Sophos XDR

Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X, güçlü genişletilmiş tespit ve müdahale (XDR) ile benzersiz uç nokta korumasını bir araya getirir. Aktif düşmanları tespit etmek için tehditleri avlayın veya IT güvenliğini korumak amacıyla IT işlemleri için yararlanın. Uzaktan bir sorun bulunduğunda, hassas bir şekilde müdahale edin. Uç nokta, sunucu, güvenlik duvarı ve e-posta dahil zengin veri kaynaklarıyla görünürlüğü uç noktanın ötesine taşıyın.

IT işlemleri ve tehdit avı sorularını yanıtlayın

İşletme için kritik öneme sahip sorulara hızlı bir şekilde yanıt alın. Hem IT yöneticileri hem de siber güvenlik profesyonelleri, günlük IT işlemlerini ve tehdit avlama görevlerini yerine getirirken gerçek katma değeri görecekler.

En iyi korumayla başlayın

Intercept X, ihlalleri başlamadan durdurur. Bu da daha iyi bir korumaya sahip olacağınız ve otomatik olarak durdurulmuş olması gereken olayları soruşturmak için daha az zaman harcayacağınız anlamına gelir. Aynı zamanda size hızlı ve bilinçli önlemler almanız için gereken bilgiyi sağlayan ayrıntılı tehdit istihbaratına erişebilirsiniz.

Ayrıntılara dalın ve hızlı müdahale edin

Daha fazla soruşturulması gereken bir şey belirlediğinizde Sophos Data Lake'ten destek alabilir ve 90 güne kadar geçmiş verilere ilaveten canlı olarak çokça ayrıntı almak için doğrudan cihaz üzerinden alabilirsiniz. Uzaktan bir sorun doğrulandığında cihaza erişebilir ve örneğin bir uygulamayı kaldırmak ve yeniden başlatmak gibi gerekli her türlü önlemi alabilirsiniz.

Ürünler arası görünürlük

Sophos XDR, uç noktanın ve sunucunun ötesine geçerek Sophos Firewall, Sophos Email ve diğer veri kaynaklarının* verileri Sophos Data Lake'e göndermelerine olanak sağlar ve kuruluşunuzun ortamı hakkında size inanılmaz geniş bir bakış açısı sunar.

Bir cihaz çevrim dışı olduğunda dahi bilgi alın

XDR işlevinin kilit bir bileşeni olan Sophos Data Lake, bir bulut veri deposudur. Uç noktalarınızdan, sunucularınızdan, güvenlik duvarınızdan ve e-postanızdan gelen kritik bilgileri depolama, bunlara erişme ve aynı zamanda bir cihaz çevrim dışı olsa bile bu cihazın bilgilerinden yararlanma olanağı sağlar.

Saniyeler içinde başlayın

Çok çeşitli IT ve güvenlik soruları sormak için önceden yazılmış SQL sorguları kütüphanesinden seçim yapabilirsiniz. İsterseniz bunları özelleştirebilir veya kendi sorgularınızı yazabilirsiniz. Sürekli sorguların paylaşıldığı Sophos topluluğuna da başvurabilirsiniz.

Öne Çıkan Noktalar

- İşletme açısından kritik IT işlemleri ve tehdit avı sorularını yanıtlayın
- IT yöneticileri ve güvenlik analizi uzmanları için tasarlandı
- Gereken cihazlarda uzaktan düzeltmeye yönelik önlemler alın
- Kuruluşunuzun IT ortamı hakkında bütünsel bir bakış açısı edinin ve gerektiğinde çok ince ayrıntılara kadar inceleyin
- Uç nokta, sunucu, güvenlik duvarı, e-posta ve diğer veri kaynaklarından* yararlanın
- Kullanıma hazır, tamamen özelleştirilebilen SQL sorguları
- Windows, macOS* ve Linux için kullanılabilir

**Cloud Optix ve Sophos Mobile çok yakında*

**XDR becerileri çok yakında macOS'te*

SOPHOS

Kullanım örnekleri

IT işlemleri

- Bir makine neden yavaş çalışıyor?
- Hangi cihazlarda bilinen güvenlik açıkları, bilinmeyen hizmetler veya yetkisiz tarayıcı eklentileri var?
- Çalışmakta olan, kaldırılması gereken programlar var mı?
- Yönetilmeyen, konuk ve IoT cihazlarını teşhis etme
- Ofis ağı bağlantısı neden yavaş? Buna hangi uygulama neden oluyor?
- 30 gün geriye doğru eksik veya imha edilmiş bir cihazdaki olağan dışı etkinliklere bakın

Tehdit avlama

- Hangi işlemler standart olmayan portlarda ağ bağlantısı kurmaya çalışıyor?
- Kısa süre önce dosyaları veya kayıt defteri anahtarları değiştirilmiş olan işlemleri görüntüleyin
- Tespit edilen ele geçirilme belirtilerini MITRE ATT&CK çerçevesinde gruplayarak listeleyin
- Bir cihazı tekrar çevrim içi yapmadan incelemeleri 30 güne uzatın
- Şüpheli ana bilgisayarları incelemek için güvenlik duvarının ATP ve IPS tespitlerini kullanın
- Kötü amaçlı bir alan adına giden trafiği belirlemek için e-posta başlık bilgilerini, SHA'ları ve diğer ele geçirilme belirtilerini karşılaştırın

Neleri kapsar?

	Genişletilmiş tespit ve müdahale (XDR)
Ürünler arası veri kaynakları	✓
Ürünler arası sorgulama	✓
Uç nokta ve sunucu sorgulama	✓
Sophos Data Lake	✓
Veri gölü tutma süresi	30 gün
Disk üzerinde veri tutma süresi	✓
SQL sorgu kütüphanesi	✓
Intercept X koruma becerileri	✓

Lisanslama konusunda daha fazla bilgi için lütfen Intercept X ve Intercept X for Server lisans kılavuzlarına bakınız.

Ücretsiz deneyin

30 günlük ücretsiz değerlendirme için sophos.com/intercept-x adresine kaydolun

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

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

21-07-08 DS-TR (PS)

SOPHOS