

MANDIANT ADVANTAGE FOR IBM QRADAR

The Mandiant Advantage app for QRadar brings Mandiant's front-line intelligence to QRadar. It highlights indicators of compromise (IOCs) in your network and lets you identify and explore the ones that matter most.

Reduce alert fatigue by applying Mandiant's Indicator Confidence scoring to ensure you're only alerted when it matters. If you identify an active breach, the Mandiant Advantage app for QRadar provides one-click access to our Incident Response professionals. They are automatically provided with the relevant data to simplify and speed up the response process.

Pre-requisites

- QRadar version 7.4.x or 7.5.x
- Outbound network connectivity to Mandiant APIs using HTTPS on port 443

Get API Key ID and Secret



To obtain a **Service API Key** (which is tied to an organization rather than an individual user) for use with third-party security technologies such as a SIEM, contact **Support** (<https://www.mandiant.com/support>).

To obtain an API Key ID and Secret for an individual user account, perform the following:

1. Navigate to the Mandiant Threat Intelligence web console.
2. Click **Account Settings**.
3. Select **API Access and Keys** from the navigation menu.
4. Click **Get Key ID and Secret**.
5. Copy and store the displayed values in a secure location.

New Install

1. Download the QRadar extension from the **IBM App Exchange** (<https://exchange.xforce.ibmcloud.com/hub/extension/3a996a7812c185dea2bf3731347b8226>).
2. Log in to the QRadar console as an admin user.
3. Open the Admin page.
4. Click **Extensions Management**.
5. Click **Add**.
6. Browse to the location that the extension file was saved to upload the extension to your system.
7. Click **Add** to upload the extension.
8. Click **Install** to install the extension.

Upgrading from 1.0.0



In-place upgrades are supported: All previously defined settings for the Mandiant Advantage Account and Input are maintained after an upgrade.

1. Download the QRadar extension from the **IBM App Exchange** (<https://exchange.xforce.ibmcloud.com/hub/extension/3a996a7812c185dea2bf3731347b8226>).
2. Log in to the QRadar console as an admin user.
3. Open the Admin page.
4. Click **Extensions Management**.
5. Click **Add**.

6. Browse to the location that the extension file was saved to upload the extension to your system.
7. Click **Add** to upload the extension.
8. Click **Install** to install the extension.
9. Leave the default option to **Replace existing items** selected to preserve the app settings.
10. Verify that your Mandiant Advantage account has been maintained.



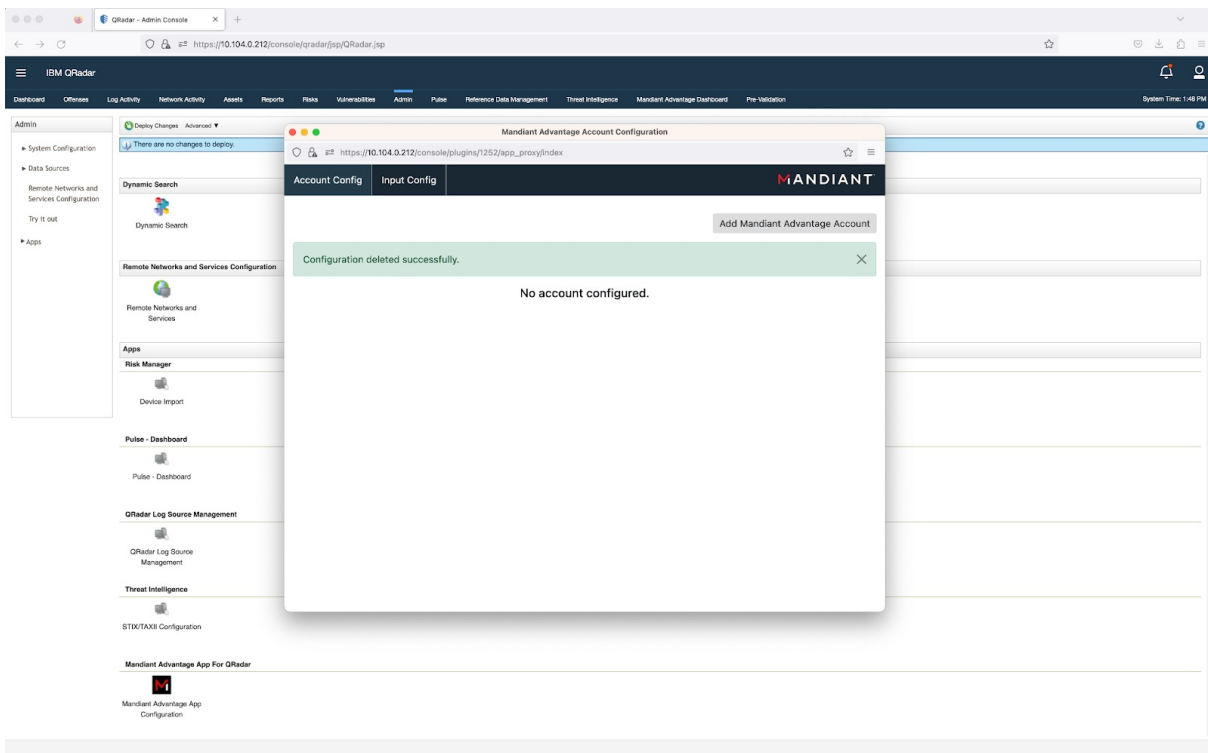
Load the Input Configuration and define the Enable / Disable Offense Enrichment setting to the desired behavior. This is a new setting that needs to be defined before it can be used. Failure to do this will prevent Offense Enrichment from running.

