EXPANSE

Expanse App Installation and User Guide For IBM QRadar Platform

This document describes how to install the Expanse app on the QRadar platform and how to use it. The Expanse app (also referred to as an extension) on the QRadar platform enables the following capabilities:

- Create the offences as events in QRadar for the Exposure incidents detected by Expanse Expander.
- Create the offences as events in QRadar for the risky network flows detected by Expanse Behavior.
- Populate the offences with the relevant information from Expander and Behavior.
- Show Asset and Exposure details for an IP address related to an Expanse event

---

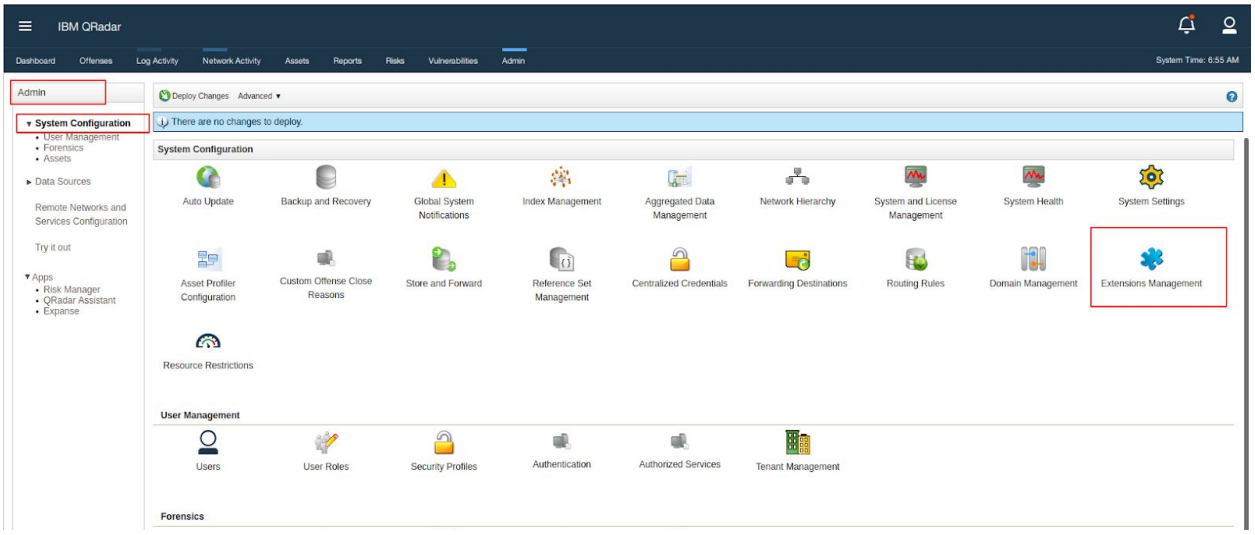
Installing The Extension

Before beginning the installation, ensure that you meet the following prerequisites:

- Your QRadar platform is running one of the following versions or later:
    - IBM Security QRadar 7.3.1: Patch 7 (7.3.1.20181123182336)
- You have already downloaded the Expanse App for QRadar file (Expanse_QRadar.zip) from the IBM Security App Exchange.
- You can log in to QRadar with Master Administrator privileges.

To install the Expanse app on QRadar, perform the following steps:

1. Log in to the QRadar console with Master Administrator privileges and then click Admin in the navigation menu .
2. In the System Configuration section, click Extensions Management.

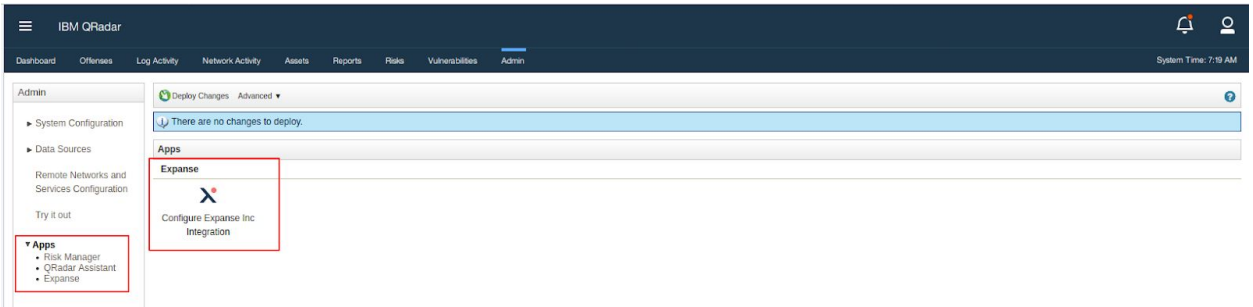


3. To upload the Expanse extension, click **Add > Browse**, browse to the downloaded file, click **Install**, and then click **Add**.
4. To view the contents of the extension, select it from the extensions list and then click **More Details**.
5. To install the extension, select it from the list and then click **Install**.
6. Review the changes that the installation makes to the system and then select **Overwrite** or **Keep existing data** to specify how to handle existing content.
7. Verify that there are **27** custom event properties and 2 log sources and then click **Install**.

