TEHDİT YOLU; TEHDİT İSTİHBARATINI AZAMİ DÜZEYE ÇIKARMA

GELENEKSEL CTI TOPLANTISI

Çoklu Veri Kaynakları: OSINT, tescilli beslemeler, kapalı forumlar ve devlet veritabanlarından toplanmaktadır.

Yüksek Maliyetler: Kuruluşlar genellikle birden fazla besleme için ödeme yapmakta ve bu durum gereksiz masraflara yol açmaktadır.

Analiz: Yanlış pozitifleri filtrelemek ve gerçek tehditlere öncelik vermek için zaman alıcı süreçler gerekmektedir.

ALTYAPI YÖNETİMİNDEKİ ZORLUKLAR

Güvenlik Duvarı Aşırı Yüklenmesi: Büyük miktarda ham veri, güvenlik duvarlarının kapasite sınırlarına ulaşmasına ve operasyonel maliyetlerin artmasına yol açabilir.

Altyapı Zorlanması: İşlenmemiş IoC'lerin işlenmesi, kaynakları zorlayarak yavaşlamalara neden olabilir veya maliyetli yükseltmeler gerektirebilir.

Genel Tehdit Listeleri: Birçok geleneksel çözüm, alakasız uyarılara ve yorgunluğa yol açan genel IoC'ler sunmaktadır.

GELENEKSEL CTI ÇÖZÜMLERİNİN SINIRLILIKLARI

Veri Aşırı Yüklenmesi: Sistemleri alakasız veya düşük öncelikli uyarılarla doldurarak verimsizliğe yol açar.

Parçalanmış Araçlar: Farklı sistemlerin entegrasyonunu gerektirir ve veri normalizasyonunu ile paylaşımını karmaşıklaştırır.

Yavaş Olay Yanıtı: Manuel işleme, tehdit yanıtını geciktirir ve saldırıların potansiyel etkisini artırır.

OTD BİLİŞİM
GLOBAL VAD

ThreatWAY
Threat Intelligence Exchange

ThreatWAY, işletmelerin kötü amaçlı faaliyetleri proaktif bir şekilde tespit edip engellemesini sağlayan ve aynı zamanda gerçek zamanlı tehdit paylaşımını kolaylaştıran bir erken uyarı sistemi görevi görür.

Özellikler:

- Saldırıları araştırarak ve otomatik olay yanıt yeteneklerini kolaylaştırarak proaktif içgörüler sunar.
- CatchProbe'un tuzaklarından ve hem açık hem de kapalı kaynaklarla API entegrasyonundan ve tarama işlemlerinden kaynaklanan açığa çıkan saldırılardan elde edilen verileri gerçek zamanlı olarak toplar ve yayar.
- Elde edilen verileri dağıtır ve kullanıcıların bunları milisaniyeler içinde kendi kuruluşları arasında paylaşmalarını sağlar.

TEHLİKEYİ YÖNET

KORUMA ETKİNLEŞTİR

DİJİTAL ADLİ BİLİŞİM

GERÇEK ZAMANLI İSTİHBARAT

Genel Değerlendirme

Dinamik Kanal ve Toplama Yönetimi

Binlerce honeypot'tan gelen hedefli saldırı verileri

Açık ve kapalı platformlarla API entegrasyonu

Yeni kayıtlı alan adı adreslerinin toplanması

Otomatik Veri Normalizasyonu

Gerçek Zamanlı Uyarılar: Olası tehditler hakkında gerçek zamanlı uyarılar alın

Özelleştirilebilir Veri Kaynakları: Gerektiğinde veri kaynakları ekleyin ve kaldırın.

API Desteği: Mevcut Güvenlik Duvarlarınız ve SIEM'lerinizle kolayca entegre edin.