11. Optional: Uninstall version 1.0.0 to clean up the system.

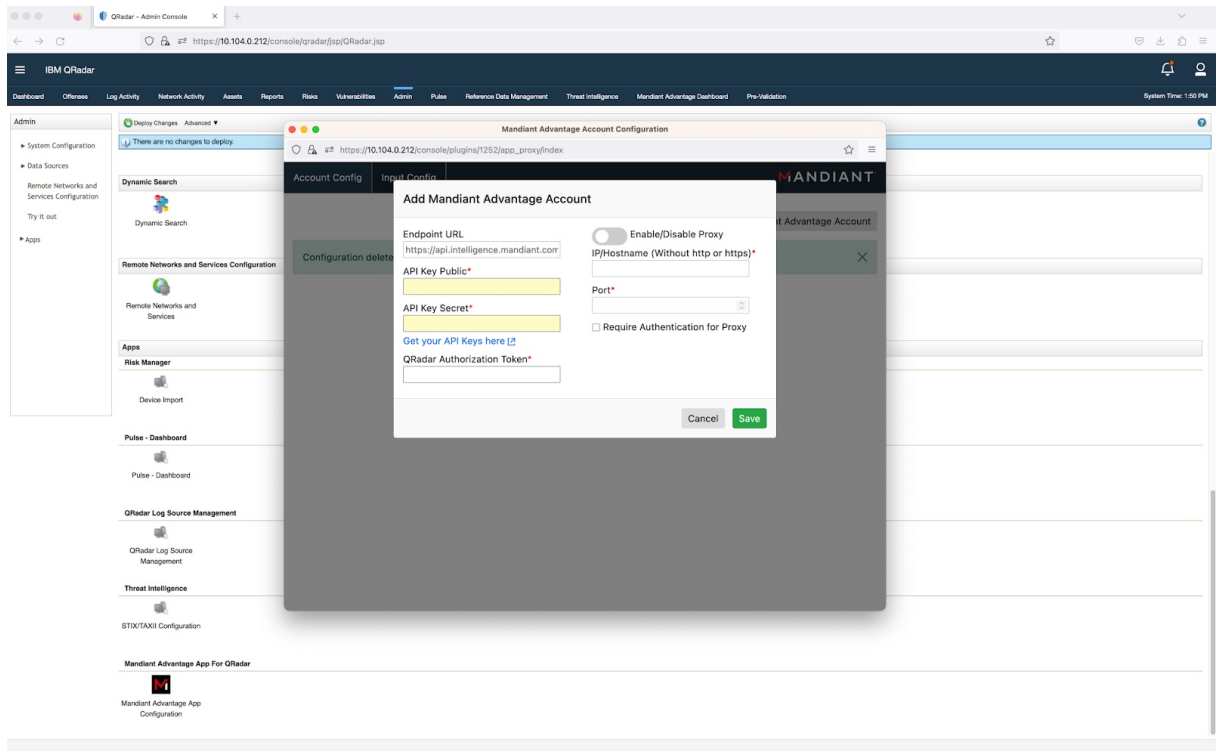
Configuration

Add a Mandiant Account

1. Log in to the QRadar console as an admin user.
2. Open the Admin page.
3. Scroll to the Apps section.
4. Click **Mandiant Advantage App Configuration** to open the following modal:



