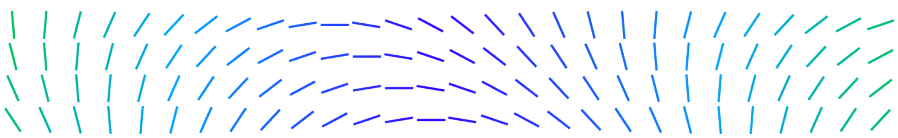
Advanced Threat Landscape Analysis System (ATLAS) User Guide

ADVANCED PROGRAMS GROUP

Table of Contents



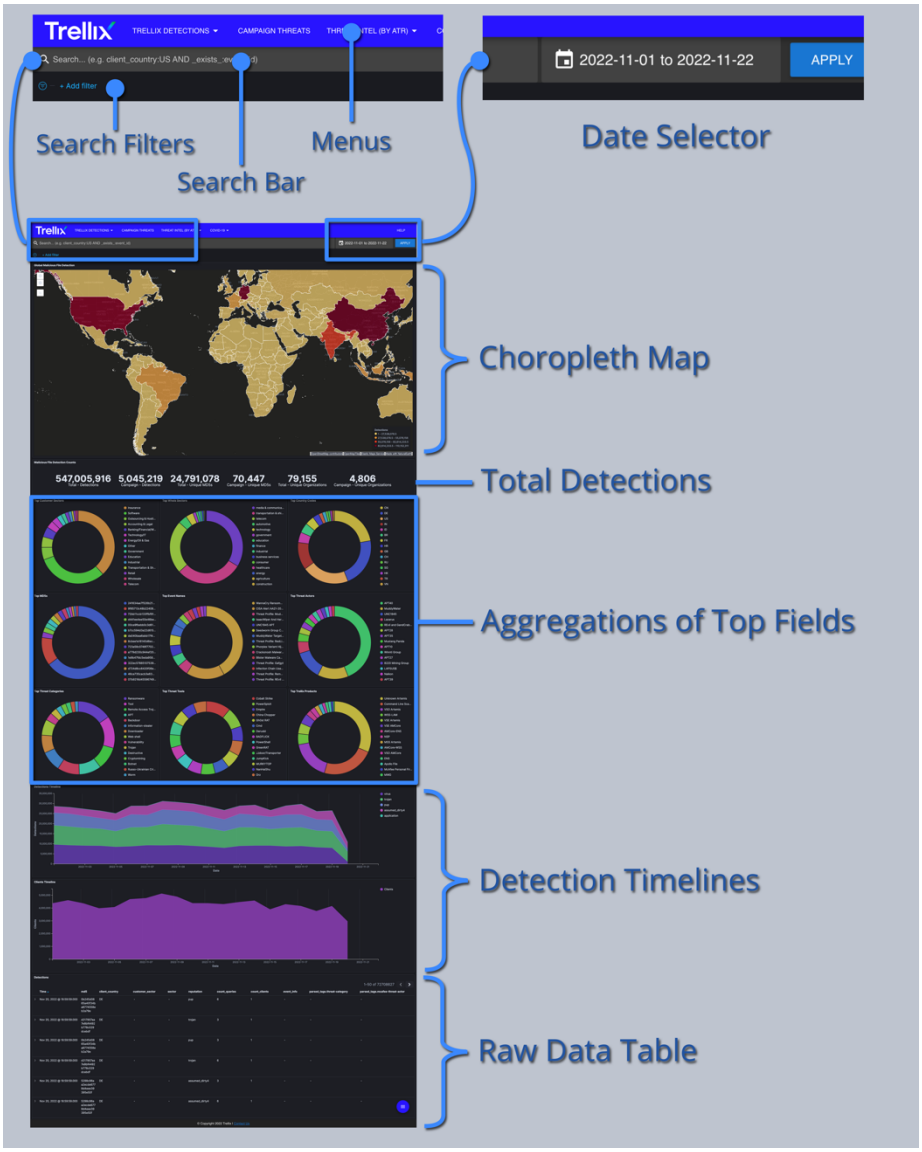
Overview

The Advanced Threat Landscape Analysis System (ATLAS) is a data analysis tool that gives customers unique global insight into the malicious file, domain, and IP detections seen worldwide from Trellix's billions of sensors around the globe. Data is aggregated from various Trellix data sources (Repper, REST, RealProtect, JCM, etc.) to provide the latest global emerging threats with enriched data such as industry sector and geolocation. ATLAS correlates these threats with campaign data containing research from Trellix's Advanced Research Center (ARC) and Threat Intelligence Group (TIG), as well as open-source data, to provide a dedicated view for campaigns consisting of events, dates, threat actors, IOCs, and more.

Dashboard Layout

ATLAS includes several standard dashboards for indicators of compromise (IOCs), threat actors and campaigns. Dashboards vary slightly from one another but share similar design elements, visualizations, and workflows.

ATLAS Detections Dashboards include several visualization types for prevalence of malicious IP addresses, files, and URLs that empower customers with comprehensive situational awareness of the global threat landscape.



6220 American Center Drive,
San Jose, CA 95002

888.847.8766

trellix.com

Prevalence Dashboards

Within the menu dropdown labelled Trellix Detections are links to the prevalence dashboards. Each of these dashboards is dedicated to one class of IOC and are populated daily with detections from the full range of Trellix products.

Within each prevalence dashboard you will find:

- Which attacks are most relevant to your organization.
- When and where they are occurring.
- What industry sectors are affected.
- Whether they belong to any organized campaigns.

File Prevalence (schema)

Includes malicious file hash detections in MD5 and SHA256 formats. Each hash is classified by reputation and trust score.

URL Prevalence (schema)

Includes detections of client interactions with malicious domains, hosts, and URLs. Detections are further categorized by risk, site function, and any malicious files that they deploy.

IP Prevalence (schema)

A catalog of attempted connections to known malicious IP addresses.

Campaigns Dashboard (schema)

Click on Campaign Threats in the menu to view the latest intelligence from our team of industry-leading researchers. The campaign dashboard collates the latest analysis of thousands of emerging threats into one location. Here you will find cutting-edge research from Trellix specialists, as well as open-source intelligence from around the world.

Campaign data is imported from Trellix's backend intelligence platform MISP. As part of this process, ATLAS automatically enriches our prevalence data with campaign IOCs.

6220 American Center Drive,
San Jose, CA 95002

888.847.8766

trellix.com

Searching and Filtering

ATLAS is extremely flexible and dynamic. Users can craft queries and filter results in any view, using any combination of fields present in the ATLAS data schema. Customers can then export the results directly within the dashboard. Trellix APG personnel can also provide training and help build more complex queries.

