Infoblox Dossier and TIDE Documentation

Quick Start Guide

06/29/2021

Table of Contents

Overview

Infoblox Dossier™ and TIDE uses highly accurate machine-readable threat intelligence data via a flexible Threat Intelligence Data Exchange (TIDE) to aggregate, curate, and enable distribution of data across a broad range of infrastructures. TIDE enables organizations to ease consumption of threat intelligence from various internal and external sources, and to effectively defend against and quickly respond to cyberthreats. TIDE is backed by the Infoblox threat intelligence team that normalizes and refines high-quality threat intelligence data feeds.

Dossier is a threat indicator research tool that gives contextual information from a dozen sources (including TIDE) simultaneously, empowering users to make accurate decisions quicker and with greater confidence. This document contains a high-level overview of how to use Infoblox Dossier and TIDE.

Prerequisites

Infoblox Dossier and TIDE are subscription-based services available within the Infoblox Cloud Services Portal. There are no requirements for access to TIDE other than possessing a valid subscription. TIDE is only available with a BloxOne Threat Defense Advanced subscription.

Access to the Cloud Services Portal

Infoblox Dossier and TIDE can be accessed by navigating to the **Dossier™ Threat Research Portal** page by clicking **Research** -> **Dossier** in the Cloud Services Portal.

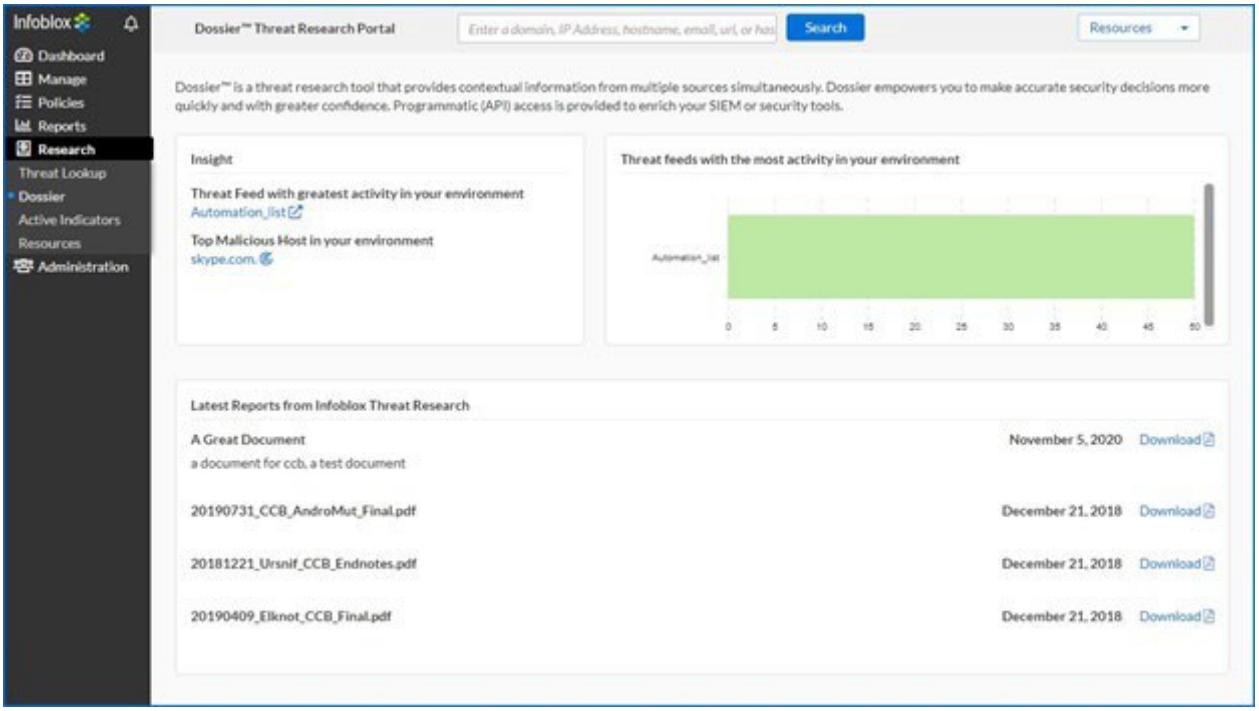

Image 1: Dossier™ Threat Research Portal

Threat Classification Guide

Each threat indicator belongs to a specific class and has a default expiration time (TTL). Expired threat indicators are still available in the database and returned by a search, but they are not included in the Infoblox/DNS Firewall feeds. The Cyber Threat Intelligence team periodically checks the indicators for validity and accuracy. The Threat Classification guide can be located through the Cloud Services Portal at **Research** -> **Resources** -> **Classification Guide**.

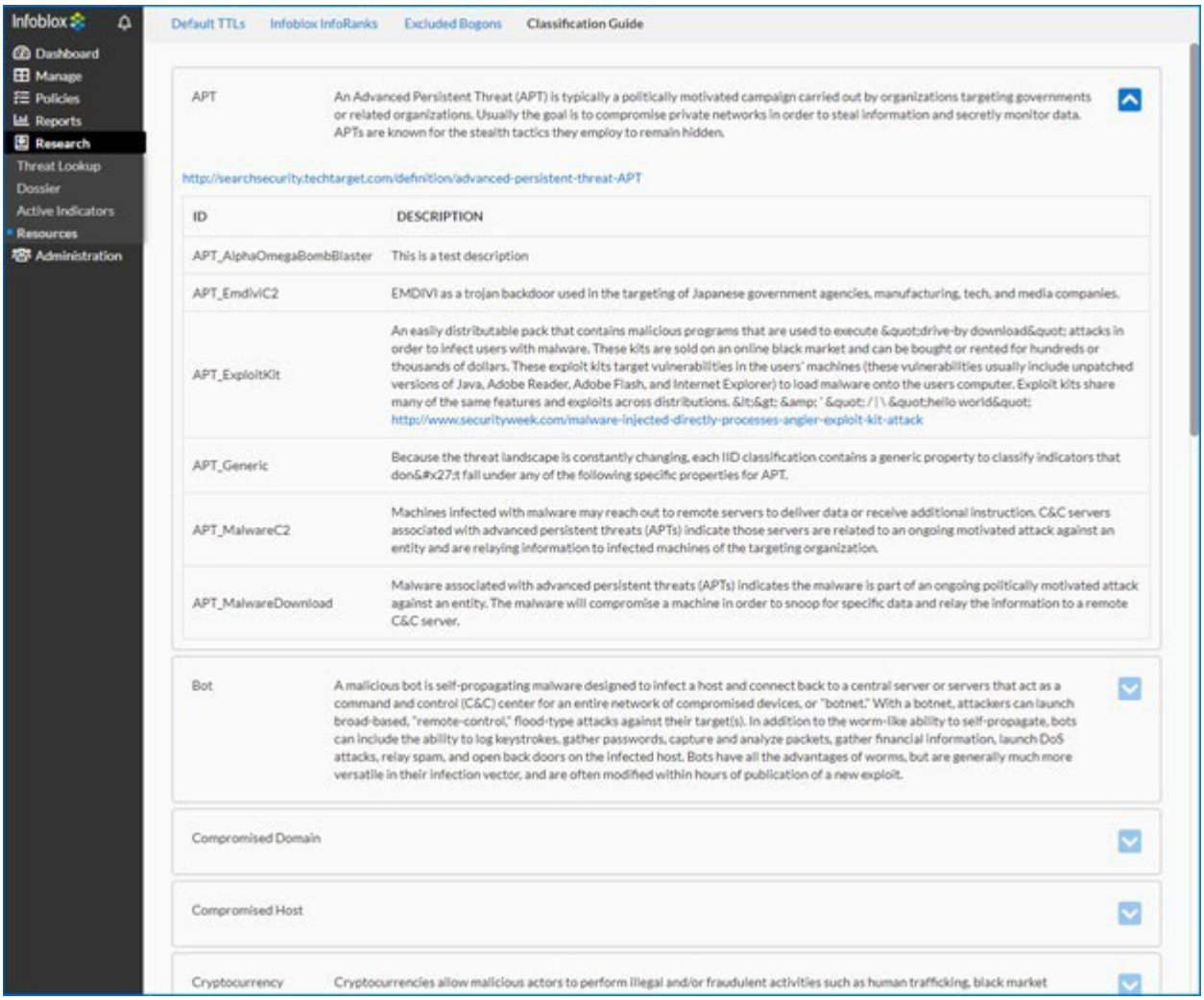

Image 2: Threat Classification Guide

Default TTLs

The default expiration time for all classes can be viewed on the Default TTLs page at **Research** -> **Resources** -> **Default TTLs**.

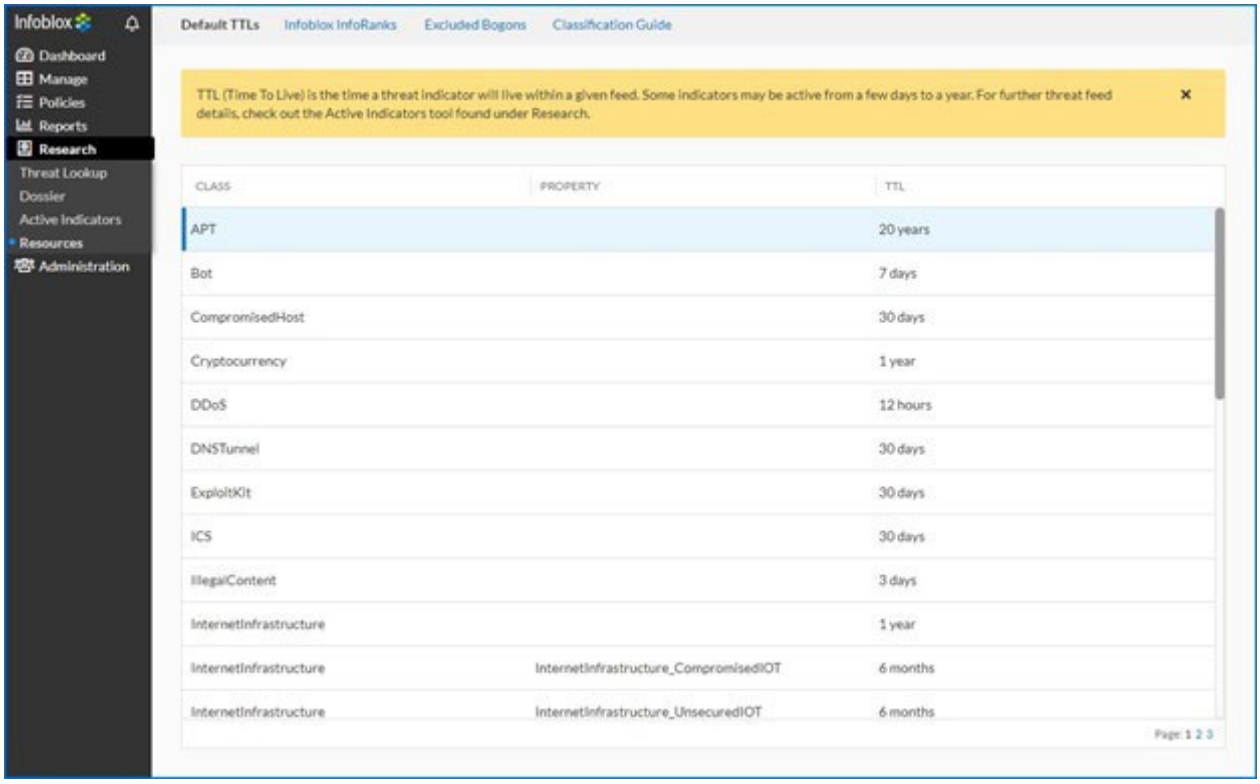

Image 3: Default TTLs

Infoblox Dossier

Infoblox Dossier is available via the web interface and a REST API. The Cloud Services Portal uses the same API so there are no differences in available filters and search results between Web and API searches.

Dossier Search

Dossier Search is located under **Research -> Dossier**, where you can use the following items in the Dossier keyword search field: IPs, URLs, Domains, Hostnames, Email addresses, MD5, SHA1, and SHA256 hashes. Not all features/data providers support all data types, e.g., Alexa supports only hostnames and domains.

