Kuruluşunuzu hedef alan tehditleri sürekli izler, algılar ve bunlara karşılık verir

Kaspersky Managed Detection and Response

kaspersky geleceği yakalayın

Şirketlerin karşılaştığı zorluklar

%55

Cihazlarına zararlı yazılım bulaştığını bildiren şirketlerin oranı*

%20

APT tehditleriyle karşı karşıya olan şirketlerin oranı**

%18

şirketlerinde meydana gelen olayların nedeninin nitelikli siber güvenlik personeli eksikliğinden kaynaklandığını bildiren katılımcıların oranı***

2.5 milyar dolar

Başarılı bir siber saldırıdan sonra yaşanan büyük kayıplar****

Yirmi dört saat yönetimli koruma ile siber güvenlik direncinizi artırın

Uzaktan çalışma, bilgi aktarım yöntemlerinin hızla gelişmesi, genişleyen küresel beceri açığı ve geleneksel otomatik önleme ve tespit kontrollerini atlatabilen siber tehditlerin sayısının artması, her büyüklükteki kuruluşu amansız bir baskı altına sokmaktadır. Hızlı ve etkili bir şekilde yanıt verebilmeleri çok önemlidir.

Kaspersky Managed Detection and Response (MDR) geleneksel otomatik güvenlik önlemlerinin gözden kaçırdığı siber tehditlere ve sofistike saldırılara karşı 24 saat yönetimli koruma sunan bir hizmettir.

Çözüm, hızlı kurulum için anahtar teslim bir hizmet sağlayarak siber güvenlik uzmanı eksikliği olan küçük ve orta ölçekli kuruluşlar için BT güvenliği düzeyini artırır. Gelişmiş siber güvenlik uzmanlığına sahip deneyimli ekipler için ek esneklik sunarak olay tespit ve sınıflandırma görevlerini Kaspersky uzmanlarına devretmelerine veya kendi tespit ettikleri olaylar hakkında ek profesyonel görüş almalarına olanak tanır.

Kaspersky MDR, kurumların siber tehditlere karşı dayanıklılığını artırır ve güçlendirir, mevcut kaynakları optimize eder ve mevcut kaynakların verimli bir şekilde kullanılmasına yardımcı olur ve BT güvenliğine yönelik gelecekteki yatırımları optimize eder.

Temel özellikler

- 7/24 sürekli izleme ve tehdit tespiti
- Mevcut durumlarıyla birlikte tüm korunan kaynaklara genel bakış
- Otomatikleştirilmiş ve yönlendirilmiş yanıt
- Kaspersky'nin SOC analistlerine doğrudan erişim
- IRP / SOAR ile entegrasyon için REST API
- Panolar ve raporları içeren Web konsolu
- Ham telemetrinin 3 ay boyunca saklanması
- Özel olayları gönderin
- Güvenlik olayları geçmişinin 1 yıl süreyle saklanması

* IT Security Economics, 2022
** Kaspersky MDR analyst report, 2023
*** Kaspersky Human Factor 360 Report, 2023
**** Global financial stability report. The Last Mile: Financial Vulnerabilities and Risks, 2024

Kaspersky MDR için telemetri ve uyarı kaynakları

- **Kaspersky Endpoint Security for Windows**
- **Kaspersky Endpoint Security for macOS**
- **Kaspersky Endpoint Security for Linux**
- **Kaspersky Virtualization Light Agent**
- **Kaspersky Anti-Targeted Attack**

Nasıl çalışır?

1

Kaspersky SOC analistleri, güvenlik uyarılarını araştırıp müşterinin ağında kurulu Kaspersky ürünlerinden alınan telemetri olaylarını proaktif olarak analiz eder. Bu telemetri, saldırganlar tarafından kullanılan bilinen, yeni ve gelişmekte olan taktikleri, teknikleri ve prosedürleri belirlemek için Kaspersky'nin dünyanın en azılı siber saldırılarından ve hedefli operasyonlarından bazılarını araştıran 25 yılı aşkın deneyimine dayanan siber tehdit istihbaratı ile karşılaştırılır. Benzersiz IoA'lar, meşru faaliyetleri taklit eden gizli kötü amaçlı yazılım içermeyen tehditlerin tespit edilmesini sağlar.

2

Kaspersky MDR'deki olay işleme sürecinin bir parçası olarak yapay zeka (AI) mekanizmaları, hatalı uyarıların sayısını azaltmaya ve SOC ekibi tarafından olay incelemesini hızlandırmaya yardımcı olur.

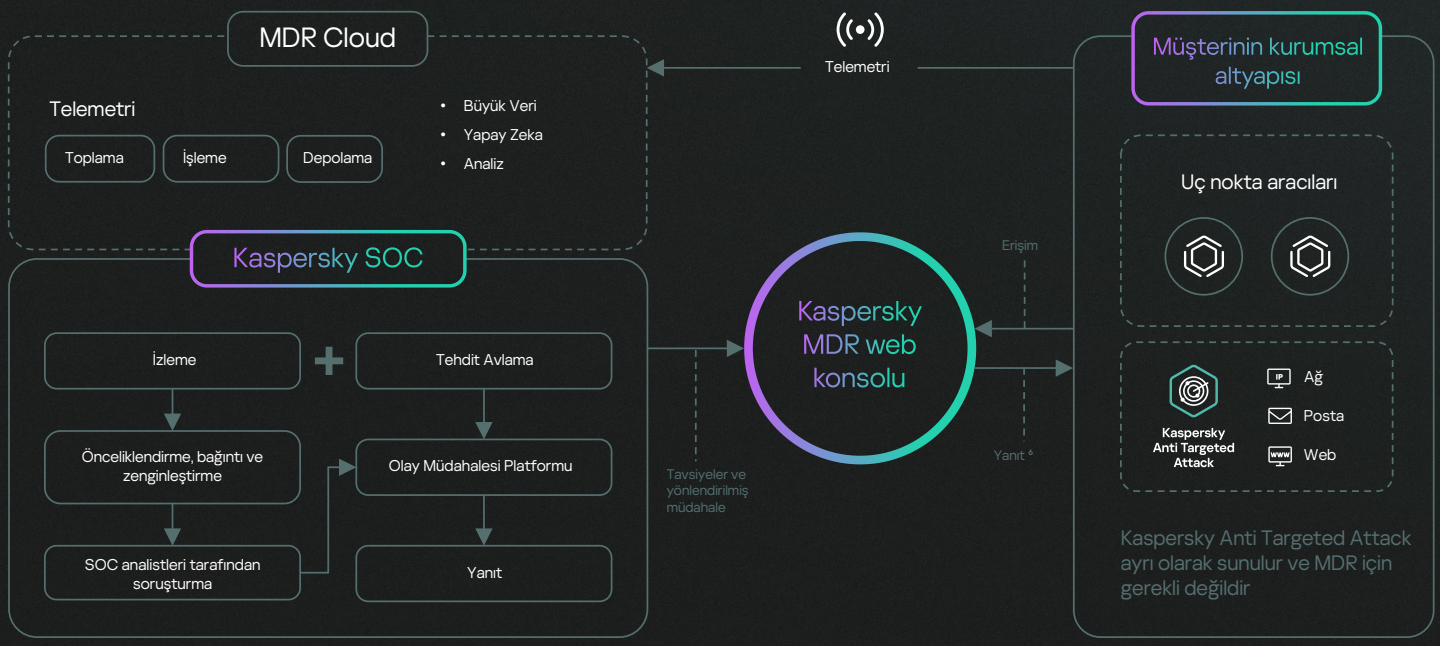
3

Potansiyel bir tehdit algılandığında, Kaspersky MDR bunu önem düzeyine göre sınıflandırır ve müşteriyi e-posta ve/veya Telegram aracılığıyla bilgilendirir. Mümkün olduğunda, kök neden analizi saldırının kaynağının belirlenmesine yardımcı olur ve tespit edilen tehditlerin nasıl kontrol altına alınacağı, bunlara nasıl yanıt verileceği ve azaltılacağı konusunda tavsiyelerde bulunur.

4

Müşteriler, yanıt* yetkilerini kısmen veya tamamen Kaspersky SOC ekibine devretmeyi tercih edebilir. Olayla ilgili tüm sorular Kaspersky MDR web konsolundaki bir sohbet üzerinden görüşülebilir.

Kaspersky MDR mimarisi



Kaspersky MDR, diğer birçok antivirüs çözümü ile uyumludur. Müşteri Kaspersky MDR portalında onayladığında otomatik yanıt başlatılır (Müşteri bunu yapmazsa, MDR portalı otomatik yanıt devreye girmeden önce onay ister).

* Olayın daha derinlemesine analiz edilmesi gerekiyorsa ve Kaspersky Incident Response için aktif bir aboneliğiniz varsa, olay incelenmek üzere Kaspersky GERT ekibine gönderilebilir.

Değer önerileri

En karmaşık, sofistike tehditlere karşı bile sürekli korumaya sahip olmanın verdiği gönül rahatlığı

Bir SOC kurma zahmetine ve masrafına katlanmak zorunda kalmadan kendi SOC'unuza sahip olmanın önemli faydaları

Genel olarak güvenlik maliyetlerinde azalma; her noktayı kapsamak için birden fazla, pahalı BT güvenlik uzmanını işe almaya ve eğitmeye gerek yok

Kurum içi BT güvenlik kaynaklarınızı iş açısından kritik diğer sorunlarla ilgilenmeye yönlendirin

Küresel tanınırlık ve eşsiz bir başarı geçmişi

Kaspersky çok çeşitli bağımsız testlere katılır ve önde gelen global analist firmalarıyla yakın işbirliği içinde çalışır. Kaspersky, dünya çapında bir siber güvenlik lideri olarak tanınmaktadır ve tüm ürünlerimiz gibi Kaspersky MDR de çok sayıda ödül almıştır. Kaspersky MDR'deki güçlü tespit ve müdahale özellikleri, sektördeki en başarılı ve deneyimli tehdit tespit ekiplerinden biri olan yüksek nitelikli ve deneyimli Kaspersky SOC ekibinin dünya çapında tanınan uzmanlığı ile tamamlanmaktadır.

Software Reviews CHAMPION 2024

Quadrant Knowledge Solutions

MITRE | ATT&CK®

GIAC CERTIFIED GCFA FORENSIC ANALYST

GIAC CERTIFIED GCIH INCIDENT HANDLER

GIAC CYBER THREAT GCTI INTELLIGENCE

GIAC NETWORK GNFA FORENSIC ANALYST

GIAC PENETRATION GPEN TESTER

GIAC EXPLOIT RESEARCHER & ADVANCED PENETRATION TESTER GXPN

GIAC REVERSE ENGINEERING GREM MALWARE

CISA

CISM

EC-Council CERTIFIED CEH

EC-Council CERTIFIED CHFI

OFFENSIVE SECURITY OSCP

OFFENSIVE SECURITY OSCE

CISSP®

Kaspersky Managed Detection and Response

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın