# infoblox.

DEPLOYMENT GUIDE

# Infoblox BloxOne<sup>™</sup> Dossier and TIDE

# **Table of Contents**

Overview	2
Prerequisites	2
Access to the Cloud Services Portal	2
Threat Classification Guide	3
Default TTLs	3
Excluded Bogons	4
Viewing Excluded Bogons	4
Infoblox Dossier	5
The Dossier Threat Indicator Report	5
Dossier API	7
Infoblox Threat Intelligence Data Exchange (TIDE)	8
Active Indicator Search	9
Extracting Datasets	9
Data Management	
InfoRanks	
Data Submission	11
Data Profiles	11
TIDE Data API	
Submitting Threat indicators	13
Search for Threat Indicators/Export Threat Indicators for 3rd-Party Solutions	14
References	15

## Overview

Infoblox BloxOne<sup>™</sup> 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<sup>™</sup> is a threat indicator research tool that gives contextual information from dozens of 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 BloxOne Dossier and TIDE.

# Prerequisites

BloxOne Dossier and TIDE are subscription-based services provided in the Infoblox Cloud. There are no specific requirements for software to access the services except a relevant <u>subscription</u>. Recent versions of Google Chrome are recommended to access BloxOne Portal.

# Access to the Cloud Services Portal

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

infoblox 🧳			<u>8</u> (Q)
Dashboard     Manage	Dossier <sup>™</sup> Threat Research Port Enter a	domain, IP Address, Hostname, EMail, URL, or Hash value Search	Resources 🔹
<ul> <li>Policies</li> <li>Reports</li> <li>Research</li> <li>Dossier</li> </ul>	Dossier " is a threat research tool that provides contextual information from m to enrich your SIEM or security tools.	Itiple sources simultaneously. Dossier empowers you to make accurate security decisions more quickly and with greater confidence. Programmati	c (API) access is provided
Active Indicators	Insight	Threat feeds with the most activity in your environment	
Threat Lab	Threat Feed with greatest activity in your environment	EECN_IP	31
😤 Administration	Top Malicious Host in your environment	suspicious-noed	11
	static.noearon.click.	radebauch-customList1	5
	Latest Reports from Infoblox Threat Research		
	Decoy Dog is No Ordinary Pupy: Separating a Sly DNS Malware from the P In April 2023, Infoblox disclosed the discovery of Decoy Dog, a malware tool capabilities and the behaviors of many ofits controller domains in the wild. W	tck dt that uses thedomain name system (DNS) to communicate. Since then, we have continued our investigation and have gained valuable insights into hat we found is alarming and mysterious. This articleprovides a brief overview of our conclusions.	July 29, 2023 Decoy Dog's
	Decoy Dog is No Ordinary Pupy: Separating a Sly DNS Malware from the P	ick	July 29, 2023
	Decoy Dog is a malware toolkit discovered by Infoblox that uses the domain controller is integrated into a DNS name server to which queries are transmi discovery was based on monitoring of DNS data. Analysis at the time confirm or whether Pupy had been modified. We expected that, with the details we p only grown.	name system (DNS) to perform command and control (C2). A compromised client communicates with, and receives direction from, a controller via [ ted through the normal resolution process. We disclosed Decoy Dog's existence in April 2023 and released a detailed report of our initial findings ed that the toolkit was built based on a remote access trojan (RAT) from as Pupto, built wasn't known what systems were being exoluted, built rovided, others in the community would locate the compromised machines and the full story would become known. However, the mystery surround and the store of the community would locate the compromised machines and the full story would become known. However, the mystery surround the store of the community would locate the compromised machines and the full story would become known. However, the mystery surround the store of the store of t	JNS queries. That on April 23rd. The Hoolkit was deployed, Jing Decoy Dog has
	Infoblox Researchers Uncover Malicious Domains Hosting Cryptocurrency	Scams	May 25, 2023
<ul> <li>Infoblox TME</li> <li>Adam Shabir</li> <li>User Agreeme</li> </ul>	Infoblox security researchers have uncovered a group of malicious domains the reviewing and analyzing queries in our networks for domains that incorporat CryptDesignBot. Further open-source intelligence enriched our findings and	hat are being used to host cryptocurrency scams, some of which have been associated with the hacking of Youtube channels. We were able to find t ed certain suspicious keywords. Armed with these initial discoveries, our researchers were able to pivot to other domains belonging to the same re provided greater context, leading us to uncover additional data linked to the ongoing compromise of Youtube channels.	he domains by gistrant organization,
Help	A deep3r look at lookal1ke attacks: new study reveals latest threat vectors		April 27, 2023
Recycle Bin	This report describes the current threat landscape by showcasing real world	examples across industries and user groups. Infoblox has been detecting lookalike domains for years and analyzes over 70 billion domain name syst	em (DNS) events daily.