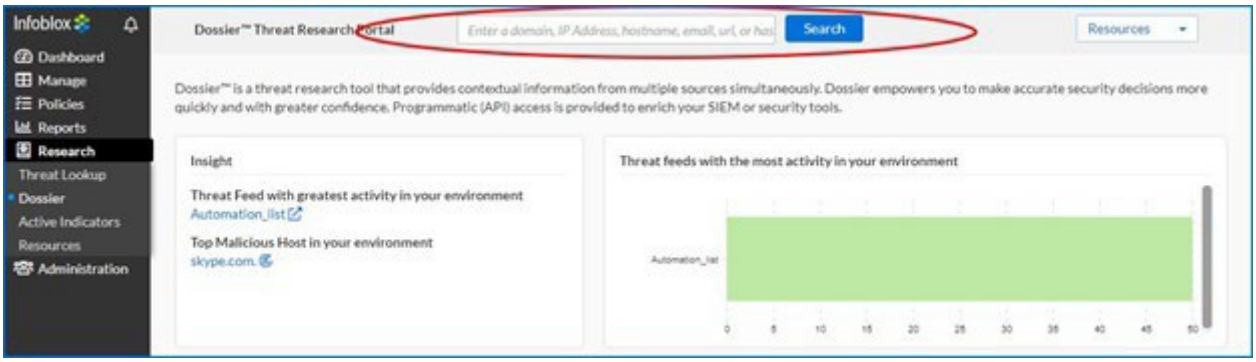

Image 4: Dossier Search

Dossier automatically detects the type of the data in a search field and performs only relevant searches. It’s intelligent and it’s possible to enter domains in a format like: "example[.]com". When a search has been completed, a set of reports are generated.

Dossier Threat Indicator Report

The Dossier Threat Indicator Report is comprised of a dozen or so smaller, self-contained reports, each focusing on a specific type of information reported in the main threat indicator report.

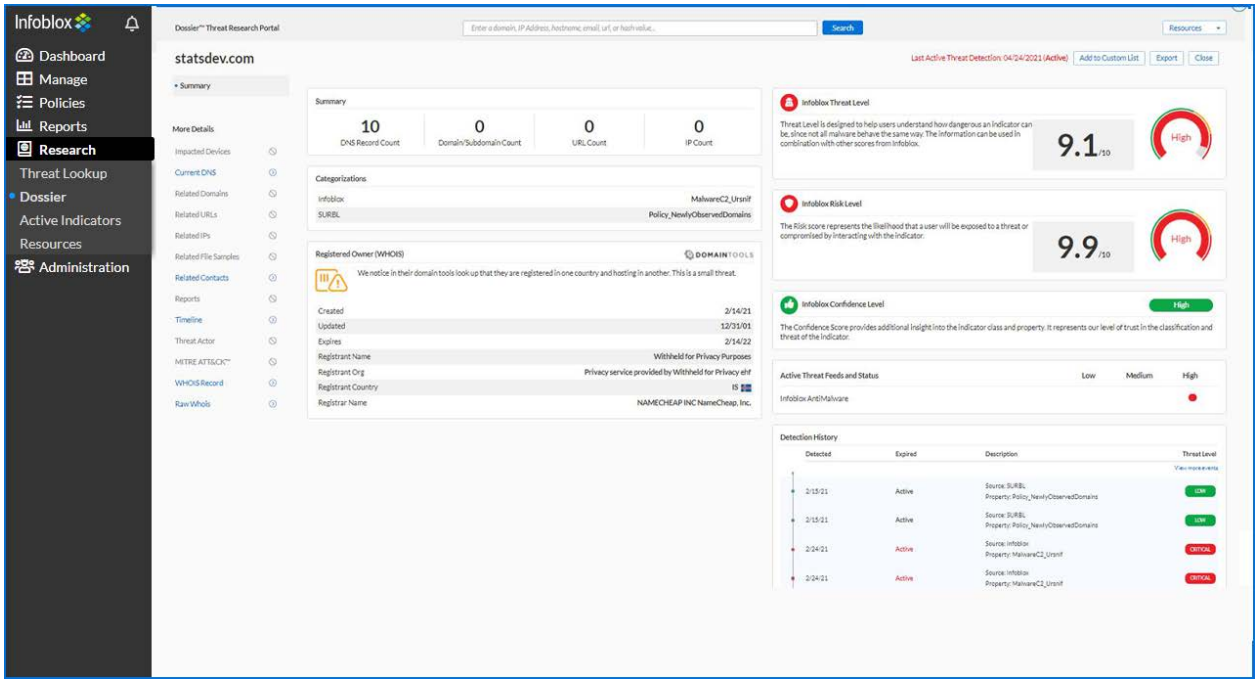

Image 5: Dossier Threat indicator Report (default summary)

All available report types are listed in the left-hand column of the report page. The reports generated include the following:

- **Summary**: The Dossier Summary report provides a comprehensive, one-page report summarizing the information obtained when conducting a threat indicator search on a threat indicator.
- **Impacted Devices**: The Dossier Impacted Devices report provides a comprehensive, one-page report detailing impacted devices information obtained when conducting a threat indicator search on a threat indicator.
- **Current DNS**: The Dossier Current DNS report provides a comprehensive, one-page report detailing current DNS information obtained when conducting a threat indicator search on a threat indicator.
- **Related Domains**: The Dossier Related Domains report provides a comprehensive, one-page report detailing current related domains and subdomains information obtained when conducting a threat indicator search on a threat indicator.
- **Related URLs**: The Dossier Related URLs report provides a comprehensive, one-page report detailing current related URLs information obtained when conducting a threat indicator search on a threat indicator.
- **Related IPs**: The Dossier Related IPs report provides a comprehensive, one-page report detailing current related IPs information obtained when conducting a threat indicator search on a threat indicator.
- **Related File Samples**: The Dossier Related File Samples report provides a comprehensive, one-page report detailing related file samples information obtained when conducting a threat indicator search.
- **Related Contacts**: The Dossier Related Contacts report provides a comprehensive, one-page report detailing related contact information obtained from Whois data reported by DomainTools.
- **Reports**: The Dossier Reports report provides a comprehensive, one-page report listing additional report information obtained when conducting a threat indicator search on a threat indicator.
- **Timeline**: The Dossier Timeline report provides a comprehensive, one-page report detailing timeline information obtained from domain registration records.
- **MITRE ATT&CK™**: **MITRE ATT&CK** is a globally accessible knowledge base of adversarial tactics and techniques based on real-world observations, **MITRE ATT&CK** provides a powerful means of classifying and studying your adversary's techniques and intentions. Only **MITRE ATT&CK** tools relevant to the current search are displayed. You can use **MITRE ATT&CK** to enhance, analyze, and test your threat hunting and detection efforts.

- **Threat Actor**: The Dossier Threat Actor report provides a comprehensive, one-page, score card detailing threat actor information obtained when conducting a threat indicator search on a threat indicator.
- **WHOIS Record**: The **WHOIS Record** report provides a comprehensive, one-page report detailing domain registration, hosting information, and the domain's creation, updated, and expiry dates. The WHOIS Record is based on public records obtained from multiple domain registrations and Internet IP authorities.
- **Raw Whois**: The Dossier Raw WHOIS report provides a comprehensive, one-page report detailing raw WHOIS information that is obtained from the Whois record.

For more information on Dossier Threat indicator Report, refer to the online documentation available *here*.

Dossier API

Dossier API Basic is commonly used by customers. It provides access to all information available on the portal. The **Dossier API Calls Reference** located under the **Resource** options tab on the **Dossier™ Threat Research Portal** page describes all available filters and options. When using the API, the same authentication method as used by other features in the Cloud Services Portal, applies when using the Dossier API.

When you execute a test query, the API returns a CURL command to request the data, response body and a response code. The following example contains a sample CURL command which retrieves information about the **"eicar.top"** domain in JSON format, which is the only supported export format for API based indicator searches.

```
curl -X POST
'https://csp.infoblox.com/tide/api/services/intel/lookup/jobs
?wait=true' \
-H 'Authorization: Token token=<CSP Auth Token>' \
-H 'Content-Type: application/json' \
-d '{"target": {"one": {"type": "host", "target": "1.1.1.1",
"sources":["alexa","atp","dns","gcs","geo","gsb","isight","ma
lware_analysis","pdns","ptr","rlabs","rwhois","sdf",
"whois"]}}}'
```

It may take some time to retrieve data depending on the quantity of data being requested. If the data is not required immediately, then a search can be executed with a **"wait"** parameter set to **"false"** and retrieved later. In this case, the first search will return **"job_id"**. The status of the job and results can be retrieved using a **"lookup_jobs_management"** call. The URL below retrieves results of a job with the **"job_id"** parameter.

```
  https://csp.infoblox.com/tide/api/services/intel/lookup/job
s/job_id/results
```

Infoblox Threat Intelligence Data Exchange (TIDE)

Infoblox Threat Intelligence Data Exchange provides access to highly curated threat indicators and data governance tools to share indicators inside the organization and/or between the organizations.

Indicator Search

Indicator Search is located at **Research** -> **Active Indicators** and is different is than Dossier search, which only returns data from the ActiveTrust database. Indicator search is not limited to a specific indicator (e.g., a hostname). The search interface currently returns a maximum of 25,000 results. It is recommended to use the API for larger data sets.