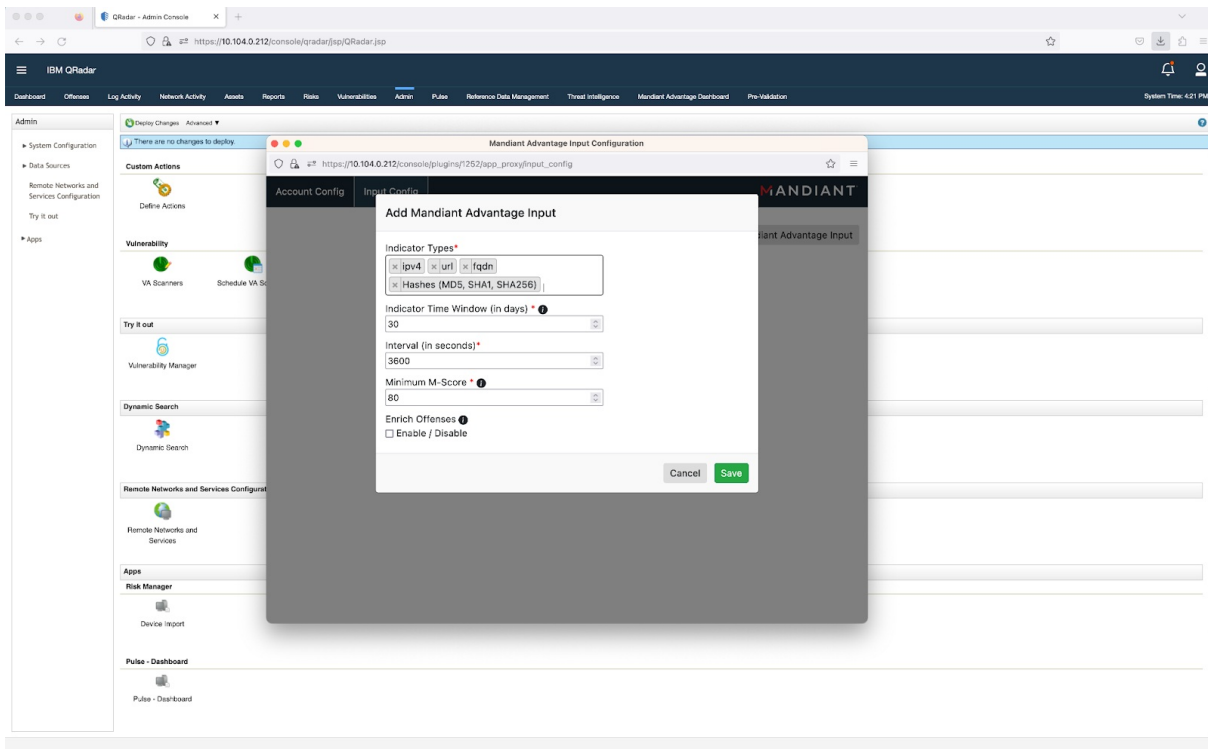
5. Click **Add Mandiant Advantage Account** to open the following modal:



6. Complete the form and click **Save**.

Add an Input

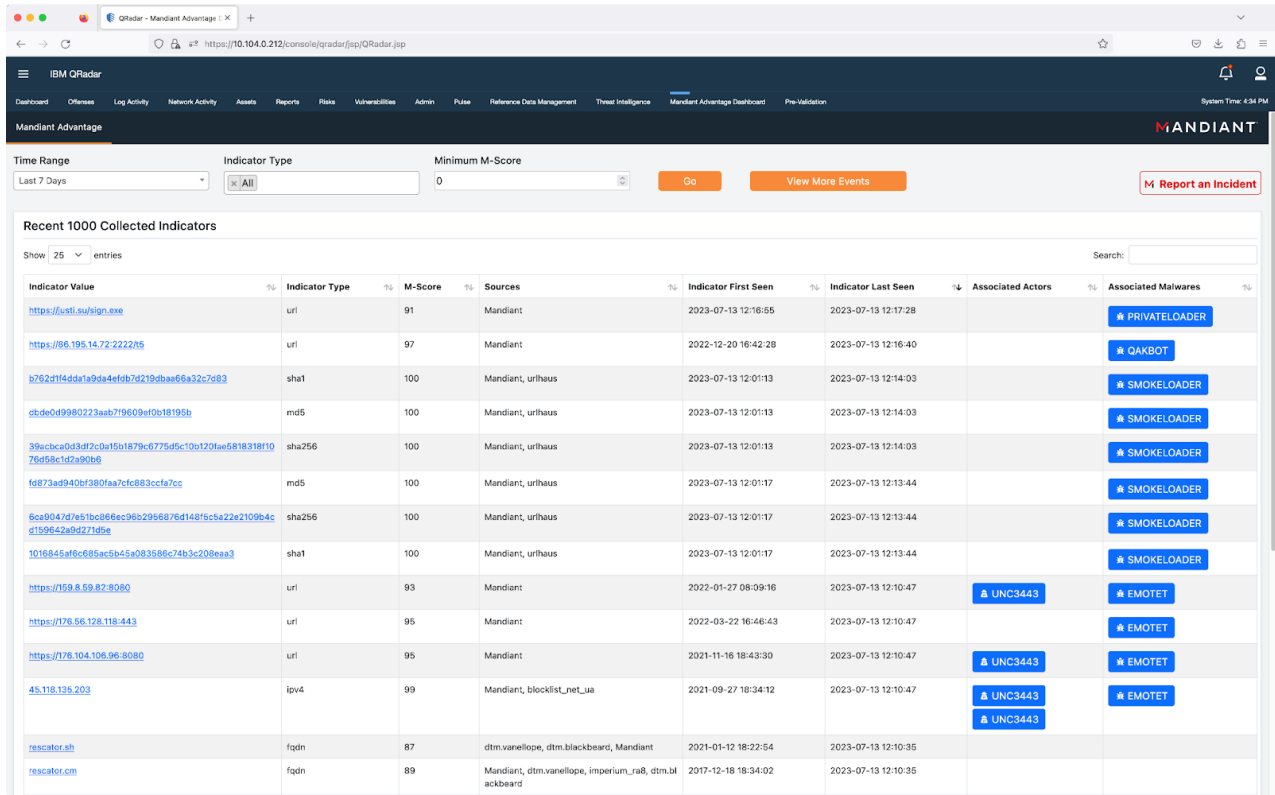
1. While logged in to the QRadar console as an admin user with the Mandiant Advantage App Configuration modal open, click **Input Config**.
2. Click **Add Mandiant Advantage Input** to display the Add Mandiant Advantage Input modal.
3. Complete the form with the desired options and click **Save**.



The Indicator Collection and Offense Enrichment processes will start to function.

Dashboard

The **Mandiant Advantage Dashboard** is accessed from the main navigation menu of the QRadar Console. It displays a list of indicators ingested into the system. Filters are provided to help you locate indicators of interest.



The screenshot shows the IBM QRadar console interface. At the top, there are navigation tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, Pulse, Reference Data Management, Threat Intelligence, Mandiant Advantage Dashboard, and Pre-Validation. Below the navigation is a search bar and a 'Report an Incident' button. The main content area displays a table titled 'Recent 1000 Collected Indicators'. The table has columns for Indicator Value, Indicator Type, M-Score, Sources, Indicator First Seen, Indicator Last Seen, Associated Actors, and Associated Malwares. The table contains 15 rows of data, with the first 10 rows showing indicators with M-Scores of 91, 97, 100, 100, 100, 100, 100, 100, 93, and 95. The last two rows show indicators with M-Scores of 87 and 89. The 'Associated Malwares' column contains buttons for PRIVATELOADER, QAKBOT, SMOKELOADER, and EMOTET. The 'Associated Actors' column contains buttons for UNC3443.