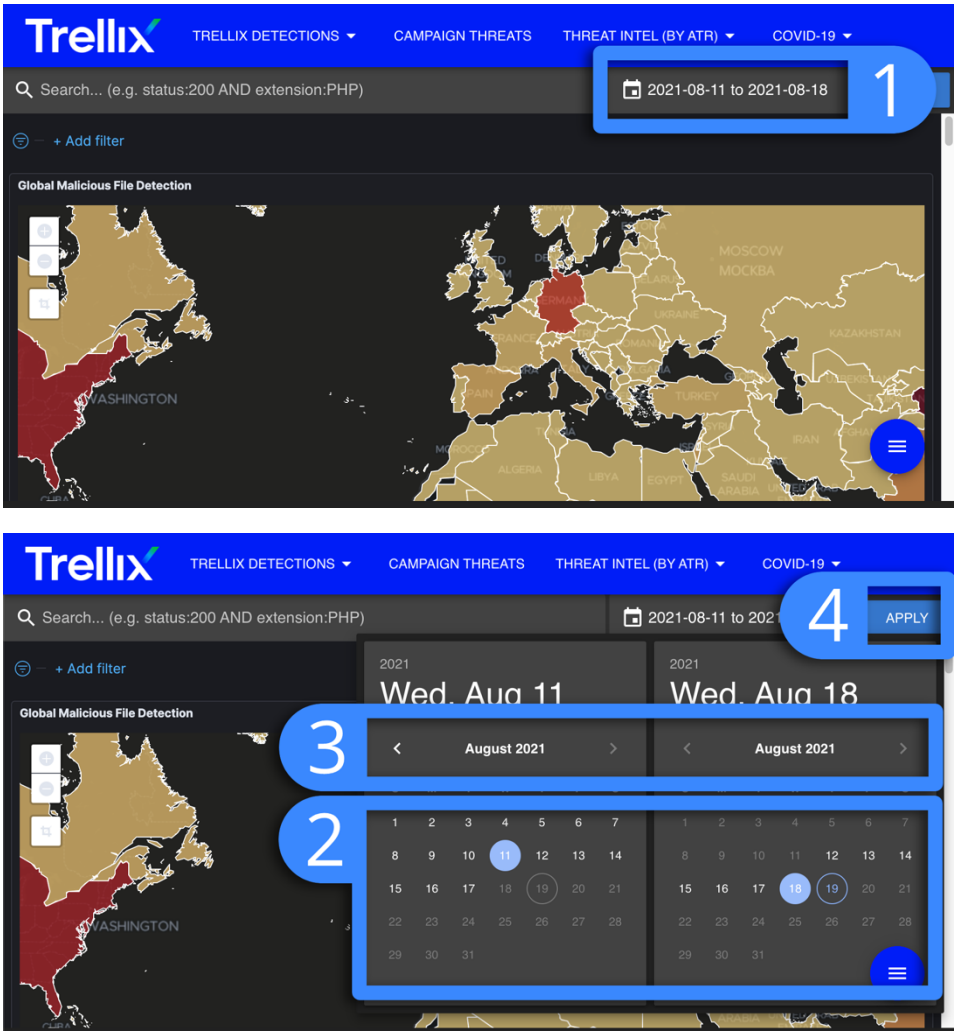
Changing the Date

Filter the date range of data displayed in the dashboard.

1. Click on the date box on the upper right of the page.
2. Click the calendar popup to change the start and end dates.
3. Use the left and right arrows to change the month and year.
4. Click `Apply`.

ATLAS may take a few moments to update, depending on the current server load and the amount of data being displayed.

Note: By default, ATLAS keeps 12 months of historical detection data active for searches. This may vary by site per the customer's requirements.



Changing the date

Querying with the Search Bar

After selecting an appropriate date range, most research tasks begin with the search bar. This section will describe some of the most common search methods as well as some tips and best practices to optimize your user experience.

Two Query Languages: KQL and Lucene

The ATLAS Dashboard uses Kibana for its visualizations and it includes two supported query languages. Since version 7.0, the default format is Kibana Querying Language (KQL also previously called Kuery), but the legacy language Lucene is also fully supported.

The examples in this guide are in the Lucene format but you can also use KQL if you like. For the basic examples below, there should be no difference in the search results.

Search Resources

Refer to these links for more information about Kibana's query languages.

Lucene: https://lucene.apache.org/core/2_9_4/queryparsersyntax.html
KQL: https://www.elastic.co/guide/en/kibana/7.10/kuery-query.html

Terms Query

Terms queries match one or more exact terms within a document's fields. The most commonly used form targets a specific field:

```
fieldname:terms
```

`sector:technology`	Matches detections from the technology sector
`sector:technology healthcare`	Matches both technology and healthcare
`event_tags:"launch agent"`	Matches the exact phrase "launch agent"

Free Text Search

If no specific field is indicated then the search will be done on all fields in the index.

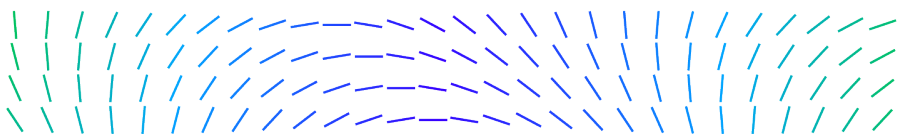
`sector:technology`	Matches detections from the technology sector
`technology`	Matches technology in any field

Note: Free text search works within all fields — including the _source field, which contains the unprocessed JSON information for each document.

Ranges

Use `[]` and `{}` to search a range on numeric and date fields. Square brackets `[]` are inclusive and curly braces `{}` are exclusive.

`count_queries:1`	Matches when `count_queries` equals 1



`count_queries:[1 TO *]`	Matches when `count_queries` is >= 1
`count_queries:[1 TO 3]`	Matches when `count_queries` is 1, 2, or 3
`count_queries:{1 TO 3}`	Matches when `count_queries` is 2

Note: When using a range, you need to follow a very strict format and use capital letters `TO` to specify the range.

Boolean Queries

You can use the logical operators `AND`, `OR` and `NOT`. Use parentheses to group statements and control the order of operations.

`technology AND client_country:US`	Matches detections with the word "technology" and in the US
`technology OR client_country:US`	Matches detections either containing the word "technology" or in the US
`(technology AND client_country:US) OR finance`	Matches detections with the word "technology" in the US or any with the word "finance"
`NOT client_country:US`	Matches detections that are not in the US

Note: Ensure that you use capital letters to define logical terms like `AND` or `OR`.
Note: Use `-`, `!`, or `NOT` to define negative terms.