List of Custom Event Properties are listed here,

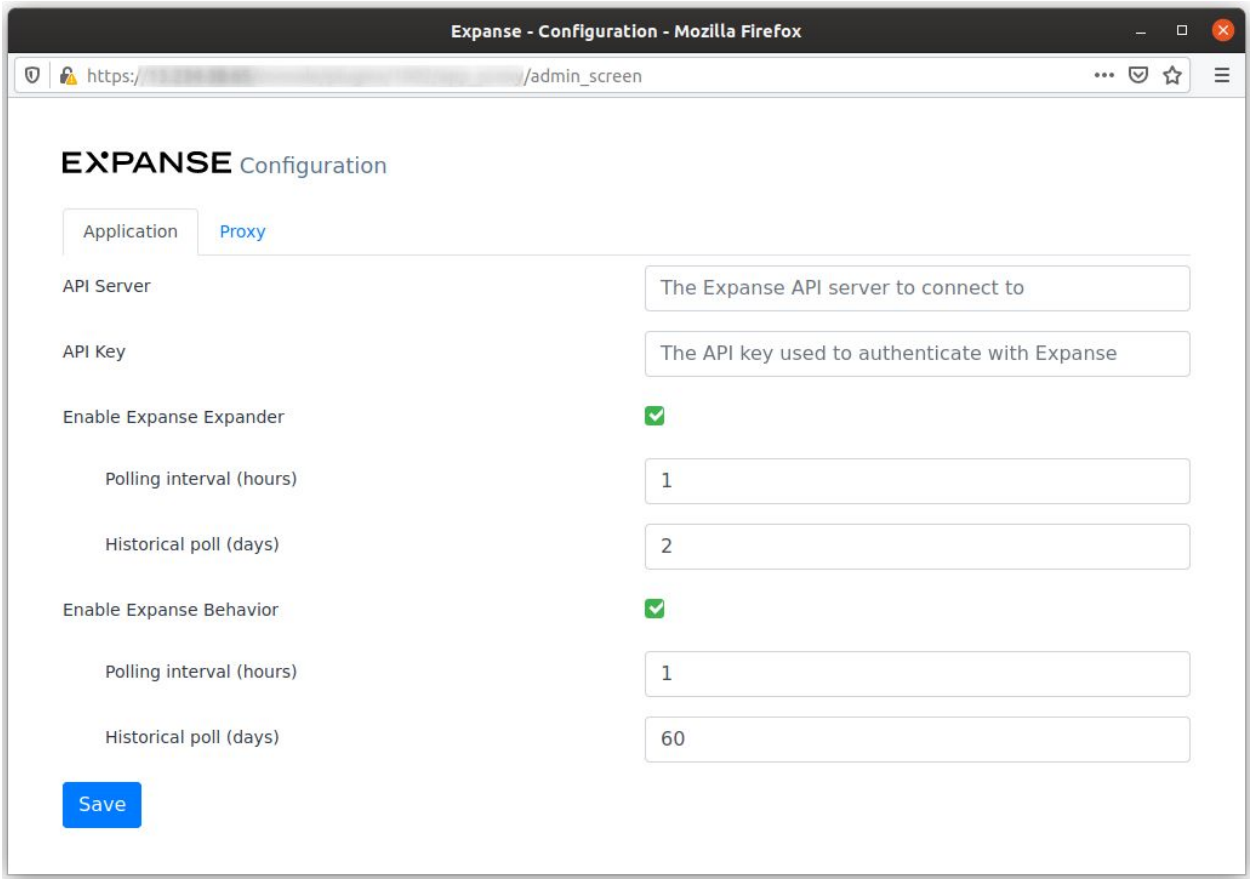
Property Name	Type	Property Description	Log Source Type ▲	Log Source	Event Name	Category	Expression	Username	Enabled	Creation Date	Modification Date
Acknowledged	Regex	Acknowledged (Expan...	ExpanseBehavior	N/A	N/A	N/A	acked=(.*?)\t	admin	True	Feb 11, 2020, 5:40 AM	Feb 13, 2020, 10:59 AM
Source Country Code	Regex	Source Country Code ...	ExpanseBehavior	N/A	N/A	N/A	srcCountryCode=(.*?)\t	admin	True	Feb 11, 2020, 5:35 AM	Feb 13, 2020, 10:59 AM
Source Domains	Regex	Source Domains (Exp...	ExpanseBehavior	N/A	N/A	N/A	srcDomains=(.*?)\t	admin	True	Feb 11, 2020, 5:40 AM	Feb 13, 2020, 10:59 AM
Destination Tags	Regex	Destination Tags (Exp...	ExpanseBehavior	N/A	N/A	N/A	destTags=(.*?)\t	admin	True	Feb 11, 2020, 5:40 AM	Feb 13, 2020, 10:59 AM
Observation Timestamp	Regex	Observation Timestam...	ExpanseBehavior	N/A	N/A	N/A	observationTimestamp...	admin	True	Feb 11, 2020, 7:12 AM	Feb 13, 2020, 10:59 AM
Business Unit Id	Regex	Business Unit Id (Exp...	ExpanseBehavior	N/A	N/A	N/A	businessUnitId=(.*?)\t	admin	True	Feb 11, 2020, 5:36 AM	Feb 13, 2020, 10:59 AM
Risk Rule Name	Regex	Risk Rule Name (Exp...	ExpanseBehavior	N/A	N/A	N/A	riskRuleName=(.*?)\t	admin	True	Feb 11, 2020, 7:19 AM	Feb 13, 2020, 10:59 AM
Risk Rule Id	Regex	Risk Rule Id (Expanse)	ExpanseBehavior	N/A	N/A	N/A	riskRuleId=(.*?)\t	admin	True	Feb 11, 2020, 5:35 AM	Feb 13, 2020, 10:59 AM
Destination Country Code	Regex	Destination Country C...	ExpanseBehavior	N/A	N/A	N/A	destCountryCode=(.*?)\t	admin	True	Feb 11, 2020, 5:35 AM	Feb 13, 2020, 10:59 AM
Source Exposure Types	Regex	Source Exposure Typ...	ExpanseBehavior	N/A	N/A	N/A	srcExposureTypes=(.*...	admin	True	Feb 11, 2020, 7:20 AM	Feb 13, 2020, 10:59 AM
Destination Exposure Types	Regex	Destination Exposure ...	ExpanseBehavior	N/A	N/A	N/A	destExposureTypes=(....	admin	True	Feb 11, 2020, 5:45 AM	Feb 13, 2020, 10:59 AM
Risk Rule Description	Regex	Risk Rule Description ...	ExpanseBehavior	N/A	N/A	N/A	riskRuleDescription=(....	admin	True	Feb 11, 2020, 5:56 AM	Feb 13, 2020, 10:59 AM
