-1: XDR, geleneksel algılama ve yanıt silolarını kırar.

Veri saklama: Saldırganlar sabırlı ve ısrarcıdır. Yavaş hareket ederlerse tespit edilmelerinin daha zor olduğunu bilirler ve karşı karşıya oldukları tespit teknolojilerinin günlük tutma sürelerini beklerler. XDR bunu onlar için kolaylaştırmamalı. Algılama sistemlerinizin ağdan, uç noktadan ve buluttan gelen verileri tek bir

havuzda toplaması, ilişkilendirmesi ve analiz etmesi gerekir, bu da 30 gün veya daha fazla geçmiş saklama süresi sunar.

Hem dahili hem de harici trafiğin analizi: Geleneksel tespit teknikleri, öncelikle harici saldırganlara odaklanır ve potansiyel tehdit aktörlerinin eksik bir görünümünü sağlar. Tespit, yalnızca çevrenin ötesinden gelen saldırıları arayamaz. Ayrıca, anormal ve potansiyel olarak kötü niyetli davranışları aramak ve kimlik bilgilerinin kötüye kullanımını belirlemek için dahili tehditlerin profilini çıkarmalı ve analiz etmelidir.

Entegre tehdit istihbaratı: Bilinmeyen saldırılarla başa çıkmak için donanımlı olmalısınız. Ölçekleri dengelemenin bir yöntemi, diğer kuruluşların ilk gördüğü bilinen saldırılardan yararlanmaktır. Algılama, küresel bir işletme ağı genelinde toplanan tehdit istihbaratına dayanmalıdır. Genişletilmiş ağ içindeki bir kuruluş bir saldırı tespit ettiğinde, kendi ortamınızdaki sonraki saldırıları belirlemek için bu ilk saldırıdan edindiğiniz bilgileri kullanabilirsiniz.

Özelleştirilebilir algılama: Kuruluşunuzu korumak, belirli sistemler, farklı kullanıcı grupları ve çeşitli tehdit aktörleriyle ilişkili benzersiz zorluklar sunar. Algılama sistemleri, ortamınızın özel ihtiyaçlarına göre son derece özelleştirilebilir olmalıdır. Bu zorluklar, hem özel hem de önceden tanımlanmış algılamaları destekleyen bir XDR çözümü gerektirir.

Makine öğrenimi tabanlı algılama: Yetkili sistem dosyalarını tehlikeye atan, komut dosyası oluşturma ortamlarını kullanan ve kayıt defterine saldıranlar gibi geleneksel kötü amaçlı yazılımlara benzemeyen saldırılarla, algılama teknolojisinin toplanan tüm telemetriyi analiz etmek için gelişmiş analitik teknikleri kullanması gerekir. Bu yaklaşımlar, denetimli ve yarı denetimli makine öğrenimini içerir.

Aşağıdaki temel görünürlük ve algılama gereksinimlerini karşılayan bir XDR çözümü arayın:

Ağ trafiğini, uç nokta olaylarını ve zaman içindeki kullanıcı olaylarını analiz ederek davranışı profillemek ve bir saldırının göstergesi olan anormallikleri tespit etmek için davranış analizi

Denetimli ve denetimsiz makine öğrenimi yetenekleri

Önceden tanımlanmış ve özelleştirilebilir davranış tabanlı algılama kuralları

Saldırıları geriye dönük olarak tespit edebilen özel kurallar

Uç nokta, ağ, bulut veya üçüncü taraf uyarılarının isteğe bağlı ayarlanması için ayrıntılı uyarı istisnaları

Bulut tabanlı kötü amaçlı yazılım analiz hizmetinden güvenlik duvarlarına, uç nokta aracılarına ve algılama ve yanıt hizmetlerine

kitle kaynaklı tehdit istihbaratını dağıtmak için paylaşılan tehdit istihbaratı

JavaScript Object Notation (JSON) ve virgülle ayrılmış değerler (CSV) formatlarında üçüncü taraf kaynaklardan gelen tehdit istihbaratı akışlarını kullanma yeteneği

Keşif, yanal hareket, komuta ve kontrol ve sızma dahil olmak üzere saldırı yaşam döngüsü boyunca saldırı tekniklerinin tespiti

MITRE Adversarial Tactics, Techniques ve Techniques aracılığıyla saldırgan taktiklerini ve tekniklerini tespit etme yeteneği gösterildi Ortak Bilgi (ATT&CK) değerlendirmeleri

Uyarılarda ve tespit kurallarında MITRE ATT&CK taktik ve tekniklerinin etiketlenmesi

Hileli cihaz keşfi ile varlık yönetimi

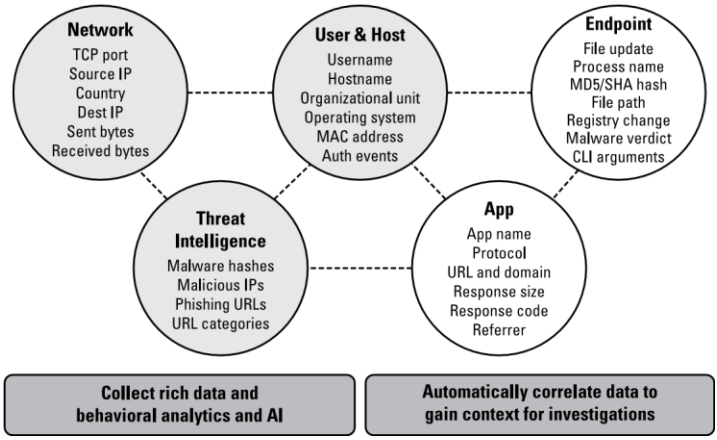
Güvenlik açığı değerlendirmesi

Ayrıntılı kullanıcı, sistem ve uygulama bilgileriyle envanteri barındırın

Soruşturma ve Müdahalenin Hızlandırılması

Ortamınızdaki olası tehditlere karşı uyarıldığınızda, bu tehditleri hızlı bir şekilde öncelik sırasına koyabilmeniz ve araştırabilmeniz gerekir. Bunu, özellikle ortamınızın birden çok bölümüne dokunan bir saldırı sırasında etkin bir şekilde yapmak, geleneksel algılama ve yanıt sistemlerinin başarısız olduğu yerdir. XDR çözümleri, aşağıdakileri içeren araştırma ve yanıt yetenekleriyle bu süreci önemli ölçüde iyileştirebilir:

- **İlgili uyarıların ve telemetri verilerinin korelasyonu ve gruplandırılması:** Kuruluşunuza yönelik saldırılar söz konusu olduğunda, zaman çok önemlidir. Bir tehdit uyarısı aldığınızda, saldırgan ortamınızdaki görevlerini yerine getirmek ve hedeflerine ulaşmak için zaten çok çalışıyor. Saldırıyı ve tam nedensellik zincirini hızlı bir şekilde anlayabilmeniz gerekir. Bu, XDR aracınızın öncelikle ilgili uyarıları otomatik olarak gruplayarak ve en acil olarak ilgilenmenizi gerektiren olaylara etkin bir şekilde öncelik vererek gürültüyü azaltması gerektiği anlamına gelir. Ardından XDR aracınız, ağınızdan, uç noktanızdan ve bulut ortamlarınızdan etkinlik günlüklerini bir araya getirerek saldırının bir zaman çizelgesini oluşturabilmelidir. Aktiviteyi görselleştirerek ve olayları sıralayarak, tehdidin temel nedeni belirlenebilir ve potansiyel hasar ve kapsam değerlendirilebilir (bkz. Şekil 2-2).



ŞEKİL 2-2: XDR, herhangi bir kaynaktan veri toplar, daha iyi tespit ve arama için bunları ilişkilendirir ve birleştirir.

Tek bir yerde tüm adli yapılara, olaylara ve tehdit istihbaratına anında erişim ile olaylara ilişkin hızlı araştırma: Olay günlükleri, kayıt defteri anahtarları, tarayıcı geçmişi ve çok daha fazlası gibi önemli yapıları inceleyerek saldırgan etkinliğini hızla tespit edin. Adli tıp, uç nokta koruması ve algılama ve yanıt için tek amaçlı aracılar performansı azaltabilir ve karmaşıklığı artırabilir. Bir olayı çözmek için giriş noktasını bulmanız ve kalıntıların izini sürmeniz gerekir - düşmanlar izlerini kapatmaya çalışsalar bile.

Hızlı bir şekilde dönme yeteneğine sahip birleştirilmiş kullanıcı arabirimleri: Güvenlik analistleriniz, uyarıları araştırmaya başladıklarında, herhangi bir kaynaktan gelen uyarıların temel nedenini tek bir tıklamayla anlamalarını sağlayan modern bir çalışma ortamına ihtiyaç duyar. Analistler, birden fazla farklı araç arasında geçiş yaparak zaman kaybetmek zorunda kalmamalıdır.