Tehdit İstihbaratı İtibar Sıralaması

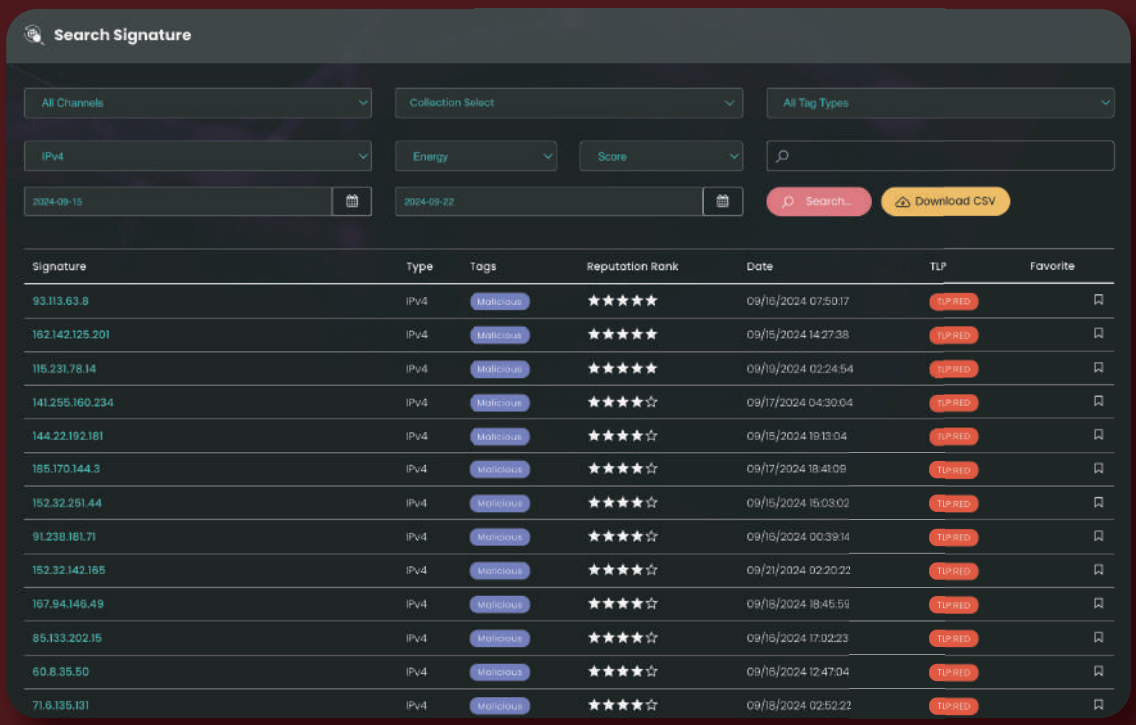
OTD BİLİŞİM
GLOBAL VAD

ThreatWAY: Gerçek Zamanlı CTI Ekosisteminize Kesintisiz Bir Şekilde Entegre Olur

Temel Ayrıştırıcılar

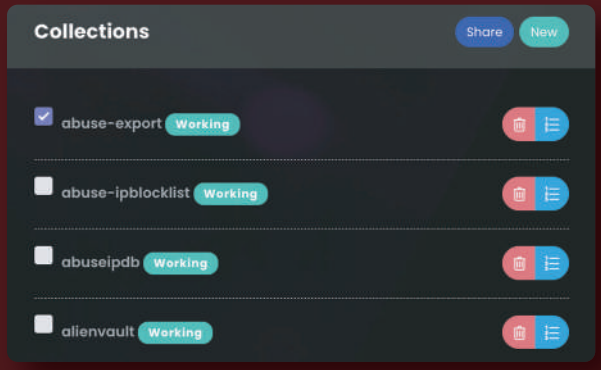
Öncelikle Kritik Tehditler: En Önemli Noktada Odaklı Koruma

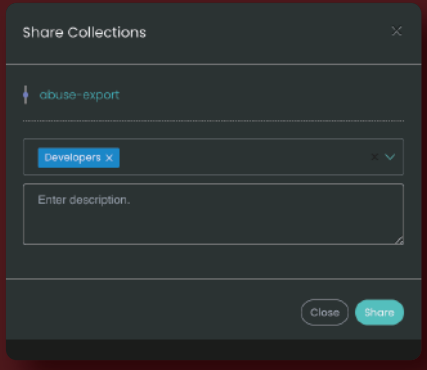
ThreatWAY, tehditleri analiz eder ve öncelik sırasına koyarak kuruluşunuzun en kritik risklere odaklanmasını sağlar. ThreatWAY, IoC'leri alaka düzeyleri ve potansiyel etkilerine göre sıralayarak, belirli ortamınız için en büyük tehlikeyi oluşturan tehditleri belirlemenize yardımcı olur, gürültüyü azaltır ve düşük riskli veya alakasız verilerden kaynaklanan dikkat dağıtıcı unsurları en aza indirir.



Otomatik Veri Toplama ve Paylaşımı

ThreatWAY'in altyapısı, işletmelerin yalnızca arama yapmalarını değil, aynı zamanda milisaniyeler içinde kurum içi ve kurumlar arası kanallarda rafine istihbarat paylaşımını da mümkün kılar.



