aa teknoloji

Sangfor Athena EPP

Uç nokta güvenliğini ve tehdit yönetimini merkezi olarak yöneten; yapay zekâ destekli analiz, gelişmiş fidye yazılımı koruması ve anlık müdahale özellikleriyle uç noktaları koruyan nesil koruma platformudur.

Modern Uç Nokta Güvenliği Zorlukları

Kurumlar; genişleyen uzaktan çalışma modelleri, artan cihaz çeşitliliği ve gelişmiş siber tehditler nedeniyle uç noktalar üzerinde tam görünürlük sağlamakta zorlanmaktadır. İzole çalışan geleneksel antivirüs yazılımları, modern ve karmaşık saldırıları tespit etmekte yetersiz kalmaktadır.
Özellikle fidye yazılımları (ransomware) ve sıfırıncı gün (zero-day) saldırıları, uç noktalara sızdıktan sonra hızla yayılarak kritik kurumsal verilerin şifrelenmesine ve iş sürekliliğinin durmasına neden olur. Güvenlik ekiplerinin ağ genelindeki dağınık alarmları manuel analiz etmesi, müdahale süreçlerini geciktirir.
Ağ güvenliği ve uç nokta sistemleri arasındaki entegrasyon eksikliği, bir tehdidin kaynağını bulmayı ve yanal hareketi (lateral movement) engellemeyi zorlaştırarak siber güvenlik operasyonlarında operasyonel verimliliği düşürür.

⚠ Hangi Sorunları Çözer?

- Gelişmiş siber saldırıların ve fidye yazılımlarının anında tespit edilememesi ve engellenememesi.
- Dağınık uç noktalarda merkezi kontrol, izlenebilirlik ve görünürlük kaybı yaşanması.
- Manuel tehdit avcılığı ve alarm analizi süreçlerinde yaşanan yüksek zaman ve verimlilik kaybı.
- Ağ ve uç nokta güvenlik ürünlerinin kopuk çalışması ve merkezi bir entegrasyon altyapısının eksikliği.

Temel İlkeler

Proaktif Koruma
Yapay zekâ ile tehditleri sisteme zarar vermeden engeller.

Otomasyon
Tekrarlayan analiz ve izolasyon süreçlerini otomatikleştirir.

Bütünleşik Güvenlik
Ağ ve uç nokta çözümlerini tek mimaride birleştirir.

Görünürlük
Tüm uç noktaları tek bir merkezi panelden izlenebilir kılar.

Sangfor Athena EPP Nasıl Çalışır?

Sangfor Athena EPP, kurumsal ağdaki tüm uç noktalardan ajanlar vasıtasıyla gerçek zamanlı veri toplayarak çalışır. Toplanan metrikler Engine Zero AI motoru ve davranışsal analiz kuralları ile incelenir; bir tehdit algılandığında sistem otomatik olarak ilgili uç noktayı izole eder ve zararlı süreci sonlandırır.

Teknik Özellikler

Tehdit Algılama ve Yapay Zekâ
- Engine Zero AI tabanlı zararlı yazılım analizi
- Davranışsal analiz ve anomali tespiti
- Dosya bütünlüğü izleme ve denetimi
- Bellek içi (in-memory) saldırı koruması

Gelişmiş Fidye Yazılımı Koruması
- Yapay zekâ destekli fidye yazılımı engelleme
- Akıllı bal küpü (honeypot) teknolojisi
- Otomatik dosya yedekleme ve geri yükleme
- Şifreleme girişimlerini anlık durdurma

Anlık Müdahale ve İzolasyon
- Tek tıkla ana bilgisayar ve uç nokta izolasyonu
- Zararlı süreçlerin otomatik sonlandırılması
- Ağ düzeyinde mikro-segmentasyon desteği
- Ağ karantinası ve uzaktan müdahale akışları

Merkezi Yönetim ve Entegrasyon
- Tek panelden tüm uç noktaların takibi
- Sangfor NGAF ve Cyber Command ile XDDR entegrasyonu
- Kapsamlı varlık envanteri ve risk skorlama
- Syslog üzerinden merkezi SOC loglama desteği

Danışmanlık ve Yönetilen Hizmetler
- Kurum ölçeğine uygun ajan mimarisi tasarımı ve lisanslama danışmanlığı
- Ajanların merkezi dağıtımı ve mevcut SIEM/SOAR sistemlerine entegrasyonu
- Gelişmiş alarm analizi ve optimizasyonu desteği
- İç BT ve siber güvenlik ekipleri için platform yönetim ve simülasyon eğitimleri

Çalışma Akışı

1. Veri Toplama ve Tarama
- Uç noktalardan canlı etkinlik logları toplanır.
- Sürekli zafiyet ve risk taraması gerçekleştirilir.
- Sistem varlık envanteri otomatik güncellenir.
- Ajanlar üzerinden sürekli izleme sağlanır.

→

2. AI Analiz ve Algılama
- Engine Zero ile zararlı yazılımlar analiz edilir.
- Şüpheli davranışlar ve anomaliler aranır.
- Fidye yazılımı şifreleme adımları tespit edilir.
- Risk skorları merkezi panelde önceliklendirilir.

→

3. Müdahale ve Raporlama
- Tehdit içeren uç nokta ağdan izole edilir.
- Zararlı dosyalar silinir ve süreçler durdurulur.
- Saldırı zinciri görsel olarak raporlanır.
- Güvenlik bulguları merkezi SOC mimarisine iletilir.

Sürekli İyileştirme
Sangfor Athena EPP, sürekli güncellenen küresel tehdit istihbaratı akışları ve yapay zekâ kural setleri sayesinde yeni nesil saldırı yöntemlerine karşı koruma yeteneklerini düzenli olarak optimize eder.

Avantajlar

Engine Zero AI Motoru
Geleneksel imza tabanlı çözümlerin kaçırdığı bilinmeyen zararlı yazılımları ve sıfırıncı gün saldırılarını yapay zekâ mimarisiyle yüksek doğrulukla tespit eder.

Etkin Tehdit Avcılığı
Gelişmiş görselleştirilmiş saldırı zinciri (kill chain) analizi sayesinde güvenlik uzmanlarının tehditlerin kök nedenini hızla bulmasını kolaylaştırır ve müdahale süresini kısaltır.

Anti-Ransomware Honeypot
Uç noktalara yerleştirilen akıllı honeypot dosyaları sayesinde, fidye yazılımlarının şifreleme faaliyetlerini gerçek dosyalara zarar vermeden önce yakalar ve engeller.

XDDR Bütünleşik Savunma
Sangfor ağ güvenliği ürünleriyle tam entegre çalışarak, uç nokta de başlayan bir tehdidin ağ seviyesinde otomatik olarak engellenmesini ve bütünleşik bir savunma hattı kurulmasını sağlar.

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.