Manuel ve otomatik tehdit avı: Artan sayıda kuruluş proaktif olarak aktif düşmanları avlayarak, analistlerinin saldırı hipotezleri geliştirmesine ve çevrede ilgili faaliyeti aramasına olanak tanır. Tehdit avcılığını desteklemek, hipotezleri kanıtlamak için kanıt aramak için güçlü arama yeteneklerinin yanı sıra genişletilmiş ağda halihazırda görülen etkinlikleri aramak için entegre tehdit istihbaratı gerektirir. Bu tehdit istihbaratı, tonlarca manuel analist çalışması gerektirmeden (örneğin, bilinen bir kötü amaçlı IP adresi için çok sayıda tehdit istihbaratı beslemesini aramak için 30 farklı tarayıcı sekmesi açmak) bir tehdidin daha önce görülüp görülmediğini netleştirecek şekilde entegre edilmeli ve otomatikleştirilmelidir.).

Koordineli müdahale: Tehdit faaliyeti tespit edildikten ve araştırıldıktan sonra, bir sonraki adım verimli ve etkili iyileştirme ve politika uygulamasıdır. Sisteminiz, ağınız, uç noktanız ve bulut

ortamlarınız genelinde etkin tehditlere yönelik bir yanıtı koordine edebilmeli ve gelecekteki saldırıları önleyebilmelidir. Bu, önleme teknolojileri arasındaki iletişimi içerir (yani, ağda engellenen bir saldırı, uç noktalardaki ilkeleri otomatik olarak günceller), ya yerel olarak ya da uygulama programlama arabirimleri (API'ler) aracılığıyla oluşturulur. Ayrıca, bir analistin doğrudan XDR arabirimi aracılığıyla yanıt eylemleri gerçekleştirme yeteneğini de içerir.

Bir XDR çözümünde aşağıdaki araştırma ve yanıt yeteneklerini arayın:

Uç nokta verileri mevcutsa, ağ uyarıları da dahil olmak üzere herhangi bir uyarının otomatik kök neden analizi

Bir uyarıya yol açan yürütme zincirlerinin görselleştirilmesi

Bir zaman çizelgesindeki tüm eylemleri ve uyarıları görmek için zaman çizelgesi analizi görünümü

Güvenlik ihlali (IOC'ler) ve uç nokta davranışları, çevrimiçi ve çevrimdışı ana bilgisayarlar, güvenlik duvarlarından ağ trafiği günlükleri ve kimlik yönetimi sağlayıcılarından kimlik doğrulama günlükleri için sorgulama

Joker karakterler, normal ifadeler, JSON, veri toplama, alan ve değer işleme, farklı kaynaklardan gelen verilerin birleştirilmesi ve veri görselleştirme desteği ile gelişmiş sorgulama dili

Bir analistin, ayrıntılı filtreleme ve sorgu sonuçlarını sıralama ile görünümler arasında kolayca geçiş yapabilme yeteneği

Araştırmaları basitleştirmek ve kötü niyetli IP adreslerine veya etki alanlarına erişimi engellemek için tehdit istihbaratı, olaylar ve ilgili olaylar dahil ilgili İnternet Protokolü (IP) veya karma bilgilerinin tek bir görünümde otomatik olarak toplanması Bir olayın bir uç nokta aracısı tarafından engellenip engellenmediğinin belirlenmesi, güvenlik duvarı veya başka bir önleme teknolojisi ve çalışan işlemleri görüntülemek, askıya almak veya sonlandırmak veya ikili dosyaları indirmek için uzaktan yetenek

Güvenlik duvarı uyarıları gibi güvenlik uyarılarının uç nokta verilerine otomatik olarak eklenmesi

Gürültü engelleme ve önemli olmayan ikili dosyaların ve dinamik bağlantı kitaplıklarının (DLL'ler) zincirden kaldırılması

taktik, teknik ve prosedürlerin SOC analist bağlamı
TTP'ler) gelecekteki araştırmalara yardımcı olmak için edinilen bilgileri kullanmak

Güvenlik düzenleme, otomasyon ve yanıt (SOAR) ve güvenlik bilgileri ve olay yönetimi (SIEM) çözümleriyle entegrasyon

En kritik tehditleri hızla sıfırlamak için yüksek riskli olayların sıralanmasına ve önceliklendirilmesine olanak tanıyan olay

puanlaması; bir uyarıdaki kullanıcılar veya ana bilgisayarlar dahil olmak üzere uyarı özelliklerine dayalı olay puanları oluşturma

Kötü amaçlı dosyaları karantinaya alma ve çalışma dizinlerinden kaldırma

Uç nokta dosyalarını dizine ekleyerek kuruluşunuzdaki dosyaları gerçek zamanlı olarak hızla bulma ve silme

Python, PowerShell veya sistem komutlarını veya betiklerini çalıştırmak için uç noktalara doğrudan erişim; aktif süreçleri gözden geçirmek ve yönetmek; ve dosyaları görüntüleme, silme, taşıma veya indirme

Güvenlik Etkinliğini Artırma

XDR, olayları ele almanın genel maliyetlerini önemli ölçüde azaltır. Ayrıca tehdit kapsamını iyileştirerek mali zararı ve kaybı en aza indirir. Bu, personel eksikliğini önlemeye veya üstesinden gelmeye yardımcı olmak için güvenlik ekibinizin verimliliğini ve etkinliğini artırmak, değerlerini artırmak için mevcut araçlarınızın entegrasyonunu iyileştirmek ve ölçeklenebilir altyapı ve yapay zeka (AI) ile zaman içinde önleme etkinliğinizi güçlendirmek anlamına gelir. Bu kriterleri karşılamak için XDR'nin aşağıdaki yeteneklere sahip olması gerekir:

Herhangi bir kaynaktan veri alımı: Günümüzde her kuruluş, birbirinden farklı, silolar halinde güvenlik araçları içeren karma bir çantaya sahiptir. Bir XDR çözümü, bu farklı araçların her birinden gelen verilere ne kadar fazla görünürlük sağlayabilirse, sağlayabileceği güvenlik o kadar kapsamlı olur. En iyi XDR çözümleri, hem değeri hem de etkinliği en üst düzeye çıkarmak için ortamınızdaki diğer araçlardan veri alma esnekliğine sahip olacaktır.

Ölçeklenebilir depolama ve bilgi işlem: Günümüzün tehdit aktörlerinin kalıcılığı göz önüne alındığında, aylar hatta yıllar sürebilen "düşük ve yavaş" saldırılarda saldırgan etkinliğinin önemli adli kanıtlarını sağlayabilecek telemetriyi atmak istemezsiniz. Tüm bu telemetriyi etkin bir şekilde kullanabilmek için analitik beygir gücüne de ihtiyacınız var. Bulut tabanlı XDR platformları, bu neredeyse sınırsız erişilebilirlik ve ölçeği sağlar.

Zamanla iyileştirme: Giderek karmaşıklaşan saldırıları tespit etmek, manuel çabaları azaltmak ve güvenlik analistlerinin daha etkili ve verimli olmasını sağlamak için otomasyon ve düzenlemenin yanı sıra yerleşik AI ve makine öğrenimi gerektirir. XDR çözümleri, deneyimlerden öğrenmeli, gelecekteki riski azaltmalı ve tespit, araştırma ve müdahale yoluyla kazanılan bilgileri uygulayarak önlemeyi sürekli olarak güçlendirmelidir.

Basitleştirilmiş dağıtım: Güvenlik ekipleri, Windows, macOS, Linux, Chrome OS ve Android sistemleri dahil olmak üzere tüm uç noktalarına XDR aracılarını hızla yükleyebilmelidir. XDR aracılarının, mobil cihazlar ve özel, genel, karma ve çoklu bulut ortamları dahil olmak üzere tüm dijital varlıkları koruması gerekir. Bulut iş yükleriyle birlikte güvenliğin ölçeklenmesini sağlamak için XDR çözümlerinin sorunsuz Kubernetes dağıtımını desteklemesi gerekir.

Raporlama ve gösterge tabloları: Güvenlik ekiplerinin, kuruluşun güvenlik duruşunu ve operasyonel ölçümlerini anlayabilmesi ve iletebilmesi gerekir. XDR çözümleri, sezgisel ve özelleştirilebilir raporlar ve panolar aracılığıyla daha iyi güvenlik sonuçları sağlama ve güvenlik durumunu özetleme yeteneğine sahip olmalıdır.

XDR, analist topluluğu, güvenlik satıcıları ve genel olarak son kullanıcılar tarafından sektörde kabul görüyor ve ilgi görüyor, ancak diğer güvenlik çözümü kategorileri gibi, bir dizi "tat" içeriyor. Ve bazı XDR "tatları" yalnızca uç nokta algılama ve yanıtın (EDR) yeniden markalaşması olduğundan, satıcılar mutlaka aynı yetenekleri paylaşmazlar. Dikkat etmekte fayda var.

O halde, bir çözümün XDR çoğunluğunu kullanan başka bir satıcının aksine gerçek XDR olup olmadığını belirlemek için piyasada bulunan çeşitli seçenekler arasında nasıl ayrım yapabilirsiniz? Aşağıdaki özellikler, ayrıntılı olmasa da, kazananları özentilerden ayırmaya yardımcı olabilir.

Gerçek bir XDR çözümü:

- Tüm veri kaynaklarından (üçüncü taraf veri kaynakları dahil) verileri alabilmeli, normalleştirebilmeli ve işleyebilmelidir.
- Verilerin basit bir korelasyonunu değil, verilerin birleştirilmesini sağlamalıdır
- Bulutta yereldir ve etkili bir şekilde sonsuz derecede ölçeklenebilir
- Ağ, uç nokta, kimlik ve bulut verilerini yerel olarak tek bir "öykü" veya çapraz veri analitiği için entegre günlük kaydında birleştirir
- Bir olayın tüm hikayesini tek bir görünümde göstermek için akıllı, gelişmiş mantık uygular
- Kanıtları ve yapıları MITRE ATT&CK çerçevesine otomatik olarak eşler
- Derin adli analiz gerçekleştirmek için yerleşik bir yetenek sağlar
- Birinci sınıf güvenlik araştırma ve güvenlik hizmetleri ekipleri tarafından desteklenmektedir

Çözüm, önce önleme yaklaşımını benimsiyor mu?

XDR, "genişletilmiş algılama ve yanıttır" ve gücü, herhangi bir tehdit ve saldırıdan önce engelleyebilen, bozabilen ve içerebilen cihazlarla derin bir entegrasyon düzeyinde birlikte çalışma yeteneğinde yatmaktadır.

hasar oluşur. Bu cihazların en önemlileri, yeni nesil ağ güvenlik duvarları ve uç noktalarıdır, çünkü ağ, iletişimin ve uç noktaların tam kaydını ve kullanıcıların tüm uygulamalar ve verilerle nasıl etkileşime girdiğini temsil eder.

Çözüm, algılamaları yalnızca uç noktada mı temel alıyor?

Çözüm, yönetilmeyen cihazlar da dahil olmak üzere kimlik, bulut ve ağ verilerine dayalı saldırıları algılayabilir mi? Bazı "XDR" satıcıları, uç nokta aracılarından toplanan ağ trafiğini gerçekten kastettikleri zaman ağ verilerini gördüklerini söyleyecektir.

Gerçek bir XDR, herhangi bir verinin tehdit etkinliğiyle ilişkilendirilmesine ve rakip hareketin daha ayrıntılı bir resmini sağlamaya yardımcı olmak için MITRE ATT&CK TTP'lerle etiketlenmesine olanak tanır.

Çözümün yerel araştırma ve yanıt yetenekleri var mı?

Gerçek bir XDR:

- Yanıt önerilerini otomatikleştirmek için güvenlik analitiğini kullanır
- Uç noktada yerel yanıt eylemlerine izin verir
- Yanıt için SOAR gibi diğer araçlarla entegrasyonları destekleyebilir, ancak gerektirmez
- Yalnızca uç nokta yerine uç nokta ağı ve bulut uygulama noktalarında yanıt verilmesini sağlar
- Analist tarafından optimize edilmiş araştırma ve arama yöntemlerini kullanarak tüm üçüncü taraf veri kaynaklarında geçici arama için yerel desteğe izin verir
- MITRE ATT&CK ile eşlenen, ilgili tüm kötü amaçlı yapıları, ana bilgisayarları, kullanıcıları ve ilişkili uyarıları ortaya çıkararak önceliklendirme ve araştırmaları optimize eder
- MITRE ATT&CK'ya dayalı olarak hedeflenen yanıt eylemleri için akıllı öneriler sağlayabilir

IN THIS CHAPTER

- » Taking a closer look at the attack life cycle
- » Exploring an example of a multifaceted attack

3. Bölüm

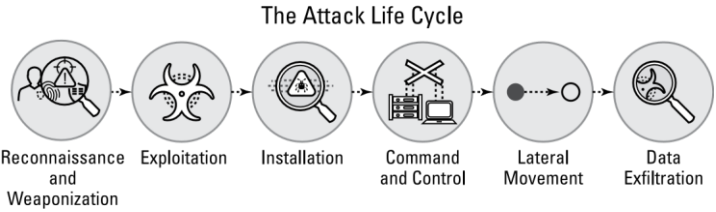
XDR ile Saldırı Yaşam Döngüsünü Kırmak

Tehdit aktörleri, yüksek değerli bir sunucuya veya varlığa yönelik doğrudan saldırılardan ("şok ve huşu"), istismarları, kötü amaçlı yazılımları, gizliliği, ve koordineli bir ağ saldırısında kaçınma ("düşük ve yavaş").

Bu bölümde, saldırı yaşam döngüsü ve genişletilmiş algılama ve yanıtın (XDR) ortamınıza yönelik saldırıları durdurmak için yaşam döngüsünü kırmanıza nasıl yardımcı olduğunu öğreneceksiniz. Bu bölüm, bir saldırının ortak aşamalarının genel bir temsilini özetlemektedir. Birçok güvenlik ekibi, bir saldırının çeşitli aşamalarında tehditleri takip etmelerine yardımcı olmak için MITRE Düşmanca Taktikler, Teknikler ve Ortak Bilgi (ATT&CK) çerçevesini benimsemiştir. Gerçek bir XDR, bir rakibin attığı her adımı tespit edebilmeli ve araştırmaları basitleştirmek için her adımı MITRE ATT&CK taktikleri ve teknikleri ile eşleştirebilmelidir.

Saldırı Yaşam Döngüsünü Anlamak

Saldırı yaşam döngüsü, bir saldırganın bir ağa sızmak ve değerli verileri sızdırmak (veya çalmak) için geçtiği olayların (veya adımların) sırasını gösterir. Bu adımlar, ilk güvenlik açığından yararlanma, kötü amaçlı yazılım yükleme, komuta ve kontrol, yanal hareket ve sızmayı içerir (bkz. Şekil 3-1).



ŞEKİL 3-1: Başarılı saldırılar birden fazla adım gerektirir.

Yaşam döngüsünün başlarındaki adımları tespit edebilirseniz, saldırganların bir saldırının sonraki aşamalarını yürütmesini durdurabilirsiniz. Aşağıdaki bölümler, saldırı yaşam döngüsüne ve XDR'nin bu yaşam döngüsünü kırmanıza nasıl yardımcı olduğuna daha yakından bakıyor.

Keşif

Tehdit aktörleri saldırılarını titizlikle planlar. Hedefleri araştırır, belirler ve seçerler, genellikle hedeflenen çalışanların sosyal medya profillerinden veya kurumsal web sitelerinden sosyal mühendislik ve kimlik avı şemaları için faydalı olabilecek kamuya açık bilgileri çıkarırlar. Saldırganlar ayrıca ağ analizörleri, ağ güvenlik açığı tarayıcıları, parola kırıcılar, bağlantı noktası tarayıcıları ve web uygulaması güvenlik açığı tarayıcıları gibi ağ güvenlik açıklarını, hizmetleri ve yararlanabilecekleri uygulamaları taramak için çeşitli araçlar kullanır.

XDR, yetkisiz bağlantı noktası ve güvenlik açığı taramalarını, ana bilgisayar taramalarını ve diğer şüpheli etkinlikleri tespit etmek ve önlemek için ağ trafiği akışlarının sürekli izlenmesi ve denetlenmesi yoluyla keşif sırasında yaşam döngüsünü kırar.

Silahlanma

Ardından, saldırganlar bir hedef uç noktanın güvenliğini aşmak için hangi yöntemlerin kullanılacağını belirler. Bir Microsoft Word belgesi veya e-posta mesajı gibi görünüşte zararsız dosyalara davetsiz misafir kodunu yerleştirmeyi seçebilirler. Veya, yüksek oranda hedefli saldırılar için, saldırganlar çıktıları hedef kuruluş içindeki bir bireyin özel ilgi alanlarına uyacak şekilde özelleştirebilir. Saldırganlar daha sonra, silahlaştırılmış yüklerini örneğin e-posta, anlık mesajlaşma (IM), doğrudan indirme (son kullanıcının web tarayıcısının otomatik olarak uç noktaya kötü amaçlı yazılım indiren bir web sayfasına yönlendirildiği) aracılığıyla hedef bir uç noktaya ulaştırmaya çalışırlar. arka planda) veya virüslü dosya paylaşımı.

