

DEPLOYMENT GUIDE

Infoblox BloxOne Add-on For Splunk (Enterprise & Cloud)

Table of Contents

Introduction.....	2
Prerequisites.....	2
Infoblox.....	2
Splunk.....	2
Known Limitations.....	2
Deploying and Using the Application.....	2
Configure the Data Connector.....	2
Configure Splunk.....	7
Install from Splunk Web UI.....	7
Download from SplunkBase (For Splunk Enterprise Only).....	9
Application Navigation.....	10
BloxOne Dashboards.....	12
Security Events Dashboard.....	12
DHCP Overview Dashboard.....	12
DNS Events Dashboard.....	13
B1TD Filters Dashboard.....	13
Events by Queries/Source IP Dashboard.....	14
Infoblox Threat Intelligence Data.....	14
Dossier.....	16
Additional Resources.....	18

Introduction

The Infoblox BloxOne® add-on for Splunk provides users the ability to view high level information about their Network's data from the BloxOne platform. The application contains predefined dashboards where users can see insights into DNS, DHCP, and Security Activity data in Splunk. Users have the ability to update dashboards as per their requirements. Please note that this Splunk add-on is not officially supported by Infoblox.

Prerequisites

The following are prerequisites for the Infoblox BloxOne Add-on for Splunk:

Infoblox

1. Infoblox BloxOne with a valid [DDI](#) or [Threat Defense](#) License.
2. An OPH (On-Prem Host) with the Data Connector service enabled. For deploying the Data Connector, refer to [this guide](#).

Splunk

1. Splunk Account, to download and install the application from Splunkbase.
2. Splunk Enterprise or Cloud with a valid license. For more information refer to the [Splunk Documentation](#).

Known Limitations

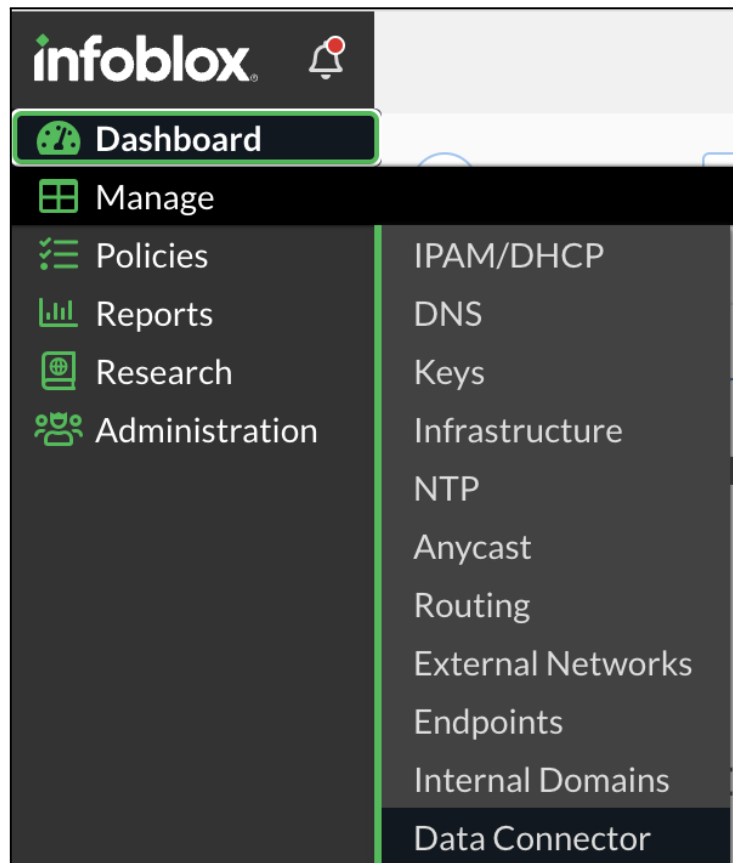
For the full functionality of the Infoblox BloxOne add-on users need to have a CSP account with access to an Infoblox CSP tenant with a BloxOne DDI and Threat Defense licenses. The application works even with one of mentioned licenses in that case the dashboards will show limited insights specific only to the available license.

Deploying and Using the Application

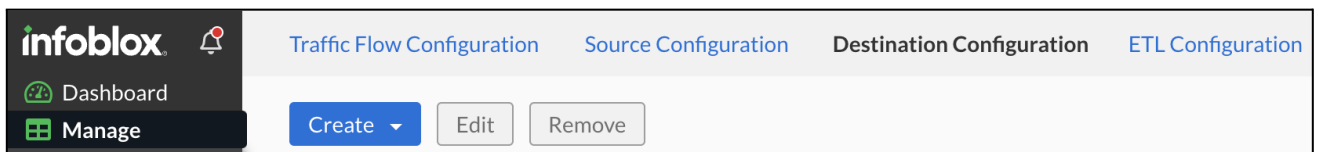
Configure the Data Connector

To use the Splunk BloxOne application a source and destination for the data connector is required. Perform the following steps to configure the Data Connector.

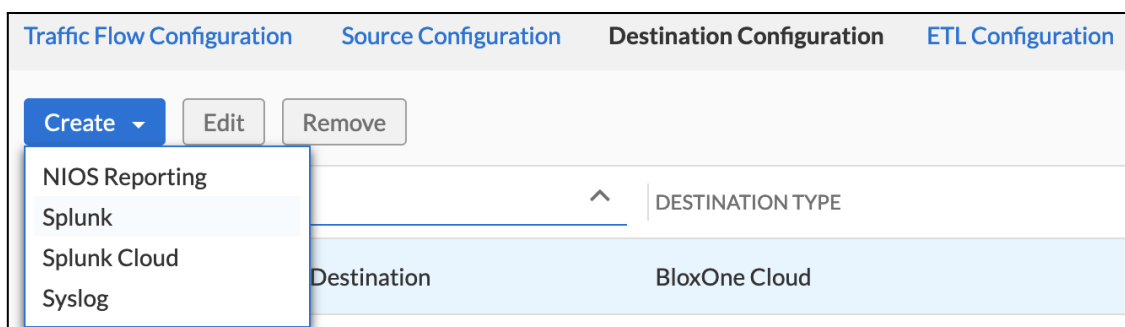
1. On the Infoblox CSP highlight on **Manage**, then click on **Data Connector** in the list that is revealed.



2. On the Data Connector page, click on the **Destination Configuration** tab located on the top of the Data Connector Page.



3. To create a new source, click on **Create** and then click on **Splunk** for Splunk Enterprise or **Splunk Cloud** for the Splunk Cloud instance in the list that is revealed.



4. Follow one of the below steps to create destination configuration based on the selection in step 3.
 - For Splunk Enterprise, on the **Create Splunk Destination Configuration** screen, enter the details of the Splunk Enterprise server (refer [Setting up Splunk](#) for more details).
 - Enter a **Name** for the configuration.

- Under **Splunk Details**, Enter the FQDN or the IP address of the Splunk indexer along with the port. For this deployment, put the **Index Name** as “main”.

