ThreatConnect – MVISION Insights

User Documentation

May 2021

Changelog

Martin Ohl	v.0.1	15. March 2021
Martin Ohl	v.0.2	21. April 2021
Martin Ohl	v.0.3	04. May 2021

Overview

The purpose of this document is to provide a detailed understanding of the integration between McAfee MVISION Insights and the ThreatConnect Platform.

MVISION Insights provides customers direct access to malicious campaign information including Indicators of Compromise (IOC's), MITRE Techniques and additional details related to the campaign and adversary.

Intelligence at Scale

Fueled by the latest data with breadth to cover multiple attacks from over 1 billion sensors.

Rank and Anticipate Threats

Focus on endpoint threat insights that matter to you based on industry, geography and local security posture.

Actionable Endpoint Insights

Powerful machine learning-based insights weigh your risk for both known and unknown threats to not just deal with an attack, but also protect against future endpoint attacks.

MVISION Insights

Detailed Threat Assessments

Learn about active global campaigns including descriptions and indicators of compromise (IoCs) from the McAfee Advanced Threat Research team pivot to MVISION EDR to enrich your investigations.

Broad Understanding

Understand the prevalence of threats beyond your organization and the impact of the threats you face, including your ability to block and protect.

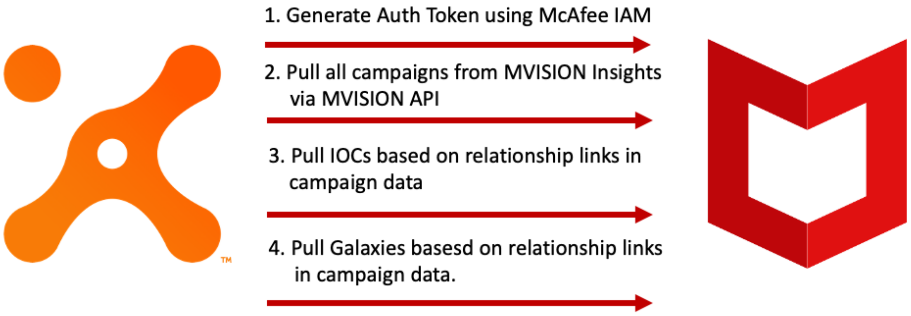
Proactive Endpoint Security

Endpoint Security posture assessments paired with the ability to take proactive action before you are hit let you improve your defenses quickly and easily.

The purpose of the integration is to pull threat data from the MVISION Insights platform on a scheduled basis via MVISION API.

The received data will be parsed and mapped to the ThreatConnect indicators and groups.

McAfee MVISION Insights will provide campaign details (descriptions, additional links, kb articles, minimum dat version, etc.), Indicator of Compromise (IOCs) and Galaxy information (MITRE Techniques, Tools, Threat Actors, etc.).



1. Generate Auth Token using McAfee IAM

2. Pull all campaigns from MVISION Insights via MVISION API

3. Pull IOCs based on relationship links in campaign data

4. Pull Galaxies basesd on relationship links in campaign data.

Requirements

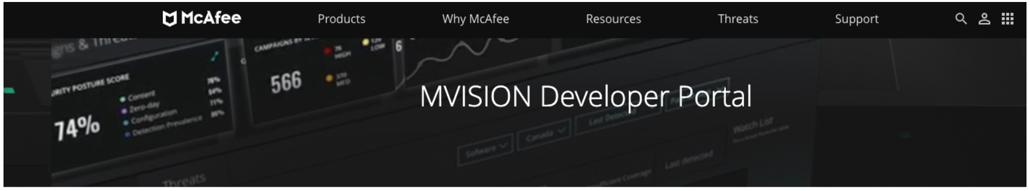
In order to use the MVISION Insights integration on the ThreatConnect platform a MVISION API license is required. This license provides access to the McAfee Developer Hub (Link) as well as the MVISION Insights APIs.

Preperation

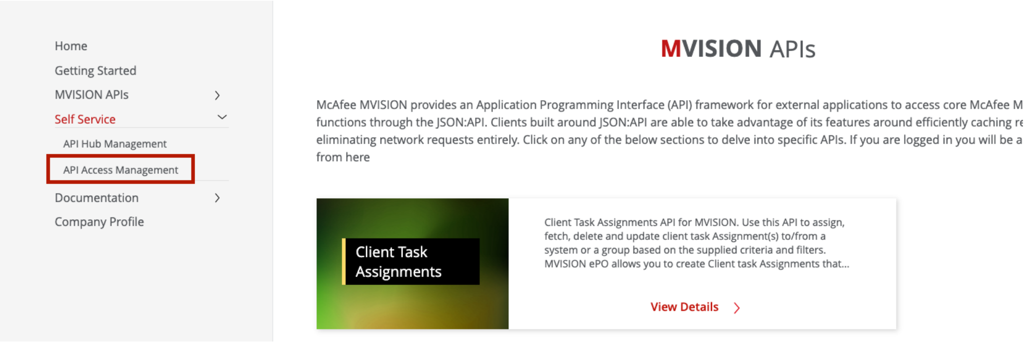
This section provides details on the API Access Management and the required scopes in order to pull data from MVISION Insights via the MVISION API Gateway.

