aa teknoloji

Imperum

Siber güvenlik, sistem ve network operasyonlarını merkezi olarak yöneten; olayları analiz eden ve otomatik aksiyonlara dönüştüren SOAR platformu.

Modern Güvenlik Operasyonlarının Zorlukları

Kurumlarda SIEM, EDR, firewall ve diğer güvenlik sistemleri genellikle birbirinden bağımsız çalışır. Bu da olay müdahale süreçlerinde gecikmelere, manuel işlem yüküne ve operasyonel verimsizliğe yol açar.
Güvenlik ekipleri farklı sistemlerden gelen alarmları manuel olarak analiz etmek, ilişkilendirmek ve aksiyon almak zorunda kalır. Bu süreç hem hata riskini artırır hem de kritik tehditlere geç müdahale edilmesine neden olur.
Artan saldırı yüzeyi, yüksek alarm hacmi ve 7/24 izleme ihtiyacı, geleneksel yöntemlerle sürdürülemez hale gelmiştir.

⚠ Hangi Ekiplere Yardımcı olur?

- Güvenlik sistemleri arasında entegrasyon eksikliği yaşayan kurumlar için
- Yüksek alarm hacmini manuel analiz eden SOC ekipleri için
- Olay müdahale süresini kısaltmak isteyen organizasyonlar için
- Standart ve otomatik güvenlik süreçleri oluşturmak isteyen kurumlar için

Temel İlkeler

Otomasyon
Tekrarlayan güvenlik işlemlerini otomatikleştirme

Hız
Olaylara gerçek zamanlı müdahale

Süreklilik
7/24 kesintisiz güvenlik operasyonu

Merkezi Yönetim
Tüm sistemleri tek platformda

Imperum Nasıl Çalışır?

Imperum, güvenlik olaylarının tüm yaşam döngüsünü merkezi olarak yönetir. Playbook tabanlı otomasyon sayesinde olaylar analiz edilir, karar mekanizmaları çalıştırılır ve gerekli aksiyonlar otomatik olarak devreye alınır. Farklı güvenlik sistemlerinden gelen veriler tek platformda toplanır ve korelasyon ile anlamlandırılır. Kritik durumlara göre otomatik veya onaylı aksiyon senaryoları tetiklenir.

Teknik Özellikler

Merkezi Güvenlik Yönetimi
- SIEM, EDR,Firewall entegrasyonu
- Olay korelasyonu ve analiz
- Merkezi dashboard ve izleme
- Alarm ve olayların tek panelden yönetimi

Otomasyon ve Playbook
- Playbook / workflow tabanlı mimari
- Otomatik aksiyon tetikleme
- Manuel onay mekanizmaları
- Koşul bazlı karar ve aksiyon akışları

Olay Müdahalesi
- IP, kullanıcı, endpoint izolasyonu
- Mail tehditlerinde karantina
- Güvenlik ürünleri kural yönetimi
- Zararlı hash ve IOC engelleme işlemleri

Raporlama ve İzleme
- Gerçek zamanlı olay raporlama
- Alarm geçmişi ve aksiyon kayıt takibi
- Dashboard tabanlı güvenlik görünürlüğü
- Çok kanallı bildirim sistemi

Yapay Zekâ
- Yapay zeka destekli olay analizi
- Alarm önceliklendirme ve risk skorlama
- Anomali ve tehdit davranışı tespiti
- Yapay zeka destekli playbook oluşturma

Çalışma Akışı

1. Olay Toplama
- SIEM, EDR, firewall ve diğer sistemlerden alarm ve log verileri alınır.
- Veriler normalize edilir ve merkezi platforma aktarılır.
- Farklı kaynaklardan gelen olaylar ilişkilendirilerek merkezi görünürlük sağlanır.

→

2. Analiz ve Karar
- Olaylar korelasyon kuralları ile analiz edilir.
- Risk seviyesine göre playbook tetiklenir.
- Otomatik veya manuel onay mekanizması devreye girer.

→

3. Aksiyon ve Müdahale
- IP engelleme, kullanıcı kilitleme, endpoint izolasyonu uygulanır.
- Firewall ve diğer sistemlerde otomatik kural oluşturulur.
- Bildirim ve raporlama süreçleri başlatılır.

Sürekli İyileştirme
Güvenlik operasyonlarının değişen tehditlere karşı sürekli güncel ve etkin kalmasını destekler.

Avantajlar

Playbook AI
Yapay zeka destekli playbook üretimi sayesinde olay tiplerine göre dinamik aksiyon senaryoları oluşturulmasını ve süreçlerin akıllı şekilde optimize edilmesini sağlar.

Merkezi Orkestrasyon
SIEM, EDR, Firewall ve diğer güvenlik sistemlerinden gelen verileri tek platformda birleştirerek merkezi görünürlük ve yönetim sağlar.

Gerçek Zamanlı Aksiyon
Tehditleri gerçek zamanlı analiz ederek IP engelleme, kullanıcı izolasyonu ve alarm tetikleme gibi aksiyonları anında devreye alır.

Entegrasyon Yeteneği
OpenAPI / REST API desteği, Connector / App tabanlı modüler yapı ve ölçeklenebilir mimarisi sayesinde mevcut kurumsal sistemlerle kolayca entegre olur.

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.