- Enable the destination by changing **State** to Enabled.

- For Splunk Cloud, on the **Create Splunk Cloud Destination Configuration** screen, enter the details of the Splunk Cloud server (refer [Setting up Splunk Cloud](#) for more details).

- Enter **Name** of the configuration.

- Splunk cloud configuration can be imported or manually configured. If the configuration is imported it auto-fills the configuration details.
- If Import configuration is selected in **Config Options**, use the downloaded Universal Forwarder Credential config file (splunkclouduf.spl) for **Splunk Cloud Configuration**. (go to **Apps > Universal Forwarder**. Click **Download Universal Forwarder Credentials**.)

SPLUNK CLOUD CONFIGURATION IMPORT

*Splunk Cloud Configuration Select file
splunkclouduf.spl

- All the details except the index will be auto-filled if configuration is imported,, else for manual configuration, fill in the required details. For this deployment, put the **Index Name** as “main”

CONNECTION DETAILS

*FQDN/IP & Port
Example: 10.10.10.1:9997,10.10.10.2:9997

*Index Name

Log Format Splunk CIM

FORWARDER CERTIFICATE

Forwarder Certificate Select file
splunkclouduf.spl

*Certificate Key Passphrase

CA CERTIFICATE

CA Certificate Select file
splunkclouduf.spl

- Enable the configuration by changing the **State** to Enabled.

State **Enabled**

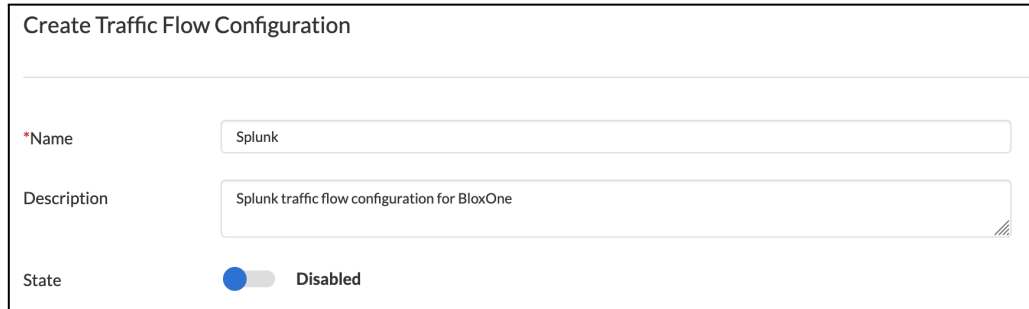
- To confirm the creation of the Splunk Destination, click **Save & Close**.
- Click on the **Traffic Flow Configuration** tab located near the top of the Data Connector page. Then, click the **Create** button to create a new Traffic Flow configuration.

Traffic Flow Configuration [Source Configuration](#) [Destination Configuration](#) [ETL Configuration](#)

Create Edit Remove Refresh

7. In the **Create Traffic Flow Configuration** screen, the below details are to be filled.

- Enter the **Name** and description of the configuration.



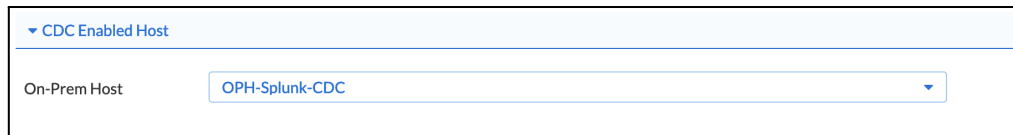
Create Traffic Flow Configuration

Name

Description

State Disabled

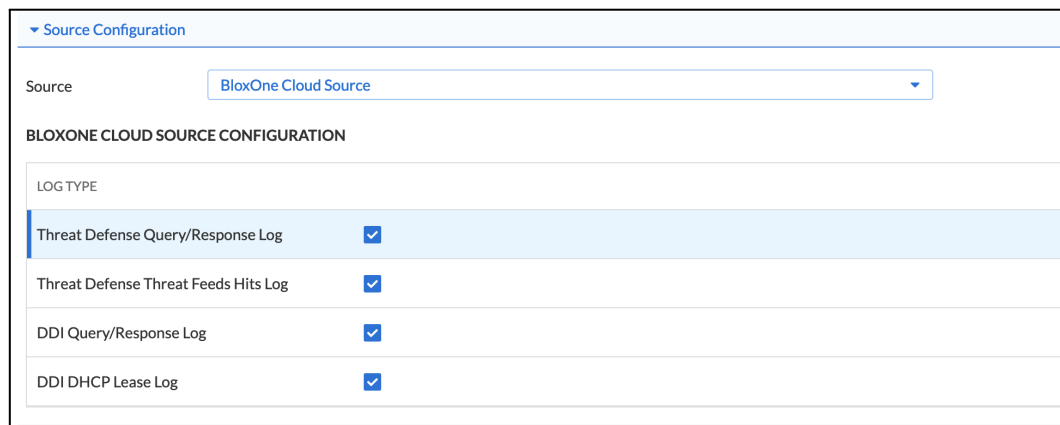
- Expand the **CDC Enabled Host** list by clicking on the CDC Enabled Host header. Then, select the OPH that was created earlier in this guide.



▼ CDC Enabled Host

On-Prem Host

- Expand the **Source Configuration** list by clicking on the Source Configuration header. Then, select BloxOne Cloud Source as the Source. In the Log Type panel, select the type of logs that will be sent to Splunk.



▼ Source Configuration

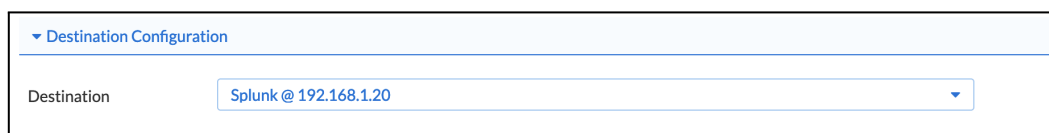
Source

BLOXONE CLOUD SOURCE CONFIGURATION

LOG TYPE

Threat Defense Query/Response Log	<input checked="" type="checkbox"/>
Threat Defense Threat Feeds Hits Log	<input checked="" type="checkbox"/>
DDI Query/Response Log	<input checked="" type="checkbox"/>
DDI DHCP Lease Log	<input checked="" type="checkbox"/>

- Expand the **Destination Configuration** list by clicking on the Destination Configuration header. Then, select the destination that was created earlier in this guide from the drop down list (Splunk or Splunk Cloud).



▼ Destination Configuration

Destination

- Enable the configuration by toggling the **State** to Enabled.



