Özel Rapor

EDR'den XDR'ye geçiş: Ne zaman ilerleyeceğinizi bilmek

kaspersky geleceği yakalayın

EDR'den XDR'ye geçiş: Ne zaman ilerleyeceğinizi bilmek

Artık kuruluşların yüksek riskli olmak için yüksek profilli olmaları gerekmiyor. Bu, siber güvenlik alanında önemli bir dönüm noktasını yansıtmaktadır. Geleneksel olarak, yalnızca büyük kuruluşlar daha gelişmiş siber saldırılar için değerli hedefler olarak kabul ediliyordu. Bu da, büyük işletmelere yönelik sağlam güvenlik çözümlerinin geliştirilmesini gerektiriyordu. Ancak, son yıllarda orta ölçekli kuruluşların da benzer türden sofistike saldırılar için cazip ve stratejik hedefler haline geldiği görülmüştür.

Bu değişim, birçok Bilgi Teknolojileri Direktörü (CIO) ve BT güvenlik uzmanını siber güvenlik stratejilerini yeniden düşünmeye zorluyor. Ayrıca, var olan birçok çözüm, özellikle daha küçük güvenlik ekipleri veya daha geniş BT departmanları tarafından kullanılanlar, artan tehdit hacmini ve modern tehditlerin karmaşıklığını yönetmede yetersiz kalıyor.

Orta ölçekli şirketler neden siber suçluların en önemli hedefleri haline geliyor?

Daha küçük siber güvenlik ekiplerine sahip işletmeler, daha gelişmiş siber saldırıların en önemli hedefleri haline gelmeye başladı. KOBİ'lerin yılda ortalama 16 saldırıya maruz kaldığını, daha büyük kuruluşların ise sektöre bağlı olarak bu sayının 18'e kadar çıktığını tespit ettik.[1] Peki, görünüşte kurumsal düzeyde korumaya ihtiyaç duymaması gereken küçük şirketlere neden bu kadar ilgi duyuluyor?

Daha büyük kuruluşlara giden basamaklar

Birçok küçük kuruluş, büyük şirketler için önemli bağlantılar görevi görür. Siber suçlular genellikle daha büyük ağları hedef alır ve en kolay giriş noktasını kullanır (exploit). Böylece, daha büyük bir tedarik zincirini bozabilir ve zincirleme hasara neden olabilirler. Sadece 2025 yılında, büyük kuruluşların %54'ü siber güvenliğin karmaşıklığının artmasının başlıca nedeni olarak tedarik zincirindeki karşılıklı bağımlılıkları gösteriyor.[2] Ancak, büyük kuruluşlar 2024 yılında siber dayanıklılıkta artış kaydederken, küçük kuruluşlar dezavantajlı konumda kalmaya devam ediyor ve %35'i siber dayanıklılığın yetersiz olduğunu belirtiyor.[2]

Nitelikli personel eksikliği

Çoğu küçük siber güvenlik ekibi, tehdit tespiti ve olay müdahale yeteneklerini geliştirmek ister, ancak bunu yapmak için gerekli kaynaklara veya bütçeye sahip değildir. Aslında, son araştırmalar, bilgi güvenliği uzmanlarının %41'inin, kuruluşlarının siber güvenlik ekiplerinin "biraz" veya "önemli ölçüde" personel eksikliği olduğunu söylediğini gösteriyor.[3] Çoğu durumda bu, KOBİ'lerin siber güvenlik görevlerini yerine getirmek için büyük ölçüde genel BT personeline güvendikleri anlamına gelir. Bu durum sadece küçük ekipleri imkanlarının ötesinde zorlamakla kalmıyor, aynı zamanda uzmanlık eğitimi eksikliği nedeniyle işletmeleri artan siber tehditlere maruz bırakıyor. Ne yazık ki, siber suçlular bu açığın bilincinde ve bunu kolaylıkla sömürüyorlar.