# **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**  $\rightarrow$  **Resources**  $\rightarrow$  **Classification Guide**.

For more information about a specific threat classification field, click on the down arrow on the right.

infoblox. ♀ ② Dashboard ③ Manage ③ Policies	Default TTLs Infobiox InfoRanks	Excluded Bogons Classification Guide Threat Insight Guide	8
Reports     Research     Dossier     Active Indicators	APT	An Advanced Persistent Threat (APT) is typically a politically motivated campaign carried out by organizations targeting governments or related organizations. Usually the goal is to compromise private networks in order to steal information and secretly monitor data. APTs are known for the stealth tactics they employ to remain hidden.	
Active Indicators • Resources Threat Lab ?몸 Administration	Bot	A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s). In addition to the worm-like ability to self- propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam, and open back doors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector, and are often modified within hours of publication of a new exploit.	
	Compromised Domain		
	Compromised Host		
	Cryptocurrency	Cryptocurrencies allow malicious actors to perform illegal and/or fraudulent activities such as human trafficking, black market sales/purchases, ransomware payments, etc. Cryptocurrencies are used because transactions that involve them are hard to track and do not involve banks or other financial institutions. From a user perspective, mining for cryptocurrencies can require large amounts of computing power, slowing hosts and increasing power costs.	
	DDoS	A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Attackers compromise these systems using a number of different methods, but with the same end results – the overload of some amount of web servers. The major advantages to an attacker of using a distributed denial-of-service attack are that: multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines.	

# Default TTLs

The default expiration time for all classes can be viewed on the Default TTLs (time-to-live) page at **Research**  $\rightarrow$  **Resources**  $\rightarrow$  **Default TTLs**.

infoblox. 🧳					
<ul><li>Dashboard</li><li>Manage</li></ul>	Default TTLs	Infoblox InfoRanks	Excluded Bogons	Classification Guide	Threat Insight Guide
듣 Policies					
🔟 Reports	TTL (Time To Liv	ve) is the time a threat in	ndicator will live withi	n a given feed. Some ind	icators may be active from
🚇 Research					
Dossier	CLASS				
Active Indicators	CLASS				PROPERTY
<ul> <li>Resources</li> </ul>	Δρτ				
Threat Lab					
😤 Administration	Bot				

infoblox. ♀ ② Dashboard ➡ Manage ⇒ Policies ➡ Research	Default TTLs Infobiox InfoRanks Excluded Bogons Classification TTL (Time To Live) is the time a threat indicator will live within a given feed. S	n Guide Threat Insight Guide Some indicators may be active from a few days to a year. For further threat feed details, o	check out the Active Indicators tool found under Research.
Dossier Active Indicators	CLASS	PROPERTY	Π
<ul> <li>Resources</li> <li>Threat Lab</li> </ul>	APT		2 years
器 Administration	Bot		7 days
	CompromisedHost		30 days
	Cryptocurrency		1 year
	Cryptocurrency	Cryptocurrency_Coinhive	60 days
	Cryptocurrency	Cryptocurrency_Cryptojacking	60 days
	Cryptocurrency	Cryptocurrency_Exchange	60 days
	Cryptocurrency	Cryptocurrency_Generic	14 days
	Cryptocurrency	Cryptocurrency_GenericThreat	14 days
	Cryptocurrency	Cryptocurrency_MiningPool	60 days
	DDoS		12 hours
	DNSTunnel		30 days

TTL field here displays the Time To Live for the Threat Indicator.