Business Unit Name	Regex	Business Unit Name (...	ExpanseBehavior	N/A	N/A	N/A	businessUnitName=(.*...	admin	True	Feb 11, 2020, 7:21 AM	Feb 13, 2020, 10:59 AM
Destination Domains	Regex	Destination Domains (...	ExpanseBehavior	N/A	N/A	N/A	destDomains=(.*?)\t	admin	True	Feb 11, 2020, 7:19 AM	Feb 13, 2020, 10:59 AM
Source Tags	Regex	Source Tags (Expanse)	ExpanseBehavior	N/A	N/A	N/A	srcTags=(.*?)\t	admin	True	Feb 11, 2020, 7:19 AM	Feb 13, 2020, 10:59 AM
Tenant Business Unit Id	Regex	Tenant Business Unit I...	ExpanseBehavior	N/A	N/A	N/A	tenantBusinessUnitId=...	admin	True	Feb 11, 2020, 7:08 AM	Feb 13, 2020, 10:59 AM
Created	Regex	Created (Expanse)	ExpanseBehavior	N/A	N/A	N/A	created=(.*?)\t	admin	True	Feb 11, 2020, 5:55 AM	Feb 13, 2020, 10:59 AM
Criticality	Regex	Criticality (Expanse)	ExpanseExpander	N/A	N/A	N/A	criticality=(.*?)\t	admin	True	Feb 11, 2020, 8:42 AM	Feb 13, 2020, 10:59 AM
Exposure Type	Regex	Exposure Type (Expa...	ExpanseExpander	N/A	N/A	N/A	exposureType=(.*?)\t	admin	True	Feb 11, 2020, 8:33 AM	Feb 13, 2020, 10:59 AM
Tags On Ip	Regex	Tags On Ip (expanse)	ExpanseExpander	N/A	N/A	N/A	TagsOnIp=((.+?))	admin	True	Feb 11, 2020, 8:33 AM	Feb 13, 2020, 10:59 AM
Business Unit Name	Regex	Business Unit Name (...	ExpanseExpander	N/A	N/A	N/A	businessUnitName=(.*...	admin	True	Feb 11, 2020, 8:33 AM	Feb 13, 2020, 10:59 AM
Certificate PEM	Regex	Certificate PEM (Expa...	ExpanseExpander	N/A	N/A	N/A	certificatePem=(.*?)\t	admin	True	Feb 11, 2020, 8:36 AM	Feb 13, 2020, 10:59 AM
Business Unit Id	Regex	Business Unit Id (Exp...	ExpanseExpander	N/A	N/A	N/A	businessUnitId=(.*?)\t	admin	True	Feb 11, 2020, 8:33 AM	Feb 13, 2020, 10:59 AM
Providers	Regex	Providers (Expanse)	ExpanseExpander	N/A	N/A	N/A	providers=(.*?)\t	admin	True	Feb 11, 2020, 8:42 AM	Feb 13, 2020, 10:59 AM
Scanned	Regex	Scanned (Expanse)	ExpanseExpander	N/A	N/A	N/A	scanned=(.*?)\t	admin	True	Feb 11, 2020, 8:36 AM	Feb 13, 2020, 10:59 AM
Exposure Id	Regex	Exposure Id (Expanse)	ExpanseExpander	N/A	N/A	N/A	exposureId=(.*?)\t	admin	True	Feb 11, 2020, 8:42 AM	Feb 13, 2020, 10:59 AM
Domain Name	Regex	Domain Name (Expan...	ExpanseExpander	N/A	N/A	N/A	domainName=(.*?)\t	admin	True	Feb 11, 2020, 8:36 AM	Feb 13, 2020, 10:59 AM