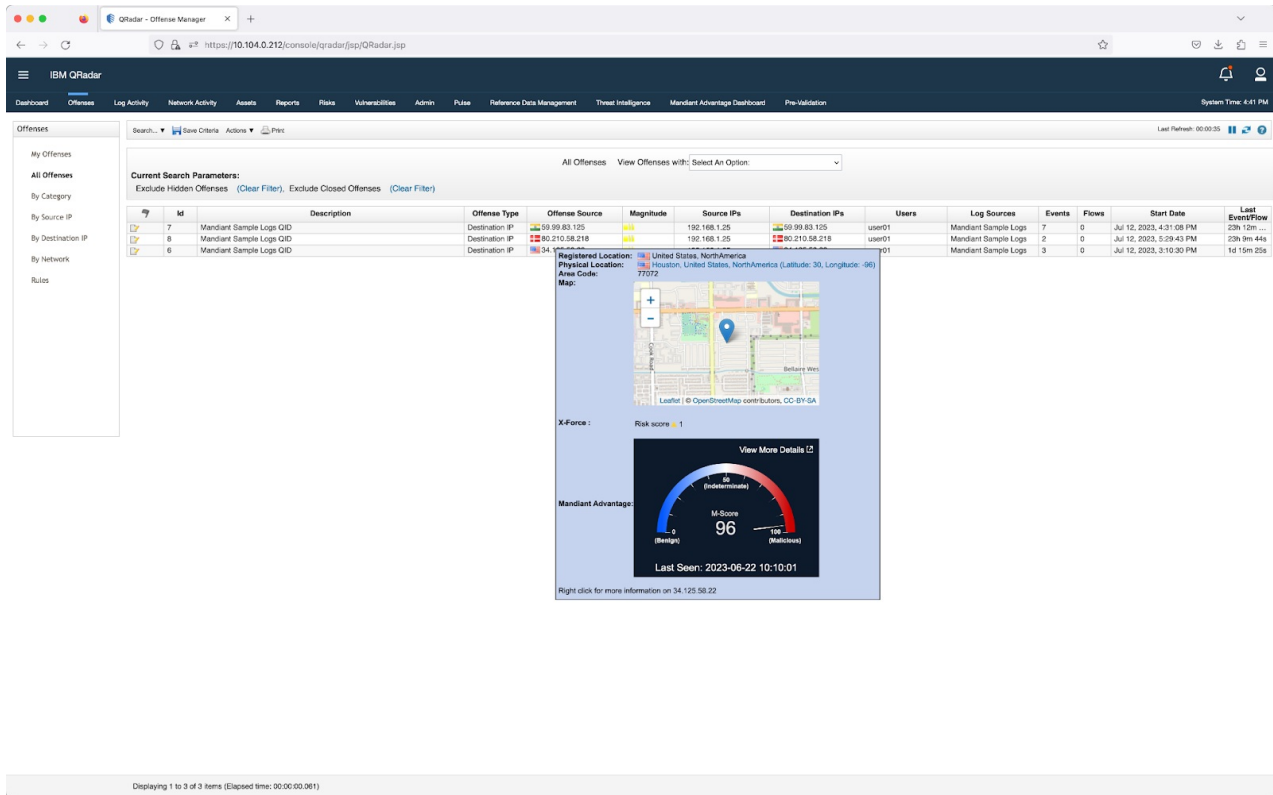
Indicator Value	Indicator Type	M-Score	Sources	Indicator First Seen	Indicator Last Seen	Associated Actors	Associated Malwares
https://ustl.sw/ign.exe	url	91	Mandiant	2023-07-13 12:16:55	2023-07-13 12:17:28		PRIVATELOADER
https://86.195.14.72:2222/5	url	97	Mandiant	2022-12-20 16:42:28	2023-07-13 12:16:40		QAKBOT
b792df14d4da19da44f0b79219dbaa66a32c7893	sha1	100	Mandiant, urlhaus	2023-07-13 12:01:13	2023-07-13 12:14:03		SMOKELOADER
cbde0d9980223aab719609ef0b18196b	md5	100	Mandiant, urlhaus	2023-07-13 12:01:13	2023-07-13 12:14:03		SMOKELOADER
39acba0d3df2c0a15b1879c6775d5c10e12Diae68183181076d58c1d7a90b6	sha256	100	Mandiant, urlhaus	2023-07-13 12:01:13	2023-07-13 12:14:03		SMOKELOADER
fd873ad940b380faa7cfc883ccfa7cc	md5	100	Mandiant, urlhaus	2023-07-13 12:01:17	2023-07-13 12:13:44		SMOKELOADER
6ca904d7d7e51bc966ec96b2956876d149f5c5a22e2109b4c6159642a9d271d5e	sha256	100	Mandiant, urlhaus	2023-07-13 12:01:17	2023-07-13 12:13:44		SMOKELOADER
1016845af6c685ac5b45a083586c74b3c208aaa3	sha1	100	Mandiant, urlhaus	2023-07-13 12:01:17	2023-07-13 12:13:44		SMOKELOADER
https://159.8.59.82:8080	url	93	Mandiant	2022-01-27 08:09:16	2023-07-13 12:10:47	UNC3443	EMOTET
https://176.56.128.118:443	url	95	Mandiant	2022-03-22 16:46:43	2023-07-13 12:10:47		EMOTET
https://176.104.106.96:8080	url	95	Mandiant	2021-11-18 18:43:30	2023-07-13 12:10:47	UNC3443	EMOTET
45.118.135.203	ipv4	99	Mandiant, blocklist_net_ua	2021-09-27 18:34:12	2023-07-13 12:10:47	UNC3443	EMOTET
rescator.sh	fqdn	87	dtm.vanellope, dtm.blackbeard, Mandiant	2021-01-12 18:22:54	2023-07-13 12:10:35		
rescator.cm	fqdn	89	Mandiant, dtm.vanellope, imperium_ra8, dtm.blackbeard	2017-12-18 18:34:02	2023-07-13 12:10:35		

