Sophos Managed Detection and Response

7/24 Tehdit Tespiti ve Müdahale

Sophos MDR, bilgisayarlarınızı, sunucularınızı, ağlarınızı, bulut iş yüklerinizi, e-posta hesaplarınızı ve daha fazlasını hedef alan siber saldırıları tespit eden ve bunlara müdahale eden ve 7/24 uzmanlar tarafından yönetilen bir hizmettir.

Fidye Yazılım ve İhlal Önleme Hizmetleri

Her zaman açık güvenlik işlemlerine duyulan ihtiyaç bir zorunluluk haline gelmiştir. Ancak modern işletim ortamlarının karmaşıklığı ve siber tehditlerin hızı, çoğu kuruluşun tespit ve müdahaleyi kendi başına başarılı bir şekilde yönetmesini giderek zorlaştırmaktadır.

Uzman ekibimiz, Sophos MDR ile insan kaynaklı gelişmiş saldırıları durduruyor. Tehditleri, iş operasyonlarınızı sekteye uğratmadan ya da hassas verilerinizi tehlikeye atmadan önce etkisiz hale getirmek için harekete geçiyoruz. Sophos MDR, farklı hizmet katmanlarıyla özelleştirilebilir ve tescilli teknolojimiz aracılığıyla ya da mevcut siber güvenlik teknolojisi yatırımlarınızı kullanarak hizmet verebilir.

Hizmet olarak sağlanan Siber Güvenlik

Sophos MDR, verilerinizin bulunduğu her yerde tam güvenlik kapsamı sağlayan genişletilmiş tespit ve müdahale (XDR) becerileri ile şunları yapabilir:

- **Güvenlik araçlarının tek başına tespit edebileceğinden daha fazla siber tehdidi tespit edebilir**
  Araçlarımız tehditlerin %99,98'ini otomatik olarak engeller, bu da analiz uzmanlarımızın yalnızca yüksek eğitimli bir kişi tarafından tespit edilip durdurulabilecek en sofistike saldırganları avlamaya odaklanmasını sağlar.
- **Tehditlerin işinizi sekteye uğratmasını önlemek için sizin adınıza harekete geçer**
  İster tam ölçekli olay müdahalesine ister doğru kararlar almak için yardıma ihtiyacınız olsun, analiz uzmanlarımız tehditleri yalnızca birkaç dakika içinde tespit eder, araştırır ve bunlara müdahale eder.
- **Gelecekteki olayları önlemek için tehditlerin temel nedenini belirleyin**
  Proaktif olarak önlemler alıyor ve kuruluşunuza yönelik riski azaltan öneriler sunuyoruz. Daha az olay, BT ve güvenlik ekipleriniz, çalışanlarınız ve müşterileriniz için daha az kesinti anlamına gelir.

Halihazırda Sahip Olduğunuz Siber Güvenlik Araçları ile Uyumlu

İhtiyacınız olan teknolojiyi ödüllü portföyümüzden sağlayabilir veya analiz uzmanlarımız tehditleri tespit etmek ve bunlara müdahale etmek için mevcut siber güvenlik teknolojilerinizden yararlanabilir.

Sophos MDR, Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace ve diğer birçok tedarikçinin güvenlik telemetrisi ile uyumludur. Telemetri, Sophos Adaptive Cybersecurity Ecosystem (ACE) ve Sophos X-Ops tehdit istihbarat biriminden gelen bilgilerle otomatik olarak birleştirilir, ilişkilendirilir ve önceliklendirilir.

Öne Çıkan Noktalar

- Tehdit müdahale uzmanlarından oluşan 7/24 çalışan bir ekiple fidye yazılımlarını ve diğer gelişmiş insan kaynaklı saldırıları durdurun
- Mevcut siber güvenlik teknolojilerinizin yatırım getirisini en üst düzeye çıkarın
- Sophos MDR'nin tam ölçekli olay müdahalesi gerçekleştirmesine, güvenlik olaylarını yönetmek için sizinle birlikte çalışmasına veya ayrıntılı tehdit bildirimleri ve rehberlik sunmasına izin verin
- 7/24 izleme ve uç nokta tespiti ve müdahale (EDR) özellikleriyle siber sigorta kapsamı uygunluğunu iyileştirin
- Dahili BT ve güvenlik personeliniz yalnızca iş geliştirmeye odaklansın

SOPHOS

Sizi Bulunduğunuz Noktada Karşılayan MDR

Sophos MDR, farklı hizmet kademeleri ve tehdit müdahale seçenekleri ile özelleştirilebilir. Sophos MDR operasyon ekibinin tam ölçekli olay müdahalesi gerçekleştirmesine, siber tehditleri yönetmek için sizinle birlikte çalışmasına veya tehditler tespit edildiğinde dahili güvenlik operasyon ekiplerinizi bilgilendirmesine izin verin. Ekibimiz bir saldırının kim tarafınca, ne, ne zaman ve nasıl gerçekleştirildiğini hızla öğrenir. Tehditlere birkaç dakika içinde müdahale edebiliriz.

