SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

Akıllı Endpoint Koruması ve Müdahale

Sophos Intercept X Advanced with EDR, sektörünün lider zararlı yazılım tespit, sistem açığına karşı koruma ve diğer rakipsiz endpoint koruma özellikleri ile birlikte akıllı endpoint tespiti ve müdahalesini entegre ederek sizi korur.

Öne Çıkan Özellikler

- En güçlü endpoint koruması ile güçlendirilmiş EDR
- Derin Öğrenimli Zararlı Yazılım Analizi (Deep Learning Malware Analysis
- Talep doğrultusunda Sophos Labs'den tehdit istihbaratı
- Makine öğrenimi şüpheli olayları tespit eder ve öncelikli hale getirir
- Rehberli denetimler EDR'ı kullanışlı ve güçlü kılar
- Tek tıklama ile vakaya müdahale eder

EDR En Güçlü Korumayla Başlar

Güvenlik tehditleri henüz açığa çıkmadan bitirmek için önlem almak hayati önem taşır. Intercept X rakipsiz koruma, endpoint tespiti ve müdahaleyi tek bir çözümde birleştirir. Bu, çoğu zararlı yazılımın daha zarar veremeden önlenmesi anlamına gelir ve Intercept X with EDR tespit, denetleme ve potansiyel güvenlik tehditlerine müdahale özellikleriyle ek siber güvenlik tedbiri olarak çalışır.

EDR'ın içeriğinde bulunan Intercept X, EDR'ın iş yükünü azaltmaktadır. Tehditler daha fazla önlendikçe, siber güvenlik ekiplerinin tespit etmesi gereken güvenlik vakalarının sayısı azalır. Bu aynı zamanda, BT işinde bulunanların yanlış pozitif ve gittikçe artan bildirim sayısıyla daha az uğraşacağı ve verilen eforun daha verimli şekilde kullanılabileceği anlamına gelmektedir.

Çalışan Sayısı Değil, Tücrübe Ekleyin

Intercept X Advanced with EDR, normalde uzman analistlerin yapması gereken görevleri birebir uygulayarak, işletmelerin ihtiyaç duyduğu uzman sayısını azaltır. Diğer EDR uygulamalarının yürüttüğü gerçek insan ile işlem yapma özelliklerine karşın, bu iş Intercept X Advanced with EDR makine öğrenimi ve Sophos Labs tehdit istihbaratı ile sağlanarak, otomasyon halinde yapılır.

Güvenlik Uzmanlığı: Intercept X Advanced with EDR, potansiyel tehditleri otomatik olarak tespit ederek ve önceliklendirilerek BT bölümünüzün hizmetine bir güvenlik uzmanlığı sunar. Makine öğrenimi ile şüpheli eylemler tanımlanır ve en kısa sürede müdahale edilmesi gereken işlem olarak belirlenir. Böylece analistler hangi cihazlar için müdahalede bulunulması gerektiğini kolayca tespit eder.

Zararlı Yazılım Uzmanlığı: Çoğu işletme, şüpheli dosyaların analizi için tersine mühendislere ihtiyaç duyar. Bu tip bir yaklaşım zaman tüketici bir metod olmasının yanında, her zaman başarıya ulaştıran bir yöntem de değildir, fakat yine de bir çok işletmenin sahip olmadığı siber güvenliğin karmaşıklığının seviyesini belirleme ihtiyacını karşılar. Intercept X Advanced with EDR, Deep Learning Malware Analysis özelliği ile zararlı yazılımları en derin detayına kadar analiz eder, dosya özelliklerini ortadan kaldırır ve milyonlarca zararlı yazılım dosyası ile karşılaştırır. Bu sayede analistler, hangi özellik ve kod segmentlerinin "bilinen iyi" ve "bilinen kötü" dosyalarla benzerlik taşıdığını ortaya çıkararak bir dosyanın engellenip, engellenmeyeceğine hızlıca karar verirler.

Tehdit İstihbaratı Uzmanlığı: Intercept X Advanced with EDR herhangi bir dosyayı ele aldığında BT yöneticileri, Sophos Labs tarafından sunulan tehdit istihbaratı sayesinde daha fazla bilgi edinir. Sophos Labs günde 400.000 adet daha önceden görülmemiş zararlı dosya için tanımlama yapar. Bu ve diğer tehdit istihbaratı ile birlikte toplanır, kümelenir ve kolay bir analiz için özetlenir. Böylece işletmelerin konuyla ilgili bir personeli olmasa dahi üst düzey siber güvenlik araştırmaları ve veri bilimi takımlarınca sağlanan desteğe sahip olur.

Rehberli Vaka Müdahalesi

Intercept X Advanced with EDR, bir saldırının nasıl başladığını, saldırı sonrasında nelerin etkilendiğini ve nasıl müdahale etmek gerektiğini bildiren bir görünürlük sunarak sistem yöneticilerine, zor sorulara kolayca cevap verebilmelerini sağlar. Rehberli denetim özelliğiyle birlikte herhangi bir uzmanlık seviyesindeki sistem yöneticisi sorunun ne olduğunu çabukça anlar ve çözüm olarak ne yapılması gerektiğini analiz eder. Bunun yanında saldırıya ait görselleştirme ile nerelere müdahale edilmesi gerektiğini kolayca kavrar.

Akıllı EDR Kullanılması Gereken Yerler

Akıllı endpoint tespiti ve müdahale, sistem yöneticilerinin görünürlüğe ve herhangi bir vakaya dair zor sorulara yönelik uzmanlığa sahip oldukları anlamına gelir.

Vakaya ilişkin zor sorulara cevap verirken aşağıdakilere de sahip olursunuz:

- Güvenlik vakalarının etkilerinin ve hedefinin ne olduğunu kavrama
- Farkedilmeyen saldırıların tespiti
- Tüm bilgisayar ağında soruna yol açan sebepleri arama
- Daha ileri düzey denetleme için eylemlere öncelik atama
- Dosyaları tehdit ya da potansiyel istenmeyen bir dosya olup olmadığını anlamak için analiz
- İstenilen ana ait güvenlik durumunun görüntüsü

EDR'dan Daha Öte

Geniş çaplı saldırıları durdurmak için Intercept X Advanced with EDR, bütünleşik derinlemesine savunma yaklaşımıyla endpoint korumasında kullanılan klasik yöntemlerin önüne geçer. Bunu ise klasik metodların yanında modern teknikleri kullanarak gerçekleştirir. Intercept X Advanced with EDR, kulvarındaki en iyi zararlı yazılım tespiti, en iyi sistem açığından faydalananları önleme özelliğini ve akıllı endpoint tespit ve müdahalesini bir arada sunar.

Bu modern teknikler içerisinde: derin öğrenimli zararlı yazılım tespiti, sistem açığı suistimalini önleme ve fidye yazılımlarına karşı koruma bulunur. Klasik yöntemler olarak ise: antivirüs, davranış analizi, zararlı veri trafiği tespiti ve veri kaybı önleme gibi özellikleri barındırır.

Intercept X Advanced with EDR, endpoint tespiti ve müdahale yetenekleriyle Intercept X içinde bulunan modern tekniklerle birlikte Sophos Central Endpoint Protection'a ait özellikleri birbirine entegre eder. Tüm bunların hepsi tek bir çözüm ve tek bir ajan ile sağlanır.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
Temel teknikler	✓	✓		✓
Derin öğrenim	✓	✓	✓	
Sistem açığı suistimali önleme	✓	✓	✓	
CryptoGuard fidye yazılım önleme	✓	✓	✓	
Endpoint tespiti ve müdahale (EDR)	✓			

SOPHOS