kaspersky GELECEĞİ YAKALAYIN

Kaspersky EDR Optimum

Kuruluşunuzun hedefli ve gelişmiş tehditlere kurban gitme riskini azaltmak, lüks olmaktan çıkıp bir gereklilik haline gelmiştir. Herkesi güvende tutarken, bu süreci basit ve uygun maliyetli hale getirmeye çalışıyoruz.

Kaspersky Endpoint Detection and Response (EDR) Optimum, gelişmiş ve hedefli saldırıları hem personelinizin hem de BT kaynaklarınızın işini kolaylaştıracak şekilde ele alan merkezi otomatik bir araçtır.

Öne Çıkan Özellikler

- Gelişmiş veya hedefli bir saldırıya kurban gitme riskinizi azaltır
- Uç noktalarınızı derinlemesine görebilmenizi sağlar
- Karmaşık tehditleri tespit eder
- BT güvenlik ekibinize kök neden analizi için gereken araçları ve bilgileri verir
- IoC'lerin yaratılmasını, içe aktarılmasını ve bunlar için sunucuların taranmasına imkan tanır
- Çeşitli otomatik ve 'tek tık' cevap seçenekleri sağlar
- Zahmetsizdir ve zaman kazandırır
- Son derece otomatiktir ancak insan girdisine ve uzmanlığına imkan tanır

Kuruluşların şu anda karşı karşıya olduğu sorunlar

Gelişmiş tehditler yaygınlaştı

Hedefli ve gelişmiş saldırılar gerçekleştirmek çok daha ucuz ve kolay bir hale geldi, bu da demek oluyor ki tehlikede olanlar artık sadece devletler ve dev firmalar değil. Bu saldırıların riski altında olduğunu düşününen kuruluşlar artık kendilerini korumalı ve uygun bir koruma aramaya koyulmalı - yalnızca bir yıl içinde kuruluşların **10'da 1'i**[1] hedefli saldırıya uğrarken **%91'i**[1] siber saldırılardan zarar gördü.

Bir saldırının ortalama maliyeti yıldan yıla artıyor

Hedefli ve gelişmiş saldırılar ciddi paralara mal oluyor. Şu anda, bir veri ihlalinin ortalama maliyeti yaklaşık **1,41 M$**'dir[2] ve bir kuruluşa uç nokta kötü amaçlı yazılım bulaşmasının maliyeti **2,73 M$**[2] civarındadır. Bu maliyetler araştırmayı, onarımı, tazminat ödemelerini ve bir saldırının sonuçlarını hafifletmeye yarayacak diğer şeyleri içermektedir.

Bu tehditleri önlemek için uygun araçlar ve uzmanlık kullanmak bunun bir parçasını oluşturur.

Kuruluşların sınırlı kaynağı vardır

İşe alabileceğiniz eğitimli güvenlik uzmanlarının sayısı ve onların bir işe adayabileceği zaman sınırsız değildir. Bu yeni bir sorun değildir ama tek başına ortadan kalkacak da değildir. Bu sorunu çözmek için en etkili yöntemlerden biri güvenlik görevlerini otomatikleştirmektir. Şu anda **3 kuruluştan 2'si**[3] bilgi güvenliği personeli eksikliği çekiyor ve 2021'e kadar **3,5 milyon**[4] siber güvenlik işinin boş kalacağı öngörülüyor.

Neyse ki, güvenlik çözümlerini yürütmek için gereken BT kaynakları var. Genellikle, kurumsal BT bütçeleri zaten gerekenden daha az. Bunun yanıtı hafif çözümlerde veya minimum BT masrafı gerektirenlerde aranmalıdır.

Nasıl yardım edebiliriz?

Kaspersky EDR Optimum, sınırlı kaynaklar karşısındaki karmaşık modern tehditlere karşı yüksek kaliteli güvenlik ihtiyacını karşılamak için geliştirilmiştir. Tehditleri tespit etmede güçlü, bunlara müdahale etmede proaktif ve günlük operasyonlar açısından pratik olacak şekilde tasarlanmıştır.

