SecuLast - MalnalysisCloud ThreatConnect Integration

Overview

The purpose of this document is to provide a detailed understanding of the integration between MalnalysisCloud from SecuLast and the ThreatConnect Platform. This document provides a high-level overview as well as details about the integration. This document is intended for the technical audience.

Integration Description

This integration allows a ThreatConnect user to perform file analysis lookups using the MalnalysisCloud by providing a file or hash (SHA1, SHA256, or MD5) and retrieve on-demand information about any potential threats. A file is analyzed within the MalnalysisCloud using our patented AI and ML technologies and a proprietary sandbox that overcomes most common forms of sandbox detection. The information made available through this integration is made available to ThreatConnect Playbooks.

Problem Statements

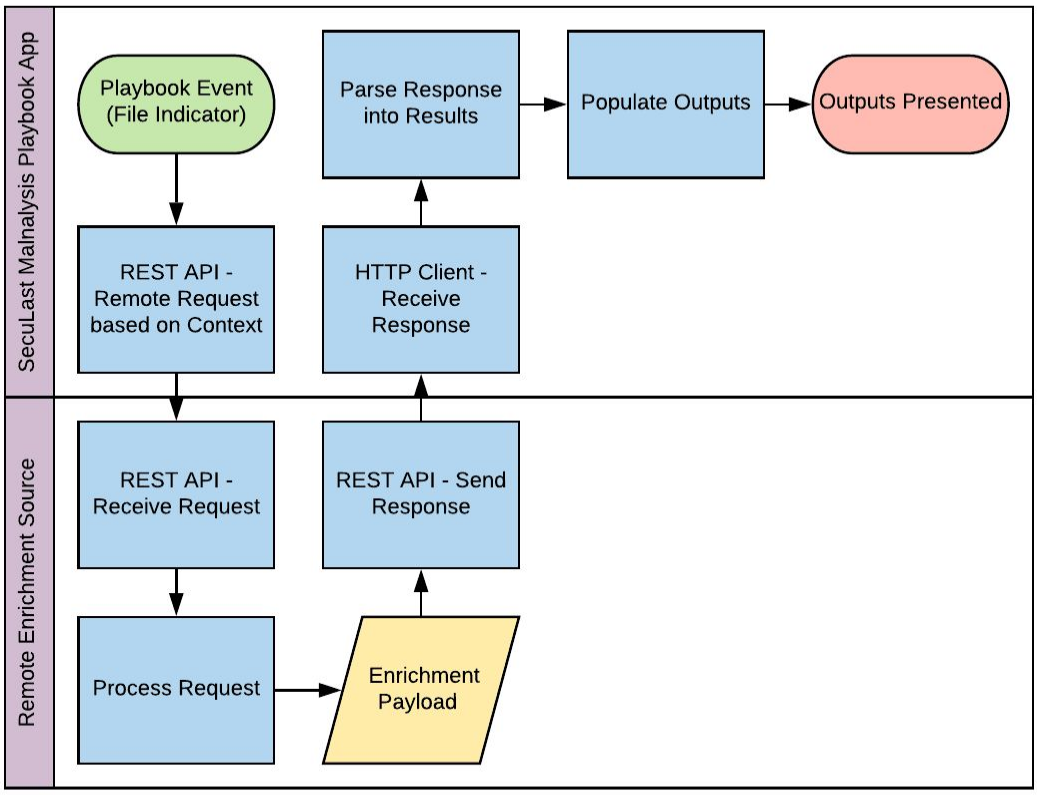
This integration addresses the following problems:

1. Customers of SecuLast that also currently use the ThreatConnect Platform have a desire to be able to retrieve the results of existing MalnalysisCloud scans into ThreatConnect Playbook flows.
2. Customers of SecuLast that also currently use the ThreatConnect Platform have a desire to be able to submit one or more files and perform an on-demand scan to be used in ThreatConnect Playbook flows.

Integration Diagram

File Hash Lookup for Previous Results

This section describes the flow used when an existing scan result is desired. A file hash is provided as input and results are provided.