Sofistike araçlar için kolay hedefler

Orta ölçekli kuruluşların kolay hedefler olduğu ve birçoğunun kendilerini karmaşık tehditlerden yeterince korumak için gerekli siber güvenlikten yoksun olduğu kanıtlanmıştır. Bununla birlikte, "kolay hedef" olmanın yalnızca BT ekibinin bir yansıması olmadığı, aynı zamanda sofistike tehditlerin her zamankinden daha kolay yayıldığı gerçeğinin de unutulmaması gerekir. Daha küçük şirketler genellikle ağ güvenliği, EPP ve CWPP gibi daha basit BT güvenlik çözümleri kullanır. Siber suçlular temel siber güvenliği kolaylıkla atlatmak için sofistike araçlardan yararlandıkça bunların hepsi daha etkisiz hale gelmeye devam ediyor.

KOBİ'ler yılda ortalama 16 saldırıya maruz kalıyor.[1]

Güncel araçlar ve faktörler saldırganların hayatını nasıl kolaylaştırıyor?

Karmaşık saldırılardaki hızlı artışı en iyi şekilde anlamak için siber suçları teknik bir tehditten öte, gelişen küresel bir girişim olarak görmemiz gerekiyor. Siber suçlular, operasyonlarını kolaylaştırmalarını, gelir akışlarını çeşitlendirmelerini ve hız ve hassasiyetle yenilik yapmalarını sağlayan ölçeklenebilir iş modelleri geliştirdiler. Gelişmiş araçların artık düşük vasıflı siber suçluları bile bu saldırıları başlatmak için donanımlı hale getirmesiyle güç çarpanlarının ortaya çıkması, sofistike saldırılardaki artışı hızlandırıyor.

Siber suçlular, saldırılarını daha verimli bir şekilde gerçekleştirmek için yeni teknolojileri ve sistemik zayıflıkları kullanarak taktiklerini sürekli olarak geliştiriyorlar.

Aşağıda, saldırganların kurbanları daha kolay istismar etmesini sağlayan temel araçlar ve faktörler verilmiştir.

Sosyal mühendislik

Kimlik avı gibi sosyal mühendislik saldırıları, özel bilgilerinizi elde etmek için ekibinizi istismar eden manipülasyon teknikleri kullanır. Yapay zeka teknolojileri ise bunu her zamankinden daha kolay hale getirmiş durumda. Örneğin, siber suç odaklı bir yapay zeka sohbet robotu, saldırganların gösterişli e-postalar ve sahte DocuSign talepleri oluşturmasına yardımcı olabilir. Saldırganlar çok az bir çabayla geleneksel kimlik avı uyarılarından kaçınabilir, sahte e-postaları kişiselleştirebilir ve aciliyet ve özgünlük hissi yaratmak için manipülasyon taktiklerini kullanabilir. Diğer sosyal mühendislik saldırıları şu çok aşamalı bir yaklaşım izler. Saldırı, sonunda çalışanları yasal yardım masası biletleri oluşturmaya zorlayan toplu e-posta spam'leri göndererek başlar. Saldırganlar daha sonra BT destek personeli gibi davranarak Microsoft Teams üzerinden çalışanlarla iletişime geçer ve onları ağ erişimi için kullanılabilecek uzaktan izleme araçları sunmak üzere tasarlanmış kötü amaçlı QR kodları almaları için kandırır.

Hizmet Olarak Casus Yazılım

Casus yazılım geliştiricileri de araçlarına erişimi genellikle dark web forumları veya kötü niyetli kanallar aracılığıyla kiralar veya satarlar. Müşteriler (genellikle bilgisayar korsanları, devletler veya insanları gizlice takibe alan kişiler) keylogger'lara, mikrofon/kamera erişim araçlarına, mobil gözetim kitlerine, uzaktan erişim araçlarına (RAT'lar), tarayıcı ve e-posta dinleme araçlarına veya GPS izleyicilere erişim için ödeme yaparlar.

Bu araçlar, kullanıcının bilgisi veya onayı olmadan kurbanın cihazından bilgi toplamak ve iletmek için kullanılabilir.