1. Go to the McAfee Developer Hub
   https://developer.mcafee.com

2. Click on Explore and go to the Self Service section and select API Access Management



MVISION Developer Portal



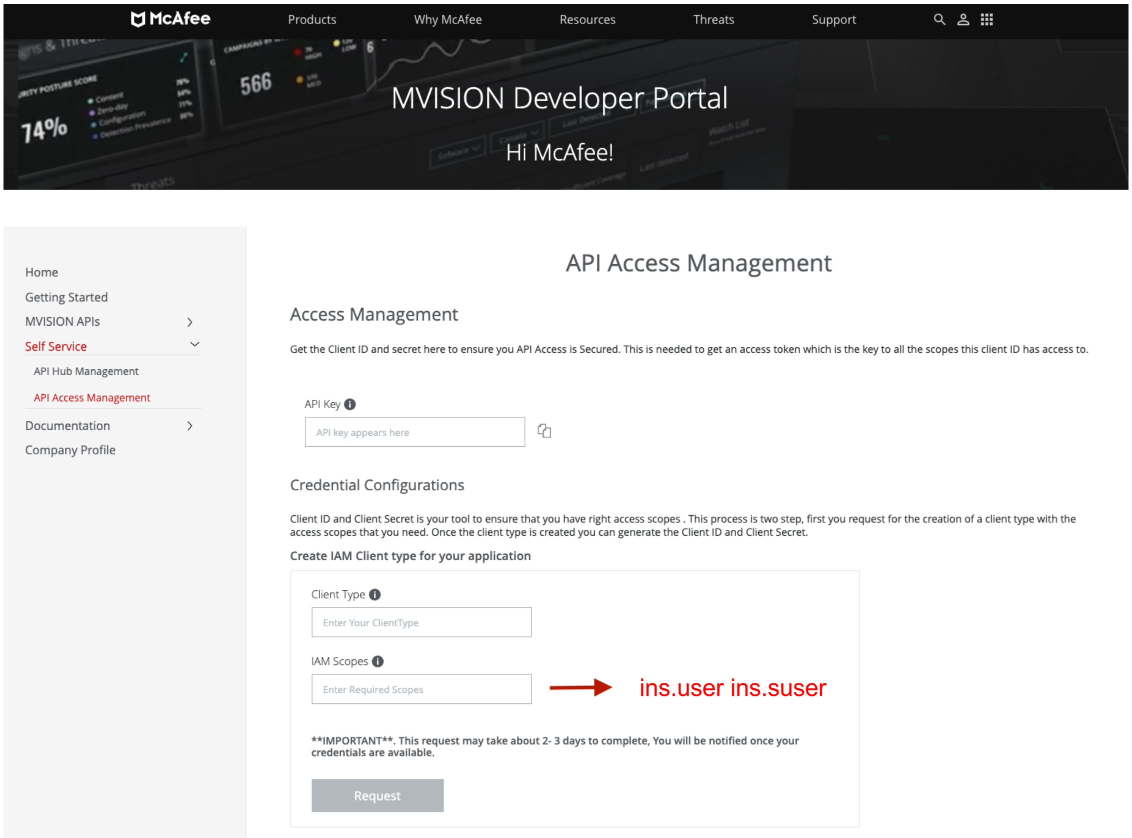
MVISION APIs

McAfee MVISION provides an Application Programming Interface (API) framework for external applications to access core McAfee M functions through the JSON:API. Clients built around JSON:API are able to take advantage of its features around efficiently caching re eliminating network requests entirely. Click on any of the below sections to delve into specific APIs. If you are logged in you will be a from here

Client Task Assignments

Client Task Assignments API for MVISION. Use this API to assign, fetch, delete and update client task Assignment(s) to/from a system or a group based on the supplied criteria and filters. MVISION ePO allows you to create Client task Assignments that...

3. Log in with your MVISION Credentials
4. In the Access Management define a client type and type **ins.user ins.suser** in the IAM scopes.



MVISION Developer Portal

Hi McAfee!

API Access Management

Access Management

Get the Client ID and secret here to ensure you API Access is Secured. This is needed to get an access token which is the key to all the scopes this client ID has access to.

API Key

API key appears here

Credential Configurations

Client ID and Client Secret is your tool to ensure that you have right access scopes . This process is two step, first you request for the creation of a client type with the access scopes that you need. Once the client type is created you can generate the Client ID and Client Secret.