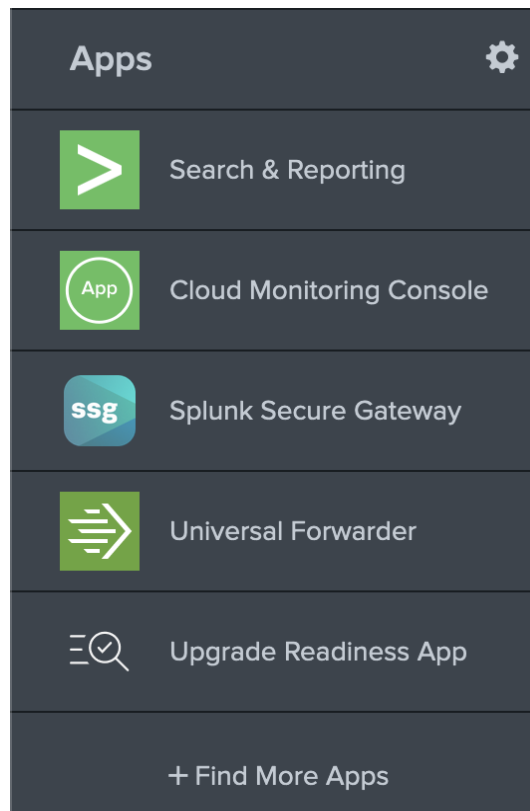
8. Click on **Save & Close** to confirm the creation of the Traffic Flow.

Configure Splunk

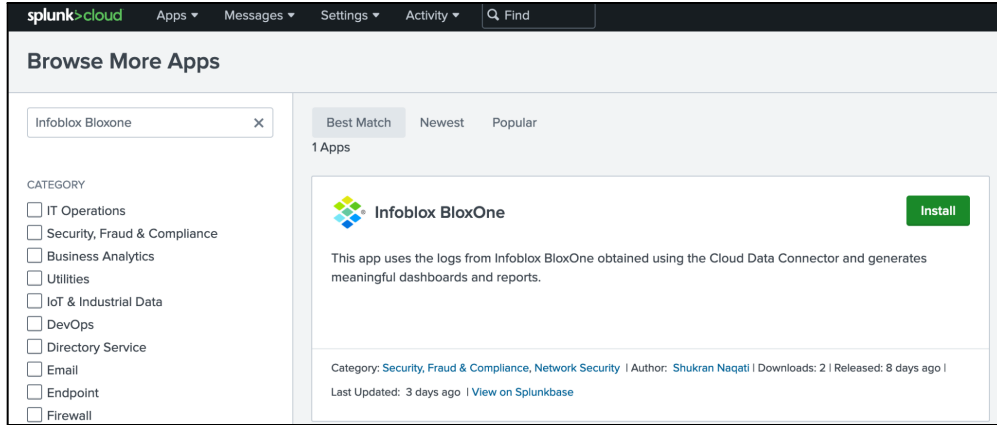
To Configure the Splunk BloxOne Application, users may install the application directly from Splunk, or download the application and add it to Splunk. Both the methods are described below.

Install from Splunk Web UI

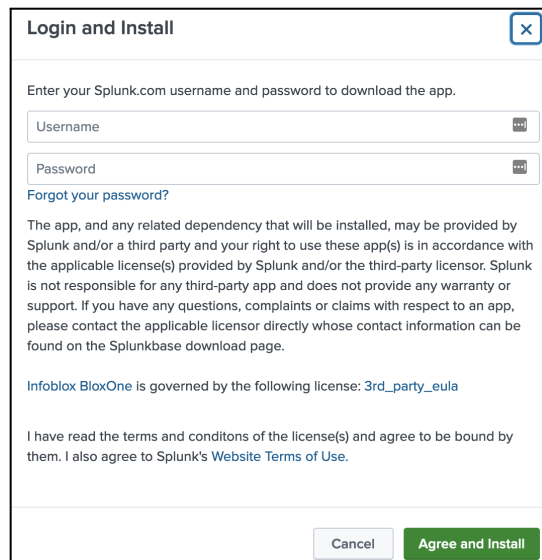
1. Navigate to the Splunk web interface and click on **+ Find More Apps** under the Apps list.



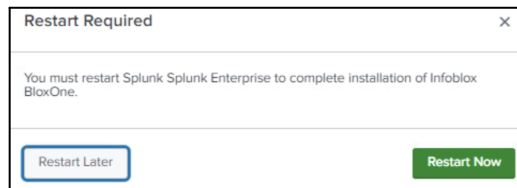
2. In the **Search** bar type **Infoblox BloxOne** and hit enter.



3. Look for the **Infoblox BloxOne** app and click on **Install**.
4. Enter your Splunk.com **username** and **password** and click on **Agree and Install** to install the application.



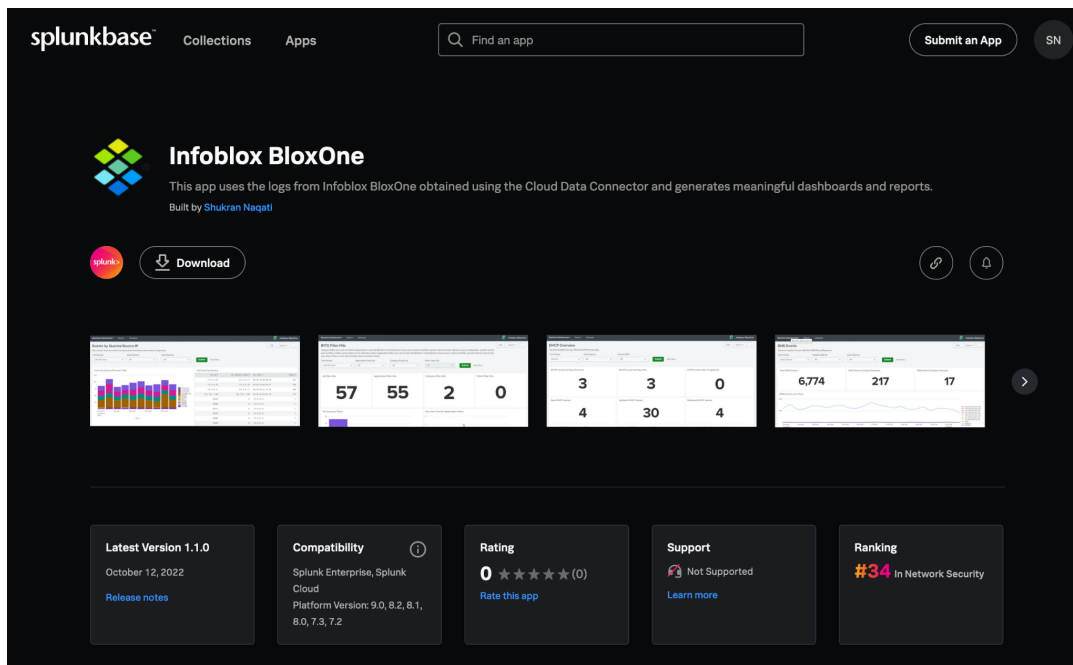
5. If prompted, Click on **Restart Now** to restart the Splunk instance.