Hizmet Olarak Fidye Yazılımı (RaaS)

RaaS kitleri, siber suçluların çok az pratik çalışma ile sofistike siber saldırılar başlatmasına olanak tanıyan, esasen "tak ve çalıştır" türünde araçlardır. Güvenlik sistemleri (antivirüs veya güvenlik duvarları gibi) tarafından tespit edilmekten kaçınmak için kodunu kolayca uyarlayabilen kötü amaçlı yazılımlar kullanırlar. Bu nedenle, birçok siber güvenlik çerçevesi RaaS ile mücadele etmek için yeterli koruma sağlamakta yetersiz kalmakta ve işletmeleri, hükümetleri ve bireyleri yüksek riskli durumlara maruz bırakmaktadır.[4]

Hizmet Olarak Yazılım (SaaS) modellerine benzer şekilde, RaaS kitleri, bağlı kuruluşların fidye yazılımı araçlarına, 7/24 teknik desteğe, ödeme işleme portallarına ve daha fazlasına aylık sadece 40 ABD doları karşılığında erişmelerini sağlar. Meseleyi daha iyi anlamak adına şu bilgiyi vermek işe yarayacaktır: ortalama bir fidye yazılımı saldırısı, kurbanına 4,91 milyon ABD doları (kesinti süresi, müşteri kaybı, para cezaları vb. dahil) maliyet getiriyor.[5]

Eski yazılımlar

Birçok işletme, yama ve güncellemeleri takip etmekte zorluk çekiyor ve bu da yazılımlarını savunmasız hale getirebiliyor. Özellikle fidye yazılımı grupları, kuruluşların yama uygulama hızını geçebileceklerini bilerek sıfırıncı gün güvenlik açıklarından yararlanıyor. Aslında, kritik güvenlik açıklarının %85'i keşfedildikten 30 gün sonra hala ortadan kaldırılmamış durumda oluyor, %47'si 60 gün sonra da ve %20'si altı ay sonra bile hala varlığını sürdürüyor oluyor.[6]

2024 yılında, olayların %41,6'sı fidye yazılımıyla ilgiliyken, 2023 yılında bu oran %33,3 idi. Fidye yazılımları, öngörülebilir gelecekte dünya genelindeki kuruluşlar için birincil tehdit olmaya devam edecek gibi görünüyor.[7]

Gelişmiş koruma ihtiyacı

Kesintiye uğrayan süreçler:

- İletişim - %41
- Müşteri desteği: - %36
- Pazarlama otomasyonu - %36
- Lojistik - %32
- Ürün geliştirme/üretim - %31
- CRM, satış- %27
- Satın alma ve ödeme - %26
- Bordrolama — %17

Güvenlik ihlalleri KOBİ'lere ayrılan siber güvenlik harcamalarının 1,5 katına mal oluyor.[1]

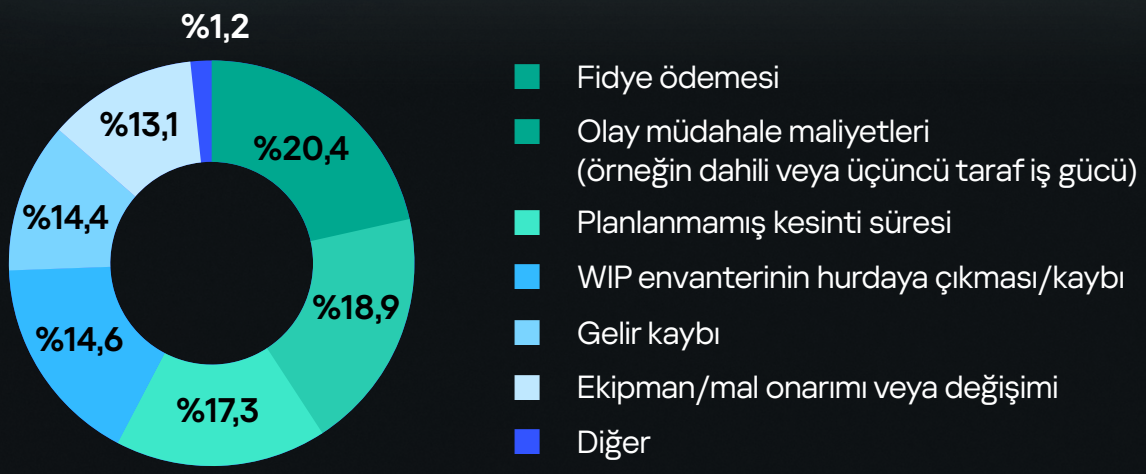
Karmaşık siber saldırıların artmasıyla birlikte, son araştırmalar, iş kaybı ve ihlal sonrası müdahale maliyetlerinin önceki yıla göre yaklaşık %11 arttığını ortaya koyuyor.[6] Bu artışın büyük ölçüde, ihlal döngülerinin uzamasına neden olan sofistike saldırılardan kaynaklandığı görülüyor.