#### **Excluded Bogons**

A bogon is an internet address prefix that should never appear in an IP address routing table. The Excluded Bogon page allows administrators to view invalid IP ranges that can be used by malicious entities.

#### **Viewing Excluded Bogons**

To view Excluded Bogons, perform the following:

- 1. From the Cloud Services Portal, click **Research**  $\rightarrow$  **Resources**.
- 2. On the Resources page, click **Excluded Bogons** in the top menu.
- 3. On the Excluded Bogons page, a list of excluded bogons is displayed.

infoblox. 🗘		
<ul><li>Dashboard</li><li>Manage</li></ul>	Default TTLs Infoblox InfoRanks Excluded Bogons Classification Guide Threat Insight Guid	e
⅔ Policies	A bogon is an internet address prefix that should never appear in an IP address routing table. The Excluded	Bogg
Reports		0050
Dossier	Excluded Bogons Last Updated: 2016-04-26T22:43:21.713Z	
Resources	10.0.0/8	
Threat Lab	172.16.0.0/12	
答 Administration	192.168.0.0/16	

#### **Infoblox Dossier**

Dossier Search is located under **Research**  $\rightarrow$  **Dossier**. You can use the following items in the Dossier keyword search field: IPs, URLs, domains, Host names, Email addresses, MD5, SHA1, and SHA256 hashes. Not all features/data providers support all data types.

Dossier™ Threat Research Portal	ame, EMail, URL, or Histh value	Resources 🔻
Dossier <sup>®</sup> is a threat research tool that provides contextual information from multiple sources simultaneously. Do	sier empowers you to make accurate security decisions more quickly and with greater confidence. Programmatic (API) access is provided to enrise	ich your SIEM or security tools.
Insight	Threat feeds with the most activity in your environment	
Threat Feed with greatest activity in your environment	NCCIC_IP	886
	Public_DOH	91
Top Malicious Host in your environment	pparker-custom-list	20
cuul windowsupuate.com.	Bogon	13

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 search is available via the web interface and a REST API. The portal uses the same API so there is no difference in filters and search results between Web and API searches.

## The Dossier Threat Indicator Report

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

infoblox. 4 Dashboard Manage	Dossier™ Thi	reat Rese	arch Port	lomain, IP Address, Hostname, EMail,	URL, or Hash value	Search	Resources 🔹
<ul><li>Policies</li><li>Reports</li><li>Research</li></ul>	cofi.hk			Last Active Th	reat Detection: 07/06/2023	(Active) Add to Custom List Generate API Request Feedb	ack on Results Export
Dossier     Active Indicators	Summary						
Resources Threat Lab 🕾 Administration	More Details		Summary	Domain Screen Image		Threat Level is designed to belo users understand how	
	Impacted Devices	$\otimes$	🔷 COFI		=	dangerous an indicator can be, since not all malware	High
	Current DNS	0	Buy,	invest & trad	behave the same way. The information can be used in		
	Related Domains	0	on th	on the most trusted crypto exchange Colhapored the concept of semics trading of different coptocements as the		combination with other scores from Infoblox.	
	Related URLs	$\odot$	cry				
	Related IPs	٥	Cofi has pir			Infoblox Risk Level	
	Related File Samples	$\odot$		Starttrading ≯ Invest →		The Risk score represents the likelihood that a user will be	High
	Related Contacts	$\odot$				exposed to a threat or compromised by interacting	• •
	Metadata	0	0		27	with the indicator.	
	Timeline	$\odot$	DNS Record Count Domai	in/Subdomain URL Count	30 IP Count	Infoblox Confidence Level	Medium
	Threat Actor	$\odot$		Count		The Confidence Score provides additional insight into the indicat	or class and property. It
	MITRE ATT&CK™	$\odot$	Categorizations			represents our level of trust in the classification and threat of the	indicator.
2	WHOIS Record	0	Infoblox Info	Virus Total key has not yet been	configured for this ac	Infoblox Threat Intelligence Group Research Notes	

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

Note: The available report types may change based on the IOC being researched.

- **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 sub-domains 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.
- **Metadata:** Metadata displays web content related to the indicator from around the web. These may be malicious, as they are unfiltered and listed to give an overall perspective on the nature of this indicator.
- **Timeline**: The Dossier Timeline report provides a comprehensive, one-page report detailing timeline information obtained from domain registration records.