Important Tips

Not case sensitive

Text searches are not case sensitive. This means that `technology` and `TeChNoLoGy` will return the same results.

*Note: There is an exception for fields that are not "analyzed" such as `client_country`. These fields are stored in their raw state and **are** case sensitive.*

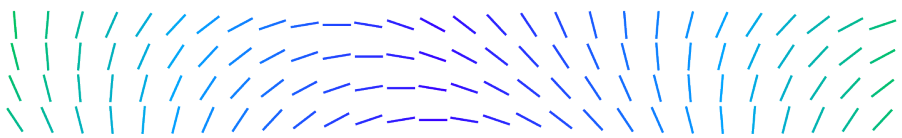
Match Exact Phrases

When you put the text within double quotes (`""`), you are looking for an exact match, which means that the exact string must match what is inside the double quotes. This is why `technology\/it` and `"technology/it"` will return different results.

Wildcard Symbols and Search

You can use the wildcard symbols `*` or `?` in searches. `*` means any number of characters, and `?` means only one character.

`client_country:US`	Matches detections in the US



`client_country:U?`	Matches US, UY, UA, UZ and UG
`sector:technology`	Matches detections from the technology sector
`sector:te*`	Matches technology and telecom

Type Dependency

Some search features depend on the type of field. Fields that are not analyzed are case-sensitive, unlike free-text search. Range searches can only be used on numerical and date type fields. Refer to the appendix for a list of field types.

exists

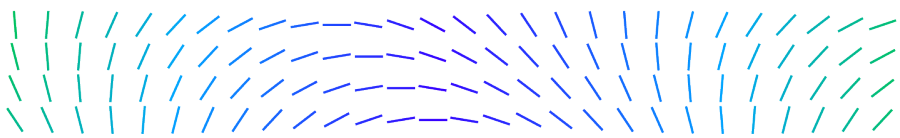
Using the `_exists_` prefix for a field will filter out documents that are missing the named field.

`_exists_:misp`	Matches detections that have the "misp" field

Special Characters

All special characters need to be properly escaped to include them in a query. The following is a list of all available special characters:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```



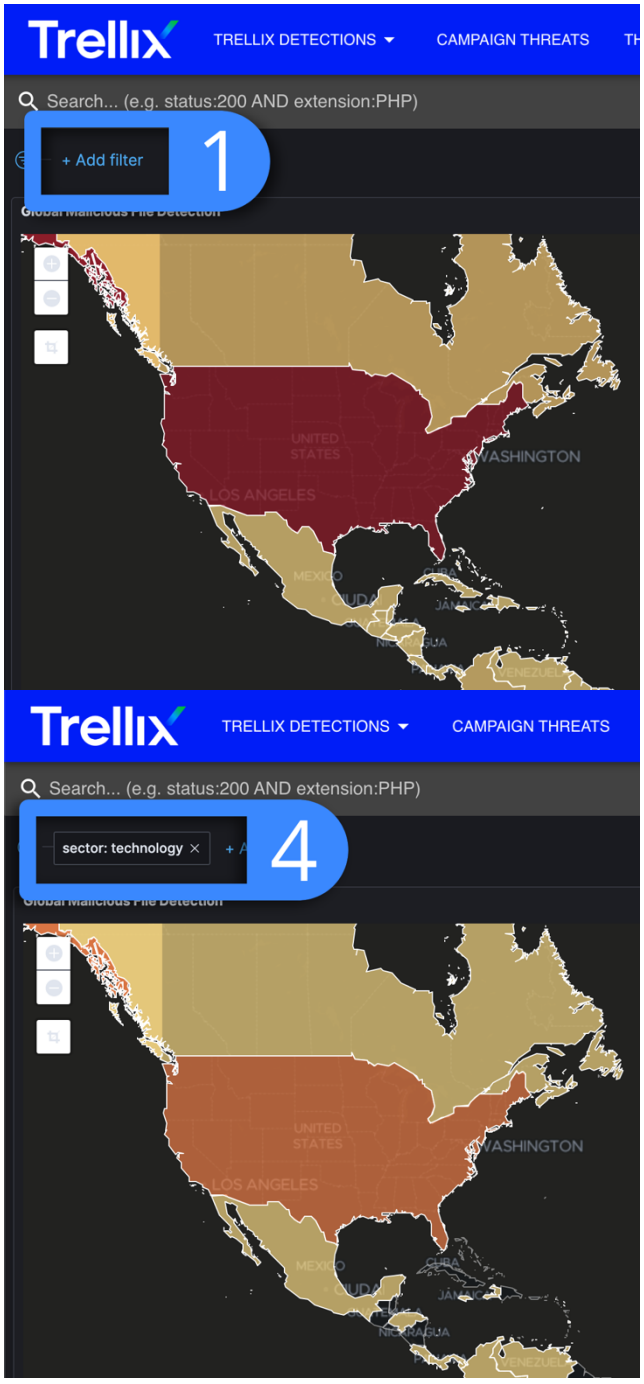
Filters

Like the search bar, the filter bar allows you to limit the data shown in the dashboard. However, filters can be switched on and off independently from one another. Use them to quickly experiment with different views, or to activate frequently used searches with a single click.

> *Note: Filters are not saved with your browser session. Closing the browser or navigating to a different dashboard will reset your searches and filters.*

