kaspersky

EDR vs MDR vs XDR

EDR
Uç Nokta Algılama ve Yanıt

Uç nokta korumasını atlayan yeni, bilinmeyen ve sinsi tehditleri tespit eder ve rutin güvenlik görevlerini otomatikleştirir

MDR
Managed Detection and Response

Kötü amaçlı yazılım olmayan yenilikçi ve karmaşık tehditlere karşı bile sürekli yönetilen koruma sağlar

XDR
Genişletilmiş Algılama ve Müdahale

Birden fazla altyapı seviyelerinde karmaşık tehditleri proaktif olarak tespit eder ve bu tehditlere otomatik olarak müdahale edip karşılık verir

Nasıl çalışır?

EDR

- Önleme mekanizmalarını atlatan tehditler için gelişmiş algılama ve avlamayı etkinleştirir
- Tehdit görünürlüğü ve görselleştirmesini iyileştirir
- Temel neden analizini basitleştirir
- Merkezî ve otomatikleştirilmiş müdahale sağlar

MDR

- Güvenlik ürünlerinden telemetriler toplar, aktif veya yaklaşan saldırı işaretlerini bulmak için sistem etkinliği meta verilerini proaktif biçimde analiz eder ve yönetilen veya yönlendirmeli müdahale sağlar

XDR

- Birden fazla aracı ve güvenlik uygulamasını entegre eder
- Karmaşık tehditleri algılayıp ortadan kaldırmak için uç noktalar, ağlar, bulutlar, web sunucuları, posta sunucular vb. üzerindeki verileri izler
- Çapraz ürün etkileşimini otomatikleştirerek bilgi güvenliği yönetimini kolaylaştırır

Kimler kullanmalı?

EDR

- Manuel yönetilen görevleri azaltmak için ayrıntılı uç nokta görünürlüğü ve merkezî müdahale gerektiren kurum içi BT güvenlik ekibine sahip işletmeler

MDR

- Temel algılama ve müdahale görevlerini devrederek kurum içi BT güvenliği kapasitesini artırmak isteyen şirketler
- Kendi şirket içi SOC'lerini oluşturmak için yeterli bütçeye veya personele sahip olmayan kuruluşlar

XDR

Tek bir platformun aşağıdakileri sağlamasını isteyen güvenlik açısından olgun kuruluşlar:

- Altyapılarında neler olup bittiğine dair kapsamlı bir görünüm
- Yerleşik tehdit avlama ve tehdit istihbaratı
- Üstün olay önceliklendirmesi ve daha az hatalı pozitif uyarısı

İş değeri

EDR

- Güvenlik personeline, uyarı beklemek yerine tehditleri etkin bir şekilde avlamak için ihtiyaç duydukları birleşik görünürlüğü ve kontrolü sunar
- Çeşitli analiz, soruşturma ve müdahale sürecini otomatik hâle getirerek mevcut BT güvenliği ekiplerinin kapasitelerini en üst düzeye çıkarır
- BT güvenliği ekiplerinin birden çok araç ve konsolla uğraşmak zorunda olmadan daha verimli şekilde çalışmalarına imkân tanıyarak maliyet verimliliği sağlar

MDR

- Karmaşık tehditlere karşı anında koruma sağlayarak siber güvenlik yetenek krizini çözer
- Sağlanan kritik sonuçlarla ilgili olarak kısıtlı ve maliyetli kurum içi kaynaklara daha iyi odaklanmak için olay yönetimi süreçlerinin dış kaynak kullanımına olanak tanır
- Karmaşık güvenlik çözümleri dağıtmaya ve kurum içinde çeşitli güvenlik uzmanları çalıştırmaya gerek olmadan genel güvenlik maliyetlerini azaltır

XDR

- Gelişen tehdit alanına karşı bütünsel bir koruma sağlar
- Ekosistem yaklaşımı, kullanılan siber güvenlik araçlarının verimliliğini en üst düzeye çıkarır, kaynaklardan tasarruf sağlar ve riski azaltır
- BT güvenlik uzmanlarının işini kolaylaştırır ve çok faktörlü saldırıları araştırmaları için gereken ek bağlamı sağlar
- Karmaşık tehditler ve hedefe yönelik saldırılarla mücadelede önemli rol oynayan MTTD ve MTTR'yi en aza indirir
- Tüm güvenlik teknolojisi yığınında merkezî ve otomatikleştirilmiş müdahale sunar

XDR becerilerinden faydalanmaya çalışan, güvenlik açısından köklü bir kuruluşa sahipseniz bir göz atın

Kaspersky Expert Security

Daha Fazla Bilgi Edinin