Siber saldırılar artık kaçınılmazdır, ancak bunları ne kadar hızlı tespit edip yanıt verdiğiniz, bir olayın küçük bir olay mı yoksa felaket niteliğinde bir ihlal mi olacağını belirler. Örneğin, 2024 yılında, ilk vektöre göre en uzun sürede kontrol altına alınabilen üç ihlal türü, kimlik avı, içeriden kötü niyetli kişiler ve çalınan/sızdırılan kimlik bilgileriydi. Bunlar aynı zamanda ilk vektöre göre en maliyetli dört ihlal türünden üçünü oluşturuyordu ve bu da bekleme süresi ile neden olduğu hasar arasındaki bağlantıyı vurguluyordu.[5]

Saldırganlar ne kadar uzun süre fark edilmeden faaliyet gösterirlerse, o kadar fazla zarar verirler. Bu noktada, ortalama tespit süresi (MTTD) olay yönetiminde anahtar bir performans göstergesi haline gelir ve ekibinizin bir olayı tespit etme veya keşfetme yeteneğini gösterir. Sonuç olarak, Ortalama Yanıt Verme Süresi (MTTR), tehdidi etkisiz hale getirmek için gereken ortalama süreyi ifade eder. Güvenlik operasyonlarının otomasyonu, bu ölçütlerin iyileştirilmesinde önemli bir rol oynar. Aslında, güvenlik süreci otomasyonu ile uğraşan kişiler, MTTR'lerinde %46'lık bir iyileşme gibi faydalar bildiriyor.[8]

Kontrol altına alınmış bir olay ile tam anlamıyla bir felaket arasındaki fark, genellikle müdahale hızına bağlıdır. MTTD, MTTR olmadan anlamsızdır – bir tehdidi hızlı bir şekilde tespit etmek, onu hızlı bir şekilde durduramazsanız hiçbir anlam ifade etmez. Vakit nakittir ve her saniye önemlidir. İhlallere hızlı bir şekilde müdahale eden kuruluşlar milyonlarca dolar tasarruf edebilir, yasal gereklilikleri kolayca yerine getirebilir ve itibarlarını koruyabilir.

Gıda ve içecek sektöründe ortalama siber güvenlik ihlali maliyetleri[9]



EDR artık yeterli olmadığında

Uzun yıllardır, Endpoint Detection and Response (EDR) araçları, herhangi bir siber güvenlik stratejisinin temelini oluşturdu ve bu haklı bir yaklaşımdı. EDR, siber güvenlik ekiplerine tehdidin temel nedenini ve ek müdahale eylemlerinin gerekip gerekmediğini belirlemek için değerli veriler ve görselleştirme araçları sağlar. Bu sayede, hem yetenek hem de etkinlik açısından geleneksel antivirüs araçlarını çok geride bırakır.

Ancak tehdit ortamı önemli ölçüde büyüdü ve olaylara müdahale ve tehdit soruşturmasının önemi de arttı. Bu durum, yüksek riskli kuruluşları yalnızca XDR işlevlerinin karşılayabileceği daha karmaşık ihtiyaçlara yöneltti.

Ancak, tam donanımlı bir XDR çözümüne yatırım yapmak, telemetriyi etkili bir şekilde yönetmek ve analiz etmek için gerekli donanım, bütçe veya nitelikli personele sahip olmayan küçük kuruluşlar için genellikle mümkün olmuyor.

Bu durum, küçük ve orta ölçekli işletmeleri zor bir ara durumda bırakmaktadır. Geçerli çözümler artık yeterli olmamakta, ancak kurumsal düzeydeki XDR çözümleri mevcut sorunlarını çözmek için çok gelişmiş, pahalı ve pratik değildir. Bir yandan saldırı yüzeyi genişliyor, diğer yandan ekibiniz analiz edilmesi gereken çok sayıda uyarı ile boğulmuş durumda.

Peki, adım atma zamanının geldiğini nasıl anlarsınız?

