Microsoft Security

Tümleşik Tehdit Korumasına Geçişin 3 Nedeni

İçindekiler

Giriş 3

1. Neden
Daha azıyla daha fazlasını yapma 5

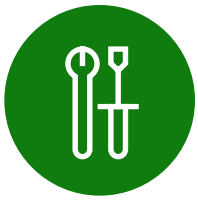
2. Neden
Yüksek değerli görevlere odaklanmak için SecOps'u güçlendirme 7

3. Neden
Çalışanların üretkenliğini artırma 10

SIEM ve XDR ile tümleşik siber tehdit koruması elde etme 12

Güvenliği takviye etmeyin. Yerleştirin. 14

Giriş



Sıradan bir kurum artık 30'dan fazla farklı güvenlik aracı kullanıyor. Bu araçlar genellikle ayrık ve "takviye edilmiş".

Güvenlik bir dönüm noktasındadır. Kurumlar, yetenek eksiklikleri ve maliyet dengelemeden hibrit çalışmanın baskılarından kurtulmaya kadar değişen zorluklarla uğraşmaya devam ederken, siber saldırılar daha karmaşık hale geliyor.

Bu arada, güvenlik pazarı her zamankinden daha parçalı ve karmaşık. Ortalama bir kurum, şu anda güvenlik operasyon merkezlerine (SOC'ler) sınırlı görünürlük ve yetersiz görüş sağlayan, genellikle ayrık ve "takviye edilmiş" 30'dan fazla farklı güvenlik aracı kullanmaktadır.

Güvenlik ve uyumluluk liderleri en güncel riskleri ve tehditleri daha iyi anlamak ister ancak aynı zamanda neyin işe yarayıp neyin yaramadığını ve nerede boşluklar olduğunu da bilmeleri gerekir.

Günümüzün güvenlik zorluklarının kapsamı bunaltıcı gibi görünse de, CISO'lar için güvenlik operasyonlarının verimliliğini ve etkinliğini iyileştirmeye yönelik iyimserliğin bir nedeni vardır. Bu sorunun yanıtı, kurumlara yardımcı olacak siber tehdit korumasına yönelik tümleşik, uçtan uca bir yaklaşımdır:

1. Neden: Daha azıyla daha fazlasını yapma

Nokta çözümlerini birleştirin ve güvenlik operasyonları (SecOps) ek yükünü azaltın.

2. Neden: Yüksek değerli görevlere odaklanmak için SecOps'u güçlendirme

Verimliliği artıran ve deneyimsiz analistleri bile her zamankinden daha yetenekli hale getiren araçlar kullanın.

3. Neden: Çalışanların üretkenliğini artırma

Kurumunuzu, çalışanlarınızın yenilikler yaparken korkusuz olmalarını sağlayacak bir yolla koruyun.

Bu yaklaşım, genişletilmiş bir algılama ve yanıt (XDR) çözümünün, yapay zeka (AI) ve otomasyon yetenekleri kullanılan buluta özel güvenlik bilgileri ve olay yönetimi (SIEM) sistemiyle tümleştirilmesiyle sağlanır. Tümleşik çözüm, SOC'nizin kurum genelindeki saldırılara karşı daha öngörülü, proaktif ve önleyici olmasına yardımcı olabilir.

1. Neden

Daha azıyla daha fazlasını yapma

Microsoft'un tümleşik çözümü ile araçları birleştirerek, yalnızca kullandığınız kadarını ödeyerek de tasarruf edebilirsiniz.

Birçok kurum güvenlik araçlarına türünün en iyisi olan çözümlere odaklanarak yaklaşmıştır. Ne yazık ki, bu yaklaşım güvenlik uzmanlarının tehditleri hızlı bir şekilde tanımlamasını ve bunlara karşılık vermesini zorlaştırabilir. Ayrıca BT harcamaları ve son kullanıcı üretkenliği üzerinde olumsuz bir etkiye sahip olabilir.

Kurumlar daha azıyla daha fazlasını yapmak istedikçe Microsoft'un SIEM ve XDR'si gibi tümleşik bir yaklaşım yararlı olabilir. Tek araçları birleştirerek karmaşıklığı azaltabilir ve buluta özel olduğundan tümleşik bir çözüm de performansı ve ölçeği iyileştirebilir.

Microsoft'un tümleşik çözümü ile araçları birleştirerek, yalnızca kullandığınız kadarını ödeyerek de tasarruf edebilirsiniz. Ayrıca, otomasyon ve entegrasyonu artırarak çözümleri yönetmek için gereken SecOps yükünü de azaltabilirsiniz.

