

THREATWAY; MAXIMIZING THREAT INTELLIGENCE

TRADITIONAL CTI GATHERING

Multiple Data Sources: Collected from OSINT, proprietary feeds, closed forums, and government databases.

High Costs: Organizations often pay for multiple feeds, leading to redundant or unnecessary expenses.

Analysis: Time-consuming processes to filter out false positives and prioritize real threats.

INFRASTRUCTURE MANAGEMENT CHALLENGES

Firewall Overload: Large volumes of raw data can cause firewalls to hit capacity limits, increasing operational costs.

Infrastructure Strain: Processing unrefined IoCs strains resources, causing slowdowns or requiring costly upgrades.

Generic Threat Lists: Many traditional solutions provide generic IoCs, leading to irrelevant alerts and fatigue.

TRADITIONAL CTI SOLUTIONS LIMITATIONS

Data Overload: Floods systems with irrelevant or low-priority alerts, leading to inefficiency.

Fragmented Tools: Requires integration of disparate systems, complicating data normalization and sharing.

Slow Incident Response: Manual processing delays threat response, increasing the potential impact of attacks.

ThreatWAY serves as an early warning system, enabling businesses to proactively identify and block malicious activity, while also facilitating real-time threat sharing.

Features:

- Offers proactive insights by investigating attacks and facilitating automatic incident response capabilities.
- Gathers and disseminates data acquired from CatchProbe's decoys and exposed attacks, sourced from both API integration with open closed sources and crawling operations, in real-time.
- Distributes the obtained data and enables users to share them with their-inter-an intra-organizations within milliseconds.



**MANAGE
THREATS**



**ENABLE
PROTECTION**



**DIGITAL
FORENSICS**



**REAL-TIME
INTELLIGENCE**

Overview

Dynamic Channel and Collection Management

Targeted attack data incoming from thousands of honeypots

API integration with open and closed platforms

Collection of newly registered domain addresses

Automated Data Normalization

Real-Time Alerts: Receive real-time alerts on potential threats

Customizable Data Sources: Add and remove data sources as needed.

API Support: Easily integrate it with your existing Firewalls and SIEMs.

Threat Intelligence Reputation Ranking

ThreatWAY: Real-Time CTI Fites Seamslessly into Your Ecosystem

Key Differentiators

Critical Threats First: Focused Protection Where It Matters Most

ThreatWAY analyzes and prioritizes threats, ensuring that your organization is focused on the most critical risks. By ranking IoCs based on their relevance and potential impact, ThreatWAY helps you identify which threats pose the greatest danger to your specific environment, reducing noise and minimizing distractions from low-risk or irrelevant data.

Search Signature

All Channels

Collection Select

All Tag Types

IPv4

Energy

Score

2024-09-15

📅

2024-09-22

📅

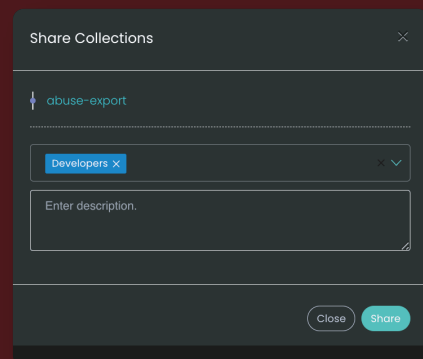
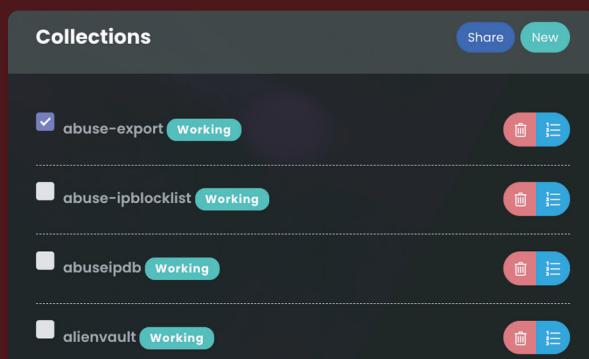
🔍 Search...

