aa teknoloji

OpenCTI

OpenCTI, siber tehdit istihbaratını merkezi olarak yönetmek isteyen SOC ekipleri, CERT yapıları ve güvenlik operasyon merkezleri için geliştirilmiş açık kaynaklı bir CTI platformudur. Tehdit verilerini ilişkilendirir, analiz eder ve operasyonel görünürlük sağlar.

Siber Tehdit İstihbaratı Zorlukları

Kuruluşlar, hızla artan tehdit verisi ve karmaşık saldırı yüzeyi nedeniyle güvenilir tehdit istihbaratını merkezi şekilde yönetmekte zorlanmaktadır. Farklı kaynaklardan gelen verilerin ilişkilendirilmesi, analiz edilmesi ve operasyon ekiplerine aktarılması önemli bir operasyonel yük oluşturur.

Tehdit göstergelerinin manuel işlenmesi, farklı güvenlik araçları arasında veri uyumsuzluğu ve dağınık istihbarat yönetimi; SOC ekiplerinin hızlı aksiyon almasını zorlaştırır. Bu durum tehditlerin geç tespit edilmesine neden olabilir.

Gerçek zamanlı tehdit görünürlüğünün eksik olması, kurumların proaktif güvenlik yaklaşımı geliştirmesini zorlaştırmaktadır.

⚠ Hangi Ekiplere Yardımcı olur?

- SOC ekipleri için merkezi tehdit görünürlüğü sağlar.
- CERT ekipleri için hızlı olay korelasyonu sunar.
- Güvenlik analistleri için veri ilişkilendirmesi sağlar.
- Kurumsal ekipler için tehdit paylaşımı kolaylaştırır.

Temel İlkeler

Açıklık
Açık kaynak ve şeffaf yapı

Korelasyon
İlişkisel tehdit analizi

Görünürlük
Merkezi tehdit görünürlüğü

Otomasyon
Hızlı ve sürekli veri akışı

Teknik Özellikler

Tehdit Yönetimi
- IOC ve TTP verilerini ilişkilendirme
- Tehdit aktörü analiz desteği
- Kampanya ve saldırı takibi
- MITRE ATT&CK uyumlu yapı

Entegrasyon Desteği
- MISP entegrasyon desteği
- SIEM sistemleriyle uyumluluk
- TAXII/STIX veri paylaşımı
- API tabanlı veri aktarımı

Veri ve Analiz
- Merkezi tehdit veri yönetimi
- Gerçek zamanlı veri işleme
- İlişkisel tehdit analizi
- Otomatik veri zenginleştirme

Erişim ve Yönetim
- Rol bazlı erişim yönetimi
- Çok kullanıcılı platform desteği
- Web tabanlı yönetim paneli
- Ölçeklenebilir mimari desteği

Otomasyon ve İş Akışları
- Otomatik tehdit akışı yönetimi
- Olay müdahale süreç entegrasyonu
- Görev ve süreç otomasyonu
- Sürekli veri senkronizasyon desteği

OpenCTI Nasıl Çalışır?

OpenCTI, farklı tehdit istihbaratı kaynaklarından topladığı verileri merkezi platformda ilişkilendirir, analiz eder ve güvenlik ekiplerine operasyonel görünürlük sağlar. IOC, tehdit aktörü ve saldırı kampanyaları arasında bağlantılar kurarak hızlı karar alma süreçlerini destekler.

Çalışma Akışı

1. Verileri Topla
- Harici tehdit kaynaklarını bağlar.
- IOC ve STIX verilerini aktarır.
- Otomatik veri toplama süreçlerini başlatır.
- Güvenlik araçlarından veri alır.

→

2. Analiz ve İlişkilendir
- Tehdit aktörlerini eşleştirir.
- Kampanya ilişkileri oluşturur.
- IOC korelasyon analizi yapar.
- Risk seviyelerini değerlendirir.

→

3. Paylaş ve Yönet
- Ekipler arası veri paylaşır.
- Merkezi olay yönetimi sağlar.
- Rapor ve analiz çıktısı üretir.
- Sürekli tehdit takibi yapar.

Sürekli İyileştirme
OpenCTI, açık kaynak yapısı ve geniş entegrasyon desteği sayesinde gelişen tehdit ortamına hızlı uyum sağlar. Ölçeklenebilir mimarisi ile kurumsal güvenlik operasyonlarını destekler.

Avantajlar

Merkezi CTI Yönetimi
Farklı tehdit istihbaratı kaynaklarından gelen verileri tek platformda toplayarak merkezi analiz ve operasyon yönetimi sağlar.

İlişkisel Tehdit Analizi
IOC, tehdit aktörleri ve saldırı kampanyaları arasında bağlantılar kurarak gelişmiş tehdit korelasyonu sağlar.

STIX/TAXII Desteği
Standart tehdit istihbaratı formatlarıyla uyumlu çalışarak güvenlik araçları arasında hızlı ve güvenli veri paylaşımı sunar.

Geniş Entegrasyon Yapısı
SIEM, MISP ve diğer güvenlik çözümleriyle entegre çalışarak mevcut güvenlik ekosistemine kolay uyum 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.