8. Review the installation summary and then click **OK**.
9. After the Installation is complete, navigate to the *Admin* section, click **Configure Expanse QRadar Integration**.



This opens an admin configuration page.

10. Provide your Expanse server details and credentials.



This allows you to poll events from Expander and flows from Behavior to QRadar.

11. Click **Save**.

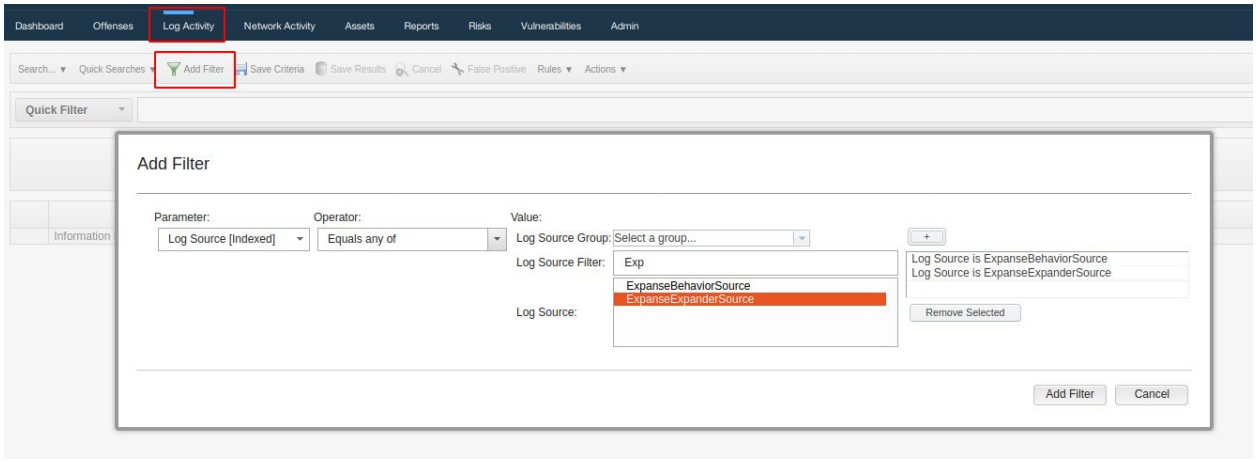
Using the Extension

The integration enables the following functionality within the QRadar console:

- View Expanse incidents as events in the QRadar *Log Activity* section.
- Show Asset and Exposure information on IP address for an event.