Create IAM Client type for your application

Client Type

Enter Your ClientType

IAM Scopes

Enter Required Scopes

ins.user ins.suser

IMPORTANT. This request may take about 2- 3 days to complete, You will be notified once your credentials are available.

****IMPORTANT**. This request may take about 2- 3 days to complete, You will be notified once your credentials are available.**

5. After the request has been accepted you will be provided with three keys that are required for the ThreatConnect MVISION Insights integration.

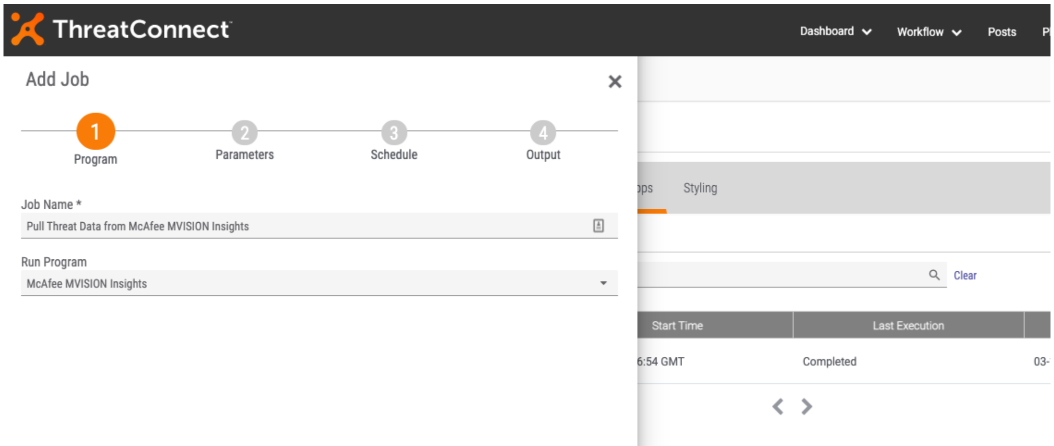
   a. **API Key**
   b. **Client ID**
   c. **Client Secret**

ThreatConnect In-Platform Installation Instruction

For installation instructions, check the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

ThreatConnect Integration Configuration

1. Add a new job in ThreatConnect, provide a Job name and select McAfee MVISION Insights under Run Program. Click Next.



Add Job

Job Name *
Pull Threat Data from McAfee MVISION Insights

Run Program
McAfee MVISION Insights

2. Under Parameters enter the API Key, Client ID and Client Secret. (Accessible through the developer portal – see Preperation)

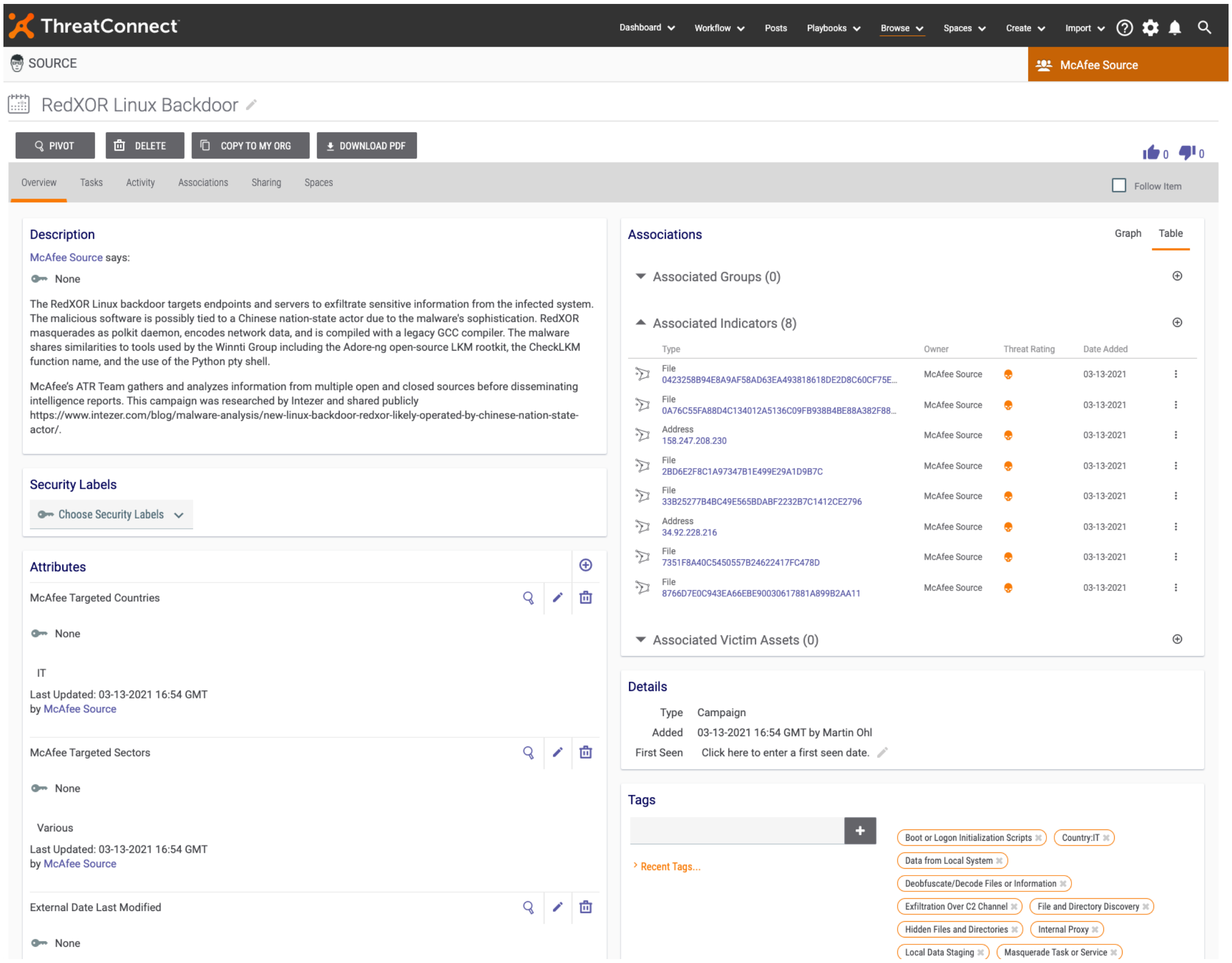
3. Leave last_run at Never. This guarantees that the initial pull will download Campaigns, assiociated indicators, MITRE techniques, Threat Actors, etc from the **last 7 days**. After the first run this field will be updated with the last pulling date.