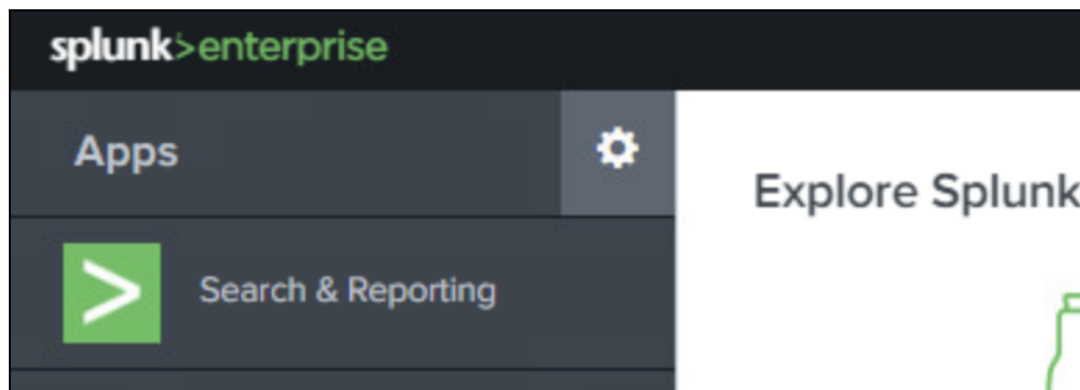
6. Once installed, the application will be visible in the Apps list.

Download from SplunkBase (For Splunk Enterprise Only)

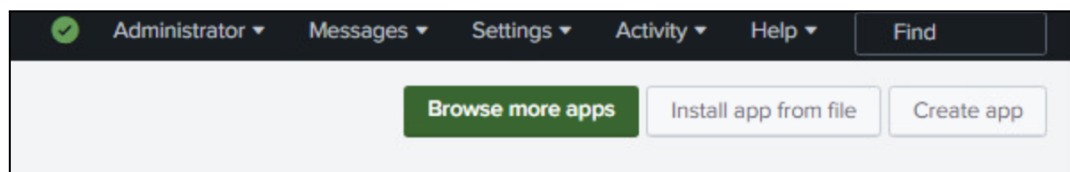
1. Go to SplunkBase and download the [Infoblox BloxOne](#) application.



2. Navigate to the Splunk Enterprise web interface and click on the **gear** icon located next to Apps.



3. Click the **Install app from file** button located near the top of the Splunk Enterprise web interface.



4. Click **Choose File**. Then, locate and select the file that was downloaded on step 1 of this section.

Install App From File

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

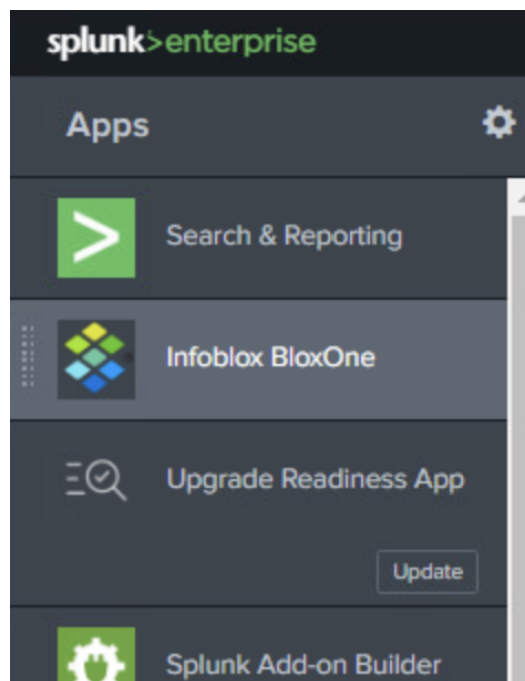
No file chosen

Upgrade app. Checking this will overwrite the app if it already exists.

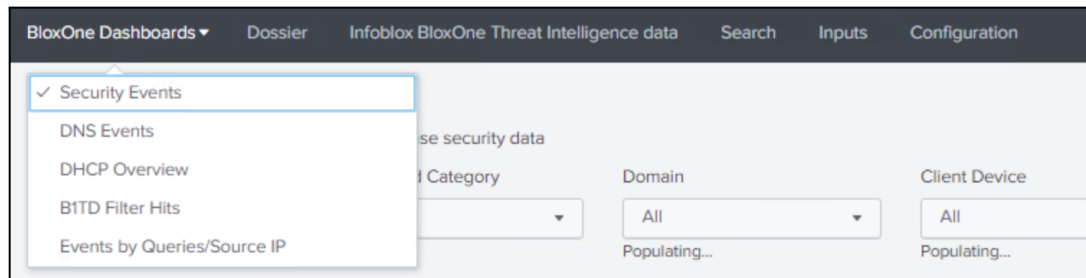
5. Click the **Upload** button to confirm the file upload.
6. Once installed, the application will be visible in the Apps list.

Application Navigation

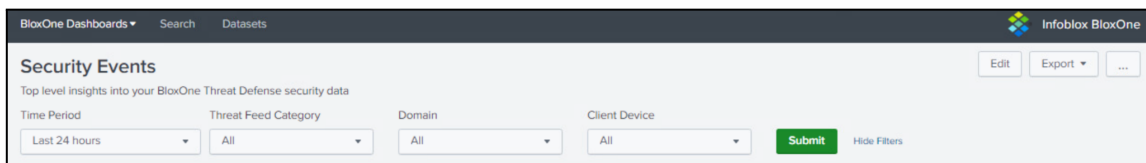
1. After installation the application should be visible in the Splunk Apps list. Click on **Infoblox BloxOne** from the list to open the application.



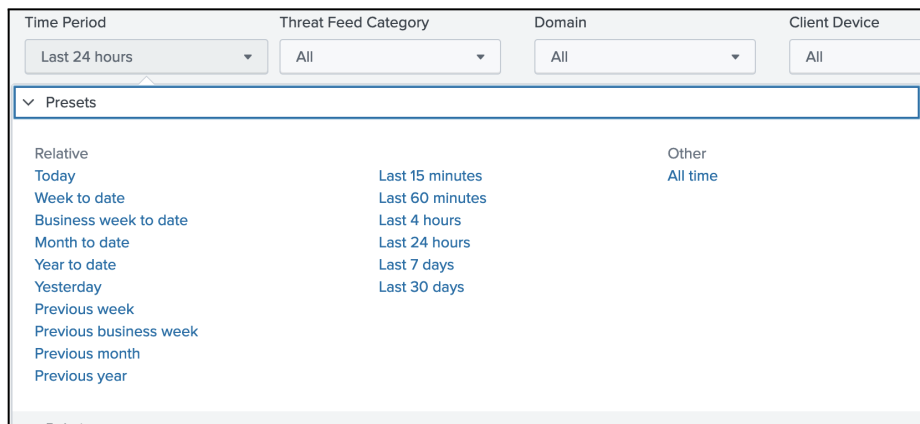
- Once users are in the application, by default, the Security Events dashboard opens up. Click on **BloxOne Dashboards** to reveal the list of other dashboards.



- The dashboards give a high-level overview of the data from the BloxOne platform. The dashboards included in the apps give users insights about DNS, DHCP, and Security activity.
- Users have the ability to edit and update the dashboard objects. Click on any of the dashboards from the list to see the high level metrics for that event.