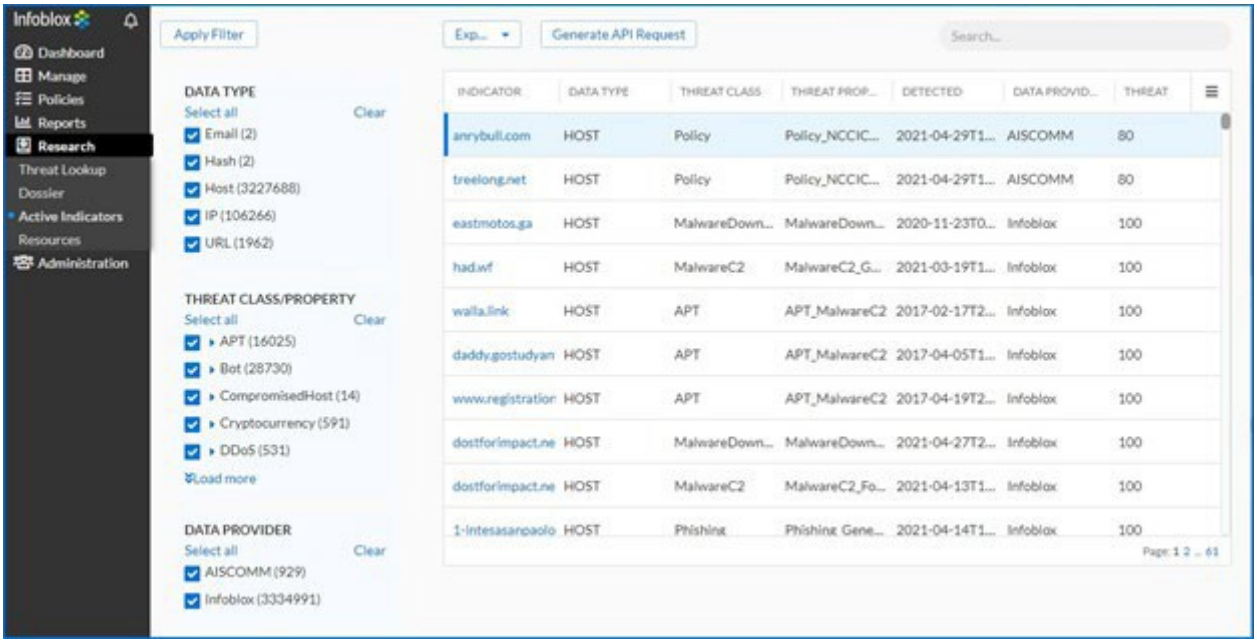

Image 6: Active Indicators search page.

Due to the size of the available data, it is recommended to apply filters to limit the resulting dataset. **NOTE**: When a keyword is used to search data, other filters are not applied even if they were specified.

The resulting dataset can be exported in XML, CSV or JSON format.

Data Management

Dossier and TIDE allows the organization's data administrator to effectively and efficiently manage data with many useful tools including Infoblox InfoRanks, data submission, and the associated data profiles. It also includes the ability to run robust API calls within the Dossier-TIDE ecosystem.

Infoblox InfoRanks

Infoblox InfoRanks provides ranking for the most used sites on the Internet. This tool provides access to the Infoblox InfoRanks Top 10,000 sites. Infoblox InfoRanks provides ranking for the most used sites on the Internet. This tool provides access to the Infoblox InfoRanks Top 10,000 sites and provides ranking based on popularity within the last 7 days.

