aa teknoloji

Siber Tehdit İstihbaratı

Kurumlara yönelik siber tehditleri, veri sızıntılarını ve dark web aktivitelerini sürekli izleyerek erken uyarı sağlayan; teknik ekiplere analiz, görünürlük ve aksiyon desteği sunan tehdit istihbaratı hizmetidir.

Siber Güvenlik Zorlukları

Kurumlar, sürekli gelişen siber tehditler, veri sızıntıları, kimlik bilgisi ifşaları ve marka kötüye kullanımı gibi risklerle karşı karşıya kalmaktadır. Tehditlerin erken aşamada tespit edilememesi operasyonel ve itibari kayıplara yol açabilir.

Dark web platformlarında paylaşılan erişim bilgileri, sahte domainler ve oltalama altyapıları çoğu zaman fark edilmeden uzun süre aktif kalabilir. Bu durum kurumların saldırı yüzeyini artırır ve güvenlik ekiplerinin müdahale süreçlerini zorlaştırır.

Kritik tehditlerin bağlamsal analiz olmadan değerlendirilmesi, yanlış önceliklendirme ve geciken aksiyon süreçlerine neden olabilir.

⚠ Hangi Sorunları Çözer?

- Güvenlik ekipleri için erken tehdit görünürlüğü
- SOC ekipleri için hızlı aksiyon desteği
- Kurumlar için veri sızıntısı görünürlüğü
- Marka ekipleri için sahte varlık tespiti

Temel İlkeler

Proaktif
Tehditleri gerçekleşmeden önce fark eder.

Görünürlük
Kritik tehditleri merkezi olarak izler.

Analiz
Bağlamsal tehdit değerlendirmesi sunar.

Müdahale
Teknik ekiplerin hızlı aksiyon almasını sağlar.

Teknik Özellikler

Tehdit İzleme
- Dark web platformlarının sürekli izlenmesi
- Fidye grubu sızıntılarının takibi
- Marka ve kurum adı bazlı tarama
- Riskli erişim ilanlarının tespiti

Veri Sızıntısı
- Kurumsal domain sızıntı taraması
- Kullanıcı adı ve parola eşleştirme
- Sızıntı tarihi ve kaynak analizi
- Alt domain bazlı görünürlük sağlama

Raporlama & Bildirim
- Kritik bulgular için anlık bildirim
- Yönetim odaklı özet raporlama
- Teknik ekipler için detaylı analiz
- Risk önceliklendirme çıktıları

Marka Koruma
- Typosquatting domain tespiti
- Sahte sosyal medya hesabı analizi
- Sahte reklam içeriklerinin izlenmesi
- Mobil uygulama takibi ve analiz

İzleme & Analiz
- Tehdit kaynaklarının sürekli takibi
- Kuruma özel risk analiz süreçleri
- Kritik bulguların önceliklendirilmesi
- Sürekli güncellenen tehdit analizi

Siber Tehdit İstihbaratı Hizmeti Nasıl Çalışır?

Hizmet kapsamında açık kaynaklar, veri sızıntı ortamları, dark web platformları ve tehdit veri akışları sürekli analiz edilir. Tespit edilen bulgular doğrulanır, önceliklendirilir ve ilgili ekipler için aksiyon alınabilir çıktılara dönüştürülür.

Çalışma Akışı

1. Veri Toplama ve İzleme
- Açık kaynak tehdit verileri toplanır.
- Dark web platformları düzenli izlenir.
- Domain ve marka taramaları yapılır.
- Veri sızıntısı kaynakları analiz edilir.

→

2. Analiz ve Yorumlama
- Bulgular teknik olarak doğrulanır.
- Risk seviyeleri önceliklendirilir.
- Kuruma özel bağlamsal analiz yapılır.
- Kritik tehditler filtrelenerek ayrıştırılır.

→

3. Bildirim & Aksiyon
- Kritik bulgular anlık iletilir.
- Teknik ekipler için analiz sunulur.
- Yönetim raporları düzenli paylaşılır.
- Önerilen aksiyon planları hazırlanır.

Sürekli İyileştirme
Siber Tehdit İstihbaratı, yeni tehdit kaynakları, veri akışları ve ihtiyaçlarına göre sürekli güncellenebilir yapıda sunulur. Ölçeklenebilir mimari sayesinde farklı kurum ihtiyaçlarına uyum sağlar.

Avantajlar

7/24 Tehdit İzleme
Kapalı forumlar, veri paylaşım platformları ve fidye yazılımı sızıntı sayfaları sürekli izlenerek kurumla ilişkili riskli içerikler tespit edilir.

Veri Sızıntısı Takibi
Kurumsal e-posta adresleri, domainler ve kullanıcı bilgileri düzenli olarak taranarak sızıntı kaynakları ve riskler görünür hale getirilir.

Marka Koruma
Typosquatting domainler, sahte sosyal medya hesapları, mobil uygulamalar ve sahte reklam içerikleri analiz edilerek marka riski azaltılır.

Aksiyon Odaklı Raporlama
Yönetim ve teknik ekiplere özel hazırlanan raporlar sayesinde tehditler önceliklendirilir ve hızlı müdahale süreçleri desteklenir.

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.