> Yeni güvenlik araçlarını benimseme sürecini başlatmak kolaydır, çünkü boşlukların geniş olmasını beklersiniz. Buradan itibaren, farklı tedarikçilerin araçlarının kendi görev alanlarında potansiyel olarak çakışabileceğini göreceksiniz. Böyle bir çakışma kontroller ve dengeler için arzu edilebilir **ancak yüksek bir finansal maliyete neden olabilir.**"
>
> **Jonathan Cassar**
> Baş Teknoloji Sorumlusu, MITA

1,6 milyon ABD doları

tedarikçi konsolidasyonu kaynaklı yıllık tasarruflar

Microsoft, Total Economic Impact™ (TEI) çalışması yürütmek ve Microsoft SIEM and XDR'ı kuran kurumların elde edebileceği potansiyel yatırım getirisini incelemek üzere Forrester Consulting'i görevlendirdi. Bunlar, toplam 8.000 çalışanı ve 10 güvenlik uzmanıyla varsayımsal bir karma kurumun temel bulgularından bazılarıydı:

- **Tedarikçi konsolidasyonu kaynaklı yıllık neredeyse 1,6 milyon ABD doları tasarruf**. Microsoft SIEM ve XDR yatırımı, bileşiğin önceki SIEM'in maliyetini (560.000 ABD doları), ilişkili kurum içi altyapıyı (360.000 ABD doları'nin üzerinde), üç XDR nokta çözümünü (192.000 ABD doları) ve bunları yönetmek için devam eden işçilik maliyetini azaltmasına olanak tanır (480.000 ABD doları).
- **Bir malzeme ihlali riskini %60 azaltma.** Daha verimli güvenlik soruşturması ve müdahale iş akışları, gelişmiş güvenlik yanıtı otomasyonu ve çoklu bulut koruması da dahil olmak üzere tüm bilişim ortamlarını koruma yeteneğinin artmasıyla bileşik, yıllık 1,6 milyon ABD doları tasarruf etkisi ile ihlal riskini azaltır.
- **%207'lik bir yatırım getirisi oluşturma.** Temsili görüşmeler ve finansal analizde, bileşik bir kurumun 5,76 milyon ABD doları maliyetle üç yıllık bir süre boyunca 17,68 milyon ABD doları fayda sağladığı ve bunun 11,92 milyon ABD doları'lik net bugünkü değere (NPV) ulaştığı tespit edildi.

2. Neden

Yüksek değerli göre-vlere odaklanmak için SecOps'u güçlendirme

Uyarıları ilişkilendirmek, en büyük tehditlere öncelik vermek ve kurum genelindeki eylemleri koordine etmek için SIEM ve XDR'i uyumlu hale getirmek son derece önemlidir.

SecOps ekipleri, manuel olarak tespit edip hafifletmesi imkansız değilse bile çok sayıda düşük güvenilirlik sinyali de dahil olmak üzere analiz etmeleri gereken sinyal miktarı karşısında bunalmış durumdadır. Tehditler arttıkça, özellikle çok noktalı çözümlerden gelen verileri analiz etmeye çalışırken aşırı yüklenmiş bir SOC'nin devam etmesi zorlaşır. Boşlukları doldurmak için daha fazla kaynak ayırmak yeterli değildir çünkü yeteri kadar yetenekli güvenlik uzmanı bulmak devam etmekte olan bir sorundur.

Bu nedenle, tehditleri proaktif olarak tespit etmek ve düzeltmek için ileri düzey yapay zeka ve otomasyonla uyarıları ilişkilendirmek, en büyük tehditlere öncelik vermek ve kurum genelinde eylemleri koordine etmek için SIEM ve XDR'yi tümleştirmek son derece önemlidir.

Örneğin tek bir düşük seviyeli sinyalin geleneksel bir SIEM'den çok fazla ilgi görmeyebileceğini düşünün. Ancak buluta özel bir SIEM, yapay zeka kullanarak bu sinyali kurumdaki diğer kaynaklardan gelen sinyallerle otomatik olarak karşılaştırabilir ve çok aşamalı saldırıları bulmak için birden çok veri kümesi arasında ilişki kurabilir.

Tümleşik SIEM ve XDR, SecOps kaynaklarını serbest bırakırken aynı zamanda deneyimsiz analistlere bile daha fazla yetenek ve güvenle destek verir.