- **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.
- MITRE ATT&CK: MITRE ATT&CK is a globally accessible knowledge base of adversarial tactics and techniques based on real-world observation.
- WHOIS Record: The WHOIS Record displays location data for a registrant and for the host of a domain or IP address, including domain registration, hosting information, and the domain's creation, updated, and expiry date
- **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 the Dossier Threat indicator Report, refer to the online documentation available <u>here</u>.

#### **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 **Resources** 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.

		z (
Dossier <sup>™</sup> Threat Research Portal	domain, IP Address, Hostname, EMail, URL, or Hash value Search	Resources -
	Dossier & T	IDE Quick Start Guide
ssier™ is a threat research tool that provides contextual information from multiple s	succes simultaneously. Dossier empowers you to make accurate security decisions more quickly and with greater confidence. Programmatic (API) access is pro	Calls Reference
	Dossier Sou	rce Descriptions
neight .	Threat feeds with the most activity in your environment Dossier Use	r Guide
bigit	Threat Class	sification Guide
nreat Feed with greatest activity in your environment	NCCIC_IP	886
	Public_DOH	91
op Malicious Host in your environment	pparker-custom-list	20
ttd.windowsupdate.com.	Bogon	13
	-	

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.

```
"type": "host",
             "target": "1.1.1.1",
             "sources": [
                 "acs",
                 "activity",
                 "atp",
                 "ccb",
                 "custom lists",
                 "dns",
                 "gcs",
                 "geo",
                 "gsb",
                 "infoblox_web_cat",
                 "inforank",
                 "isight",
                 "malware analysis",
                 "malware analysis v3",
                 "pdns",
                 "ptr",
                 "rlabs",
                 "rpz feeds",
                 "rwhois",
                 "whitelist",
                 "whois",
                 "ssl cert",
                 "urlhaus",
                 "nameserver",
                 "threatfox"
             ]
        }
    }
} '
```

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. Here, 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.

# 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.

Infoblox TIDE uses a powerful REST API allowing access to indicators of compromise in the TIDE database in formats like JSON, XML, STIX, CEF, CVS, etc. This allows easy integrations with other solutions without additional transformation/mediation layers. SIEM, NGFW, SWG are good examples where the indicators can be applied to improve overall security in an organization.

# **Active Indicator Search**

Active Indicator Search is located at **Research**  $\rightarrow$  **Active Indicators** and is different from Dossier search, which only returns data from the database. Indicator search is not limited to a specific indicator (e.g., a hostname). The search interface currently returns limited results. There is no limit to the number of records that can be returned via API. Therefore, it is recommended to use the API for larger data sets.

Filter	Apply Filter	Export • Genera	te API Request				Search		
Data Type		INDICATOR	DATA TYPE	THREAT CLASS	THREAT PROPERTY	DETECTED	DATA PROVIDER	THREAT	=
Select all	Clear (10)	autosale.buzz	HOST	Policy	Policy_NCCICwatchlist	2022-11-16T20:01:29.8	AISCOMM	80	
✓ Hash	(440)	autosale.buzz	HOST	MalwareC2	MalwareC2_Generic	2022-11-16T20:01:29.8	AISCOMM	80	
IP	(4,877,537)	ois.is	HOST	Policy	Policy_NCCICwatchlist	2022-11-17T16:01:25.1	AISCOMM	80	
VRL	(147,225)	sinkhole.eicar.network	HOST	Sinkhole	Sinkhole_Generic	2017-07-24T17:27:39.4	AISCOMM	100	
Select all	Clear	compromiseddomain.eicar.	HOST	CompromisedDomain	CompromisedDomain_G	2017-07-24T17:24:54.7	AISCOMM	75	
<ul> <li>API</li> <li>CompromisedE</li> </ul>	(4,514) Domain (2)	example.versisoton.com	HOST	Policy	Policy_NCCICwatchlist	2022-11-17T16:46:28.9	AISCOMM	80	
<ul> <li>Compromised</li> <li>Cryptocurrency</li> </ul>	Host (1) y (351)	malwarec2.eicar.network	HOST	MalwareC2	MalwareC2_Generic	2017-07-24T17:22:09.3	AISCOMM	100	
DDoS + Show more	(103)	maliciousnameserver.eicar.	HOST	MaliciousNameserver	MaliciousNameserver_G	2017-07-24T17:27:11.2	AISCOMM	100	
Data Provider		apt.eicar.network	HOST	APT	APT_Generic	2017-07-24T17:24:26.6	AISCOMM	100	
Select all           AISCOMM           Infoblox	Clear (406) (5,261,768)	compromisedhost.eicar.net	HOST	CompromisedHost	CompromisedHost_Gen	2017-07-24T17:22:40.0	AISCOMM	100 Page: 1 2	2 82