- Some filters are added to all dashboards which help users to get filtered data based on their selection. A common filter for all dashboards is the time range where the users can select a time period that they want to view the data for.



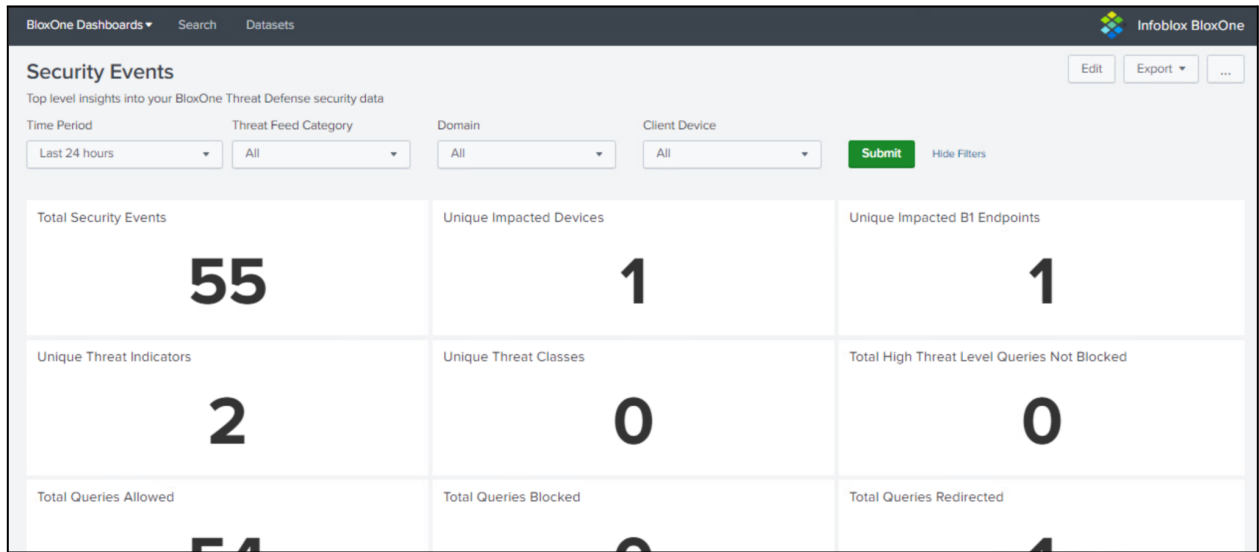
- Other filters include device IP, Infoblox product, device MAC, domains, etc. based on the dashboard the user is currently viewing.

BloxOne Dashboards

Following are some screenshots of the different dashboards with their filter and some metrics that they display.