Sistem daha sonra, siber saldırının altyapıya nasıl girdiğine dair bağlam sunarken nasıl yayıldığına dair zaman çizelgesiyle birlikte verileri normalleştirir, analiz eder ve ilişkilendirir. Bu, SOC ekiplerinin ihlali tek bir konsoldan görselleştirip etkin bir şekilde ele almasını sağlar.

> Birçok CISO **20 farklı cam bölmeyle veya nokta çözümleriyle ekiplerine dayatılan ek yük** ile ilgili yıllık maliyetlerin farkında değildir... Tek bir tedarikçiyle araç yorgunluğu büyük oranda ortadan kaldırdık."
>
> **Terence Jackson**
> Baş Bilgi Güvenliği ve Gizliliği Sorumlusu, Thycotic

Bir kurum, bir güvenlik çözümünün değerini ortaya çıkarmak için derin uzmanlığa ihtiyaç duymamalıdır. Tümleşik SIEM ve XDR, SecOps kaynaklarını serbest bırakırken aynı zamanda deneyimsiz analistlere bile daha fazla yetenek ve güvenle destek verir.

Microsoft SIEM ve XDR'nin tümleşik yaklaşımı, tehditleri araştırma süresini %65 oranında azalttı.

Microsoft tarafından yaptırılan Forrester Total Economic Impact™ (TEI) çalışması, bileşik kurumunda bu tür SecOps verimliliğini gösterdi:

- **Tehditleri araştırma süresini %65 oranında, tehditlere yanıt verme süresini ise %88 oranında azaltma.** Microsoft SIEM ve XDR'nin güvenlik tehdidi araştırma ve yanıtına yönelik tümleşik yaklaşımı, bu iş akışlarını bileşik kurumun güvenlik uzmanları için daha verimli hale getirir. Tehditleri tanımlamak için artık birden çok araç arasında geçiş yapmaları gerekmiyor, güvenlik otomasyonu özellikleri ise yanıt iş akışlarını daha da geliştiriyor.
- **Yeni bir çalışma kitabı oluşturma süresini %90, yeni güvenlik uzmanlarını işe alma süresini ise %91 azaltma.** Microsoft SIEM ve XDR'nin tümleşik yaklaşımı, ek güvenlik uzmanı iş akışlarını da daha verimli hale getirir. SIEM logları bir dizi çözümle tümleştiğinden, çalışma kitabı oluşturma neredeyse otomatikken tekil bir oturum açma özelliği, yeni güvenlik uzmanlarının yaklaşık 16 hafta daha hızlı bir şekilde devreye girmesini sağlar.

3. Neden

Çalışanların üretkenliğini artırma

Tümleşik bir SIEM ve XDR çözümü, kurumunuzun son kullanıcılar için üretkenliği artırmasına yardımcı olabilir.

Daha azıyla daha fazlasını yapma ve SecOps verimliliğini artırmanın yanı sıra tümleşik bir SIEM ve XDR çözümü kurumunuzun son kullanıcılar için üretkenliği iyileştirmesine yardımcı olabilir.

SecOps ekiplerinin de bildiği gibi, güvenliği zorlaştırdığınızda, çalışanlar bunu aşmaya çalışır. Dolayısıyla, son kullanıcı deneyimleri çalışanların üretkenliği bakımından yararlı olmaktansa, daha fazla güvenlik riskine ve daha yüksek maliyete açık bir kurum bırakabilir. Zayıf veya kayıp parolalar, kişisel cihazlar üzerinden güvenli olmayan erişim veya hassas verilerin serbestçe paylaşılması bu zorluklardan yalnızca birkaçıdır.

> [Geçmişte] birisi bir sorundan şüphelenirse körelmiş araçlar kullanırdık. Kurumu olumsuz etkileyen şeyleri kapatıp erişimi sonlandırırdık. Bu herkes için çok netti çünkü her şey geçici olarak çalışmayı durduracaktı. Microsoft Sentinel'de olup bitenlere cerrahi olarak karşılık verebileceğimiz bir neşterimiz var. **Kurum genellikle bir tehdide ne zaman karşılık verdiğimizi bile bilmiyor** ve bu başarımızın çok önemli bir ölçüsü."
>
> **Rick Gehringer**
> Bilişim Kurulu Başkanı, Wedgewood

Neredeyse
68.000
Microsoft SIEM ve XDR, diğer çalışanların üretkenliğini yılda toplam 68.000 saat artırdı.