Bir saldırının bu aşamasında yaşam döngüsünü kırmak zordur çünkü silahlanma genellikle saldırganın ağı içinde gerçekleşir. Bununla birlikte, yapıtların analizi

(hem kötü amaçlı yazılım hem de silah yapıcı), teslimat denendiğinde etkili sıfır gün koruması sağlamak için önemli tehdit istihbaratı sağlayabilir. XDR, kötü amaçlı veya riskli web sitelerini, uygulamaları ve İnternet Protokolü (IP) adreslerini etkili bir şekilde engellemek ve bilinen ve bilinmeyen kötü amaçlı yazılımları ve açıklardan yararlanmaları önlemek için tüm ağ trafiğinde görünürlük sağlar.

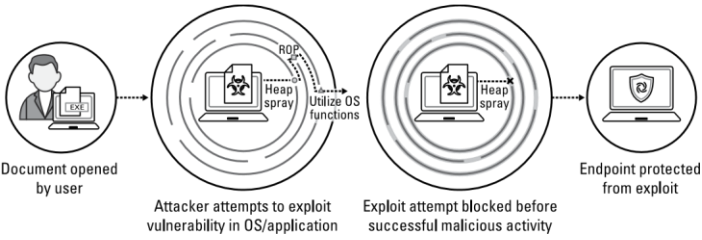
sömürü

Silahlaştırılmış bir yük, hedef bir uç noktaya teslim edildikten sonra tetiklenmelidir. Bir son kullanıcı, örneğin kötü amaçlı bir bağlantıyı tıklatarak veya bir e-postadaki virüslü bir eki açarak farkında olmadan bir istismarı tetikleyebilir veya bir saldırgan, hedef ağdaki bilinen bir sunucu güvenlik açığına karşı bir istismarı uzaktan tetikleyebilir.

Bir saldırının bu aşamasında yaşam döngüsünü kırmak, aşağıdakileri içeren XDR özelliklerini gerektirir:

- Güvenlik açığı ve yama yönetimi
- Kötü amaçlı yazılım algılama ve önleme
- Tehdit istihbaratı (bilinen ve bilinmeyen tehditler dahil)
- Riskli, yetkisiz veya gereksiz uygulama ve hizmetleri engelleme
- Tüm ağ, uç nokta ve bulut etkinliğini günlüğe kaydetme ve izleme

Etkili bir XDR aracısı, saldırganların uygulamaları manipüle etmek için kullandığı istismar tekniklerini engelleyerek bilinen, sıfır gün ve yama uygulanmamış güvenlik açıklarını önler. Binlerce istismar olmasına rağmen, bunlar genellikle nadiren değişen küçük bir dizi istismar tekniğine dayanır. XDR, bu teknikleri bloke ederek, uç noktalar tehlikeye atılmadan önce istismar girişimlerini önler (bkz. Şekil 3-2).



ŞEKİL 3-2: Gelişmiş bir XDR çözümü, istismarların kendisinden ziyade istismar tekniklerine ve davranışlarına odaklanır.

Kurulum

Ardından, bir saldırgan, güvenliği ihlal edilen uç noktada ayrıcalıkları yükseltir (örneğin, uzaktan kabuk erişimi kurarak ve kök setleri veya başka kötü amaçlı yazılımlar yükleyerek). Uzaktan kabuk erişimiyle, saldırgan uç noktanın denetimine sahiptir ve sanki fiziksel olarak uç noktanın önünde oturuyormuş gibi bir komut satırı arabiriminden (CLI) ayrıcalıklı modda komutları yürütebilir. Saldırgan daha sonra, saldırı kodunu yürüterek, diğer fırsat hedeflerini belirleyerek ve kalıcılık sağlamak için ek uç noktalardan ödün vererek hedefin ağı boyunca yanal olarak hareket edecektir.

Bir saldırının bu aşamasında yaşam döngüsünü kırmanın anahtarı, uç noktaya yüklemeyi önlemek ve saldırganların ağ içindeki yanal hareketini sınırlamak veya kısıtlamaktır. XDR, kurulumu önlemek için uç nokta algılama ve yanıt (EDR) ve uç nokta koruma platformu (EPP) teknolojilerinden yararlanır. XDR ayrıca Zero Trust modelinde bölgeler veya segmentler arasındaki tüm trafiği izler ve denetler ve ortamda izin verilen uygulamaların ayrıntılı kontrolünü sağlar.

Komuta ve kontrol

Tehdit aktörleri, İnternet üzerinden komuta ve kontrol sunucularına geri şifreli iletişim kanalları kurar. Bu yaklaşım, kurban ağı içinde ek fırsat hedefleri tespit edildiğinden saldırı amaçlarını ve yöntemlerini değiştirmelerine ve ayrıca saldırı yapaylıkları keşfedilirse kuruluşun uygulamaya çalışabileceği yeni güvenlik önlemlerinden kaçınmalarına olanak tanır. Saldırganın saldırıyı uzaktan yönetmesini ve saldırı hedeflerini gerçekleştirmesini sağladığı için iletişim bir saldırı için çok önemlidir. Bir saldırının başarılı olması için komuta ve kontrol trafiğinin esnek ve gizli olması gerekir.

Bir saldırının bu aşamasında yaşam döngüsünü kırmak aşağıdakileri gerektirir:

- Tüm ağ trafiğini denetleme (şifreli iletişimler dahil)
- Komut ve kontrol karşıtı imzalarla giden komut ve kontrol iletişimlerini engelleme (dosya ve veri deseni yüklemeleriyle birlikte)
- Bilinen kötü amaçlı Tekdüzen Kaynak Buluculara (URL'ler) ve IP adreslerine giden tüm iletişimleri engelleme
- Bağlantı noktası kaçırma yöntemlerini kullanan yeni saldırı tekniklerini engelleme
- Ağ üzerinde anonimleştiricilerin ve proxy'lerin kullanımını önleme
- Etki Alanı Adı Sistemini (DNS) kötü amaçlı etki alanları için izleme ve DNS çöküntüsü veya DNS zehirlenmesi ile mücadele

Güvenliği ihlal edilmiş uç noktaları belirlemek veya engellemek ve saldırı trafiğini analiz etmek için kötü niyetli giden iletişimleri bal küplerine yönlendirmek

Yanal hareket ve sızma

Saldırganların çoğu zaman veri hırsızlığı da dahil olmak üzere birden çok farklı saldırı hedefi vardır; kritik sistemlerin, ağların ve verilerin yok edilmesi veya değiştirilmesi; ve hizmet reddi (DoS). Yaşam döngüsünün bu son aşaması, bir saldırgan tarafından saldırının erken aşamalarını başka bir hedefe ilerletmek için de kullanılabilir. Örneğin, bir saldırgan, birincil hedef olan bir iş ortağını ihlal etmek için bir şirketin extranetini tehlikeye atabilir. Bu tür tedarik zinciri saldırıları 2020 yılında SolarWinds saldırısıyla manşet oldu.

Bu aşamada yaşam döngüsünü kırmak, veri hırsızlığını ve diğer kötü niyetli veya yetkisiz eylemleri otomatik olarak algılayabilen ve önleyebilen XDR araçlarını gerektirir.

Bir Saldırı Örneğine Bakmak

Saldırı yaşam döngüsünün tüm adımlarını ve bir saldırıdaki rollerini görselleştirmeye yardımcı olmak için, varsayımsal bir saldırıya daha yakından bakalım. Şekil 3-3'te, bir tehdit aktörü bir hedefe saldırmak için aşağıdaki adımları uygular: 1. Sömürü.

Saldırgan, sunucunun kontrolünü ele geçirmek için web sunucusundaki hatalardan yararlanır.

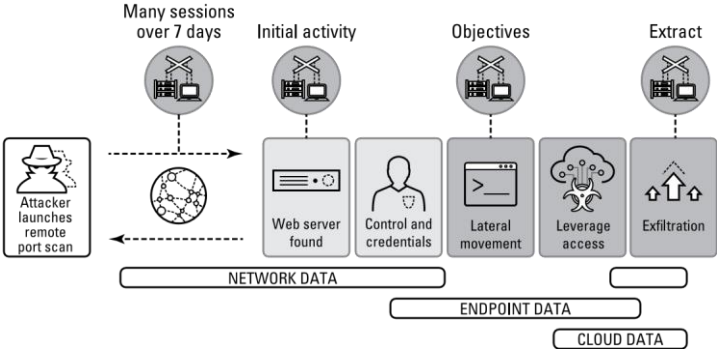
2. Kurulum.
Saldırgan, mimikatz'i yüklemek ve yönetici kimlik bilgilerine erişmek için sunucunun denetimini kullanır.