Adding a Filter

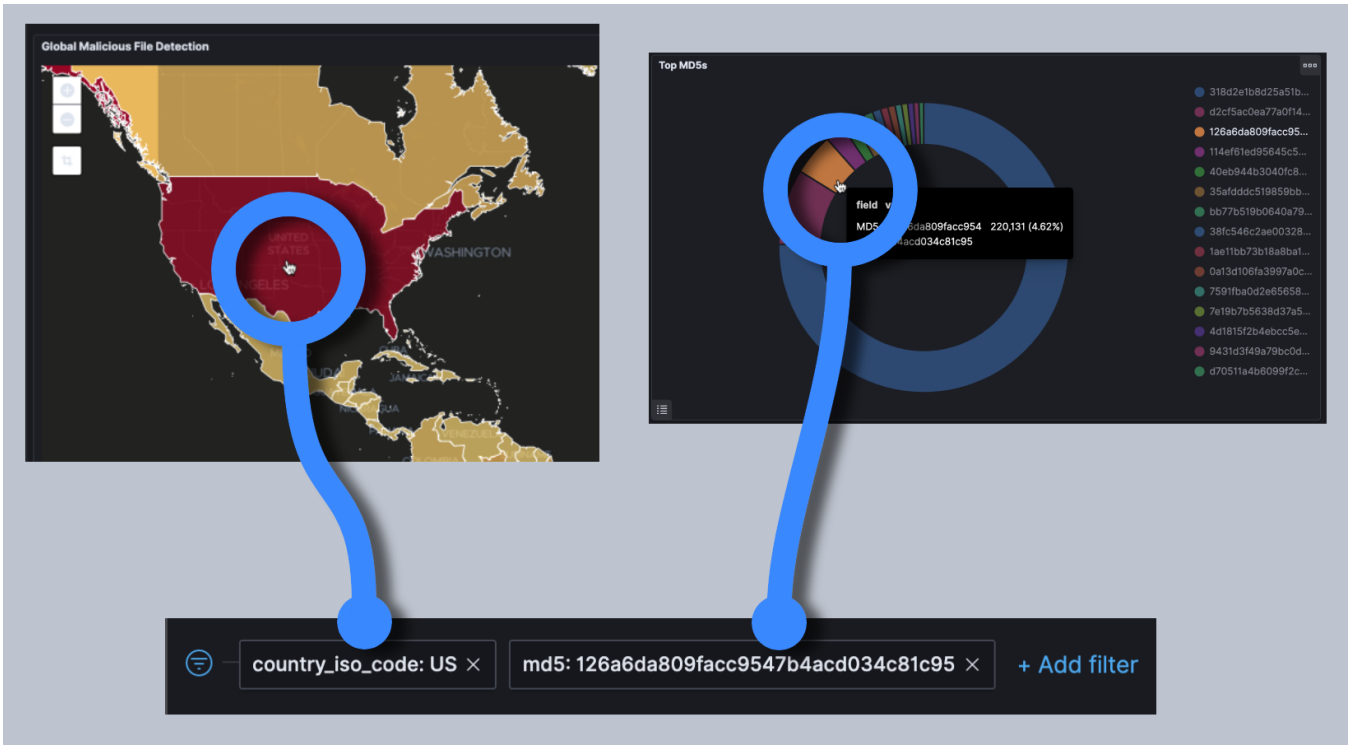
1. Click on `Add filter` at the top of the page.
2. Enter a field, operator, and value.
3. Click `Save`.
4. The dashboard will refresh to display the new search parameters.



Adding filters

Adding Filters from Visualizations

You can create filters quickly by clicking on elements in most visualizations. Try pie and bar charts, or the choropleth map.



Click visualizations to create filters

Filter Options

Click on the filter to bring up the filter's settings menu. Click the button on the left of the filter bar to change settings for all filters.

- **Pin across all apps**: This feature doesn't currently have a function in ATLAS dashboards, as each dashboard is backed by an independent data set. It may become available in the future.
- **Edit Filter**: Changes the filter's parameters.
- **Include/Exclude Results**: Inverts the filter, showing what was previously filtered out.
- **Temporarily Disable/Re-enable**: Toggles the filter on and off.
- **Delete**: Removes the filter.

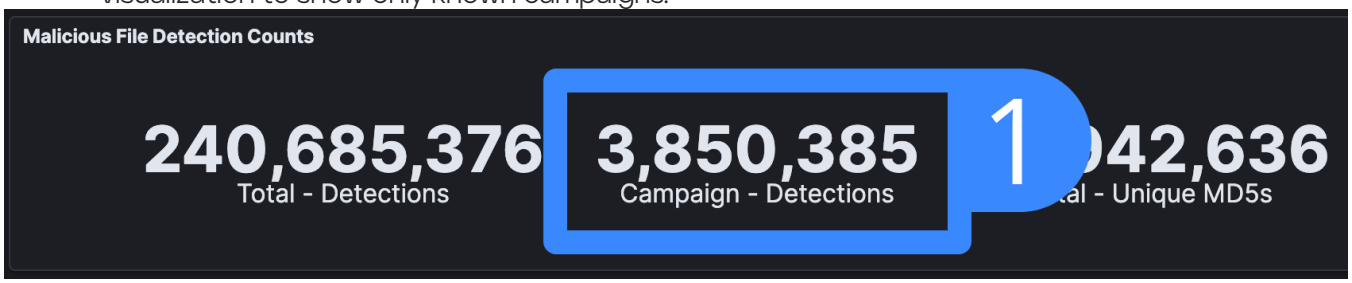
Tutorials

Use Browser Bookmarks to Save Searches

Frequently used queries can be saved for later by bookmarking the page, or saving the URL elsewhere. Filters cannot be saved using this method.

Quick Campaign Filter

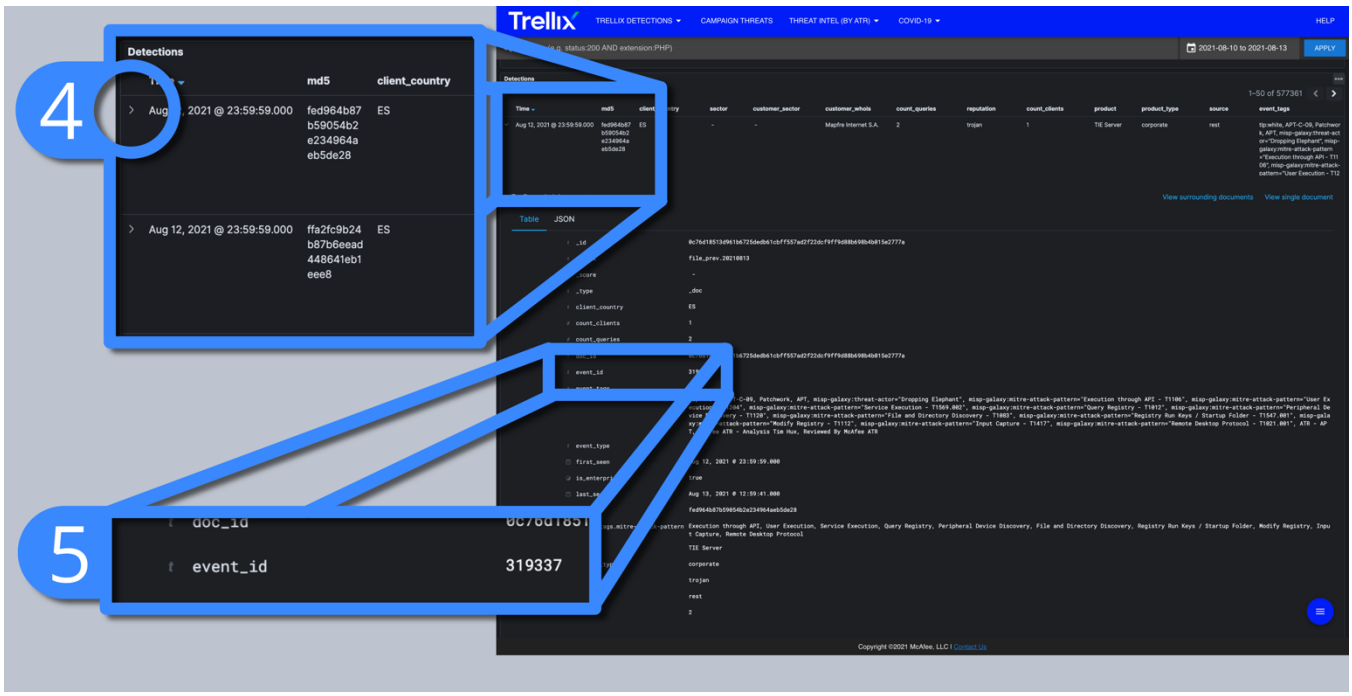
1. In any of the prevalence dashboards, click on "Campaign – Detections" in the total detections visualization to show only known campaigns.