Log Activity Events

After the QRadar and Expanse integration is complete, the Expanse app will start ingesting events from the Expanse server and displaying them as QRadar events.
Navigate to the **Log Activity** tab and filter the log source to show entries from “Expanse”.
To apply a filter – Click **Add Filter**, select **Log Source [Indexed]**

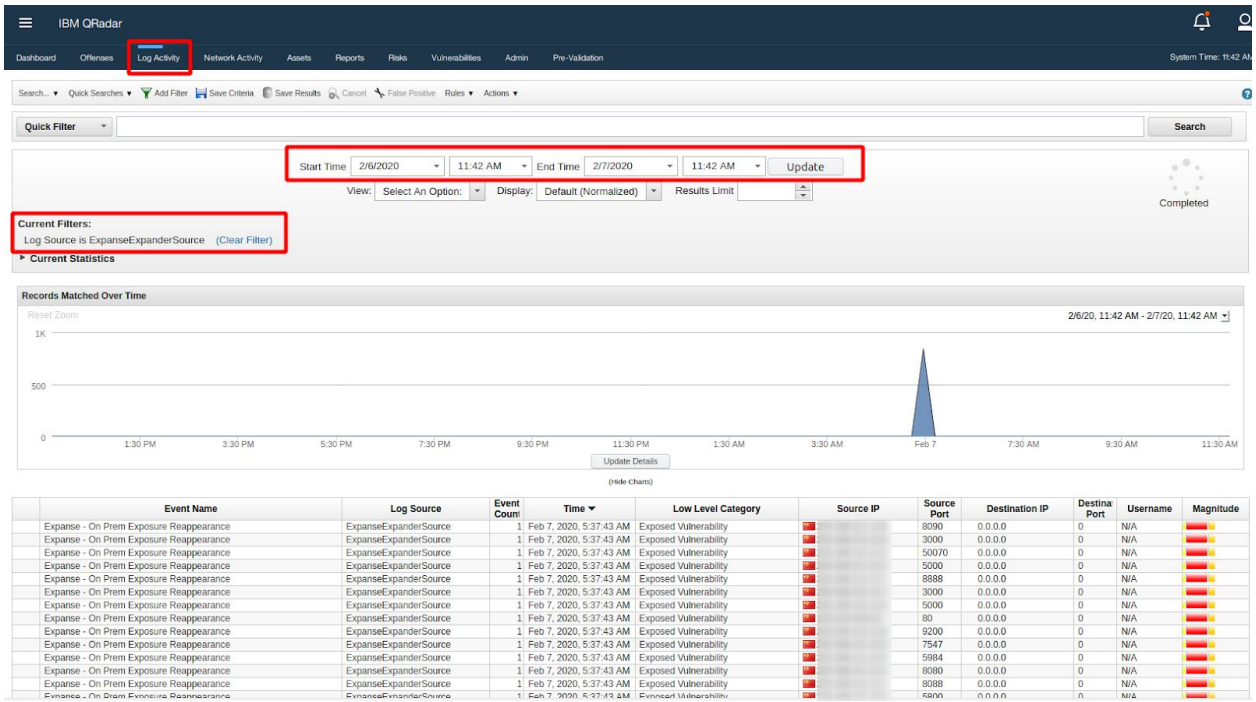


Once the Filter is added, Expanse Exposure and Behavior events will be listed after providing the time range in the **View real time events**.