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.

You can use the API/CURL Command to Retrieve All Active Indicators Data. To pull all Active Threats indicator data, perform the following:

- 1. From the Cloud Services Portal, click Research  $\rightarrow$  Active Indicators.
- 2. Click Generate API Request to generate the CURL command for downloading all records.
- 3. From the Generate API Request pop-up window, copy the CURL command to run the PULL request.

<b>Filter</b>	Apply Filter	Export  Generate API Request Search	h
Data Type		IND Generate API Request	OVIDER
Select all	Clear (10)	sup curl -X GET -H "Authorization: Token token= <api_key>" "https://csp.infoblox.com/tide/api/data/threats?type=email" blox</api_key>	
Hash	(10)	hel blox	
Host	(5,539,969)	OK	
IP	(238,479)		
URL	(146,657)	jkukuj47@gmail.com EMAIL MalwareC2 MalwareC2_Generic 2022-03-16T22:40:4 Infoblox	

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

#### **Extracting Datasets**

The datasets can be exported in XML, CSV or JSON format. To extract in any format, do the following:

1. Click on Research  $\rightarrow$  Active Indicators.

infoblox. 🧷					
🐵 Dashboard	_				
🖽 Manage	<b>Filter</b>	Apply Filter	Export 🔹	Generate API Request	
듣 Policies			CSV		
🔟 Reports			JSON		
🚇 Research	Data Type		XMI	DATA TIPE	THREAT CLASS
Dossier	Select all	Clear	compromised	Jost.eicar.net HOST	CompromisedHost
<ul> <li>Active Indicators</li> </ul>	🗹 Email	(1)			· · · · · · · · · · · · · · · · · · ·
Resources	🗹 Hash	(12,257)	webappattack	.eicar.networ HOST	WebAppAttack
Threat Lab	🗹 Host	(17,494,631)			
😤 Administration	🔽 IP	(1,150,187)	webdata.ohca.	skyoffices.co HOST	UncategorizedThreat

2. Click on **Export** and click on the required format in the dropdown menu. This will download the dataset in the selected format.

#### Data Management

Dossier and TIDE allow 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.

#### InfoRanks

Infoblox InfoRanks provides rankings 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. Navigate to **Research**  $\rightarrow$  **Resources**  $\rightarrow$  **Infoblox InfoRanks** 

infoblox. 🧷		
Dashboard	Default TTLs Infoblox InfoRanks Excluded Bogons Classification Guide Threat Insight Guide	
H Manage		
Reports	The InfoRanks list provides the most popular second-level domains (SLDs) updated each day from an aggregated dataset based on DN	NS records from various
🚊 Research	combination with statistical inference techniques to accurately estimate the SLDs' true ranks over time. You can filter the results by D	omain or Rank by clicki
Dossier		
Active Indicators	Find Search Go	
<ul> <li>Resources</li> <li>Threat Lab</li> </ul>	RANK A DOMAIN	INTERVAL
谷子 Administration	1 amazonaws.com	[1, 1]
	2 akamaiedge.net	[2, 3]

InfoRanks returns the ranking of host indicators curated on the Infoblox InfoRank list. The InfoRank list provides the most popular second-level domains (SLDs) updated each day from an aggregated dataset based on DNS records from various data sources. The process to determine the rank for each domain uses count information in combination with statistical inference techniques to accurately estimate the SLDs' true ranks over time.