📄 Download CSV

Signature	Type	Tags	Reputation Rank	Date	TLP	Favorite
93.113.63.8	IPv4	Malicious	★★★★★	09/16/2024 07:50:17	TIP-RED	🔖
162.142.125.201	IPv4	Malicious	★★★★★	09/15/2024 14:27:38	TIP-RED	🔖
115.231.78.14	IPv4	Malicious	★★★★★	09/19/2024 02:24:54	TIP-RED	🔖
141.255.160.234	IPv4	Malicious	★★★★☆	09/17/2024 04:30:04	TIP-RED	🔖
144.22.192.181	IPv4	Malicious	★★★★☆	09/15/2024 19:13:04	TIP-RED	🔖
185.170.144.3	IPv4	Malicious	★★★★☆	09/17/2024 18:41:09	TIP-RED	🔖
152.32.251.44	IPv4	Malicious	★★★★☆	09/15/2024 15:03:02	TIP-RED	🔖
91.238.181.71	IPv4	Malicious	★★★★☆	09/16/2024 00:39:14	TIP-RED	🔖
152.32.142.165	IPv4	Malicious	★★★★☆	09/21/2024 02:20:22	TIP-RED	🔖
167.84.146.49	IPv4	Malicious	★★★★☆	09/18/2024 18:45:56	TIP-RED	🔖
85.133.202.15	IPv4	Malicious	★★★★☆	09/16/2024 17:02:23	TIP-RED	🔖
60.8.35.50	IPv4	Malicious	★★★★☆	09/16/2024 12:47:04	TIP-RED	🔖
71.6.135.131	IPv4	Malicious	★★★★☆	09/18/2024 02:52:22	TIP-RED	🔖

Automated Data Collection and Sharing

ThreatWAY's infrastructure enables businesses to not only collect but also share refined intelligence accross intra-and inter-organizational channels in milliseconds.



Effortless Integration, Real-Time Action

ThreatWAY empowers businesses by seamlessly delivering verified indicators of Compromise (IoCs) directly to your firewalls, SIEMs and SOAR platforms. Whether through a REST API or direct integration using custom rules, ThreatWAY ensures that threat intelligence is rapidly actionable within your existing security infrastructure.

Option #1

Firewall New Registration Back Add New

Title

Tag

Total number of records

IP Address

Firewall Type

Choose Firewall Type

Update Time

Collections

smartdeceptive-daily-mitre

×

White List

+

Option #2



Q Search

Introduction

SEARCH Endpoint

Search Data

GET DATA Endpoint

CHECK Endpoint

COLLECTION Endpoint

CREATE COLLECTION Endpoi...

ADD DATA Endpoint

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=  
--header 'API-KEY: YOUR_OWN_API_KEY' \  
--header 'Accept: application/json'
```

Response:

```
"data": [  
  
  "value": "113.193.82.33",  
  "pattern_type": "IPv4",  
  "risk_score": 5.
```

Customizable Data Sources

ThreatWAY offer seamless integration of over 200 platforms through API, alongside DarkMAP's advanced crawling operations and SmartDECEPTIVE's decoys and exposed attacks, while also allowing you to easily add or remove customized data sources to ensure only most relevant intelligence is available for your specific needs in real-time.

Collections Process Create

Name	Url	Status	User	Company	Working Status	Transactions
cybercrime-tracker	https://cybercrime-tracker.net/ccprngate.php	Active	ThreatWay Admin	CatchProbe	Working	×
otx-domain	https://otx.alienvault.com/otxapi/indicators/?type=domain&include_inactive=0&sort=-modified&q=modified:3C30d&page=1&limit=10000	Active	ThreatWay Admin	CatchProbe	Working	×
botscout-ld	https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/botscout_ld.ipset	Active	ThreatWay Admin	CatchProbe	Working	×
proxylists	https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/proxylists_ld.ipset	Active	ThreatWay Admin	CatchProbe	Working	×
stamparam-ipsum	https://raw.githubusercontent.com/stamparam/ipsum/master/ipsum.txt	Active	ThreatWay Admin	CatchProbe	Working	×
viriback	http://tracker.viriback.com/dump.php	Active	ThreatWay Admin	CatchProbe	Working	×
ciarmy	http://cinsscore.com/list/ci-badguys.txt	Active	ThreatWay Admin	CatchProbe	Working	×
hashblacklist	https://ssllabuse.ch/blacklist/sslblacklist.csv	Active	ThreatWay Admin	CatchProbe	Working	×
virushare-hashfiles-5	https://virushare.com/hashfiles/VirusShare_00005.md5	Active	ThreatWay Admin	CatchProbe	Working	×
urlhaus	https://urlhaus.abuse.ch/downloads/text/	Active	ThreatWay Admin	CatchProbe	Working	×

Show 10 record per page

1 2 3 4 5 6 7 8 9 10 21

Total 205 record found.