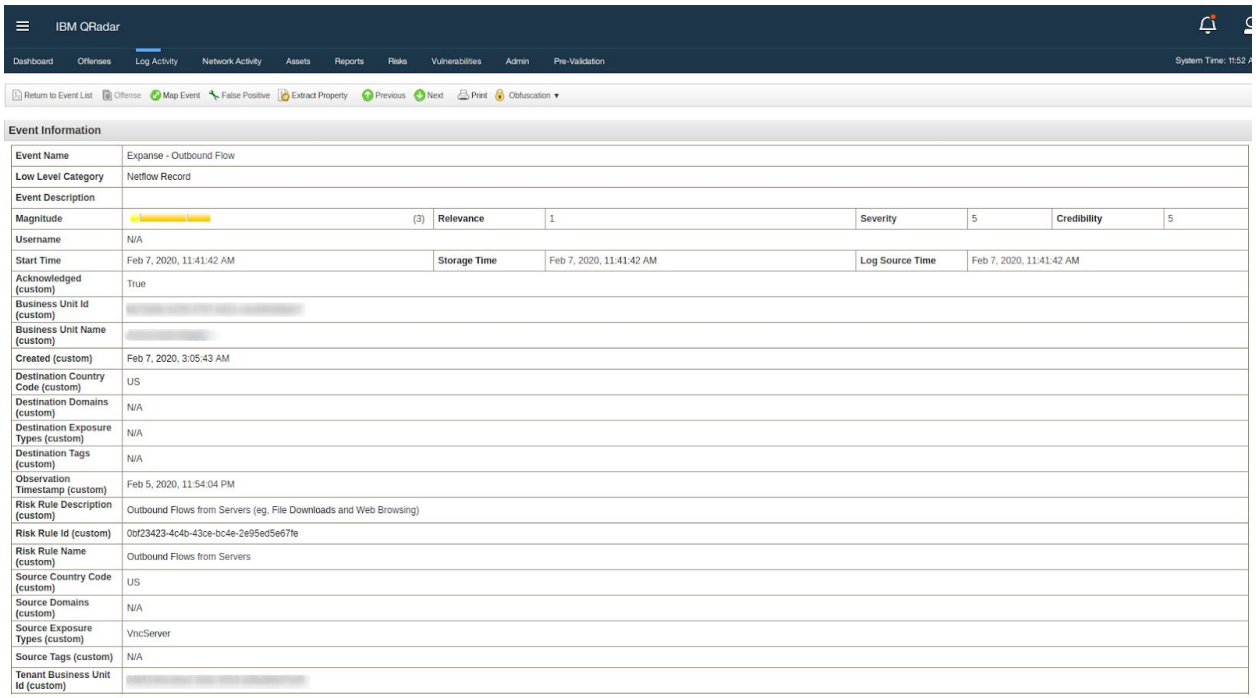
The Expanse app categorizes the events from Expanse into two types:

- Exposure Events
- Behavior Alerts

Click **View** to choose various time range, else by default that will be set to ‘Real Time Events’



Double-click on the logged event to see all the fields related to the event



Expander

The extension ingests the following 6 types of exposure events from Expanse Expander:

1. On Prem Exposure Appearance
2. On Prem Exposure Reappearance
3. On Prem Exposure Disappearance
4. Cloud Exposure Appearance
5. Cloud Exposure Reappearance
6. Cloud Exposure Disappearance

Please reference the Expander documentation for more details about the meaning of these event types.

Behavior

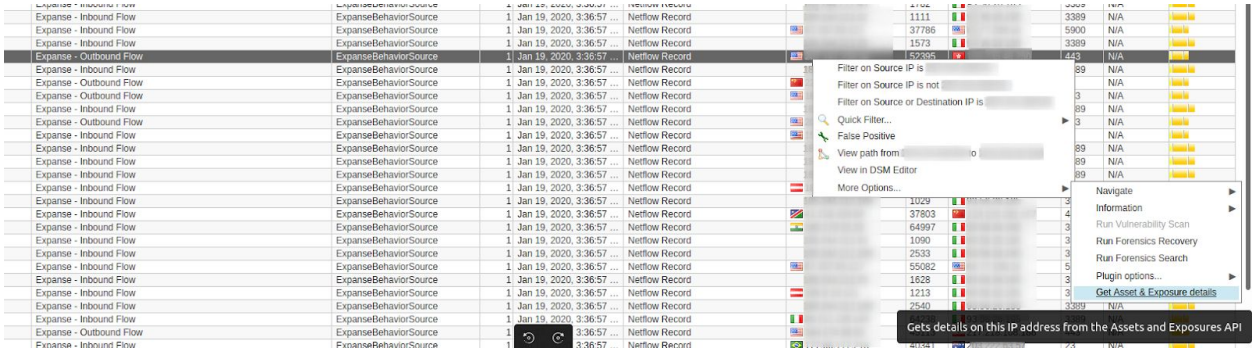
The extension creates the following 3 types of flow events, based on the Expanse Behavior alerts you have configured and the directionality of the alerted flow:

1. Inbound
2. Outbound

3. Unknown

Asset and Exposure Details

Right-Click on the IP address field of an event in *Log Activity*. In the context menu select **More Options**. In the sub-menu click on **Assets & Exposure Details**.



A new page opens with all the details on the selected IP address from Expander, including Business Unit information and relevant Points of Contact. The information is fetched from the Expanse server Asset and Exposure APIs.