#### **Data Submission**

Customers can submit/upload their own threat indicator data via the API or via the Cloud Services portal under Manage  $\rightarrow$  TIDE Data  $\rightarrow$  Data Upload.

Infoblox 4 Dashboard Manage	Data Upload Data Profiles Custom RPZ Country Based RPZ	
IPAM/DHCP DNS Keys Infrastructure NTP Anycast External Networks Routing	<ul> <li>Step 1 - Choose a data profile</li> <li>Data profiles are associated with governance policies, which control who has access to your organization's data, and must be specified when data is submitted. When a data profile is created it must be associated with a governance policy.</li> <li>Choose a data profile</li> <li>Step 2 - Choose a file</li> <li>Supported ble formate include XML_ISON and common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common/tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files must follow the common (tab (sing concepted values. Data files.))</li> </ul>	Upload History
Endpoints Internal Domains Data Connector Discovery Notifications * TIDE Data 2 Policies	ActiveTrust Platform API Guidelines for file and record-level fields. Records must contain a recognized threat class or property.  Drag a file here or browse for a file	

#### **Data Profiles**

**Manage**  $\rightarrow$  **TIDE Data**  $\rightarrow$  **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.

infoblox. ♀	Data Upload Data Profiles Custom RPZ	Country Based RPZ			
IPAM/DHCP DNS Keys Infrastructure NTP Anycast External Networks Routing Endpoints Internal Domains Data Connector Discovery Notifications TIDE Data	Create Profile Deactivate Profiles				
	PROFILE	▲ DESCRIPTION	FEED NAME	USE DEFAULT TTLS	ACTIVE
	□			Yes	Yes
	$\Box \equiv$ test-profile			No	Yes

Users can submit threat indicators through the portal or via Data API. In order to submit data, a data profile must be created. Users can submit data 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 comprises 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></feed>
<profile>SampleProfile</profile>
<record_type>ip</record_type>
<record></record>
<ip>127.1.0.1</ip>
<property>Phishing_Phish</property>
<pre><detected>20170602T154742Z</detected></pre>
<record></record>
<ip>8.8.8.8</ip>
<property>Scanner Generic</property>
<pre><detected>19980927T154242Z</detected></pre>
<duration>42y0m0w0d42h</duration>

**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 Data API

The Data API is used to submit and retrieve threat indicators. The Cloud Services Platform provides <u>API</u> <u>Guides</u>, which describes 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.

To create a user API key please refer to the <u>Infoblox documentation</u>. You can learn more about the Tide Data APIs <u>here</u>.

#### **Submitting Threat indicators**

The following example contains a sample curl command used to submit threat indicators in JSON format to the Cloud Services Portal. 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			
<pre>curllocation 'https://csp.infoblox.com/tide/api/data/threats /host?profile=IID&amp;dga=false&amp;from_date=2017-06-0 4T00%3A00%3A00Z&amp;data_format=csv&amp;rlimit=100' \header 'Authorization: Token <api_key_from_csp>'</api_key_from_csp></pre>	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.			
<pre>curllocation 'https://csp.infoblox.com/tide/api/data/threats /state/host?Profile=IID&amp;data_format=json' \header 'Authorization: Token <api_key_from_csp>'</api_key_from_csp></pre>	All currently active hostname threats detected by Infoblox (IID).			
<pre>curllocation 'https://csp.infoblox.com/tide/api/data/threats ?type=host&amp;profile=IID.=30min&amp;data_format =json' \header 'Authorization: Token <api_key_from_csp>'</api_key_from_csp></pre>	Infoblox-sourced hostnames for the past 30 minutes.			

```
curl --location
'https://csp.infoblox.com/tide/api/data/threats
?profile=IID&period=1w&data_format=csv%20' \
--header 'Authorization: Token
<API_Key_from_CSP>'
```

#### References

- 1. Infoblox TIDE API FAQs Guide.
- 2. Infoblox API Getting Started Guide
- 3. Infoblox Dossier<sup>™</sup> Call Reference
- 4. Implementing Infoblox TIDE feeds into Palo Alto Networks Firewalls (PDF)

# infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters 2390 Mission College Blvd, Ste. 501 Santa Clara, CA 95054 +1.408.986.4000 www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).