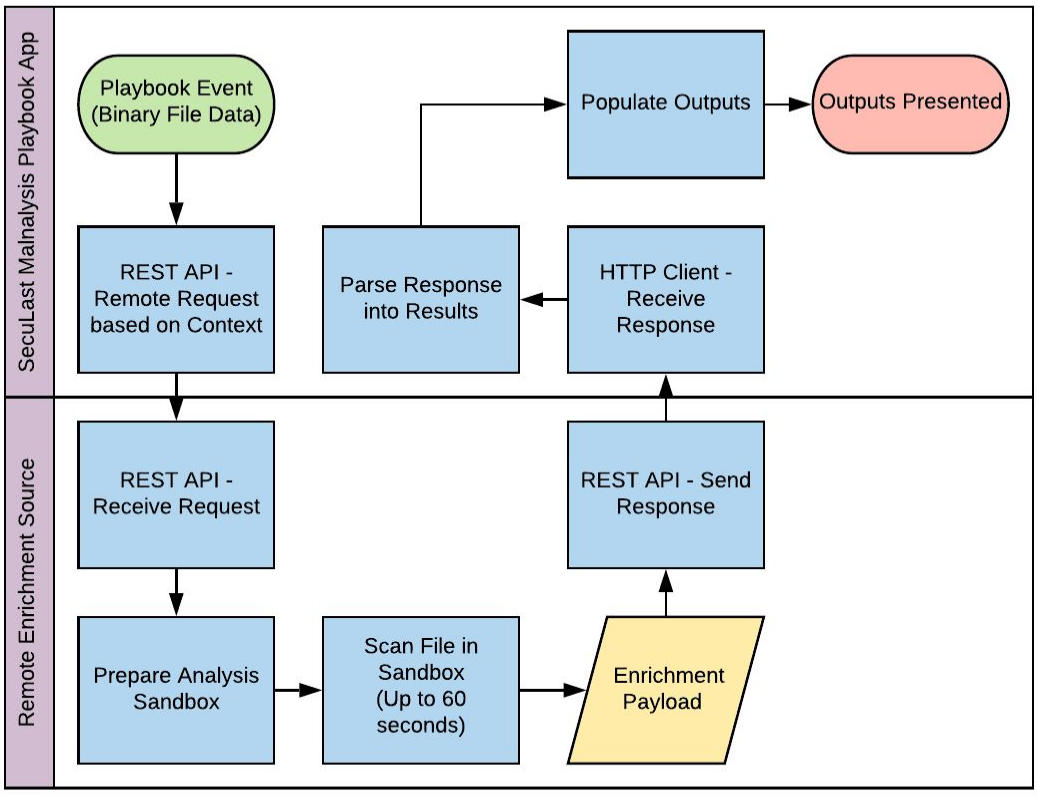


In this diagram above, the following sequence of events takes place:

1. The SecuLast Malnalysis app is used in a Playbook workflow. A file hash is provided as input.
2. The SecuLast Malnalysis app performs a lookup against the Malnalysis Cloud environment.
3. The available attributes about this file from the SecuLast Malnalysis Cloud are provided back in a response.
4. The response results are prepared into outputs for the Playbook app.

File Analysis in Sandbox

This section describes the flow used when a new file should be scanned using the Malnalysis Cloud sandbox environment. A binary file is provided and uploaded for analysis. Results of the scan are provided.



In this diagram above, the following sequence of events takes place:

1. The SecuLast Malnalysis app is used in a Playbook workflow. A binary variable or Document object is provided as input.
2. The SecuLast Malnalysis app uploads the file data to the Malnalysis Cloud environment.
3. A sandbox environment is prepared on-demand to scan this file.
4. The file is analyzed within the sandbox environment (for up to 60 seconds).
5. The available attributes about this file from the SecuLast Malnalysis Cloud are provided back in a response.
6. The response results are prepared into outputs for the Playbook app.

Integration Details

File Hash Lookup for Previous Results

This function of the integration is responsible for providing the ability to retrieve existing scan results for a file from the Malnalysis Cloud environment.