3. Komuta ve kontrol.
Saldırgan, kalıcılık ve komuta ve kontrol iletişimi kurmak için ek kötü amaçlı yazılım ve uzaktan erişim araçları yükler.

4. Yanal hareket.
Düşman ağ üzerinde yanal olarak hareket eder, birden çok uç noktadan ödün verir ve özel ve genel bulut uygulamalarına erişir.

5. Erişim ve sızma.

Saldırgan sunucudaki yapılandırma dosyalarına bakar, arka uç veritabanı konumunu bulur, veritabanını sorgular ve sonuçları yerel bir dosyaya kaydeder. Toplanan veriler, "yetkili" veya "yaptırım uygulanmış" bir bulut depolama konumuna yüklenir. Saldırgan daha sonra verileri içeren dosyayı veritabanından siler, yerel günlükleri temizler ve oturumu kapatır.



ŞEKİL 3-3: XDR, her kaynaktan veri topladığı ve diğer araçların kaçırdığı saldırı taktiklerini tespit edip durdurabildiği için bu gelişmiş, çok adımlı saldırıları benzersiz bir şekilde durdurabilir.

Bir XDR platformu, saldırı yaşam döngüsü boyunca düşman taktiklerini tespit etmek ve durdurmak için çok sayıda veri türünü toplar ve analiz eder.

IN THIS CHAPTER

- » Detecting threat activity with XDR
- » Managing and validating alerts
- » Accelerating investigations and response
- » Enabling proactive threat hunting

4. Bölüm

XDR Kullanım Durumlarını Keşfetmek

Bu bölümde, kuruluşunuzun algılama, uyarı triyaj ve doğrulama, otomatikleştirme dahil algılama ve yanıt yeteneklerini geliştirmesine yardımcı olacak en yaygın kullanım örneklerini tanıtıyorum.
soruşturma ve müdahale ve tehdit avcılığı.

Tespit etme

Başarılı siber saldırıları durdurmak için saldırı yaşam döngüsünün her aşamasında saldırıları tespit etmeye odaklanmalısınız. Genişletilmiş algılama ve yanıt (XDR), kuruluşunuzun benzersiz özelliklerini keşfetmek için makine öğrenimini kullanır ve manuel analiz veya statik korelasyon kurallarıyla mümkün olanın ötesinde tehdit etkinliği ile normal etkinlik arasında ayrım yapmasına olanak tanır. Bu makine öğrenimi, gelişmiş analitik, profil oluşturma ve davranışsal tehdit algılamayı destekler. Bu kapsamlı algılama sayesinde bir XDR çözümü, hedefli saldırılar, kötü niyetli kişiler ve daha fazlası dahil olmak üzere kötü niyetli etkinlikleri algılama yeteneğini geliştirir.

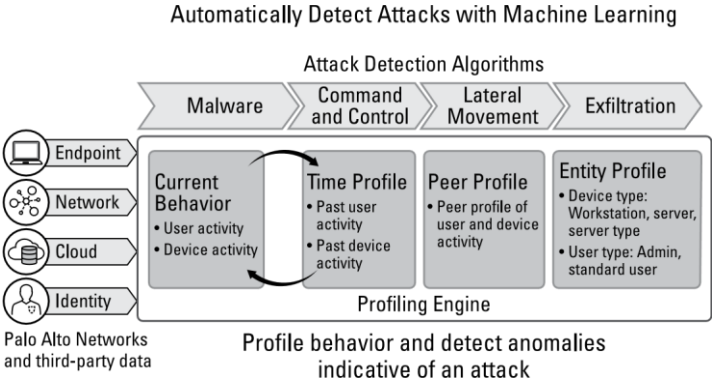
Hedefli saldırılar

Saldırganlar, saldırı yaşam döngüsünün her aşamasında faaliyetlerini meşru kullanımla harmanlamaya çalışırlar. XDR'nin algılama için herhangi bir kaynaktan veri toplama ve gelişmiş çapraz veri analitiği için önemli güvenlik verilerini otomatik olarak birleştirme yeteneği ile en gizli saldırıları tespit edebilirsiniz. Analitik sayesinde, kullanıcı davranışının profilini çıkarabilir ve bir saldırganın hassas verileri arayarak ve dışarı sızdırarak aygıtların güvenliğini

aşma ve ağ üzerinde yanlamasına hareket etme girişimleri gibi anormal davranışları saptayabilirsiniz.

Kötü niyetli kişiler

Kötü niyetli kişiler, algılanmadan kurumsal verileri çalmak için güvenilir kimlik bilgilerini ve erişimlerini kullanır. XDR, kullanıcı davranışı ve etkinliğindeki anormallikleri arayarak bu tehdidi ele alır (bkz. Şekil 4-1). XDR çözümleri, net bir risk puanı ile her kullanıcının 360 derecelik bir görünümünü sunarak analizi kolaylaştırabilir.



ŞEKİL 4-1: Davranış analitiği, kullanıcı, uygulama ve cihaz düzeyinde anormallikleri keşfeder.

Kasıtsız risk

İyi niyetli çalışanlar, yetkisiz erişimin kötüye kullanılması ve kötüye kullanılması yoluyla kuruluşları istemeden gereksiz risklere maruz bırakabilir. Bir XDR çözümü, bir çalışanın güvenlik politikalarını kasıtsız olarak veya değil, ihlal ettiğini tespit etmek için kullanıcı etkinliğini izleyerek ve riskli davranışları belirleyerek kuruluşların en iyi güvenlik uygulamalarını izlemesine olanak tanır.

Güvenliği ihlal edilmiş uç noktalar

Saldırganlar genellikle bir uç noktadan ödün vererek ve ağda yanal olarak hareket ederek hedeflenen ağlara sızmak için kötü amaçlı yazılım kullanır. XDR, kötü amaçlı yazılım ve diğer zararlı etkinlikler tarafından oluşturulan anormal trafiği aramak için güvenlik verilerini ağlar ve uç noktalar arasında bir araya getirir. Bu güvenlik verileri ayrıca, saldırının kapsamını belirlemek için ortam genelinde araştırma yapmak için araçlar sağlar.

Örneğin, bir tehdit aktörü Otomatik Çalıştırma kayıt defteri anahtarına yeni bir değer eklerse, bir XDR çözümü yeni Otomatik Çalıştırma değerini algılayabilir ve MITRE ATT&CK taktiği ve tekniği ile zengin araştırma bağlamı dahil olmak üzere bu şüpheli etkinliğin net bir açıklamasıyla bir uyarı oluşturabilir. . XDR

çözümü, hangi işlemin Otomatik Çalıştırma değerini eklediğini ve saldırının eksiksiz bir öyküsünü sağlamak için güncellemeye yol açan olayların sırasını bile belirleyebilir.

XDR, etkin saldırıları benzersiz bir hassasiyetle algılar ve güvenlik ekiplerinin şunları yapma yeteneğini artırır:

Ağda, uç noktalarda ve bulutta gerçekleşen etkinlikler arasında kalıplar bularak hem dahili hem de harici kaynaklardan gelen kötü amaçlı etkinlikleri tespit edin.

Yanlış pozitiflerin düzeyini artırmadan anormal etkinlikleri belirlemek için önemli miktarda güvenlik verisi üzerinde en yeni analitik teknikleri kullanın.

Geçmiş saldırılardan öğrenmek ve bu deneyimi daha az karmaşık analistlerin erişimine sunmak için dahili yanıt ve harici tehdit istihbaratından yararlanın ve tüm güvenlik ekibinin performansını iyileştirin.

Uyarı Triyaj ve Soruşturma

XDR çözümleri, uyarıların temel nedenini ortaya çıkararak uyarı triyajını ve analizini basitleştirir ve araştırmayı çok daha hızlı hale getirir. Yalnızca uç nokta verileri mevcutsa, uç nokta kök nedeni sunulur. Ağ ve uç nokta verileri mevcutsa, XDR platformu ağ etkinliğini uç nokta olaylarıyla otomatik olarak ilişkilendirebilir. Örneğin, XDR yalnızca bir ağ uyarısından hangi uç nokta yürütülebilir dosyasının sorumlu olduğunu belirlemekle kalmaz, yürütülebilir dosyayı hangi uygulamanın başlattığını da bulabilir.