4. Click Next

5. The integration is intended to run **once per day**. During the execution the integration will only ingest new or updated campaigns (and associated indicators, galaxies, etc.).

MVISION Insights Data in ThreatConnect

McAfee MVISION Insights data will be ingested on scheduled basis. All Campaigns, Indicators, Mitre Techniques, Threat Actors, Targeted Sectors and Targeted Verticals are associated to each other which allows the pivot from a Campaign to the associated indicators and threat actors.



RedXOR Linux Backdoor

Description

McAfee Source says:

None

The RedXOR Linux backdoor targets endpoints and servers to exfiltrate sensitive information from the infected system. The malicious software is possibly tied to a Chinese nation-state actor due to the malware's sophistication. RedXOR masquerades as polkit daemon, encodes network data, and is compiled with a legacy GCC compiler. The malware shares similarities to tools used by the Winnti Group including the Adore-ng open-source LKM rootkit, the CheckLKM function name, and the use of the Python pty shell.

McAfee's ATR Team gathers and analyzes information from multiple open and closed sources before disseminating intelligence reports. This campaign was researched by Intezer and shared publicly https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/.

Security Labels

Choose Security Labels

Attributes

McAfee Targeted Countries

None

IT

Last Updated: 03-13-2021 16:54 GMT
by McAfee Source

McAfee Targeted Sectors

None

Various

Last Updated: 03-13-2021 16:54 GMT
by McAfee Source

External Date Last Modified

None

Associations

Associated Groups (0)

Associated Indicators (8)

Type	Owner	Threat Rating	Date Added
File 0423258B94E8A9AF58AD63EA493818618DE2D8C60CF75E…	McAfee Source	●	03-13-2021
File 0A76C55FA88D4C134012A5136C09FB938B4BE88A382F88…	McAfee Source	●	03-13-2021
Address 158.247.208.230	McAfee Source	●	03-13-2021
File 2BD6E2F8C1A97347B1E499E29A1D9B7C	McAfee Source	●	03-13-2021
File 33B25277B4BC49E565BDABF2232B7C1412CE2796	McAfee Source	●	03-13-2021
Address 34.92.228.216	McAfee Source	●	03-13-2021
File 7351F8A40C5450557B24622417FC478D	McAfee Source	●	03-13-2021
File 8766D7E0C943EA66EBE90030617881A899B2AA11	McAfee Source	●	03-13-2021

Associated Victim Assets (0)

Details

Type	Campaign
Added	03-13-2021 16:54 GMT by Martin Ohl
First Seen	Click here to enter a first seen date.

Tags

Recent Tags...

Boot or Logon Initialization Scripts
Country:IT
Data from Local System
Deobfuscate/Decode Files or Information
Exfiltration Over C2 Channel
File and Directory Discovery
Hidden Files and Directories
Internal Proxy
Local Data Staging
Masquerade Task or Service

McAfee Support

For additional information and support please contact McAfee Support

https://support.mcafee.com/