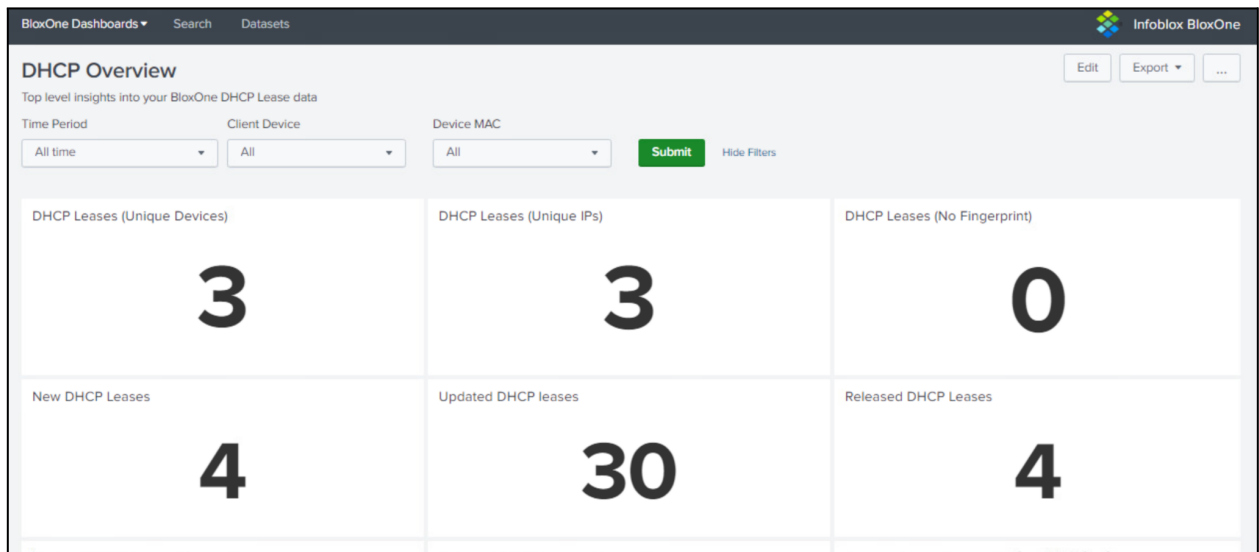
Security Events Dashboard

This dashboard gives top level insight into BloxOne security events



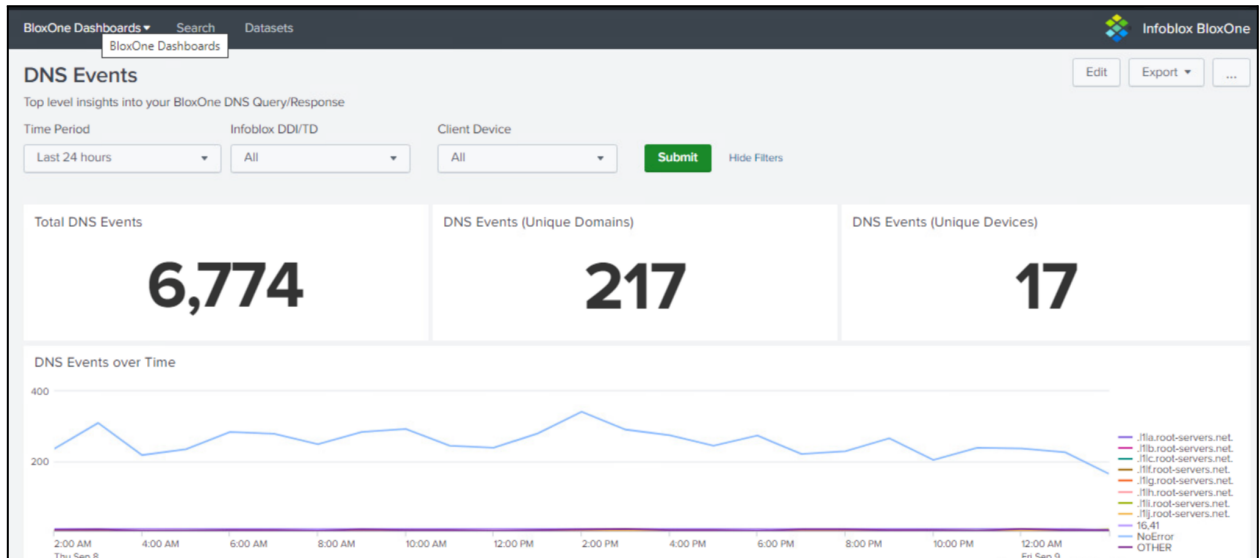
DHCP Overview Dashboard

The dashboard gives top level insights into BloxOne DHCP data



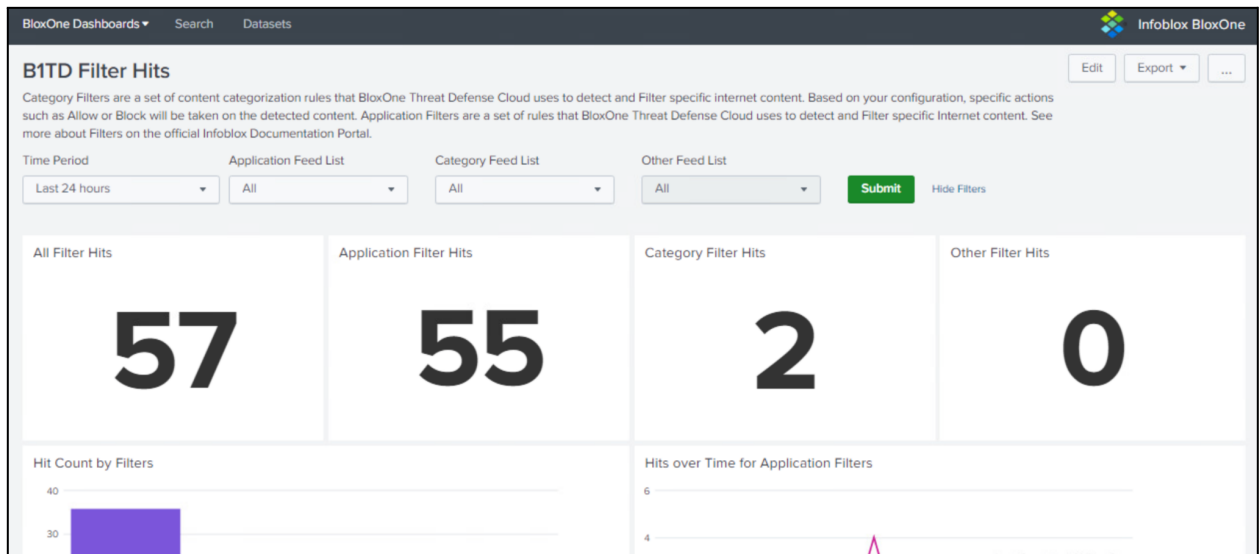
DNS Events Dashboard

The dashboard gives top level insights into BloxOne DNS Query/Response



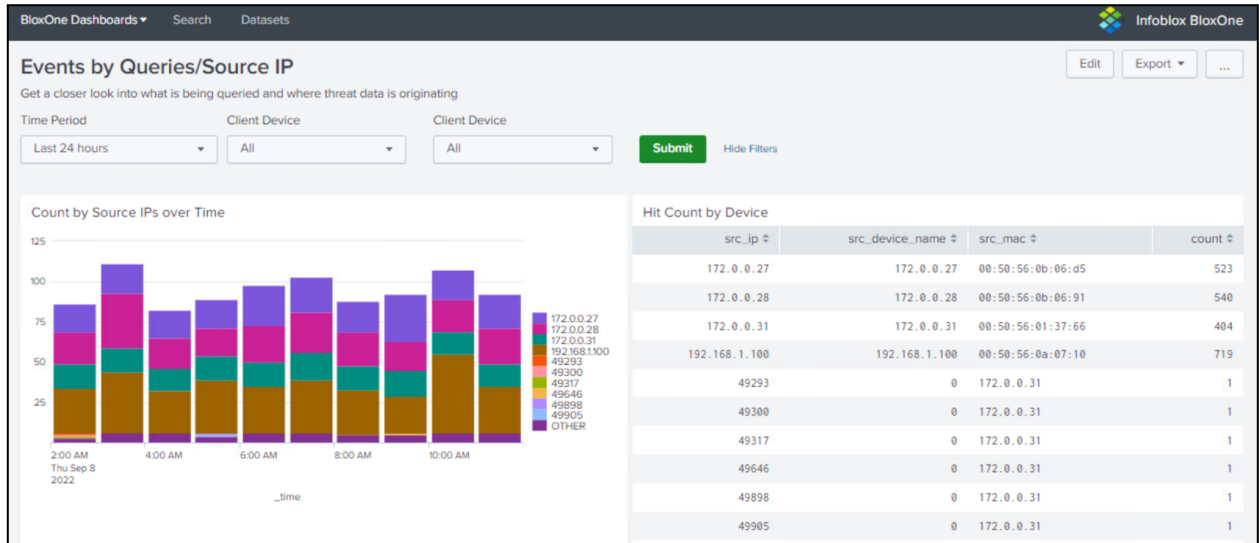
B1TD Filters Dashboard

Two types of filters can be configured using the Cloud Services Portal. Users can configure category filters and application filters. Based on the configuration, specific actions such as Allow or Block will be taken on the detected content. This dashboard gives information about the queries matching the filters.



Events by Queries/Source IP Dashboard

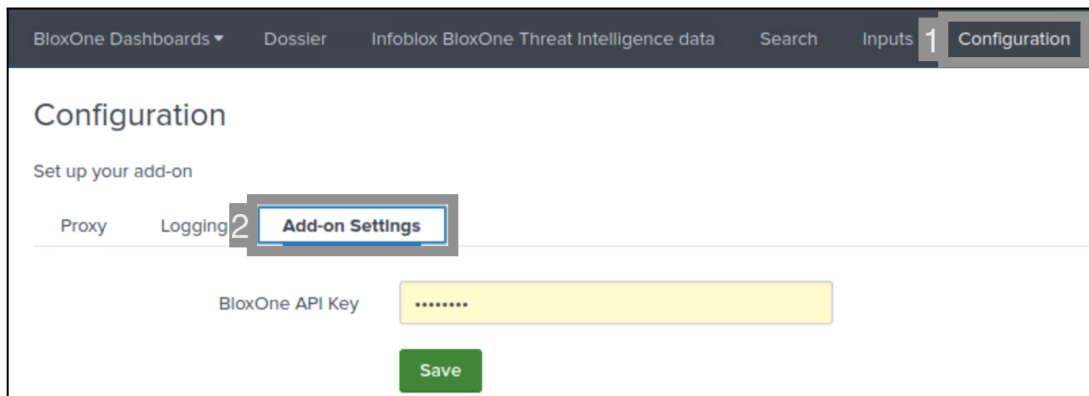
Gives users a closer look into the queries and where they are originating from.



