

ThreatQuotient



Infoblox BloxOne CDF

Version 1.0.0

June 09, 2024

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation..... 8

Configuration 9

ThreatQ Mapping..... 12

 Infoblox BloxOne - DNS Events..... 12

Average Feed Run..... 14

Change Log 15

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com

Support Web: <https://support.threatq.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.26.0
Support Tier	ThreatQ Supported

Introduction

The Infoblox BloxOne CDF retrieves DNS Events from the InfoBlox BloxOne Cloud platform and ingests the data into the ThreatQ platform in the form of Events and Related Indicators.

The integration provides the following feed:

- **Infoblox BloxOne - DNS Events** - retrieves DNS events and related indicators from InfoBlox BloxOne.

The integration ingests Event and Indicator type system objects.

Prerequisites

The following is required in order to run the integration:

- An Infoblox BloxOne instance.
- An Infoblox BloxOne API Key.

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. The feed will be added to the integrations page. You will still need to [configure and then enable](#) the feed.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.


To configure the integration:


1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.


3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API IP/Hostname	Enter your Infoblox BloxOne instance hostname or IP address.
API Key	Enter your API key for your Infoblox BloxOne instance.
Add RPZ Events	Optional - Enable this parameter to ingest Infoblox BloxOne events as ThreatQ events.
	 While the RPZ Filters listed below are optional, it is highly recommended that you utilize them in order to avoid ingesting an extreme amount of events.
RPZ Network (If Add RPZ Events is selected)	Optional - Filter RPZ events by Source Network (NAT case) / On-Prem Host name / AT Endpoint.
RPZ Query IP (If Add RPZ Events is selected)	Optional - Filter RPZ events by the device IP that sent the DNS query.

PARAMETER	DESCRIPTION
RPZ Policy Name <i>(If Add RPZ Events is selected)</i>	Optional - Filter RPZ events by the policy on InfoBlox BloxOne that created the event.
RPZ Threat Level <i>(If Add RPZ Events is selected)</i>	Optional - Filter the RPZ events by the threat level of the event. Options include: <ul style="list-style-type: none"> ◦ Low ◦ Medium ◦ High
RPZ Threat Category <i>(If Add RPZ Events is selected)</i>	Optional - Filter the RPZ events by the Threat Category (Threat Class).
Add Analytic Events	Optional - Enable this parameter to ingest Infoblox BloxOne analytic (Threat Insight) events into ThreatQ. <div>  <p>While the Analytic Filters listed below are optional, it is highly recommended that you utilize them in order to avoid ingesting an extreme amount of events.</p> </div>
Analytic Network <i>(If Add Analytic Events is selected)</i>	Optional - Filter Analytic events by Source Network (NAT case) / On-Prem Host name / AT Endpoint.
Analytic Query IP <i>(If Add Analytic Events is selected)</i>	Optional - Filter Analytic events by the device IP that sent the DNS query.
Analytic Policy Name <i>(If Add Analytic Events is selected)</i>	Optional - Filter Analytic events by the policy that created the event.
Analytic Threat Level <i>(If Add Analytic Events is selected)</i>	Optional - Filter Analytic events by the threat level. Options include: <ul style="list-style-type: none"> ◦ Low ◦ Medium

PARAMETER	DESCRIPTION
	◦ High
Analytic Threat Category <i>(If Add Analytic Events is selected)</i>	Optional - Filter Analytic events by the Threat Category (Threat Class).

< Infoblox BloxOne - DNS Events



Disabled ☒ Enabled
Uninstall

Additional Information

Integration Type: Feed
Version:

Configuration
Activity Log

API IP/Hostname
Hostname or IP address of the Infoblox BloxOne instance

API Key
This is the API Key used to connect to your Infoblox BloxOne instance. Your API Key can usually be found under User Preferences (bottom left corner).

☒ **Add RPZ Events**
(Optional) Select this box if you want to upload Infoblox BloxOne RPZ events to ThreatQ. The data will be uploaded as ThreatQ Events with related indicators. **WARNING:** Although the RPZ parameters are optional, your TQ instance could be flooded with an enormous amount of events if they are not used.

RPZ Network
(Optional) Source Network (NAT case) / On-Prem Host name / AT Endpoint

RPZ Query IP
(Optional) Device IP that sent the DNS query

RPZ Policy Name
(Optional) Policy on Infoblox BloxOne that created an RPZ event

RPZ Threat Level
LOW
(Optional) Threat level of an RPZ event in Infoblox BloxOne

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Infoblox BloxOne - DNS Events

The Infoblox BloxOne - DNS Events feed ingests DNS Events from a Infoblox BloxOne cloud instance.

GET https://{{hostname}}/api/dnsdata/v2/dns_event

Sample Response:

```
{
  "result": [
    {
      "app_category": "",
      "app_name": "",
      "category": "",
      "confidence": "HIGH",
      "country": "",
      "device": "test-VirtualBox",
      "dhcp_fingerprint": "",
      "dns_view": "",
      "endpoint_groups": "All BloxOne Endpoints (Default)",
      "event_time": "2024-05-29T08:07:22.000Z",
      "feed_name": "Default Block",
      "feed_type": "FQDN",
      "mac_address": "08:00:27:97:03:68",
      "network": "BloxOne Endpoint",
      "os_version": "Ubuntu 24.04 LTS",
      "policy_action": "Block",
      "policy_name": "Default Global Policy",
      "private_ip": "10.0.2.15",
      "qip": "84.232.150.150",
      "qname": "shadowserver.org.",
      "qtype": "A",
      "rcode": "NXDOMAIN",
      "rdata": "NXDOMAIN",
      "rip": "84.232.150.150",
      "severity": "MEDIUM",
      "tclass": "DefaultCustomList",
      "tfamily": "Default Block",
      "threat_indicator": "shadowserver.org",
      "tproperty": "Default Block",
      "user": "test",
      "user_groups": "$ib_authn_b1e$"
    }
  ],
  "status_code": "200"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result[].tproperty, result[].event_time	Event.Title	N/A	result[].event_time	Default Block - 2024-05-29	Only for Analytic events
result[].qname	Event.Title	N/A	result[].event_time	shadowserver.org.	Only for RPZ events
result[].event_time	Event.Happened_At	N/A	result[].event_time	2024-05-29T08:07:22.000Z	N/A
result[].tproperty	Event.Attribute	Link to Event on InfoBlox	result[].event_time	{.hostname}/#/atlas/app/tab/atc/reports/security-activity/threat-insight/view/Default Block/detections	Only for Analytic events
result[].rcode	Event.Attribute	Response Type	result[].event_time	NXDOMAIN	N/A
result[].severity	Event.Attribute	Severity	result[].event_time	MEDIUM	If the attribute already exists, the value will be updated
result[].policy_name	Event.Attribute	Policy Name	result[].event_time	Default Global Policy	N/A
result[].device	Event.Attribute	Device	result[].event_time	test-VirtualBox	N/A
result[].confidence	Event.Attribute	Confidence	result[].event_time	HIGH	If the attribute already exists, the value will be updated
result[].tclass	Event.Attribute	Threat Class	result[].event_time	DefaultCustomList	N/A
result[].qip	Related.Indicator	IP Address	result[].event_time	84.232.150.150	N/A
result[].qname	Related.Indicator	FQDN	result[].event_time	shadowserver.org.	Only for RPZ events
result[].rdata	Related.Indicator	IP Address	result[].event_time	NXDOMAIN	Only for RPZ events

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	2 minutes
Events	4
Event Attributes	28

Change Log

- Version 1.0.0
 - Initial release