Temel Özellikler

7/24 Tehdit İzleme ve Müdahale

Tehditleri, verilerinizi tehlikeye atmadan veya kesintiye neden olmadan önce tespit ediyor ve bunlara müdahale ediyoruz. Altı küresel güvenlik operasyon merkezi (SOC) tarafından desteklenen Sophos MDR, günün her saati hizmet sağlar.

Sophos Dışı Güvenlik Araçları ile Uyumlu

Sophos MDR, Sophos ACE'nin bir parçası olarak üçüncü taraf uç nokta, güvenlik duvarı, kimlik, e-posta ve diğer güvenlik teknolojilerinden gelen telemetriyi entegre edebilir.

Tam Ölçekli Olay Müdahalesi

Aktif bir tehdit tespit ettiğimizde, Sophos MDR operasyon ekibi, düşmanı uzaktan engellemek, kontrol altına almak ve tamamen ortadan kaldırmak için sizin adınıza kapsamlı bir dizi müdahale eylemi gerçekleştirebilir.

Haftalık ve Aylık Raporlama

Sophos Central, gerçek zamanlı uyarılar, raporlama ve yönetim için tek kontrol panelinizdir. Haftalık ve aylık raporlar, güvenlik araştırmaları, siber tehditler ve güvenlik duruşunuz hakkında içgörüler sağlar.

Sophos Adaptif Siber Güvenlik Ekosistemi

Sophos ACE, kötü niyetli etkinlikleri otomatik olarak önler ve tespit etmek, araştırmak ve ortadan kaldırmak için insan müdahalesi gerektiren tehditlerde zayıf sinyalleri aramamızı sağlar.

Uzman Yönetiminde Tehdit Avlama

Yüksek eğitimli analiz uzmanları tarafından gerçekleştirilen proaktif tehdit avlamaları, güvenlik ürünlerinin kendi başlarına tespit edebileceğinden daha fazla tehdidi ortaya çıkarır ve hızla ortadan kaldırır. Sophos MDR operasyon ekibi, üçüncü taraf tedarikçilerin telemetrisini kullanarak da tehdit avlamaları gerçekleştirebilir ve kullanılan araç setlerinin tespitinden kaçan saldırgan davranışlarını belirleyebilir.

Doğrudan Çağrı Desteği

Ekibiniz, olası tehditleri ve aktif olayları incelemek için Güvenlik Operasyon Merkezimize (SOC) doğrudan çağrı erişimine sahiptir. Sophos MDR operasyon ekibi 7/24/365 ulaşılabilir durumdadır ve dünya çapında 26 lokasyondaki destek ekipleri tarafından desteklenmektedir.

Özel Olay Müdahale Ekibi Yöneticisi

Sizin için, bir olayı tespit eder etmez dahili ekibiniz ve harici iş ortağınızla/ortaklarınızla işbirliği yapan ve olay çözülene kadar sizinle birlikte çalışan özel bir Olay Müdahale Ekibi Yöneticisi görevlendiriyoruz.

Kök Neden Analizi

Güvenli duruşunuzu iyileştirmek için proaktif öneriler sunmanın yanı sıra, bir olaya yol açan altta yatan sorunları belirlemek için kök neden analizi yapıyoruz. Gelecekte ihlal edilmemeleri için güvenlik zayıflıklarını ele almak üzere size adım adım rehberlik sağlıyoruz.

Sophos Hesap Sağlık Kontrolü

Sophos XDR tarafından yönetilen uç noktaların ayarlarını ve yapılandırmalarını sürekli olarak gözden geçiriyor ve en üst düzeyde çalıştıklarından emin oluyoruz.