Uyarı yorgunluğu ekibinizi bunaltıyor

Kuruluşunuz çok sayıda uyarı üreten çeşitli siber güvenlik araçları kullanıyorsa, BT güvenlik ekibiniz hızla aşırı yüklenebilir. Bu, özellikle ekibinizin bu uyarıları etkili bir şekilde önceliklendirmek ve araştırmak için yeterli bağlama sahip değilse geçerlidir. Bu süreç sıkıcı olabilir ve ekibiniz manuel olarak çalışırsa gelen tehditleri gözden kaçırma olasılığı giderek artacaktır. Ekibiniz tükenmişlik yaşayabilir ve bu da onların başka yerlerde yeni fırsatlar aramasına neden olabilir.

> "Bir siber güvenlik uzmanı işini iyi yaptığında, hiçbir şey olmaz ve günlük işleri büyük ölçüde sıradan olur: günlükleri ve kuralları kontrol etmek, hesapları incelemek, ilke uyumluluğunu sağlamak gibi. Bunlar karmaşık adımlar değildir, ancak çok önemlidir. Bunları manuel olarak yapmak hızla tükenmişliğe yol açar."
>
> Kaspersky Birleşik Platform Başkanı, Ilya Markelov

EDR platformları uç nokta düzeyindeki anormallikleri iyi bir şekilde tespit etse de, saldırının tam kapsamını anlamak için gereken daha geniş bağlamdan genellikle yoksundur. Sonuç olarak, analistler dedektiflik yapmaya mecbur kalıyorlar. Bu nedenle, uyarıları etkili bir şekilde sınıflandırmanın ve net bir görünürlük elde etmenin bir yolunu bulmak çok önemlidir.

Saldırı yüzeyi büyüyor, ancak kaynaklarınız aynı kalıyor

Sistem güçlendirme, küçük ve orta ölçekli kuruluşların saldırı yüzeyini azaltmalarına yardımcı olan çok önemli bir bileşendir. Esasen, sistem güçlendirme, potansiyel saldırı vektörlerini en aza indirmek ve saldırganların kolayca faydalanabileceği gereksiz hizmetleri veya özellikleri ortadan kaldırmak için siber güvenlik zayıflıklarını belirlemeyi ve düzeltmeyi içerir.

Ancak, sistemleri sağlam tutmak için sürekli izleme ve yeni güvenlik açıklarını gidermek için yama uygulamak gerekir; hızla değişen siber güvenlik düzenlemelerine uyum sağlamanın getirdiği yükten bahsetmeye bile gerek yok. Etkili sistem güçlendirme, sınırlı kaynaklara sahip küçük ekipler için genellikle zorlu bir görevdir.

Çalışanlarınız, kimlik avı ve sosyal mühendislik girişimlerine karşı koymakta zorlanır.

EDR'ye yatırım yapmanıza rağmen, çalışanlarınızın kimlik avı ve sosyal mühendislik saldırılarının kurbanı olduğunu görebilirsiniz. Bu, EDR'nin başarısızlığı değil, tehdit ortamının geliştiğinin bir işaretidir. EDR, bilinen kötü amaçlı yazılımları tanımlama, sistem davranışını izleme ve anormallikleri işaretleme konusunda etkilidir, ancak ihlallerin %22'sinde rol oynayan insan hatalarını önlemek için tasarlanmamıştır.[5]

Kimlik avı saldırıları, yazılımdaki bir güvenlik açığını kullanmak zorunda değildir; insan davranışındaki bir güvenlik açığını da kullanabilir. İyi hazırlanmış bir e-posta veya sahte bir oturum açma sayfası, bir çalışanın kimlik bilgilerini vermesini veya kötü amaçlı dosyaları indirmesini sağlayarak, sağlam EDR platformlarını bile atlatabilir.

Çalışanlarınız bu tür saldırıları tanımakta zorlanıyorsa, bu durum siber güvenlik stratejinizin EDR'nin ötesine geçmesi gerektiğinin açık bir göstergesidir. Proaktif savunma, kimlik korumasını kolaylaştıran sürekli eğitim ve araçlarla desteklenen bir güvenlik kültürü oluşturmak anlamına gelir. EDR'nin bir adım ötesine geçmek, tüm riskleri, özellikle de sosyal mühendislikten kaynaklanan riskleri ele almak anlamına gelir.