Data Submission

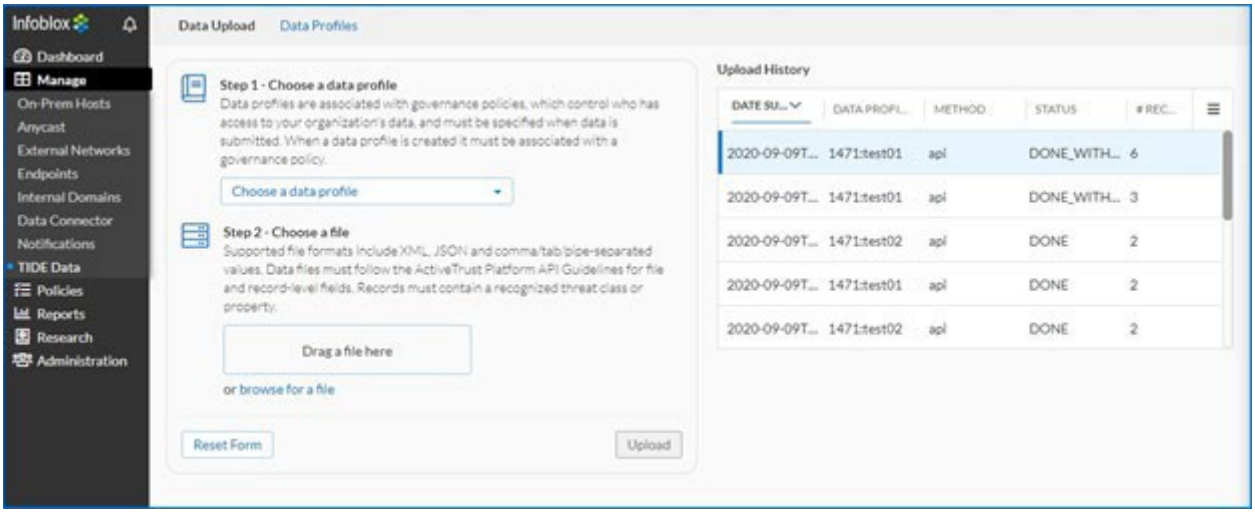

Image 7: TIDE Data Upload page.

Data profiles **Manage** -> **TIDE Data -> Data Profiles** are used to identify data in the platform from one or many data submissions. A data profile must be specified when data is submitted.

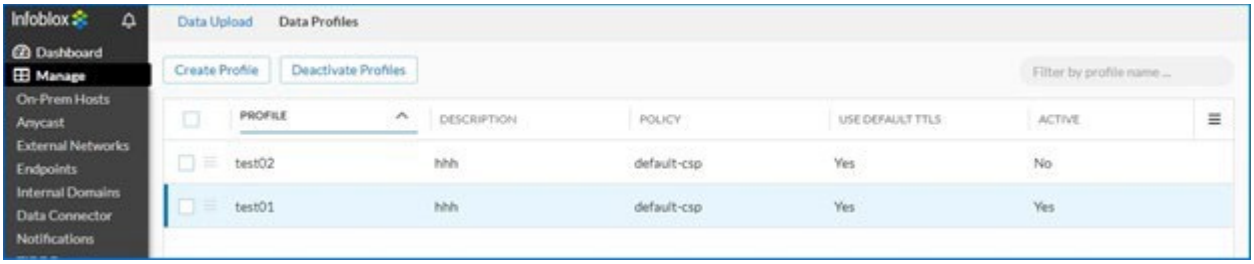

Image 8: TIDE Data Profiles page.

Users can submit threat indicator data through the portal or via Data API using the following formats: JSON, CSV, XML, TSV (tab separated values). For all data formats the submitted data must identify the data/record type in addition to the list of data records. For CSV and TSV the record type must be provided as one of the columns. For JSON and XML the record type is defined in a separate top-level field. The record type field can be one of the following values: **"host"**, **"ip"**, or **"url"**. It is not possible to upload data using different profiles or different record types in the same file. Threat data consists of file level fields and record-level fields. The table below contains descriptions of all available fields.

Data Profiles	
FIELD NAME	**DESCRIPTION**
File-level fields	
profile	data profile id or name
record_type	host, ip, or url
external_id	string indicating an external ID to assign to the batch
record	surrounds the individual record(s) in the XML and JSON formats
Record-level fields	
host	threat hostname
ip	threat IP address
url	threat URL
property	threat type
target	target of threat
detected	date/time threat was detected, in ISO 8601 format
duration	duration of this threat in XyXmXwXdXh format, expiration date will be set to the detected date + this duration

XML format:

```
<feed>
 <profile>SampleProfile</profile>
 <record_type>ip</record_type>
 <record>
 <ip>127.1.0.1</ip>
 <property>Phishing_Phish</property>
 <detected>20170602T154742Z</detected>
 </record>
 <record>
 <ip>8.8.8.8</ip>
 <property>Scanner_Generic</property>
 <detected>19980927T154242Z</detected>
 <duration>42y0m0w0d42h</duration>
 </record>
</feed>
```