Configuration

This function of the app has the following inputs in this configuration (based on Layouts):

- Operation - set to “File Hash Lookup”
- A file hash (SHA1, SHA256, or MD5) or File Indicator (TCEntity) object - String or TCEntity
- SecuLast Malnalysis Cloud API ID - String
- SecuLast Malnalysis Cloud API Secret - String
- Fail on error - Checkbox (default to True)
- Fail on no results - Checkbox (default to False)

Outputs

The following outputs are provided with this operation.

Output Name	TC Data Type	Possible Values	Notes
sl.results.status	String	“Success” or “Failure”	Designates whether or not the call succeeded.
sl.results.status.code	String	“200”, “404”, or “500”	Status code for the request. 200 - Results provided. 404 - No hash found. 500 - Error with the submission.
sl.results.status.msg	String	Text description of an error response.	Only applicable on 404 and 500 status_code.
sl.results.file.hash_sha256	String	Valid SHA256	SHA256 of the file lookup.
sl.results.file.hash_sha1	String	Valid SHA1	SHA1 of the file lookup. This value may not always be available.
sl.results.file.hash_md5	String	Valid MD5	MD5 of the file lookup. This value may not always be available.
sl.results.file.malware_family	StringArray	Text strings of name	Names of the malware families represented by this hash.
sl.results.file.tags	StringArray	Text strings of name	Tags applied by the Malnalysis Cloud for this sample.
sl.results.file.attack_mapping	KeyValueArray	KVA of StringArrays	Dictionary object with a key of the MITRE ATT&CK tactic and values of the MITRE ATT&CK techniques applicable to this sample. These values are based on MITRE ATT&CK Enterprise.
sl.results.threat_rating	String	0-5	Mapped from the threat rating scale of 1-10 from SecuLast.

sl.results.threat_confidence	String	0-100	Mapped from the threat confidence scale of 1-50 from SecuLast.

Requirements

This scenario has the following requirements:

- SecuLast Malnalysis subscription (Free or higher)

Assumptions

This scenario has no known assumptions.

File Analysis in Sandbox

This function of the integration is responsible for providing a facility to receive a file, perform an on-demand analysis, and provide the scan results for the input file from the Malnalysis Cloud environment.

Configuration

This function of the app has the following inputs in this configuration (based on Layouts):

- Operating - set to “File Analysis”
- File - Binary input of the file to be analyzed
- SecuLast Malnalysis Cloud API ID - String
- SecuLast Malnalysis Cloud API Secret - String
- Fail on error - Checkbox (default to True)

Outputs

The following outputs are provided with this operation.

Output Name	TC Data Type	Possible Values	Notes
sl.results.status.code	String	“200”, “404”, or “500”	Status code for the request. 200 - Results provided. 202 - File accepted but still being analyzed. Check again later. 500 - Error with the submission.
sl.results.status.msg	String	Text description of an error response.	Only applicable on 500 status.code.
sl.results.file.hash_sha256	String	Valid SHA256	SHA256 of the file.
sl.results.file.hash_sha1	String	Valid SHA1	SHA1 of the file.

sl.results.file.hash_md5	String	Valid MD5	MD5 of the file.
sl.results.file.malware_family	StringArray	Text strings of name	Names of the malware families represented by this hash. Only applicable with 200 status.code.
sl.results.file.tags	StringArray	Text strings of name	Tags applied by the Malnalysis Cloud for this sample. Only applicable with 200 status.code.
sl.results.file.attack_mapping	KeyValueArray	KVA of StringArrays	Dictionary object with a key of the MITRE ATT&CK tactic and values of the MITRE ATT&CK techniques applicable to this sample. These values are based on MITRE ATT&CK Enterprise. Only applicable with 200 status.code.
sl.results.threat_rating	String	0-5	Mapped from the threat rating scale of 1-10 from SecuLast. Only applicable with 200 status.code.
sl.results.threat_confidence	String	0-100	Mapped from the threat confidence scale of 1-50 from SecuLast. Only applicable with 200 status.code.

Requirements

This scenario has the following requirements:

- SecuLast Malnalysis subscription (Professional or higher)

Assumptions

This scenario has the following assumptions:

- The size of File is less than 200MB.