Saldırılar çok geç fark ediliyor

Saldırganlar meşru kanallardan erişim sağladığında, EDR'niz erişim çoktan verildikten sonra, saldırıyı çok geç tespit edebilir. IBM, 2024 yılında kuruluşların bir ihlali tespit etmek için ortalama 194 gün, bunu kapsayıcı olarak kontrol altına almak için ise ek olarak 64 gün harcadığını tespit etti.[5]Bu, önemsiz bir gecikme değildir. Bu, aylarca sürecek potansiyel veri sızdırma, yanal hareket ve kalıcılık anlamına gelir.

Her gün tespit edilmeyen bir olay, hassas verilerin çalınması, sistemlerin tehlikeye atılması veya fidye yazılımının kullanılması riskini artırır.

Manuel müdahale süreci sizi yavaşlatıyor

Güçlü ve düzenli olarak test edilen olay müdahale planlarına sahip şirketler, bu tür planları olmayan şirketlere kıyasla ortalama %58 maliyet tasarrufu sağlıyor.[10]Peki, bir olay müdahale planını "güçlü" yapan nedir? Kısacası, her şey hızla ilgilidir. Modern saldırı çerçeveleri hızla kısalıyor; örneğin, fidye yazılımları kritik sistemleri sadece dakikalar içinde kilitleyebiliyor ve günümüzün hızla gelişen tehdit ortamında manuel olay müdahalesi buna ayak uyduramıyor.

Otomatik sistemlerin aksine, siber güvenlik olaylarına manuel müdahale daha yavaştır ve en ufak bir gecikme bile daha büyük bir tehlikeye ve riske yol açabilir.

Olay müdahalesinde otomasyonun önemi göz ardı edilemez. Ekipler, otomasyondan yararlanarak tehditleri gerçek zamanlı olarak tespit edip önleyebilir ve maruz kalma süresini önemli ölçüde azaltabilir. Dahası, ekibinizin uzmanlıklarını gerektirebilecek diğer kritik görevlere odaklanmasına olanak tanıyarak size zaman, para ve kaynak tasarrufu sağlar.

Genişletmek mi, genişletmemek mi?

Tam teşekküllü XDR çözümleri - gelişmiş tehditlere karşı korunmak için çok önemli olsa da - henüz daha küçük BT ve siber güvenlik ekiplerinin özel ihtiyaçlarını karşılayamamaktadır.

Orta ölçekli şirketleri karmaşık siber saldırılara karşı savunmasız hale getiren güçlükler (sınırlı bütçe, kaynak eksikliği) aynı zamanda bu şirketlerin gelişmiş koruma önlemlerini etkili bir şekilde uygulamakta zorlanmalarının nedenleridir.

Bu özel çözümlerin uygulanması ve yönetilmesi oldukça karmaşıktır ve genellikle küçük BT ekipleri için çok dik bir öğrenme eğrisi gerektirir. Ancak en azından bazı XDR işlevlerine duyulan ihtiyaç giderek daha önemli hale geliyor ve bunlara ihtiyaç duyanlar sadece işletmeler değil. MDR Analist Raporumuz şöyle diyor: "2024 yılında, siber olayların araştırılması ve raporlanması için geçen ortalama süre 2023 yılına kıyasla %48 artarak saldırı karmaşıklığındaki önemli artışı yansıtmaktadır. Bu durum, büyük çoğunluğu özel XDR araçlarından gelen tetiklenmiş tespit kurallarının ve Saldırı Göstergelerinin (IoA) analiziyle desteklenmiştir. Bu durum önceki yıllardan değişiklik göstermektedir, burada OS (işletim sistemi) günlükleri ile yapılan tespitler önemli bir rol oynamıştır. Bu koşullar altında, XDR gibi özelleştirilmiş araçlar modern tehditlerin başarılı bir şekilde tespit edilmesi ve araştırılması için esastır.[7]

Kaspersky nasıl yardımcı olabilir?

Küçük ekipler için optimize edilmiş kurumsal düzeyde koruma

Kaspersky NEXT XDR Optimum, küçük BT ve siber güvenlik ekipleri için tasarlanmıştır. Çözüm, olay müdahalesini güçlendirir ve zaman alan rutin görevlerin ek yükü olmadan uzmanlık oluşturur.

