

TEHDİT YOLU; TEHDİT İSTİHBARATINI AZAMİ DÜZEYE ÇIKARMA

GELENEKSEL CTİ 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 loC'lerin işlenmesi, kaynakları zorlayarak yavaşlamalara neden olabilir veya maliyetli yükseltmeler gerektirebilir.

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

GELENEKSEL CTİ 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 karmaşılaştırır.

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



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
ADLI 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

ThreatWAY: Gerçek Zamanlı CTI Ekosisteminize Kesintisiz Bir Şekilde Entegre Olur

Temel Ayırıştırıcılar

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.

Search Signature						
All Channels	Collection Select	All Tag Types				
IPv4	Energy	Score				
2024-09-15	2024-09-22	Search	Download CSV			
Signature	Type	Tags	Reputation Rank	Date	TLP	Favorite
93.113.63.8	IPv4	Malicious	★★★★★	09/16/2024 07:50:17	TLP:RED	
162.142.125.201	IPv4	Malicious	★★★★★	09/16/2024 14:27:38	TLP:RED	
115.231.78.14	IPv4	Malicious	★★★★★	09/16/2024 02:24:54	TLP:RED	
141.255.160.234	IPv4	Malicious	★★★★☆	09/17/2024 04:30:04	TLP:RED	
144.22.192.181	IPv4	Malicious	★★★★☆	09/16/2024 19:13:04	TLP:RED	
185.170.144.3	IPv4	Malicious	★★★★☆	09/17/2024 18:41:06	TLP:RED	
152.32.251.44	IPv4	Malicious	★★★★☆	09/16/2024 15:03:02	TLP:RED	
91.238.181.71	IPv4	Malicious	★★★★☆	09/16/2024 00:39:14	TLP:RED	
152.32.142.165	IPv4	Malicious	★★★★☆	09/21/2024 02:20:22	TLP:RED	
167.94.148.49	IPv4	Malicious	★★★★☆	09/18/2024 18:45:58	TLP:RED	
85.133.202.15	IPv4	Malicious	★★★★☆	09/16/2024 17:02:23	TLP:RED	
60.8.35.50	IPv4	Malicious	★★★★☆	09/16/2024 12:47:04	TLP:RED	
71.6.135.131	IPv4	Malicious	★★★★☆	09/18/2024 02:52:22	TLP:RED	

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.

Collections		Share	New
☒	abuse-export Working		
☐	abuse-ipblocklist Working		
☐	abuseipdb Working		
☐	allenvault Working		

Share Collections

abuse-export

Developers x

Enter description.

Close Share

Zahmetsiz Entegrasyon, Gerçek Zamanlı Aksiyon

ThreatWAY, işletmelere doğrulanmış Tehlike Göstergelerini (IoC'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

Firewall New RegistrationBackAdd New

Title

Tag

Total number of records

Title

Tag

Total number of records

IP Address

Firewall Type

Update Time

IP Address

Choose Firewall Type

Enter In Minutes

Collections

White List

enprodeceptive-daily-mitre x

Option #2

CATCH INTELLIGENCE
PROBE TECHNOLOGIES

SEARCH Endpoint

In this endpoint, the mandatory part is the 'value' parameter because you query the value you'd like to retrieve with this parameter. Since there's a possibility of retrieving multiple values, you can specify how many values you want to see on a page using the 'page' and 'page_size' parameters.

There is a limitation of 300 in the 'page_size' parameter which means you retrieve a maximum of 300 values in a single request..

With the 'maxAgeInDays' parameter, you specify how far back in time, from the time of the query, you want the results to be.

You can also sort the results by either creation date or risk score using the 'sort' parameter. For sorting by creation date, the value of the sort parameter should be 'date', and for risk score, it

cURL

Python

```
curl 'https://threatway-taxii2.catchprobe.net/api/search?value=113.193.82.33' \
--header 'API-KEY: YOUR_OWN_API_KEY' \
--header 'Accept: application/json'
```

Response:

```
{
  "data": [
    {
      "value": "113.193.82.33",
      "pattern_type": "IPv4",
      "risk_score": 5
    }
  ]
}
```

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.

Collections ProcessCreate

Name	Url	Status	User	Company	Working Status	Transactions
cybercrime-tracker	https://cybercrime-tracker.net/ccprngate.php	Active	ThreatWay Admin	CatchProbe	Working	×
otr-domain	https://otr.alienvault.com/otrap/indicators?type=domain&include_inactive=0&sort=-modified&q=modified:3C30d&page=1&limit=10000	Active	ThreatWay Admin	CatchProbe	Working	×
botscout-lid	https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/botscout_lid_ipset	Active	ThreatWay Admin	CatchProbe	Working	×
proxylis	https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/proxylis_lid_ipset	Active	ThreatWay Admin	CatchProbe	Working	×
stamptom-ipsum	https://raw.githubusercontent.com/stamptom/ipsum/master/ipsum.txt	Active	ThreatWay Admin	CatchProbe	Working	×
viriback	http://tracker.viriback.com/dump.php	Active	ThreatWay Admin	CatchProbe	Working	×
ciarmy	http://cinscore.com/list/ci-badguys.txt	Active	ThreatWay Admin	CatchProbe	Working	×
hashblacklist	https://ssllabuse.ch/blacklist/sslblacklist.csv	Active	ThreatWay Admin	CatchProbe	Working	×
virusshare-hashfiles-5	https://virusshare.com/hashfiles/VirusShare_00005.md5	Active	ThreatWay Admin	CatchProbe	Working	×
urihaus	https://urihaus.abuse.ch/downloads/text/	Active	ThreatWay Admin	CatchProbe	Working	×

Show 10 record per page

12345678910

Total 205 record found.