Bölüm 1'de tartışılan güvenlik becerileri boşluğunun sunduğu zorluklar göz önüne alındığında, XDR, daha az deneyimli bir analistin, uyarıları olaylara göre gruplandırarak ve bu olaylar içinde etkinlikleri veya eylemleri bağlam ekleyen etiketler halinde özetleyerek potansiyel bir saldırıyı algılama ve doğrulama yeteneğini geliştirir. . Bu esneklik, bilginin tüm ekip için yakalanmasını ve kullanılmasını sağlar.

XDR, uyarıya yol açan olayların bir zaman çizelgesini oluşturur ve entegre tehdit istihbaratı sağlar. Tüm bunlar, analistlerin bir uyarının temel nedenini, tehdidin tam doğasını ve ne yapılması gerektiğini anlamalarına olanak tanır.

XDR, olay analizini ve araştırmaları basitleştirmeye şu şekilde yardımcı olur: **1.** Değerlendirme.

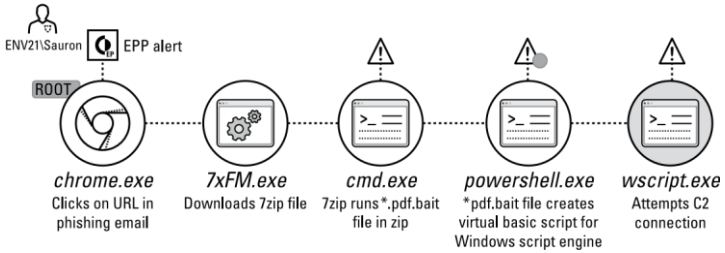
Süreç, XDR çözümünün olası şüpheli davranışları belirlemek için hem harici uyarıları (üçüncü taraf güvenlik araçlarından gelenler gibi) hem de dahili olarak oluşturulan uyarıları (kurallara ve diğer göstergelere dayalı olarak) değerlendirmesiyle başlar.

2. Önceliklendirme.

Ardından XDR aracı, analistleri en büyük tehdidi oluşturan olaylara yönlendirmek için bu uyarıları otomatik olarak olaylar halinde gruplandırır ve her olaya bir öncelik düzeyi atar. Analistler, her bir olaya tıklayabilir ve uyarının tam kapsamını anlamaya yardımcı olmak için uyarıların, cihazların, ilişkili tehdit istihbaratının ve diğer bağlamların tam listesini görebilir.

3. Analiz.

XDR, olayla ilgili her şeyi ve her şeyi toplamak ve ek bağlam, nedensellik sağlamak ve daha hızlı ve daha iyi analiz sağlamak için çeşitli telemetri kaynaklarından yararlanan görsel bir saldırı zinciri sağlar (bkz. Şekil 4-2). Saldırı zinciri, son saldırı adımına yol açan süreçlerin sırasını ortaya çıkararak bir saldırganın attığı adımları gösterir. XDR aracısı için bir EPP uyarısı da dahil olmak üzere ilgili uyarıları görüntülemenin yanı sıra, temel nedeni de tanımlar.



ŞEKİL 4-2: XDR kullanan görselleştirilmiş bir saldırı zinciri örneği.

4. Zenginleştirme.

Saldırı zinciri, daha sonra, uyarının nasıl oluşturulduğuna dair ayrıntılı bir görünüm de dahil olmak üzere, ek bağlamsal bilgilerle zenginleştirilir; onun temel nedeni; ilgili diğer uç nokta, ağ ve bulut cihazları; ve tüm adli eserlerin itibarı.

> Her gün gelen binlerce uyarıyla, önceliklendirme sürecini otomatikleştirmek ve analistlere zenginleştirilmiş bağlamsal bilgiler sağlamak, hacmi yönetmenin tek yoludur. XDR ile güvenlik ekipleri, zamanlarını ve enerjilerini en büyük etkiye sahip olacakları yere, yani en fazla hasara neden olma potansiyeline sahip uyarıları düzeltmeye odaklayabilirler.
>
> XDR ile analistler şunları yapma konusunda artan bir yeteneğe sahiptir:

Olay yönetimi, akıllı uyarı gruplandırması ve araştırma bağlamı ile uyarı birikimlerini azaltın.

Kaçırılan bir saldırı olasılığını önemli ölçüde azaltın.

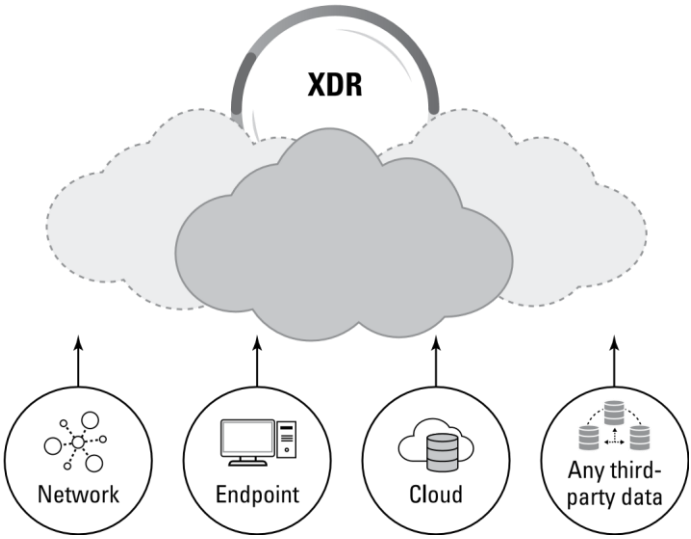
Algılamayı iyileştirmek için uyarıları analiz edin ve ayrıca aşağı yönlü üretkenlik ve savunmaların olumsuz etkilenmemesini sağlayın.

Önceliklendirme sürelerini iyileştirmek için yeni davranışsal tetikleyiciler uygulayın ve isteğe bağlı olarak algılama kurallarını kapalı döngü önleme için önleme kurallarına dönüştürün.

Otomatikleştirilmiş ve Basitleştirilmiş Soruşturmalar ve Müdahale

Bir uyarıya öncelik verildikten ve önceliklendirildikten sonra, daha derinlemesine bir araştırma yapılması garanti edilir. XDR'nin otomasyonu, tehdidin net bir resmini sağlayarak, kök neden analizi yaparak, itibarı doğrulayarak ve saldırı ilişkisini çözerek zaman alan manuel görevleri ortadan kaldırarak herhangi bir uyarı veya av kampanyasının araştırma sürecini hızlandırır.

XDR araçları, bulut veri gölü gibi bir güvenlik veri havuzundaki tüm telemetriyi toplayarak başlar (bkz. Şekil 4-3). XDR çözümü, araştırma süresini azaltmak için, algılama araçlarından gelen uyarıları, kullanıcı, uygulama ve cihaz hakkında bilgiler dahil olmak üzere az sayıda doğru, eyleme dönüştürülebilir olay halinde ilişkilendirebilir ve gruplayabilir. XDR, hangi işlemin veya yürütülebilir dosyanın bir saldırı başlattığını belirlemek için uç noktaları sorgulayarak adli tıp araştırmalarına da yardımcı olabilir.



ŞEKİL 4-3: XDR araçları, bulut tabanlı bir veri havuzunda farklı sensörlerden gelen verileri bir araya getirir.

Olayın daha derinine inmek için bir XDR çözümü, uç nokta sürecinin kötü amaçlı olup olmadığını belirler. Bunu, süreci analiz etmek için tehdit istihbarat kaynakları ve hizmetleri ile entegre ederek yapar. Bir XDR çözümü, güvenlik analistlerinin ihtiyaç duydukları tüm bilgileri tek bir arayüzde sunarak saldırıları doğrulamasını kolaylaştırır.

XDR araçları ayrıca, daha önce bulunan herhangi bir tehdidin başarılı bir şekilde tekrarlanmasını otomatik olarak önlemek için önceki olaylardan ve av kampanyalarından elde edilen bilgileri uygulayarak savunmaları uyarlayabilir. Bu "destekli öğrenme", ortamda daha önce görülenlere dayalı olarak saldırıların erken tespit edilmesini sağlar.

Tehdit doğrulandıktan sonra, olay müdahale ekipleri saldırıyı durdurmak, takip eden saldırıları önlemek, hasarlı veya silinmiş dosyaları geri yüklemek ve daha fazlası için düzinelerce uzaktan müdahale ve iyileştirme tekniği arasından seçim yapabilir. Yanıt seçenekleri arasında uç noktaların yalıtılması, dosyaların engellenmesi, silinmesi veya karantinaya alınması, dosyaların ve kayıt defterinin temiz bir duruma döndürülmesi, uç noktalara doğrudan erişim ve komut dosyalarının yürütülmesi yer alır. Güvenlik ekibi son derece verimli hale gelecek, daha az eğitim gerektirecek, daha deneyimli olay müdahale ekiplerinin yükünü azaltacak ve olay çözüm sürelerini en aza indirecektir.