Infoblox Threat Intelligence Data

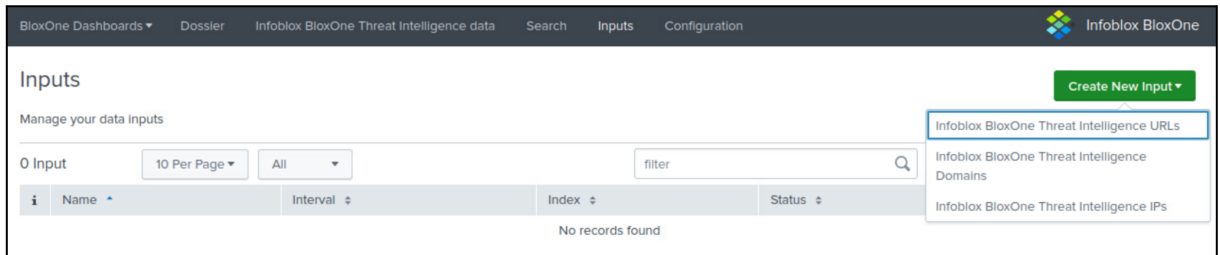
To index Infoblox TIDE data into Splunk the add-on needs to be configured and inputs need to be defined. To configure TIDE inputs follow the below steps:

1. Click on the **Configuration** tab then click on **Add-on Settings**.



2. Generate an API key from your CSP user profile page and paste it in **BloxOne API Key** field and click on **Save** button. To generate API Key follow the below steps.
 - o From the Cloud Services Portal, click your user name at the lower left-hand corner of the portal and select **User Profile** -> **User API Keys** tab.
 - o On the **User API Keys** tab, click **Create**.

- In the Create User API Keys dialog, fill in **Name** and **Expires At**.
 - Click **Save & Close** to save the configuration.
 - Click **Copy** in the confirmation dialog to copy the user API key.
3. After configuring the add-on click on **Inputs** tab on configure TIDE inputs.



4. Click on **Create New Input** and select a desired input type to index TIDE URL, Domain or IP data.
5. To configure the input:
- Enter a unique **Name** for the input.
 - Select a time **Interval** you want to pull in the data.
Note: Select interval as 1 hour or more.
 - Select an **Index** for the data.
 - To fetch all previous threat indicators during the first run check the **First run get past IOCs**.
 - Click on **Add** to save the data input

Add Infoblox BloxOne Threat Intelligence URLs ✕

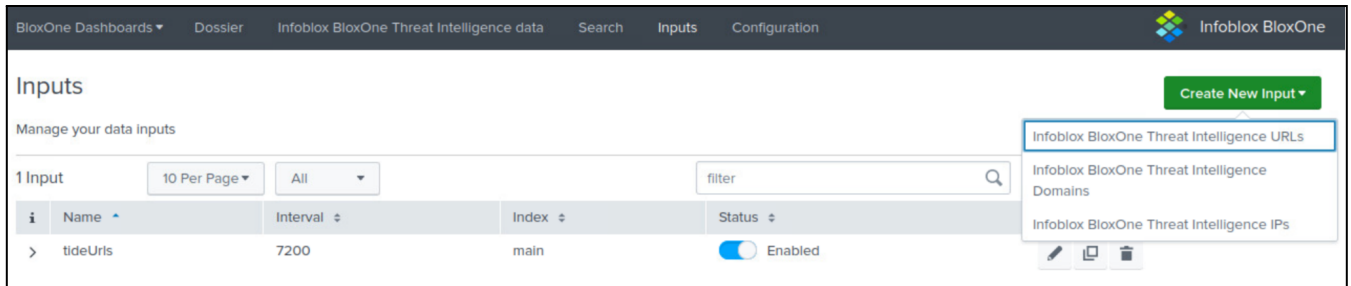
Name
Enter a unique name for the data input

Interval
Time interval of input in seconds.

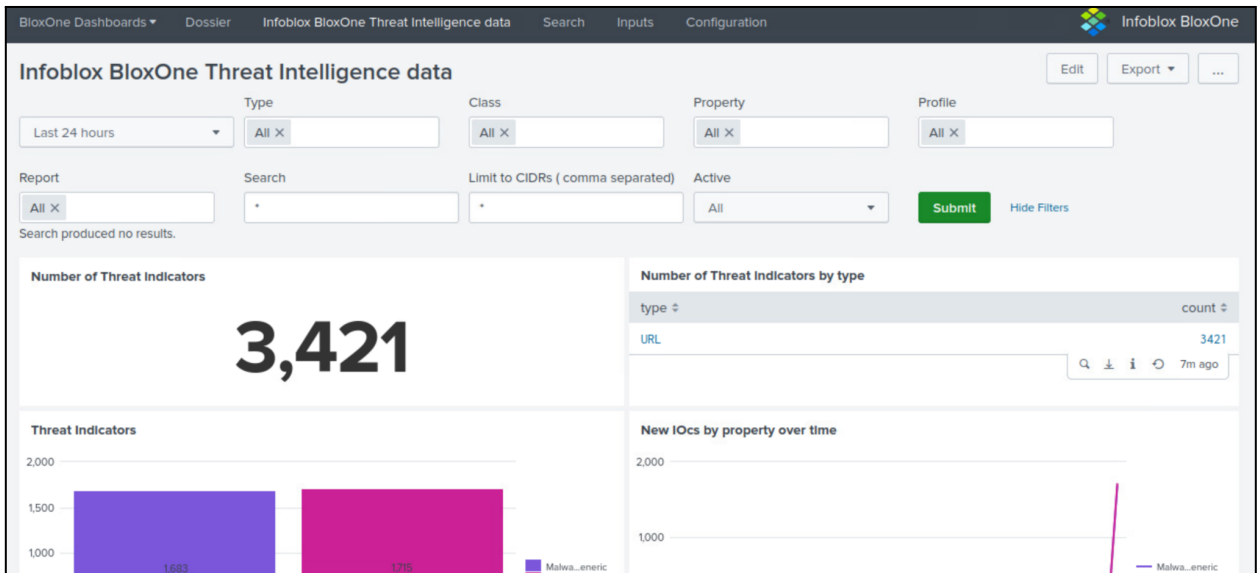
Index

First run get past IOCs

- Follow the same steps to configure Domain and IP data. Once configured data should get indexed in 15 to 20 mins.

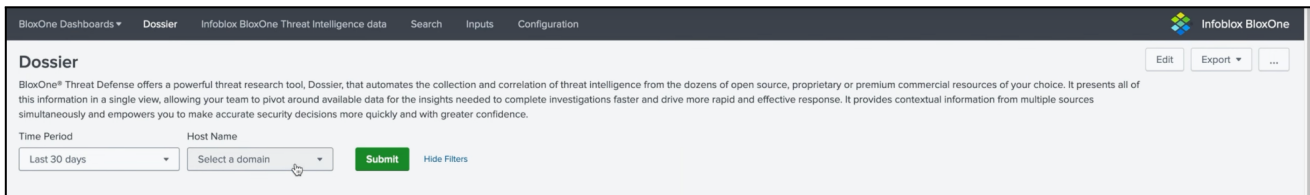


The Infoblox BloxOne Threat Intelligence data dashboard shows metrics related to threat intelligence data pulled from BloxOne like number of threat indicators, different types of threat indicators, threat indicators segregated by threat, risk, and confidence score.