Tehdidin kontrol altına alınması

Sophos MDR'ın tam ölçekli olay müdahalesi gerçekleştirmesini tercih etmeyen kuruluşlar için Sophos MDR operasyon ekibi, tehdidi durdurarak ve yayılmasını önleyerek tehdidi kontrol altına alma eylemlerini gerçekleştirebilir. Bu sayede iç güvenlik operasyon ekiplerinin iş yükü azalır ve hızlı bir şekilde iyileştirme eylemlerinde bulunmaları sağlanır.

İstihbarat Brifingleri: "Sophos MDR ThreatCast"

Sophos MDR operasyon ekibi tarafından sunulan "Sophos MDR ThreatCast", Sophos MDR müşterilerine özel olarak sunulan aylık bir brifingdir. En son tehdit istihbaratı ve en iyi güvenlik uygulamaları hakkında bilgi sağlar.

İhlal Koruma Garantisi

Tüm Sophos MDR Complete'in yıllık (bir - beş yıllık) veya aylık lisanslarına dahil olan garanti, 1 milyon dolara kadar müdahale masraflarını karşılar. Garanti kademeleri, minimum sözleşme koşulları veya ek satın alma gereksinimleri yoktur.

Sophos Hizmet Kademeleri

	Sophos Tehdit Danışmanı	Sophos MDR	Sophos MDR Complete
7/24 uzman yönetiminde tehdit izleme ve müdahale	✓	✓	✓
Sophos dışı güvenlik ürünleriyle uyumlu	✓	✓	✓
Haftalık ve aylık raporlama	✓	✓	✓
Aylık istihbarat brifingi: "Sophos MDR ThreatCast"	✓	✓	✓
Sophos Hesap Sağlık Kontrolü		✓	✓
Uzman yönetiminde tehdit avlama		✓	✓
Tehdidin kontrol altına alınması: saldırılar kesintiye uğratılarak yayılması engellenir Tam Sophos XDR birimini (koruma, algılama ve müdahale) veya Sophos XDR Sensor (algılama ve müdahale) kullanır		✓	✓
Aktif olaylar sırasında doğrudan çağrı desteği		✓	✓
Tam ölçekli olay müdahalesi: tehditler tamamen ortadan kaldırılır Tam Sophos XDR birimini gerektirir (koruma, algılama ve müdahale)			✓
Kök Neden Analizi			✓
Özel Olay Müdahale Ekibi Yöneticisi			✓
İhlal Koruma Garantisi 1 milyon dolara kadar müdahale masraflarını karşılar			✓

Sophos MDR Dahil Entegrasyonlar

Aşağıdaki kaynaklardan gelen güvenlik verileri, Sophos MDR operasyon ekibi tarafından ek bir ücret ödemeden kullanılmak üzere entegre edilebilir. Telemetri kaynakları, ortamınızdaki görünürlüğü genişletmek, yeni tehdit algılamaları oluşturmak ve mevcut tehdit tespitlerinin doğruluğunu artırmak, tehdit avı yapmak ve ek müdahale becerileri sağlamak için kullanılır.

Sophos XDR

Yerel uç nokta, sunucu, güvenlik duvarı, bulut, e-posta, mobil ve Microsoft entegrasyonlarını birleştiren tek XDR platformu

Sophos MDR ve Sophos MDR Complete Fiyatlandırmasına Dahil

Sophos Firewall

Gelişmiş tehditleri zarar verme şansı bulamadan durdurmak için gelen ve giden ağ trafiğini izleyin ve filtreleyin

Ürün ayrı satılır; ek ücret alınmadan entegre edilir

Microsoft Graph Güvenliği

- Uç Nokta için Microsoft Defender
- Bulut için Microsoft Defender
- Bulut Uygulamaları için Microsoft Defender
- Kimlik için Microsoft Defender
- Kimlik Koruması (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Güvenlik ve Uyumluluk Merkezi
- Azure Bilgi Koruması

Sophos Endpoint

Gelişmiş tehditleri engelleyin ve meşru kullanıcıları taklit eden saldırganlar da dahil olmak üzere kötü niyetli davranışları tespit edin

Sophos MDR ve Sophos MDR Complete Fiyatlandırmasına Dahil

Sophos Email

Gelen kutunuzu kötü amaçlı yazılımlardan koruyun ve hedef odaklı kimliğe bürünme ve kimlik avı saldırılarını durduran gelişmiş yapay zekadan yararlanın

Ürün ayrı satılır; ek ücret alınmadan entegre edilir

Office 365 Yönetim Etkinliği

Office 365 ve Azure Active Directory günlüklerinden kullanıcı, yönetici, sistem ve ilke eylemleri ve olayları hakkında bilgi sağlar