XDR ile, olaya müdahale edenlerin aşağıdakileri yapma yetenekleri artar:

Tehdit istihbaratından ve davranışsal analitikten yararlanarak gizli tehditleri daha hızlı bulun.

Ağlardan, uç noktalardan ve buluttan toplanan derin ve kapsamlı telemetri aramaları sağlayarak araştırmayı ve yanıtlamayı basitleştirin ve hızlandırın.

Tehdit Avcılığı

XDR çözümleri, ortamınızdaki kötü amaçlı etkinliğin hem otomatik hem de geçici olarak tanımlanması yoluyla tehdit avlama yeteneklerinizi geliştirir. Tehdit avcıları gelişmiş sorgular gerçekleştirebilir ve anında sonuç alabilir. XDR'nin farklı tehdit avı yöntemlerini desteklemek için gerekli yetenekleri nasıl sağladığına dair bazı örnekler şunları içerir:

Intel tabanlı: Bu, avcıya aramadan önce potansiyel bir tehdit hakkında bir ipucu verildiği en yaygın tehdit avı alıştırması türüdür. İster tehdit istihbaratından gelen bir ipucu, ister yeni keşfedilen bir uzlaşma göstergesi (IOC), kuruluş içindeki birinden gelen ipucu veya sadece şüphe olsun, intel tabanlı tehdit avcılığının karmaşıklığı, istihbaratın sağladığı ayrıntı düzeyine bağlı olacaktır. Birden çok tehdit istihbarat sağlayıcısına bağlı entegre bir veri kaynağından yararlanan bir XDR çözümü, hızlı ve sağlam arama sonuçları sağlamak için farklı standartlardan yapay nesneleri veya IOC'leri manuel olarak içe aktarabilir.

Kurşunsuz tabanlı: Tehdit avcılığına yönelik yaygın yaklaşımlar açısından yakın bir saniye olan kurşunsuz, avcının bir bilgisayar, uygulama, kullanıcı, veri veya ağın nasıl kullanılması gerektiğine dair kendi veya aranan bilgilerini kullandığı ve hedeflediği yerdir. anormal veya anormal kullanımı tanımlayın. Bu tür gelişmiş tehdit avı, genellikle sonuçlara ulaşmak için veri oyma ve analitik gibi teknikleri kullanan en deneyimli ekip üyelerine bırakılır. Bir XDR çözümü, bu gelişmiş teknikleri arayüzüne yerleştirerek bu süreci basitleştirir ve herhangi bir deneyim seviyesindeki avcıların bu tekniklerden komut dosyaları, ek araçlar veya yeni bir sorgu dili öğrenme ihtiyacı olmadan yararlanmasına olanak tanır.

Sonuca dayalı: Bu yaklaşımda, avcı geçmiş karantinaya alınmış uyarıları, tamamlanmış araştırmaları veya çözülmüş diğer tehditleri inceler ve bunları tehdidin çeşitlerini, potansiyel yeni tehditleri veya açık saldırı vektörlerini belirlemek için kullanır. Kaliteli bir XDR çözümü, otomatik ve sürekli olarak sonuca dayalı tehdit avcılığını doğrudan güvenlik uyarıları ve olay işleme iş akışına dahil edebilir. Tekrarlanan saldırılardan etkilenmemeniz için her soruşturmadan alınan dersler uygulanır.

Uyumluluğa dayalı: Bu tehdit avı yaklaşımı, yetkisiz sistemlerde depolanan hassas veriler veya yönetici kullanıcılar tarafından ayrıcalıkların yükseltilmesi gibi uygunsuzluğu gösteren rutin aramalar gerçekleştirerek dahili, sektörel ve resmi

gereksinimlerle uyumluluğu sağlamaya odaklanır. Güvenlik analistlerini bu tür faaliyetler konusunda uyarmak ve durumu hızlı bir şekilde araştırmak için bir araç sağlamak için bir XDR çözümü yapılandırılabilir.

Makine öğrenimi tabanlı: Makine öğrenimi sistemleri, neyin normal olup neyin olmadığını anlamak için bir kuruluşun tipik davranışlarını temel alır. Büyük ölçekli analitik kullanan XDR çözümleri, davranışları izlemek ve bu temellerden sapan anormallikleri belirlemek için makine öğrenimini kullanır. Bu davranışsal uzlaşma göstergeleri
BIOC'ler), bir analistin manuel olarak tanımlayamayacağı birçok gizli tehdidi yakalar ve makine öğrenimi modelini geliştirmek için zaman içinde sürekli olarak optimize edilir. Bu tehdit avı biçimi, analistler için nihai zaman tasarrufunu temsil eder ve güvenlik sonuçlarını optimize etmek için kritik öneme sahiptir.

XDR ile tehdit avcıları şunları yapma konusunda artırılmış bir yeteneğe sahiptir:

Arama ve analiz için ağ, uç nokta ve bulut verilerinden yararlanın.

Tüm ağ, uç nokta ve bulut etkinliklerinde arama yapmak için otomasyondan yararlanın.

Tehdit kitaplığınızda depolanan geleneksel IOC'ler ve BIOC'ler tarafından tanımlanan hem dahili hem de harici tehditleri bulmak için yüksek düzeyde yapılandırılabilir aramalar ve sihirbazlar kullanın.

Güvenlik kontrolleriyle entegrasyon yoluyla saldırıları düzeltin.

IN THIS CHAPTER

- Ensuring robust threat prevention and complete visibility
- Simplifying investigations with analytics, machine learning, coordinated response, and orchestration features
- Maximizing flexibility with a full protection suite
- Looking at third-party validation, innovative road maps, and total value

5. Bölüm

On Temel XDR Yeteneği ve Özelliği

Extended algılama ve yanıt (XDR), kuruluşların başarılı siber saldırıları önlemesine ve tehdit algılama ve müdahaleye yönelik proaktif bir yaklaşım kullanarak güvenlik süreçlerini basitleştirmesine ve güçlendirmesine olanak tanır. XDR, herhangi bir kaynaktan veri toplayıp analiz ederek modern saldırıları durdurur. Eşsiz güvenlik ve operasyonel verimlilik sağlamak için önleme, tespit, araştırma ve müdahaleyi birleştirir.

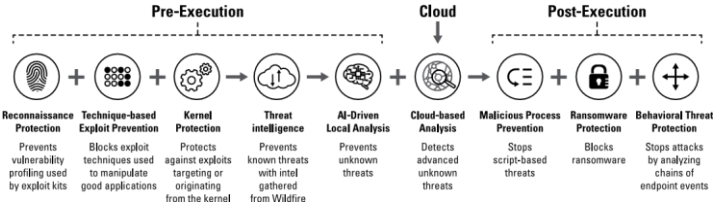
Bu bölüm, kuruluşunuz için bir XDR çözümünde aranması gereken on "olmazsa olmazı" ortaya koymaktadır. Ayrıca, endüstrinin ilk genişletilmiş algılama ve yanıt platformu olan Cortex XDR'nin bu temel özellikleri nasıl sağladığını da açıklıyor.

Sınıfının En İyisi Uç Nokta Tehdit Önleme

Kuruluşunuzu korumak, bilinen ve bilinmeyen kötü amaçlı yazılımları, fidye yazılımlarını, dosyasız saldırıları ve açıklardan yararlanmaları engelleyen sınıfının en iyisi uç nokta tehdit önleme ile başlar.

Cortex XDR, buluttan yönetilen tek bir aracıyla tehdit önleme, algılama ve yanıt için ihtiyacınız olan her şeyi sağlar. Endüstrinin en iyisi, yapay zeka (AI)

tarafından yönlendirilen yerel analiz ve davranışa dayalı koruma ile uç noktalarınızı korur (bkz. Şekil 5-1).



ŞEKİL 5-1: Cortex XDR, eksiksiz uç nokta tehdit önleme sağlar.

sağlayan yeni nesil antivirüsü arayın.

Kötü amaçlı yazılım, fidye yazılımı ve dosyasız tehdit koruması

Bulut tabanlı gerçek zamanlı küresel tehdit istihbaratı

Makine öğrenimi yoluyla yerel analiz

Davranışsal tehdit koruması

Granüler alt süreç koruması

İstismar öncesi ve teknik tabanlı istismar önleme

Çekirdek istismarını önleme

Kimlik bilgisi hırsızlığı koruması

Esnek Uç Nokta Koruması Özellikleri Paketi

Uç nokta risklerini belirlemek ve önceliklendirmek, saldırı yüzeyinizi azaltmak ve veri kaybını durdurmak için kolay bir yola ihtiyacınız var. Aşağıdakiler dahil uç nokta koruma özelliklerini arayın:

Güvenlik açığı değerlendirmesi: Dijital varlıklarınızın kuruluş çapında bir görünümünü elde etmek için güvenlik açığı değerlendirmesinden, yönetilen ve yönetilmeyen uç noktalarda uygulama görünürlüğünden ve daha fazlasından yararlanın.