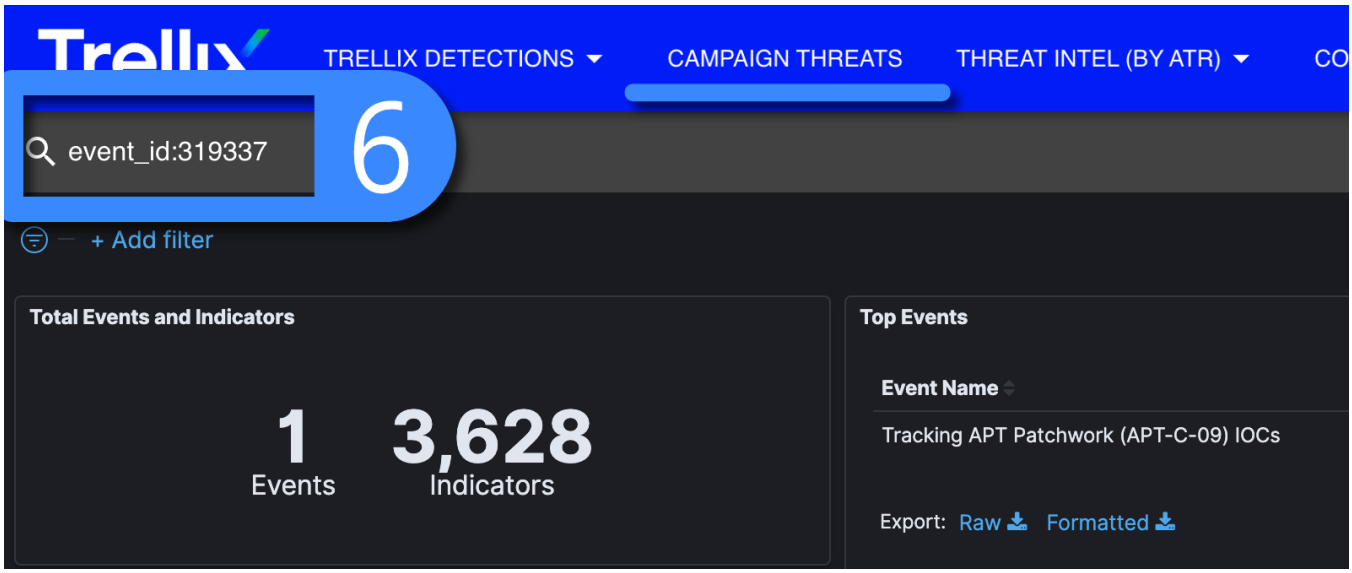
Cross Reference Prevalence and Campaign Data

Prevalence to Campaigns

1. Open any prevalence dashboard.
2. Filter for campaigns as shown above.
3. Add further filters or queries if needed.
4. In the detections table at the bottom of the page, click on an arrow in any table row to expand it.
5. Copy the `event_id`.
6. Load the campaigns dashboard and search for the `event_id`.



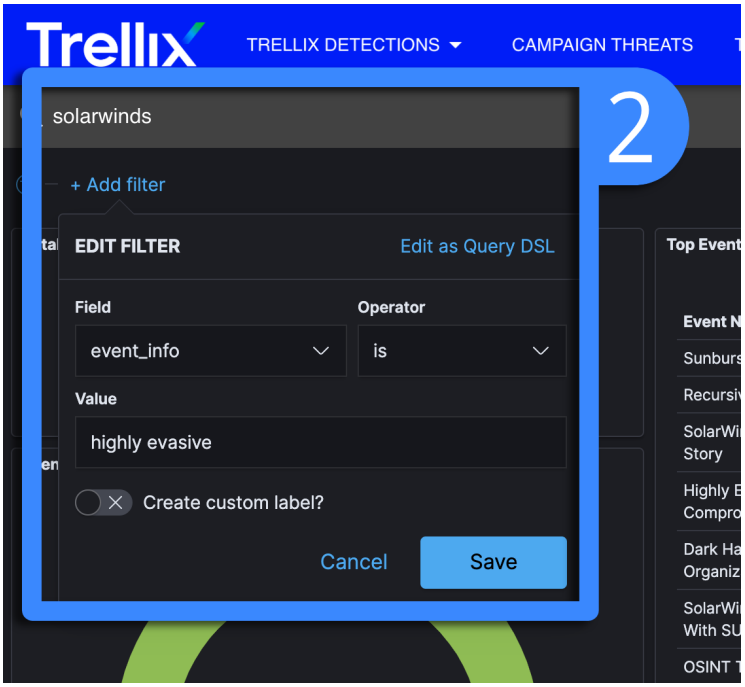
Expanding a table row and finding the event_id