Sophos Cloud

Bulut ihlallerini durdurun ve AWS, Azure ve Google Cloud Platform dahil olmak üzere kritik bulut hizmetlerinizde görünürlük elde edin

Ürün ayrı satılır; ek ücret alınmadan entegre edilir

90 Günlük Veri Saklama Süresi

Tüm Sophos ürünlerinden ve üçüncü taraf (Sophos dışı) ürünlerden gelen verileri Sophos Data Lake'de tutar

Üçüncü Taraf Uç Nokta Koruması

Şunlarla uyumludur:

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- Trellix
- BlackBerry (Cylance)
- Symantec (Broadcom)
- Malwarebytes

Eklenti Entegrasyonları

Aşağıdaki üçüncü taraf kaynaklardan gelen güvenlik verileri, Entegrasyon Paketleri satın alınarak Sophos MDR operasyon ekibi tarafından kullanılmak üzere entegre edilebilir. Telemetri kaynakları, ortamınızdaki görünürlüğü genişletmek, yeni tehdit algılamaları oluşturmak ve mevcut tehdit tespitlerinin doğruluğunu artırmak, tehdit avı yapmak ve ek müdahale becerileri sağlamak için kullanılır.

Sophos Ağ Tespiti ve Müdahale

Cihazlar arasında meydana gelen ve başka türlü görünmeyen şüpheli eylemleri tespit etmek için ağınızdaki etkinliği sürekli olarak izleyin

SPAN port yansıtma ile herhangi bir ağ ile uyumlu

Firewall

Şunlarla uyumludur:

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall

Identity

Şunlarla uyumludur:

- Okta
- Duo
- ManageEngine

Kamusal Bulut

Şunlarla uyumludur:

- AWS Security Hub
- AWS CloudTrail
- Orca Security
- Google Cloud Platform Security

Email

Şunlarla uyumludur:

- Proofpoint
- Mimecast

Network

Şunlarla uyumludur:

- Darktrace
- Tinkst Canary
- Skyhigh Security

1 Yıllık Veri Saklama Süresi

Sophos MDR Destekli Oryantasyon

Ek bir ücret karşılığında Sophos MDR Destekli Oryantasyon uzaktan kurulum desteği için kullanılabilir. Bu hizmet, sorunsuz ve verimli bir kurulum için uygulamalı destek sağlar, en iyi uygulama yapılandırmalarını sağlar ve MDR hizmet yatırımınızın değerini en üst düzeye çıkarmak için eğitim verir. Sophos Profesyonel Hizmetler organizasyonundan, uygulamanızın başarılı olduğundan emin olmak için ilk 90 gün boyunca size eşlik edecek özel bir irtibat kişisi sağlanır. Sophos MDR Destekli Oryantasyon şunları içerir:

1. Gün - Uygulama

- Proje başlangıcı
- Sophos Central'ı yapılandırma ve özellikleri gözden geçirme
- Kurulum sürecini oluşturma ve test etme
- MDR entegrasyonlarını yapılandırma
- Sophos NDR sensörünü/ sensörlerini yapılandırma
- Kurumsal çapta kurulum

30. Gün - XDR Eğitimi

- Bir SOC gibi düşünmeyi ve hareket etmeyi öğrenin
- Ele geçirme belirtilerini nasıl avlayacağınızı anlayın
- İdari görevler için XDR platformumuzu kullanma konusunda anlayış kazanın
- Gelecekteki araştırmalar için sorgular oluşturmayı öğrenin

90. Gün Güvenli Duruş Değerlendirmesi

- En iyi uygulama önerileri için mevcut politikaları gözden geçirin
- Ek koruma sağlayabilecek kullanımda olmayan özellikler hakkında bilgi alışverişinde bulunun
- NIST çerçevesini takip eden güvenlik değerlendirmesi
- İncelememizden elde edilen tavsiyeleri içeren özet raporu alın

Daha fazlasını öğrenmek için web sitemizi ziyaret edin:

sophos.com/mdr

İstanbul
Tel: +90 216 663 61 61
Palladium Ofis ve Residence Binası,
Barbaros Mahallesi Halk Caddesi No:8/A Kat:2-3,
Ataşehir, 34746 İstanbu

Orta Doğru ve Afrika
Tel: +971 (0)43754332
E-posta: salesmea@sophos.com

23-01-24 DS-TR (PC)

SOPHOS