Hover Enrichment

Wherever one of the following data types are displayed in the QRadar console, Hover Enrichment is available for the value:

- IP Address
- Indicator Value
- URL
- SHA 256 Hash
- File Hash

On hover, the value is checked against the Mandiant API. If the value is known to Mandiant, the **IC Score**, **Last Seen** date, and a link to the indicator in the Mandiant Advantage platform is displayed.



The screenshot shows the IBM QRadar console interface. The main area displays a table of offenses with columns for ID, Description, Offense Type, Offense Source, Magnitude, Source IPs, Destination IPs, Users, Log Sources, Events, Flows, Start Date, and Last Event/Flow. A map view is overlaid on the table, showing a location in Houston, United States, with a risk score of 1 and a Mandiant Advantage score of 96. The map includes a registered location, physical location, and area code. The console also shows search parameters and navigation tabs like Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, Pulse, Reference Data Management, Threat Intelligence, Mandiant Advantage Dashboard, and Pre-Validation.

ID	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start Date	Last Event/Flow
7	Mandiant Sample Logs QID	Destination IP	59.99.83.125	High	192.168.1.25	59.99.83.125	User01	Mandiant Sample Logs	7	0	Jul 12, 2023, 4:31:08 PM	23h 12m ...
8	Mandiant Sample Logs QID	Destination IP	80.210.58.218	High	192.168.1.25	80.210.58.218	User01	Mandiant Sample Logs	2	0	Jul 12, 2023, 5:29:43 PM	23h 9m 44s
6	Mandiant Sample Logs QID	Destination IP	34	High			User01	Mandiant Sample Logs	3	0	Jul 12, 2023, 2:10:30 PM	1d 15m 25s

Troubleshooting

Accessing the container to view logs

QRadar apps run as Docker containers on the QRadar host. To access a shell of the container running the app:

1. Run this command to find the installed apps:

```
psql -U qradar
select id, name from installed_application;
```

2. View what apps are running:

```
docker ps -a
```

3. Look for the ID of the Mandiant app and copy the Container ID.
4. Run this command to start a shell on the container:

```
docker container exec -it CONTAINER_ID /bin/bash
```



Log files are written to this directory: `opt/app-root/store/log`

Release Notes

- v1.1.1

- **New Features:**

- Added a setting to override the Syslog server for use when ingesting data.
- Added a setting to **Enable/Disable** automated Offense enrichment.
- Added a setting to **Include/Exclude** Open Source indicators.



Default is **Exclude** to limit the number of indicators added to QRadar Reference Sets.

- The Mandiant Indicator QRadar Reference Sets are now recreated on every update to ensure they always contain the latest Threat Intelligence.
 - Indicators that drop below the **Minimum IC Score** specified in the **Input** definition are now included in the QRadar index so the lifecycle of an indicator can be seen in QRadar.
 - The app now uses the Mandiant API Base URL.
- **Bug Fixes:**
- Fixed an issue where QRadar Offenses were enriched multiple times with the same information.
 - Fixed an issue where the app would fail to connect to QRadar through Syslog, causing data ingestion to fail.