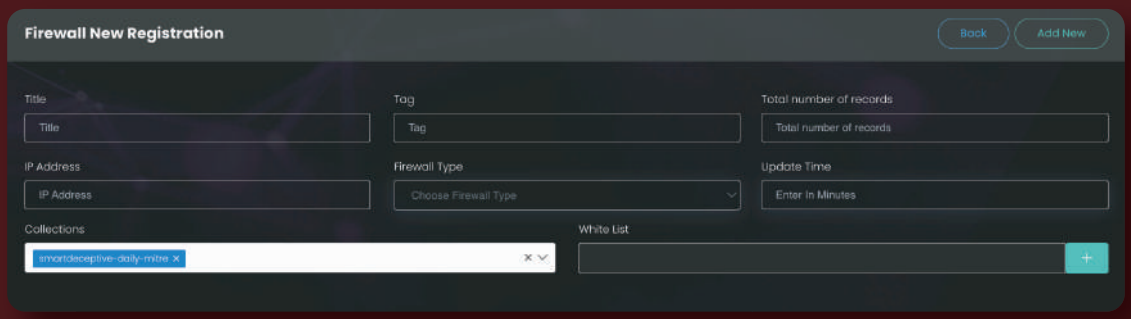


OTD BİLİŞİM
GLOBAL VAD

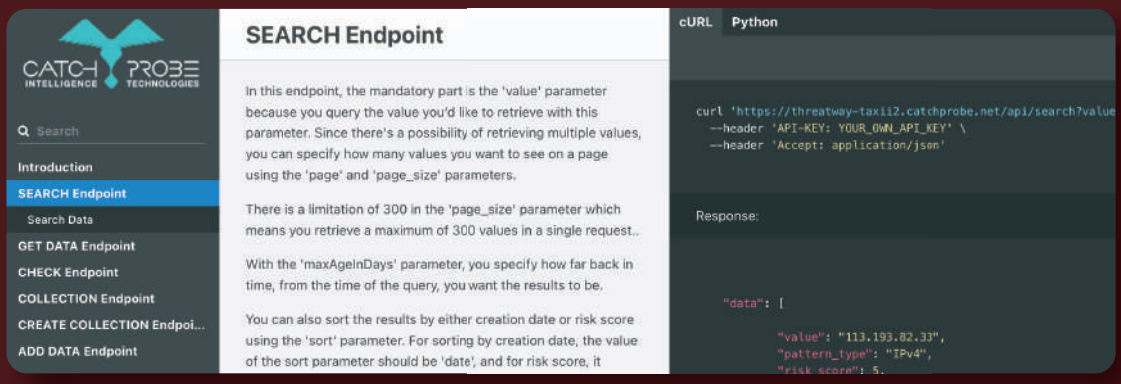
Zahmetsiz Entegrasyon, Gerçek Zamanlı Aksiyon

ThreatWAY, işletmelere doğrulanmış Tehlike Göstergelerini (loC'ler) doğrudan güvenlik duvarlarına, SIEM sistemlerine ve SOAR platformlarına sorunsuz bir şekilde sunarak güç kazandırır. İster bir REST API aracılığıyla, ister özel kurallar kullanılarak doğrudan entegrasyon yoluyla olsun, ThreatWAY, tehdit istihbaratının mevcut güvenlik altyapınız içinde hızla eyleme dönüştürülebilir olmasını temin eder.

Option #1

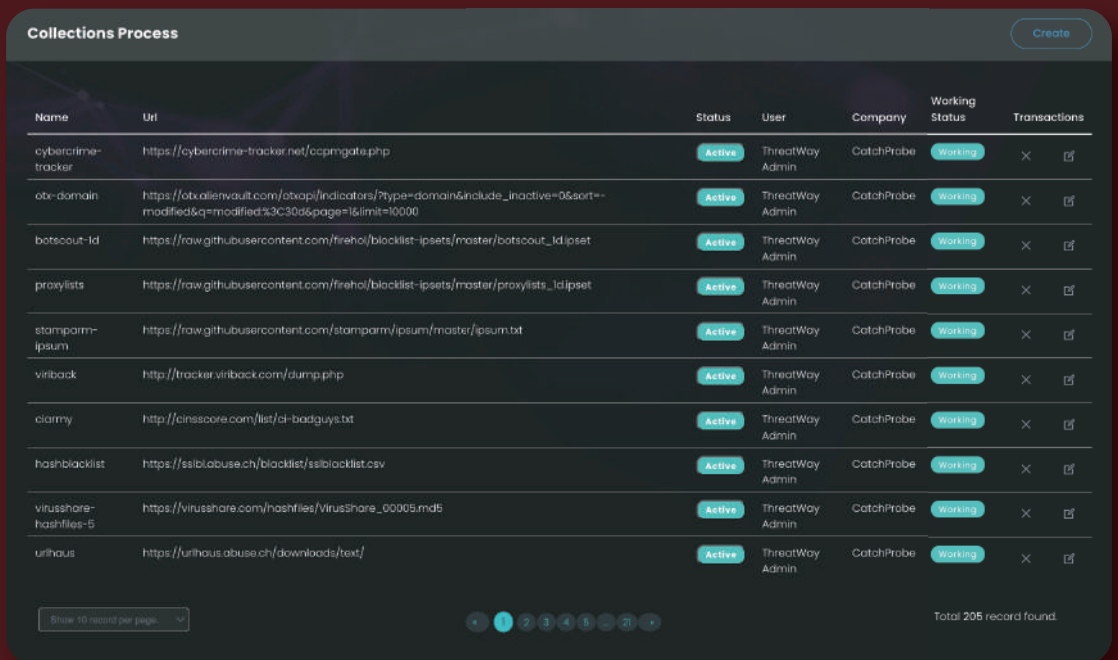


Option #2



Özelleştirilebilir Veri Kaynakları

ThreatWAY, DarkMAP'in gelişmiş tarama işlemleri ve SmartDECEPTIVE'in tuzakları ile açığa çıkan saldırılarıyla birlikte API aracılığıyla 200'den fazla platformun kusursuz entegrasyonunu sağlarken, aynı zamanda gerçek zamanlı olarak özel ihtiyaçlarınız için yalnızca en ilgili istihbaratın mevcut olmasını temin etmek amacıyla özelleştirilmiş veri kaynaklarını kolayca ekleyip kaldırmanıza olanak tanır.



OTD BİLİŞİM
GLOBAL VAD