Otomatikleştirilmiş birden fazla süreçle, en önemli olan konulara odaklanabilirsiniz.

Üstün uç nokta korumasını açığa çıkarın

İş kesintilerini önlemek için otomatik korumadan yararlanın. Sektörde kendini kanıtlamış makine öğrenimi tabanlı fidye yazılımı ve kötü amaçlı yazılımdan koruma araçlarıyla, hem bilinen hem de bilinmeyen tehditlerden kaynaklanan bulaşmaları zahmetsizce önleyebilirsiniz.

Güvenlik alanında aktif bir rol oynamaları için tüm ekibinizi eğitin

Güvenliği sağlamak için BT personeliniz ve teknik olmayan çalışanlarınızı bilgi ve kabiliyetler ile donatın. BT güvenlik ekibinizi güçlendirirken, iş gücünüz genelinde güçlü ve güvenlik bilincine sahip bir kültür oluşturun.

Sistemi güçlendirme ve eğitim üzerinden zayıf noktaların sorununu giderin

Kullanıcı davranışına dayalı sistem sertleştirme ile saldırı yüzeyinizi küçültün. Merkezi zayıf nokta, yama ve şifreleme yönetimi ile zamandan tasarruf edin ve yeni siber güvenlik yeteneklerinizden en iyi şekilde yararlanmak için ekibinizin ihtiyaç duyduğu tüm eğitimleri sağlayın.

Güvenebileceğiniz bulut güvenliği ile gölge BT'yi kontrol edin

Zayıf noktalarınızı azaltın ve gölge BT'yi kontrol ederek verileriniz ve çalışanlarınızı koruyun. Hangi bulut hizmetlerinin kullanımda olduğunu görün, yetkisiz erişimi engelleyin ve Microsoft 365 uygulamalarında hangi hassas verilerin depolandığını öğrenin.

Algılama ve müdahale yeteneklerinizi artırın

Tehditler ve bunların uç noktaların içinde ve ötesinde nasıl hareket ettikleri hakkında bilgi edinin. Saldırılara karşı koymak için otomasyon ve yönlendirilmiş müdahale ve bu saldırıların faaliyetlerini izlemek için temel araştırma araçlarını kullanın.

Uyarı yorgunluğunu en aza indirin

Next XDR Optimum'un uyarı toplama özelliği, etkili ve kanıtlanmış uç nokta koruması ile birleştiğinde ekiplerin analiz etmesi gereken uyarı sayısını azaltır. Bu, verimliliği artırır ve uyarı yorgunluğunu azaltır ve ekibinizin diğer kritik görevlere odaklanmasını sağlar.

XDR artık sadece büyük şirketler için değil

Daha küçük ekipler için optimize edilmiş bir üst düzey çözümü keşfedin.

Kaspersky Next XDR Optimum

Daha fazla bilgi

Kaynakça:

[1] Kaspersky, B2B BT güvenlik risk takip raporu, (Kaspersky, 2024)
[2] Tuteja, Akhilesh, Karmaşık bir siber güvenlik ortamında tedarik zinciri karşılıklı bağımlılıklarından kaynaklanan 5 risk faktörü, (Dünya Ekonomik Forumu, 2025)
[3] Kaspersky, Modern bir İnfosec profesyonelinin portresi, (Kaspersky, 2024)
[4] Willie, Alan, Hizmet Olarak Fidye Yazılımlarının (RaaS) Evrimi: Yapay Zekanın Siber Suç ve Karşı Önlemlerdeki Rolü, (Stanford Üniversitesi, 2025)
[5] IBM, Veri İhlallerinin Maliyeti Raporu 2024, (IBM, 2024)
[6] Verizon, 2024 Veri İhlali Araştırmaları Raporu, (Verizon, 2024)
[7] Kaspersky, Kale ateş altında: siber tehdit günlükleri 2024, (Kaspersky MDR Analist Raporu, 2024)
[8] Verizon, 2024 Veri İhlali Araştırmaları Raporu, (Verizon, 2024)
[9] Kaspersky ve VDC Genişletilmiş Anket Bulguları, (OT ortamlarının güvenliğini sağlama, 2024)
[10] IBM, Veri İhlallerinin Maliyeti Raporu 2022, (IBM, 2022)

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın