aa teknoloji

Falcon Insight EDR

Siber güvenlik ekipleri için tasarlanan Falcon Insight; gerçek zamanlı uç nokta izleme, otomatik tehdit algılama ve akıllı yanıt mekanizmalarıyla siber tehditleri görünür kılan gelişmiş bir EDR platformudur.

Uç Nokta Güvenliği Zorlukları

Büyüyen dijital altyapılar ve artan cihaz sayıları, kurumsal ağların karmaşıklığını zirveye taşıyor. Geleneksel güvenlik araçlarının yetersiz kalması, kör noktalar oluşturarak gelişmiş tehditlerin sızmasına ve operasyonel süreçlerin yavaşlamasına yol açıyor.
Dağınık uç noktalardaki aktivitelerin tek bir merkezden izlenememesi ağ görünürlüğünü kısıtlıyor. Tehditlerin gerçek zamanlı tespit edilememesi ve manuel analiz süreçleri, olay müdahale hızını düşürüp zafiyet yaratıyor.
Yoğun alarm yorgunluğu ve bağlamdan yoksun veriler, siber güvenlik ekiplerinin kritik tehditleri gözden kaçırmasına neden olan bir darboğazdır.

⚠ Hangi Ekiplere Hitap Eder?

- Geleneksel araçlarla uç noktalarda kör nokta yaşayan ekipler için
- Aşırı alarm yoğunluğu nedeniyle siber yorgunluk çeken analistler için
- Tehdit analiz ve olay müdahale sürecinde vakit kaybeden ekipler için
- Karmaşık kurulum ve manuel güvenlik süreçleriyle boğuşan yapılar için

Temel İlkeler

Görünürlük
Kör noktasız tam uç nokta izleme.

Hız
Gerçek zamanlı tehdit tespiti.

Koruma
Gelişmiş siber tehditleri durdurma.

Otomasyon
Yapay zekâ ile akıllı olay analizi.

Teknik Özellikler

Tehdit Algılama & Analiz
- Davranışsal analiz ile IOA (Saldırı Göstergeleri) tespiti
- MITRE ATT&CK çerçevesi ile tam uyumlu eşleştirme
- Çekirdek (kernel) sürücüsüyle derinlemesine veri toplama
- Forensic modülü ile 400'den fazla ham log türünü yakalama

Olay Müdahale & Yanıt
- Real Time Response (RTR) ile anında canlı aksiyon
- Falcon Fusion ile otomatik SOAR iş akışları oluşturma
- Tespit edilen tehditlerin ağda yayılmasını engelleme
- İzole edilen cihazlar üzerinde uzaktan güvenli analiz

İstihbarat & Tehdit Avı
- Entegre global istihbarat verileriyle saldırgan tespiti
- Tehditleri proaktif olarak arama ve tehdit avcılığı yetenekleri
- Tehdit aktörlerinin bağlamsal analizi
- Saldırıların kök nedenlerini ilişkilendirme

Kimlik & Durum Doğrulama
- Zero Trust Assessment ile uç nokta cihaz sağlığı kontrolü
- Güvenlik politikaları uyumluluk ve sıkılaştırma kontrolü
- Risk skoruna göre dinamik koşullu erişim desteği
- CrowdScore ile kurumsal düzeyde öncelikli tehdit skorlaması

Bulut & Altyapı Yönetimi
- Tek ve hafif ajanla hızlı canlı kurulum
- Sunucusuz bulut mimarisi ile sıfır yük
- 90 güne kadar geriye dönük log arşivi
- Sıfır performans kaybı ile sürekli izleme

Falcon Insight EDR Nasıl Çalışır?

Falcon Insight, hafif ajanıyla uç noktalardan topladığı verileri bulut mimarisinde işler. Gelişmiş yapay zekâ ve tehdit istihbaratıyla siber saldırıları anında tespit eden 3 adımlık akışla altyapınızı kesintisiz korur.

Çalışma Akışı

1. Sürekli İzleme
- Hafif ajanla uç noktaları anlık izler.
- Çekirdek sürücüsüyle ham olayları toplar.
- Etkinlik verilerini bulut hattına iletir.
- Sıfır performans kaybı ile sürekli çalışır.

→

2. Tehdit Algılama
- Yapay zekâ ve Threat Graph ile analiz eder.
- Davranışsal IOA göstergelerini tespit eder.
- Saldırıları MITRE matrisi ile eşleştirir.
- CrowdScore ile tehditleri önceliklendirir.

→

3. Anında Müdahale
- Siber saldırıları gerçek zamanlı durdurur.
- Tehdit içeren cihazı ağdan izole eder.
- RTR özelliğiyle uzaktan müdahale sağlar.
- Falcon Fusion ile SOAR akışlarını tetikler.

↗ **Entegrasyon ve Yüksek Güvenlik Standartları**
SIEM ve log altyapılarına tam uyum sağlayan esnek entegrasyon modeli sunar. Sıkılaştırılmış veri yalıtımı ve en yüksek güvenlik standartlarıyla kritik kurumsal ağlarınızı koruma altına alır.

Avantajlar

Gelişmiş Tehdit Algılama
Geleneksel imzaların ötesine geçerek karmaşık saldırgan aktivitelerini davranışsal analiz yöntemleriyle gerçek zamanlı olarak yakalar.

Real-Time Olay Müdahalesi
Tehdit içeren uç noktalara uzaktan doğrudan erişim sağlayarak zararlı aktiviteleri anında izole eder ve sistemlerden hızla temizler.

Kök Neden ve Görsel Analiz
Saldırı zincirini tek ekranda görselleştirerek MITRE ATT&CK çerçevesiyle eşleştirir ve kök neden analizini büyük ölçüde hızlandırır.

CrowdScore Akıllı Analiz
Dağınık alarmları tek bir kurumsal tehdit skoru altında birleştirerek ekiplerin alarm yorgunluğunu azaltır ve kritik vakalara odaklar.

aa teknoloji

AA Teknoloji, modern haber merkezleri için geliştirilen yapay zekâ destekli medya teknolojileri platformudur. Haber akış sistemlerinden dijital arşiv çözümlerine, gerçek zamanlı yayın altyapılarından çok kanallı içerik yönetimine kadar uzanan entegre çözümlerimiz; medya kuruluşlarının dijital dönüşüm süreçlerini hızlandırır ve ölçeklenebilir yayın operasyonları sunar.

Daha fazla bilgi için, aateknoloji.tr'yi ziyaret edin veya @aateknoloji LinkedIn hesabını takip edin.