1 – Kaspersky Lab Global BT Riski Raporu, Kaspersky, 2019

2 – 2019'daki BT güvenlik ekonomileri, Kaspersky, 2019

3 – Siber güvenlik işgücü çalışması, (ISC)², 2019

4 – Resmi Yıllık Siber Güvenlik İşleri Raporu, Siber Güvenlik Girişimi, 2019

Güçlü

Kendinizi bir saldırıya karşı korumanın ilk adımı tehdidin farkında olmaktır, bu yüzden güçlü tespit ve araştırma, her EDR çözümünün temel taşıdır."

Kaspersky EDR Optimum, aşağıdakiler dahil ancak bunlarla sınırlı olmamak üzere, bir saldırının her türlü izini sürebilen çeşitli teknikler kullanır:

- Kötü amaçlı yazılım içermeyen saldırılar
- Yanal hareket
- Şüpheli eylem
- ve diğerleri

Proaktif

Bir tehdidi tespit etmek yeterli değildir - hem virüs bulaşmış sunucuda hem de ağdaki diğer sunucularda bununla zamanında başa çıkabilmeniz gereklidir. Kaspersky EDR Optimum ortaya çıkan tehditlere karşılık verebileceğiniz çeşitli yollar sunar:

- Sunucuyu izole edin
- Ana sunucunun taramasını başlatın
- (Karantinaya alınmış) dosyayı kaldırın
- İşlemi kesin
- İşlemin yürütülmesini önleyin

Pratik

Güvenlik ekibinizin tehditleri analiz etmek ve bunlara yanıt vermek için ne kadar zaman ve efor harcadığı, tespit oranları ve yanıt teknikleri kadar önemlidir. Kaspersky EDR Optimum ile özel bir uzmanlığa, büyük bir ekibe veya koruma altında olmak için koca bir güne ihtiyacınız kalmaz. Detaylı veri sağlar, son derece otomatiktir ve BT kaynaklarınıza kolaylık sağlar. Bütün bunlar size aşağıdakileri güçlü bir şekilde verir:

Görünürlük

- Olaylara dair tam bilgi
- Öldürme zincirinin görselleştirilmesi
- Olay geçmişi ve kök neden analizi

Otomatikleştirme

- Tek-tık yanıt seçenekleri
- Bir olaydan IoC'lerin otomatik olarak yaratılması (veya içe aktarılması)
- IoC'ler için sunucu arama ve tehditlere otomatik olarak yanıt verme

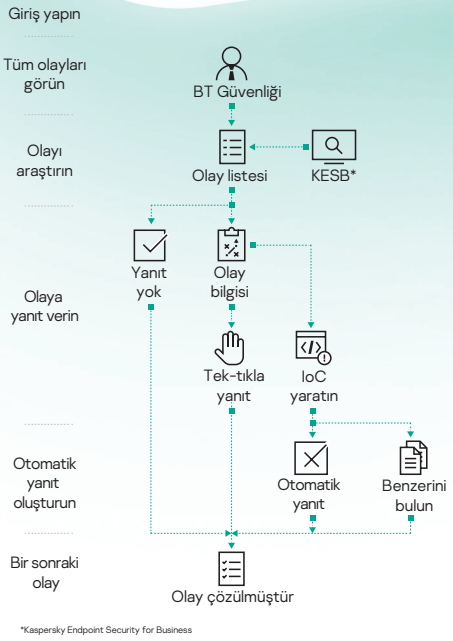
Performans

- Ek maliyet yok
- Kaspersky Endpoint Security ile entegre edilmiştir
- Kaspersky Security Center konsolu tarafından kontrol edilir

Kullanım senaryoları

Kaspersky EDR Optimum'un çeşitli tehditleri tespit etmek araştırmak ve bunlara karşılık vermek için kullanılabileceği birkaç basit örnek:

Tespit etme	Araştırma	Yanıt Verme
Kötü amaçlı dosya tespit edilmiş ve olay listesinde gösterilmiştir	Öldürme zinciri görselleştirmesi bu dosyanın işaretsiz bir işlem tarafından bırakıldığını göstermektedir	İşlemin yürütülmesini tek bir tıkla engelleyin ve bırakılan dosyayı karantinaya alın
İşlem enjeksiyonu tespit edilmiştir	Olaya dair tüm bilgiler sunucu bilgilerini, dosya oluşturma ve değiştirme tarihini, yazarı ve imzayı vb. gösterir. Bu bilgiye ve öldürme zincirine dayanarak, dosya şüpheli olarak kabul edilir	Sunucuyu izole edin ve ağdaki diğer sunucularda benzer olayları araştırın
Şüpheli bağlantı tespit edilmiştir	Olay verileri, bağlantının kurulduğu adresi gösterir. Öldürme zinciri görselleştirmesi bu bağlantıyı, her ikisi de aynı işlemle başlatılan bir kayıt defteri anahtarı değişikliğiyle ilişkilendirir	Sunucuyu izole edin. Periyodik arama için diğer sunucular üzerinde periyodik arama oluşturun ve otomatik bir yanıt oluşturun



*Kaspersky Endpoint Security for Business

Nasıl çalışır?

Kaspersky EDR Optimum, aynı aracı kullanırken gelişmiş görünürlük, kök neden analiz kapasitesi ve mevcut güçlü EPP'ye (Kaspersky Endpoint Security for Business) otomatik yanıt ekler.

Veriler bu sunuculardan toplanır ve analiz edilir ve olaylara ilişkin raporlama, detaylı olay bilgisi ve yanıt seçenekleri Kaspesky Security Center konsolu aracılığıyla sağlanır.

Olaylara yanıtlar otomatik veya 'tek tık' olabilir. Otomatik yanıtlar, çeşitli sunuculardaki benzer olaylara insan müdahalesi olmadan yanıt verebilmek için oluşturulur ve bu sunucularda kendiliğinden oluşturulmuş veya içe aktarılmış IoC'ler tespit edildikten sonra harekete geçirilir.

Kaspersky EDR Optimum'u mümkün olduğunca basit bir şekilde kullanılacak hale getirdik. Kurulumdan sonra, BT güvenlik personelinizin ortaya çıkan olayları işlemek, kök neden analizi yapmak ve olaylara yanıt vermek için konsolu yalnızca arada bir kontrol etmesi gerekir.

Bu yüksek düzeyde otomasyon ve görünürlük, güvenlik görevlisinin her gün büyük miktarlarda veri kontrol etmesine duyulan gereksinimi ortadan kaldırır. Bunun yerine, onlara ihtiyaçları olan tüm bilgiyi vererek dikkatlerini şüpheli eylemlere vermelerine yardımcı olur.

Kaspersky EDR Optimum'un güvenlik ekibinize ve kaynaklarınıza kolaylık sağlarken siber tehditleri nasıl ele aldığını öğrenmek için http://www.kaspersky.com/enterprise-security/edr-security-software-solution adresini ziyaret edin.

Siber Tehdit Haberleri: www.securelist.com
BT Güvenlik Haberleri: business.kaspersky.com
KOBİ'ler için BT Güvenliği: kaspersky.com.tr/business
Kurumsal BT Güvenliği: kaspersky.com.tr/enterprise

www.kaspersky.com.tr

Başarımız kanıtlanmıştır. Bağımsızız. Şeffafız. Kendimizi teknolojinin hayatlarımızı geliştirdiği daha güvenli bir dünya inşa etmeye adadık. Bu yüzden teknolojiyi güvenli hale getiriyoruz ve böylelikle sunduğu sayısız fırsatlardan herkesin her yerde faydalanmasına katkıda bulunuyoruz. Daha güvenli yarınlar için siber güvenliği yakalayın.

Daha fazla bilgi için kaspersky.com.tr/transparency

Proven. Transparent. Independent.