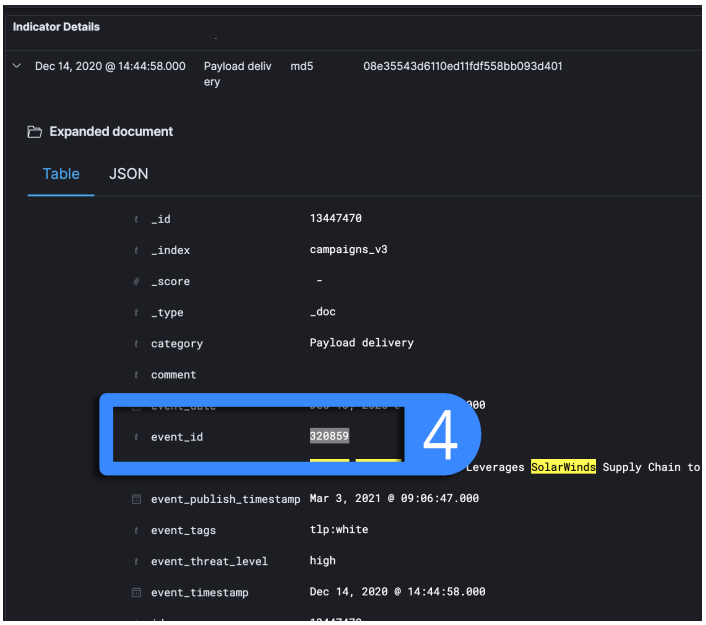
Querying event_id in campaigns dashboard

Campaigns to Prevalence

1. Open the campaigns dashboard.
2. Find any campaign of interest with queries or filters. In this example we're looking for the Solar Winds campaign with a further filter for the terms "highly evasive".
3. In the indicator details table at the bottom of the page, click on an arrow in any table row to expand it.
4. Copy the `event_id`.
5. Load any prevalence dashboard and search for the `event_id`.



Querying campaigns dashboard



Find the event_id

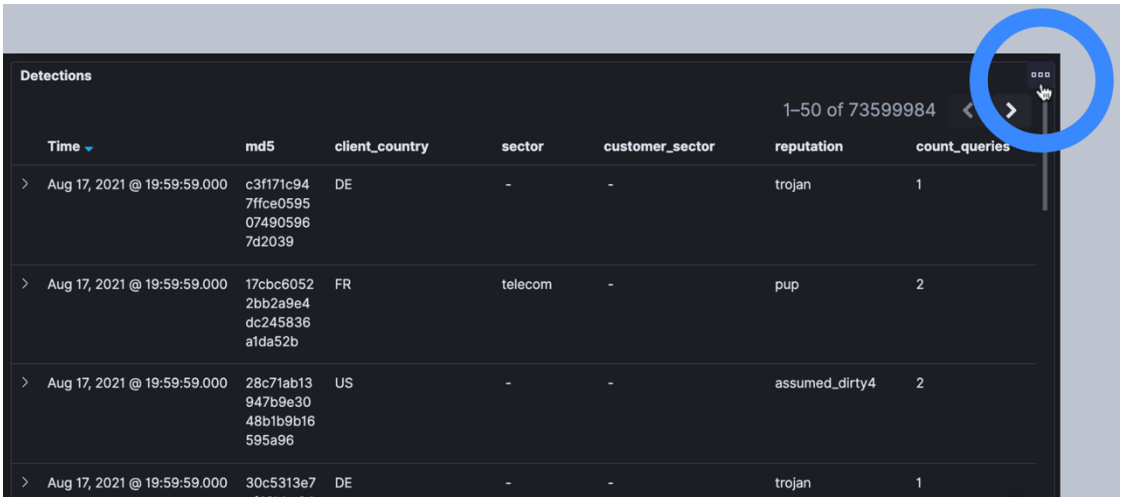
Querying event_id in file prevalence dashboard

Exporting

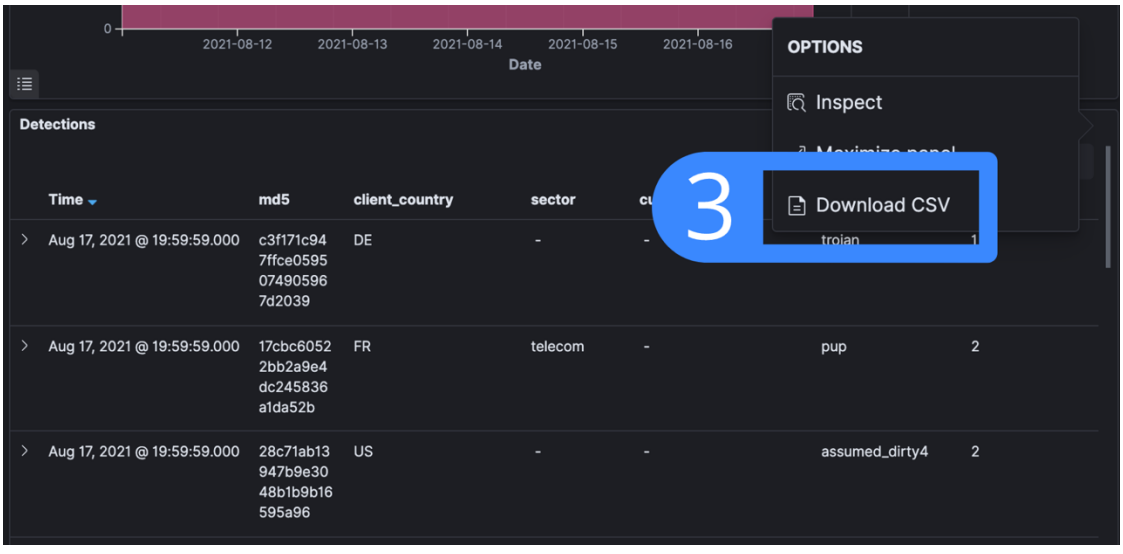
Note: Most ATLAS visualizations contain aggregated data and exports from them won't include details about the individual detections they display. Export from the 'Detections' table at the bottom of the dashboard to get all field data from individual detections.

Export Detailed Detection Data in CSV Format

1. Scroll to the `Detections` table at the bottom of the dashboard.
2. Hover the mouse over the table. Click the options button that appears at the top right.
3. Click `Download CSV`.