Güvenlik duvarı barındırın: Cortex XDR yönetim konsolundan uç noktalarınızdaki gelen ve giden iletişimleri merkezi olarak yönetin.

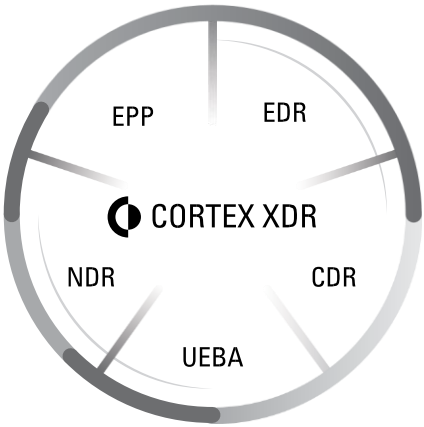
Disk şifreleme: Uç noktalarınıza şifreleme veya şifre çözme ilkeleri uygulayın ve tüm şifrelenmiş sürücülerin listelerini görüntüleyin.

Cihaz kontrolü: Uç noktalarınızı korumak için Evrensel Seri Veri Yolu (USB) erişimini izleyin ve ayrıntılı olarak kontrol edin.

Veri Kaynaklarında Genişletilmiş Görünürlük

Başarılı bir saldırı riskini azaltmak için, kör noktaları ortadan kaldıran, doğruluğu artıran ve ağ, bulut ve uç nokta dahil tüm ortamlarda araştırmaları kolaylaştıran bütünsel bir algılama ve yanıt yaklaşımına ihtiyacınız var.

Cortex XDR, karmaşık saldırıları durdurmak için uç nokta, ağ ve bulut verilerini yerel olarak entegre eden endüstrinin ilk XDR platformudur. Cortex XDR, ağ algılama ve yanıt (NDR), uç nokta algılama ve yanıt (EDR), uç nokta koruma (EPP), bulut algılama ve yanıt (CDR) ve kullanıcı ve varlık davranışı analitiğinin (UEBA) tüm özelliklerini aşağıdaki şekilde gösterildiği gibi sunar: Şekil 5-2.



ŞEKİL 5-2: Cortex XDR, EPP, EDR, NDR, CDR ve UEBA araçları tarafından geleneksel olarak sağlanan yetenekleri sağlamak için zengin verileri toplar ve analiz eder.

Basitleştirilmiş Soruşturmalar

Günümüzün silolanmış güvenlik araçları, sınırlı bağlamla sonsuz uyarılar üretir. Ponemon Enstitüsü'nün 2020 *Veri İhlalinin Maliyeti Raporuna göre*, bir ihlali tespit etmek ve kontrol altına almak için ortalama süre 280 gündür. Yanıt sürelerini azaltmak için güvenlik araçları, zengin araştırma ayrıntılarıyla olayların eksiksiz bir resmini sağlamalıdır.

Cortex XDR, uyarıların temel nedenini, olay sırasını ve tehdit istihbarat ayrıntılarını otomatik olarak ortaya çıkararak araştırmaları basitleştirir. Ağ, uç nokta ve bulut uyarılarının temel nedenini ve zengin bağlamını ortaya çıkararak araştırma süresini yüzde 88 azaltır ve akıllı uyarı gruplandırma ve veri tekilleştirme ile uyarıları yüzde 98 azaltır.

Analitik ve Makine Öğrenimi

Tehdit aktörleri, saldırılarının ölçeğini ve etkinliğini artırmak için bulut ve makine öğrenimi teknolojilerinden yararlanır. Hızla gelişen tehditlerin bir adım önünde olmak ve karmaşık saldırılara karşı koymak için kapsamlı bir makine öğrenimi ve analitik teknikleri setine ihtiyacınız var.

Cortex XDR sağlar

- Kötü amaçlı yazılımları engellemek için yapay zeka destekli yerel analiz
- İzinsiz girişleri ve aktif saldırıları tespit etmek için davranışsal analitik
- Algılama doğruluğunu ve kapsamını iyileştirmek için küresel analitik

Koordineli Yanıt

Ortamınızdaki tehditleri belirledikten sonra bunları hızla kontrol altına almanız gerekir. Ekibinizin, saldırıları daha fazla hasar vermeden önce hızlı ve etkili bir şekilde durdurmak için entegre ve esnek yanıt seçeneklerine ihtiyacı var. Bir XDR çözümü, ekibinizin kötü amaçlı yazılımın yayılmasını uzaktan durdurmasını, cihazlara ve cihazlardan ağ etkinliğini kısıtlamasını ve uygulama noktalarıyla sıkı entegrasyon yoluyla kötü etki alanları gibi tehdit önleme listelerini güncellemesini sağlamalıdır.

Cortex XDR, güvenlik ekibinizin ağ, uç nokta ve bulut tehditlerini tek bir konsoldan anında ortadan kaldırmasını sağlar.

Güvenlik Görevlerinin Otomasyonu

Manuel görevler ve süreçler, olay yanıtını yavaşlatır ve güvenlik operasyonlarının maliyetini artırır. Uç noktaya ve diğer önemli uygulama noktalarına yerel olarak bir dizi yanıt eylemi yürüten XDR çözümleri, tehditleri hızla içerebilir. Gelişmiş SOC'ler, çalışma kitapları tarafından kontrol edilen karar mantığı ve iş akışı düzenlemesini içeren ve farklı satıcılardan çok çeşitli güvenlik ve BT araçlarına yönelik çeşitli eylemler içeren süreçler gerektirebilir. Düzenleme mantığı sağlayan ve kapsamlı iş ortağı entegrasyonları ile önceden oluşturulmuş içerik ve çalışma kitaplarına sahip tam özellikli bir güvenlik otomasyonu ve düzenleme çözümü bu gereksinimleri karşılayabilir. Bu nedenle,

endüstri lideri bir SOAR platformuyla sıkı bir şekilde bütünleşen bir XDR çözümü arayın.

Cortex XDR, eksiksiz tehdit istihbarat yönetimi için Cortex XSOAR ile sıkı bir şekilde bütünleşir ve güvenlik operasyonlarınızı bir sonraki seviyeye taşıyabilmeniz için 750'den fazla ortak entegrasyonu ve 680 içerik paketi sunar.

Bağımsız Test ve Doğrulama

Bir XDR çözümü seçerken, bağımsız ve nesnel bir bakış açısı elde etmek için her zaman üçüncü taraf testlerini, analist doğrulamasını ve müşteri referanslarını gözden geçirmelisiniz.

Cortex XDR, MITRE ATT&CK 3. tur değerlendirmesinde en iyi birleşik algılama ve korumanın elde edilmesi ve AV-Comparatives Endpoint Prevention and Response (EPR) testinde "Stratejik Lider" derecesi dahil olmak üzere olağanüstü test sonuçları elde etti. Hem müşterilerden hem de gözden geçirenlerden övgü toplayan Cortex XDR, uç noktalarınızı ve verilerinizi korumak için güvenilir olabilir.

Hızlı İnovasyon Hızı

Hızlı hareket eden rakipleri geride bırakmak için, ürünlerinin yeteneklerini sürekli olarak güçlendiren veya genişleten satıcılar arayın.

Cortex XDR, güvenlik operasyon ekiplerinin karmaşık modern tehditleri nasıl ele aldığını ve daha fazla verimlilik sağladığını yeniden tanımlamaya devam ediyor. XDR, verileri toplama, entegre etme ve analiz etme sistem entegrasyonu sorununu ele alarak ve bunları yüksek düzeyde optimize edilmiş ve otomatikleştirilmiş iş akışlarını başlatma yeteneğiyle birleştirerek, algılama, araştırma ve yanıt verme zorluklarını konsolide bir şekilde büyük ölçekte çözmeye yardımcı olur.

Eşsiz Yatırım Getirisi

Güvenlik altyapınızın önemli bir öğesini seçerken, paydaşlarınız için kolayca gösterilebilecek gerçek değer sağlayacağından emin olmak istersiniz.

Cortex XDR, geleneksel araçlara kıyasla toplam sahip olma maliyetini (TCO) ortalama yüzde 44 oranında düşürür:

Algılama ve müdahale için sensörler olarak mevcut güvenlik araçlarınızı kullanma

Bulut dağıtımıyla şirket içi günlük sunucularını ortadan kaldırma

Veri birleştirme, uyarı gruplandırma ve kök neden analizi ile işlemleri basitleştirme