JSON format:

```
{
 "feed": {
 "profile": "SampleProfile",
 "record_type": "host",
 "record": [
 {"host": "www.google.com", "property": "Scanner_Generic",
"detected": "19980927T154242Z", "duration: "42y0m0w0d42h"},
 {"host": "www.example.com", "property": "Phishing_Phish",
"detected": "20170602T154742Z"}  ]
 }
}
```

CSV format:

```
    record_type,url,profile,detected,property
  url,"https://example.com/page1.html",
  "SampleProfile","20170602T154742Z",
  "UnwantedContent_Parasite"
  url,"http://example.com/gift.html",
  "SampleProfile","20170602T154742Z",
  "Scam_FakeGiftCard"
```

TIDE API

TIDE API consists of the Data API. The Data API is used to submit and retrieve threat indicators. The Cloud Services Platform provides API Guides, which describe all available filters and options when running API calls. Before using any of the API guides, you need to verify your account using the Cloud Services Platform's token authentication service.

The TIDE API leverages the Basic Auth method in HTTP/HTTPS to transport the API key. The API key is passed in the username field. The password field should be set to an empty string. All data fields (including filter) represented in ISO 8601 format.

Data API

The Data API consist of the following:

- **Threat Batch APIs (batch)**: Used to submit threat indicators and retrieve details about uploaded batches.
- **Property APIs (property)**: Used to retrieve threat properties registered on the Cloud Services Portal.
- **Threat APIs (threat)**: Used to search threat indicators on the Cloud Services Portal.
- **Threat Class APIs (threat_class)**: Used to retrieve threat classes registered on the Infoblox Cloud Services Platform.

Submitting Threat indicators

The following example contains a sample curl command used to submit threat indicators in JSON format to the Cloud Services Portal.

```
curl -X POST -H "Content-Type: application/json" --data-
binary @DATA_FILE_NAME.json
http:// csp.infoblox.com/tide/api/data/batches -u
[YOUR_API_KEY]:
```

The system determines the format of the input data based on the Content-Type HTTP header (application/xml, text/xml, application/json, text/plain, text/csv, text/tab-separated-values, text/tsv, text/psv). If the Content-Type doesn't match with predefined types, or isn't specified, it tries to determine the format dynamically by reading the first part of the data. Best practice is to specify the format in the Content-Type.

Search for Threat Indicators/Export Threat Indicators for 3rd Party Solutions

Data Threat API calls are used to search threat indicators. Submitted threat indicators are also available for the search. The resulting dataset can be formatted in JSON, XML, STIX, CSV, TSV, PSV, CEF.

The threat indicators can be used by 3rd party solutions, e.g., with Palo Alto NGFW (check Implementing Infoblox TIDE feeds into Palo Alto Networks Firewalls deployment guide for details) after a simple post-processing.

It is highly recommended to limit the amount of retrieved data by applying filters. The table below contains sample requests using CURL commands.

Searching and Exporting 3rd-Party Indicators	
REQUEST	**DESCRIPTION**
`curl https://csp.infoblox.com/tide/api/data/threats/host?profile=IID&dga=false&from_date=2017-06-04T00:00:00Z&data_format=csv&rlimit=100 -u [YOUR_API_KEY]:`	1,000 threat indicators in CSV format which were added after 2017-06-04 GMT (Date/Time is in ISO 8601 format) by Infoblox and are not DGA.
`curl "https://csp.infoblox.com/tide/api/data/threats/state/host?Profile=IID&data_format=json" -u [YOUR_API_KEY]:`	All currently active hostname threats detected by Infoblox (IID).
`curl "https://csp.infoblox.com/tide//data/threats?type=host&profile=IID&period=30min&data_format=json" - u [YOUR_API_KEY]:`	Infoblox-sourced hostnames for the past 30 minutes.
`curl "https://csp.infoblox.com/tide/api/data/threats?profile= AIS-FEDGOV,iSIGHTPARTNERS&period=1w&data_format=csv " -u [YOUR_API_KEY]:`	iSight Partners and DHS AIS IPs for the past week in CSV format.

References

1. *Infoblox TIDE API FAQs Guide*.
2. *Infoblox API Getting Started Guide*
3. *Infoblox Dossier™ Call Reference*
4. *https://www.infoblox.com/wp-content/uploads/infoblox-deployment-guide-implementing-infoblox-tide-feeds-into-palo-alto-networks-firewalls.pdf*