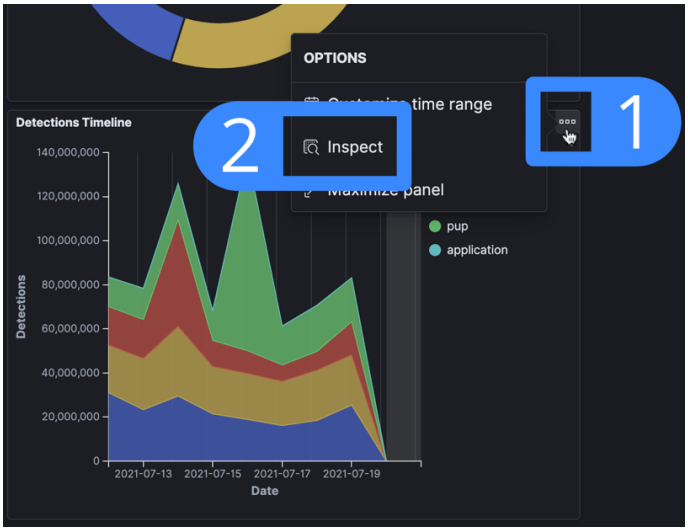
Click ellipsis to open visualization menu



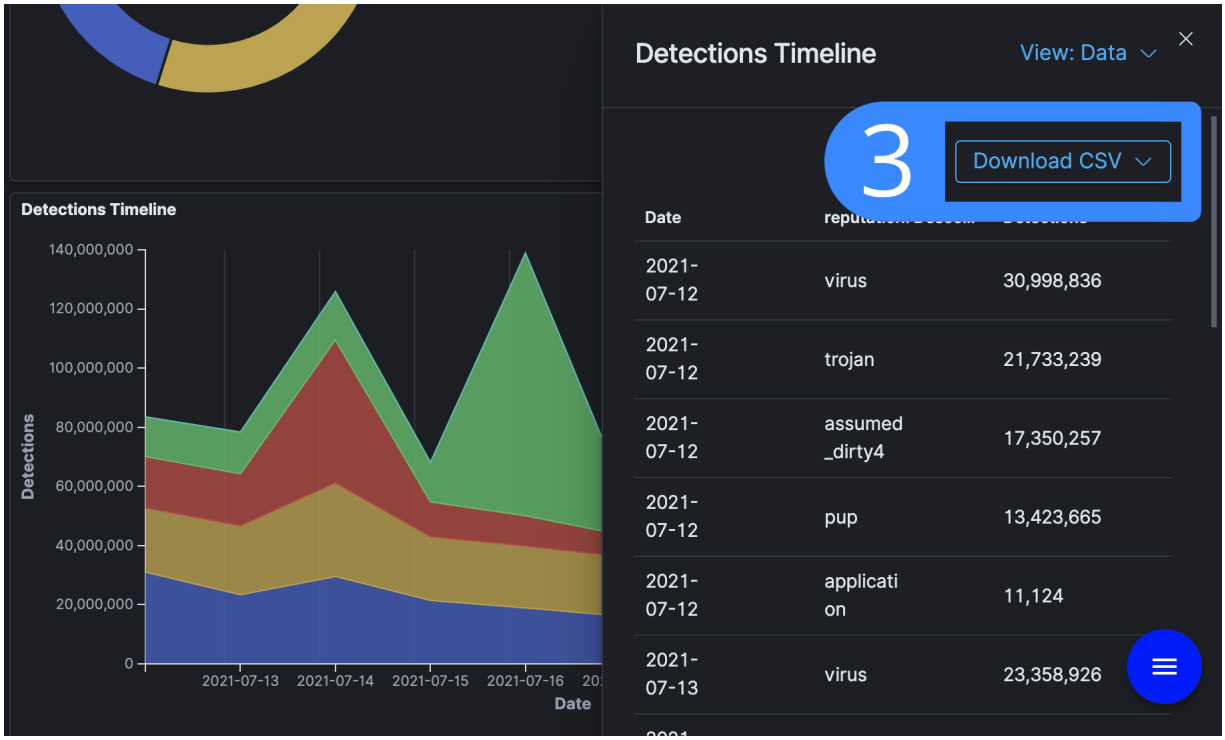
Downloading table data

Export Another Visualization's Data

1. Hover the mouse over the visualization. Click the options button that appears at the top right.
2. Click `Inspect`.
3. On the panel that appears, click `Download CSV`. Select `Raw CSV` or `Formatted CSV`.



Opening visualization's `inspect` menu



Downloading visualization data

Note: Formatted CSV makes minor presentation changes, such as adding commas to large numbers and formatting the date. Formatted CSV may be easier for an analyst to read. Choose Raw CSV when you want to manipulate or import the data with another program.

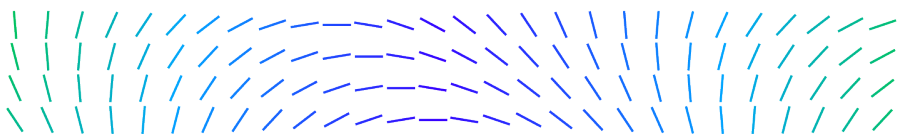
Note: Exports from the Detections table are always in the raw format.

Appendix A – Data Schema

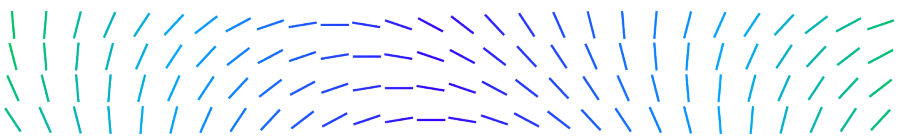
`client_country` uses the ISO 3166-1 alpha-2 standard:
https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2

File Prevalence

Field	Description
source	Trellix source of the record
md5	File MD5 in lowercase
sha256	File SHA-256 in lowercase
product	Trellix product name
client_country	Client country ISO code
customer_id	Customer ID
customer_sector	Customer sector (based on customer_id)
sector	Customer sector (based on customer_whois)
reputation	GTI reputation
trust	Reputation trust score
first_seen	First seen timestamp for group
last_seen	Last seen timestamp for group
count_queries	Aggregated count of queries/reports for group
count_clients	Aggregated count of distinct clients for group
is_enterprise	If it is an enterprise client
event_id	List of MISP event IDs if associated with a campaign
event_info	List of MISP event names
event_tags	List of MISP event tags
event_type	Type of detection (file, domain, ip)
parsed_tags.mitre-attack-pattern	List of MITRE ATT&CK patterns
parsed_tags.threat-category	List of TIG threat categories
parsed_tags.threat-profile-type	TIG threat profile type
parsed_tags.tool	List of malware tools
parsed_tags.threat-actor	List of threat actors
parsed_tags.threat-actor-country	List of country codes of the threat actors

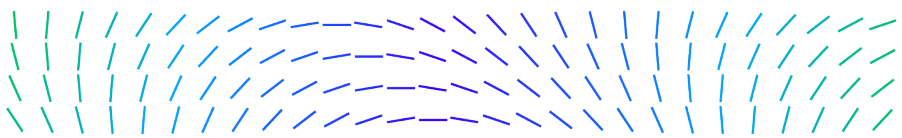


Field	Description
parsed_tags.targeted-country	List of countries targeted by the campaign(s)
parsed_tags.targeted-sector	List of sectors targeted by the campaign(s)