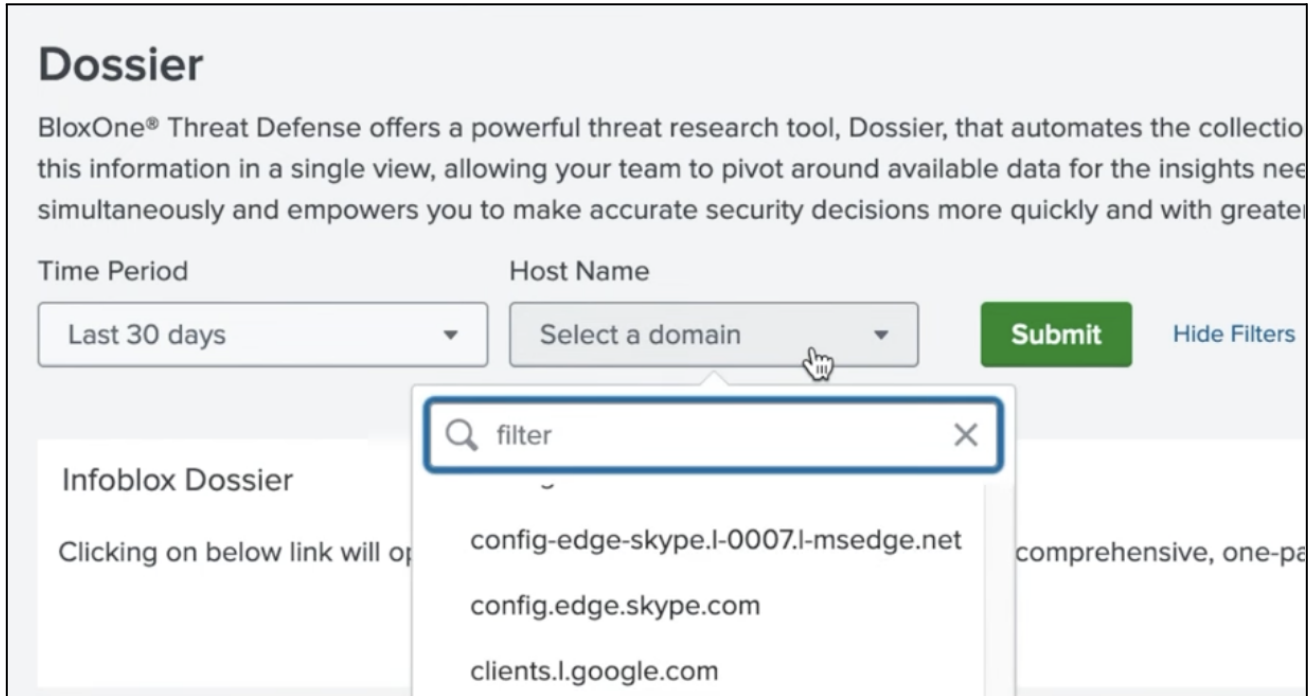


Dossier

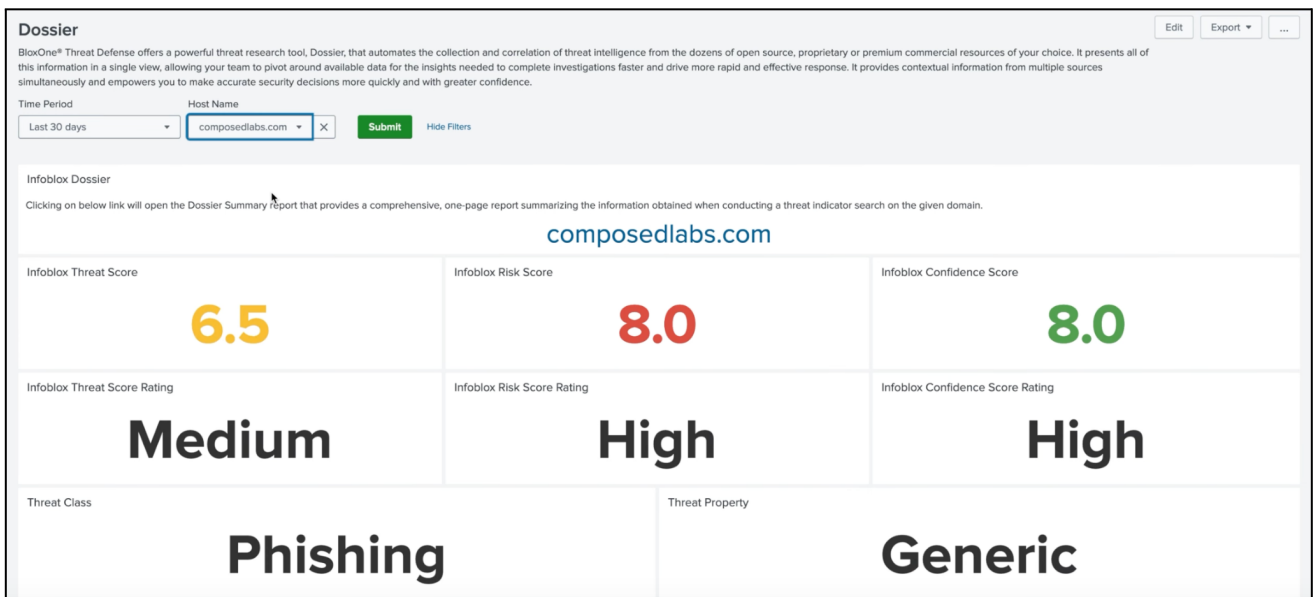
The application features a Dossier dashboard, which generates a link to the Infoblox BloxOne Dossier summary page for the selected domain along with some of the insights from Infoblox Threat Intelligence Data.



1. On the Dossier dashboard select the domain from the **Domain** dropdown.



2. On selecting a domain from the list a link with the same domain name will be displayed below. On clicking the link, a new tab will open which will redirect users to the BloxOne Dossier summary page for the selected domain. The page also displays metrics for the selected domain from TIDE data if the domain is present.



Additional Resources

For more information regarding Infoblox or Splunk, access these websites:

1. Infoblox Documentation Website: [Infoblox Documentation Portal](#)
2. Infoblox Data Connector Docs: [Data Connector - BloxOne Threat Defense - Infoblox Documentation Portal](#)
3. Splunk Documentation Portal: [Splunk Documentation](#)
4. Setting up Splunk - BloxOne Resource: [Setting Up Splunk](#)
5. Setting up Splunk Cloud - BloxOne Resource: [Setting Up Splunk Cloud](#)
6. Infoblox BloxOne Application - Splunkbase: [Infoblox BloxOne | Splunkbase](#)
7. Infoblox Website: [Infoblox](#)
8. Infoblox Community Website: [Infoblox Community](#)



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