Tümleşik bir SIEM ve XDR yaklaşımı, çalışanlarınızı günlük deneyimlerinin tüm yönlerinde hem üretken hem de güvende tutan sorunsuz kullanıcı deneyimleri sunmanıza yardımcı olur. Hizmetleri kapatmak veya makineleri yalıtarak yeniden tasarlamak gibi üretkenlik üzerindeki olumsuz etkileri azaltabilir. Ancak tümleşik SIEM ve XDR, son kullanıcı üretkenlik kazanımları için daha fazla self servis güvenlik desteği, daha iyi dashboard'lar ve raporlama ile daha az güvenlik aracısı çalıştırmanın daha hızlı yanıt müdahale süreleri gibi yeni fırsatlar da oluşturabilir.

Microsoft tarafından yaptırılan Forrester Total Economic Impact™ (TEI) çalışmasında, toplam 8.000 çalışanı bulunan teorik bileşik kurum, Microsoft SIEM ve XDR'yi kurarak çalışan üretkenliğinde artış gösterdi:

- **Diğer çalışanların üretkenliğini yılda toplam 68.000 saat artırma.** Microsoft SIEM ve XDR, verimsiz güvenlik işlemlerinden kaynaklanan diğer çalışanlar üzerindeki olumsuz etkileri önler. Örneğin, bileşik BT uzmanlarının güvenlik güncelleştirmeleri ve önerileriyle ilgili yeni self servis olma özelliği sayesinde yılda 4.000 saat tasarruf sağlıyor. Ayrıca, çalışan makinelerde uzaktan güvenlik tabanlı sorun giderme imkanı veriyor ve makinelerde çalışan güvenlik aracılarının sayısını azaltarak son kullanıcı üretkenliğinde yılda yaklaşık 64.000 saat tasarruf sağlıyor.

Güvenlik, teknolojik başarının önemli bir kolaylaştırıcısı haline gelmiştir. Bu nedenle kurumların, büyümeyi sağlayan üretkenliği ve yeniliği koruyup mümkün kılmak için modern saldırılara karşı mümkün olduğunca esneklik sağlayan güvenlik önlemlerine ihtiyacı vardır.

SIEM ve XDR ile tümleşik siber tehdit koruması elde etme

Sektör lideri ürünlerin bu entegrasyonu, tek bir kapsamlı çözümde siber tehdit önleme, algılama ve yanıt imkanı veriyor.

Microsoft, tüm bulutlarda ve platformlarda uçtan uca görünürlük sağlayan ilk ve tek tümleşik SIEM ve XDR çözümünü sunuyor. Sektör lideri ürünlerin bu entegrasyonu, tek bir kapsamlı çözümde siber tehdit önleme, algılama ve yanıt imkanı veriyor.

Microsoft SIEM ve XDR, yapay zeka ve otomasyonun gücünden ve siber tehdit algılama ve analizine yönelik derin, devam eden yatırımlardan yararlanıyor. Uzman görüşlerine ve her gün 43 trilyon sinyale görünürlük sağlıyor. SOC ekipleri, bu ürünler arasında entegrasyon ile kritik siber tehditleri daha hızlı bir şekilde avlamak ve çözmek için her zamankinden daha fazla bağlamla donatılıyor:

Microsoft Sentinel

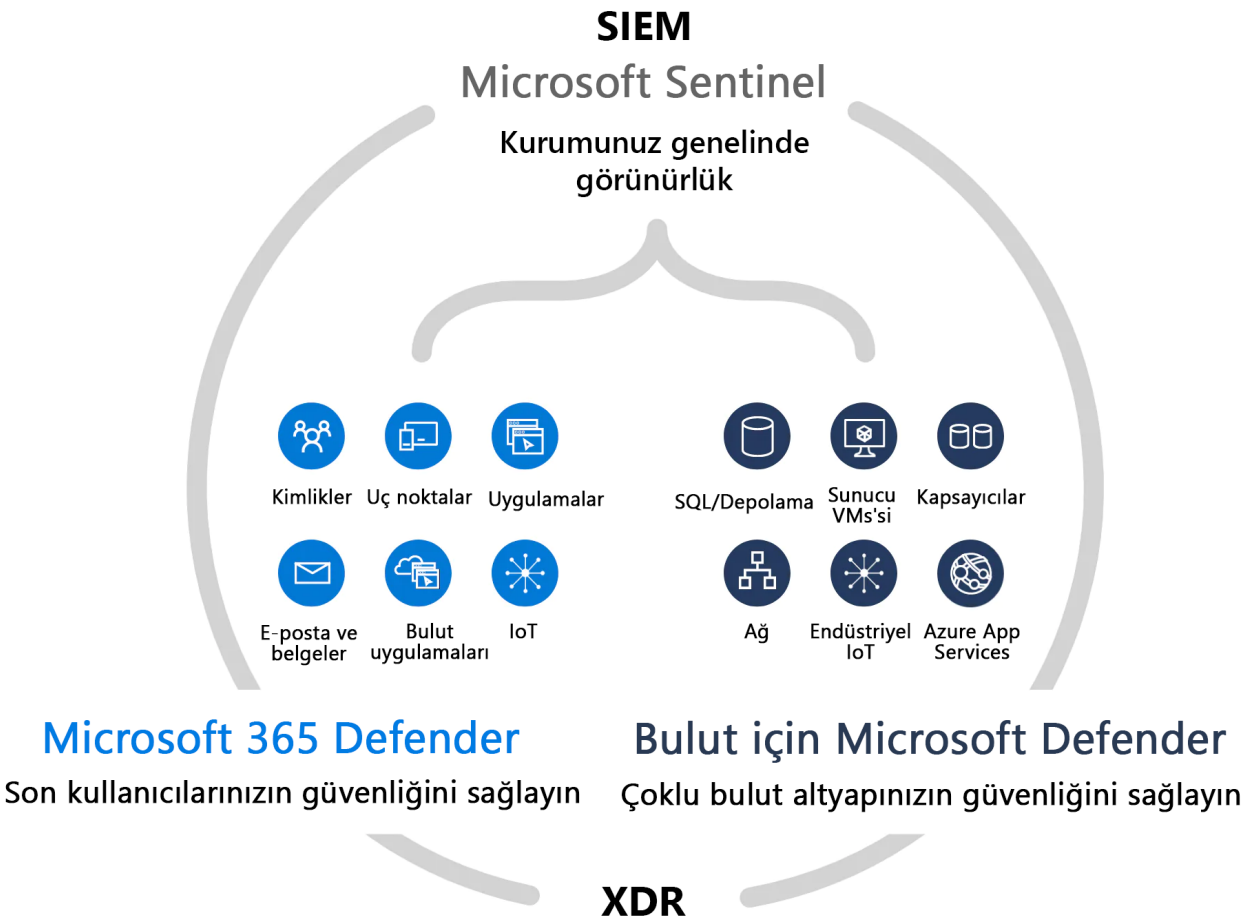
Microsoft'un buluta özel SIEM'i ile kurum genelinde kuşbakışı bir görüş elde edin. Güvenlik verilerini sanal olarak herhangi bir kaynaktan toplayın ve yapay zekayı gürültüleri yasal olaylardan ayırın, karmaşık siber saldırı zincirleri arasında uyarılarla ilişkilendirin ve yerleşik düzenleme ve otomasyonla siber tehditlere müdahaleyi hızlandırın.

Microsoft Defender XDR

XDR özelliklerine sahip kimlikleriniz, uç noktalarınız, uygulamalarınız, e-postanız, verileriniz ve bulut uygulamalarınıza yönelik siber saldırıları önleyin ve tespit edin. Kullanıma hazır, sınıfının en iyisi koruma ile saldırıları inceleyin ve siber saldırılara müdahale edin. Tehditleri avlayın ve tek bir dashboard'dan müdahalenizi kolayca koordine edin.

Bulut için Microsoft Defender

Yerleşik XDR özellikleriyle çoklu bulut ve hibrit bulut iş yüklerinizi koruyun. Sunucularınızı, depolama alanlarınızı, veritabanlarınızı, kapsayıcılarınızı ve daha fazlasını güvenceye alın. Öncelikli uyarılarla en önemli noktalara odaklanın.



Güvenliği takviye etmeyin. Yerleştirin.

Doğru araçları ve zekayı doğru kişilerin ellerine verin. Uçtan uca, buluta özel, tümleşik bir çözümle modern saldırılara karşı savunma yapın.

Microsoft'un SIEM ve XDR çözümleri ile tümleşik siber tehdit koruması hakkında daha fazla bilgi edinin >

Microsoft Security

©2024 Microsoft Corporation. Tüm hakları saklıdır. Bu belge "olduğu gibi" sunulmuştur. URL ve diğer internet web sitesi referansları dahil bu belgedeki bilgiler ve görüşler bildirimde bulunmaksızın değiştirilebilir. Belgenin kullanımından doğan risk size aittir. Bu belge size, Microsoft ürünlerinin fikri mülkiyeti konusunda herhangi bir yasal hak sağlamaz. Bu belgeyi kendi kurum içi referans amaçlarınız doğrultusunda kopyalayabilir ve kullanabilirsiniz.