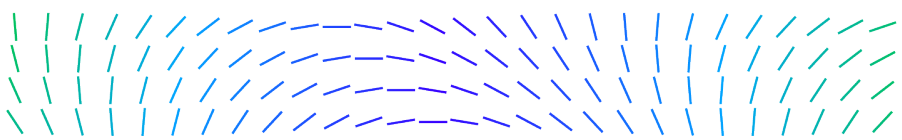


URL Prevalence

Field	Description
source	Trellix source of the record
domain	First level domain
host	Hostname
url_path	URL path
port	Port number
download_md5	MD5 of downloaded file/content
product	Trellix product name
client_country	Client country ISO code
customer_id	Customer ID
customer_sector	Customer sector (based on customer_id)
sector	Customer sector (based on customer_whois)
reputation	GTI reputation
trust	Reputation trust score
category	List of TrustedSource URL category codes
category_name	List of category names of the category codes
category_risk_group	List of category risk groups of the category codes
category_functional_group	List of category functional groups of the category codes
first_seen	First seen timestamp for group
last_seen	Last seen timestamp for group
count_queries	Aggregated count of queries/reports for group
count_clients	Aggregated count of distinct clients for group
is_enterprise	If it is an enterprise client
event_id	List of MISP event IDs if associated with a campaign
event_info	List of MISP event names
event_tags	List of MISP event tags
event_type	Type of detection (file, domain, ip)
parsed_tags.mitre-attack-pattern	List of MITRE ATT&CK patterns
parsed_tags.threat-category	List of TIG threat categories
parsed_tags.threat-profile-type	TIG threat profile type
parsed_tags.tool	List of malware tools



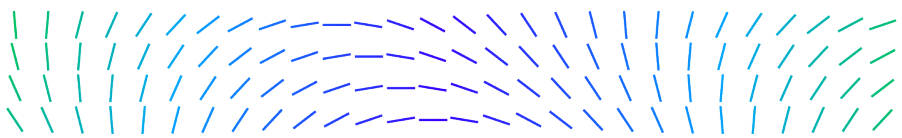
Field	Description
parsed_tags.threat-actor	List of threat actors
parsed_tags.threat-actor-country	List of country codes of the threat actors
parsed_tags.targeted-country	List of countries targeted by the campaign(s)
parsed_tags.targeted-sector	List of sectors targeted by the campaign(s)



IP Prevalence

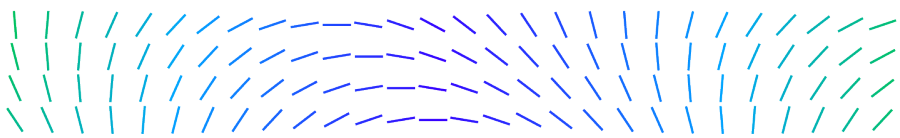
Field	Description
source	Trellix source of the record
ip	IP address
connected_ip	IP address on the other side of the connection
port	Port number
connected_port	Port used on the other side of the connection
is_destination	True if destination IP, false if source IP, null if unknown
is_inbound	True if inbound request, false if outbound request, null if unknown
is_ipv4	True if IP address is IPv4, false if IP address is IPv6, null if unknown
protocol	Communication protocol
host	Hostname associated with IP address
attack_id	NSM Attack ID
product	Trellix product name
client_country	Client country ISO code
customer_id	Customer ID
customer_sector	Customer sector (based on customer_id)
sector	Customer sector (based on customer_whois)
reputation	GTI reputation
trust	Reputation trust score
ip_country	Country ISO code associated with the IP address
first_seen	First seen timestamp for group
last_seen	Last seen timestamp for group
count_queries	Aggregated count of queries/reports for group
count_clients	Aggregated count of distinct clients for group
is_enterprise	If it is an enterprise client
event_id	List of MISP event IDs if associated with a campaign
event_info	List of MISP event names
event_tags	List of MISP event tags
event_type	Type of detection (file, domain, ip)
parsed_tags.mitre-attack-pattern	List of MITRE ATT&CK patterns
parsed_tags.threat-category	List of TIG threat categories

Field	Description
parsed_tags.threat-profile-type	TIG threat profile type
parsed_tags.tool	List of malware tools
parsed_tags.threat-actor	List of threat actors
parsed_tags.threat-actor-country	List of country codes of the threat actors
parsed_tags.targeted-country	List of countries targeted by the campaign(s)
parsed_tags.targeted-sector	List of sectors targeted by the campaign(s)



Campaigns

Field	Description
category	Category of IOC
city	City of IOC (if IP)
comment	Additional IOC comments
country	Country of IOC (if IP)
event_date	Date event was created
event_id	Event ID this IOC is a part of
event_info	Event/Campaign name
event_publish_timestamp	Timestamp (in seconds) of last event publish in MISP
event_tags	Tags for the event
event_threat_level	Event threat level
event_timestamp	Timestamp (in seconds) of last event update
id	Unique ID of IOC
location	Latitude,Longitude location of IOC (if IP)
timestamp	Timestamp (in seconds) IOC was created/updated
type	Type of IOC
value	Value of IOC
parsed_tags.mitre-attack-pattern	List of MITRE ATT&CK patterns
parsed_tags.threat-category	List of TIG threat categories
parsed_tags.threat-profile-type	TIG threat profile type
parsed_tags.tool	List of malware tools
parsed_tags.threat-actor	List of threat actors
parsed_tags.threat-actor-country	List of country codes of the threat actors
parsed_tags.targeted-country	List of countries targeted by the campaign
parsed_tags.targeted-sector	List of sectors targeted by the campaign



Reputation to Trust Score Mapping

GTI Reputation	Reputation Trust Score
FILE	
FILE_KNOWN_CLEAN	99
FILE_ASSUMED_CLEAN	85
FILE_NXDOMAIN	50
FILE_UNKNOWN	45
FILE_AD1	30
FILE_AD2	25
FILE_AD3	20
FILE_AD4	15
FILE_PUP	4
FILE_APPLICATION	3
FILE_TROJAN	2
FILE_VIRUS	1
URL / IP	
MINIMAL	100
MINIMAL	99
MINIMAL	85
MINIMAL	70
DEFAULT	50
UNVERIFIED	45
UNVERIFIED	40
MEDIUM	30
HIGH	15
HIGH	1