SecuLast - Malware Threat Intelligence ThreatConnect Integration

Overview

The purpose of this document is to provide a detailed understanding of the integration between Malware Threat Intelligence 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 the ingestion of the threat intelligence data provided in the SecuLast Malware Threat Intelligence feeds into the ThreatConnect Platform. Malware Threat Intelligence is offered in 3 different feeds: Addresses (C2 servers), Hosts (C2 servers), Files (MD5, SHA1, and SHA256 hashes). Using this integration, this data becomes usable within the ThreatConnect Platform as part of security activities.

Problem Statements

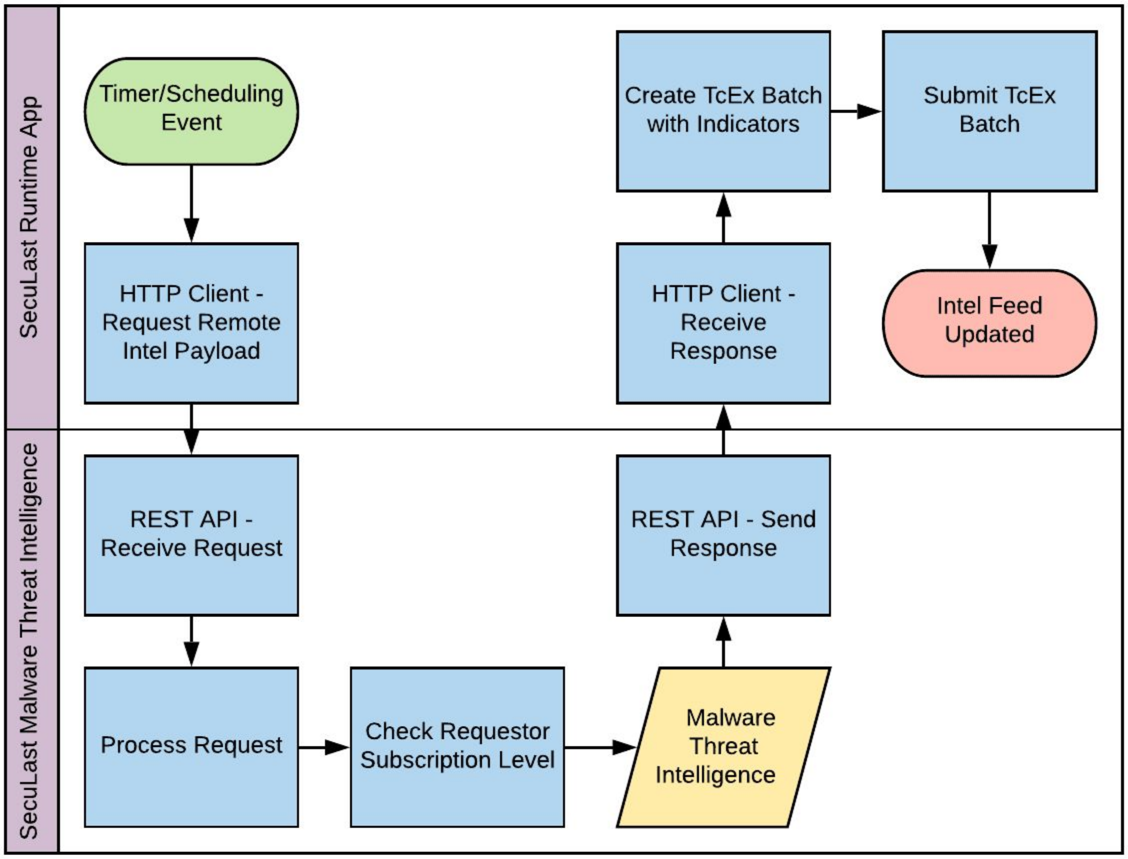
This integration addresses the following problems:

1. Customers of SecuLast that also currently use the ThreatConnect Platform have a desire to be able to ingest the Malware Threat Intelligence feeds into the ThreatConnect Platform for analysis, collaboration, and action.
2. Existing customers and prospects of ThreatConnect may desire a unique Malware Threat Intelligence solution that provides a validated and curated set of high-rating, high-confidence indicators.

Integration Diagram

Malware Threat Intelligence Flow

This section describes the function of the Malware Threat Intelligence at a high-level. See Malware Threat Intelligence for additional detail.


SecuLast Runtime App
SecuLast Malware Threat Intelligence
Timer/Scheduling Event
HTTP Client - Request Remote Intel Payload
REST API - Receive Request
Process Request
Check Requestor Subscription Level
Malware Threat Intelligence
REST API - Send Response
HTTP Client - Receive Response
Create TcEx Batch with Indicators
Submit TcEx Batch
Intel Feed Updated

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

1. A timer/scheduling event takes place in the ThreatConnect Platform to initiate the SecuLast Runtime App.
2. An HTTP client requests the Malware Threat Intelligence payload. This request will include data about the specific intelligence requested along with the SecuLast API Key for identification.
3. The SecuLast systems receive this request via our REST API.
4. The SecuLast system will process the request to determine what information is being requested.
5. The SecuLast system will check the subscription level for the supplied SecuLast API Key to determine how much historical data will be included in the response.
6. The Malware Threat Intelligence is compiled together in a payload.
7. The SecuLast REST API responds with this payload.
8. The HTTP client in the SecuLast Runtime App receives the response.
9. The data is parsed and turned into a TcEx Batch.
10. Once all data is parsed, the TcEx Batch is submitted into the platform to store the Malware Threat Intelligence data.
11. The SecuLast Runtime App cycle is complete.

Integration Details

Malware Threat Intelligence

This function of the integration is responsible for acquiring and storing the SecuLast Malware Threat Intelligence within the ThreatConnect platform. This is the sole function of this integration.

Configuration

The SecuLast Malware Threat Intelligence Runtime App will be configured using the Feed Deployer Wizard in the ThreatConnect Platform. The following configuration values are required:

1. Minimum SecuLast threat rating to be ingested.
2. Specific SecuLast Malware Threat Intelligence feeds to be consumed.
3. Score Rounding for going up or down when performing division against the SecuLast score.

The default timing for the Feed Deployer Wizard job will be to run every 2 hours at all times.

Data Mapping

The table below documents the data mapping that takes place between the SecuLast Malware Threat Intelligence data and the ThreatConnect Platform.

Malware Threat Intelligence Field	ThreatConnect Field/Object	Possible Values	Notes
C2Address	Addresses, Tag “C2 Address”	Any valid IP address	
C2Hostname	Hosts, Tag “C2 Hosts”	Any valid hostname	
MalwareFileHashes (SHA1|SHA256|MD5)	Files (MD5:SHA1:SHA256)	Any valid hash values for the given types	If a hash is unavailable, this field will be left blank in the ThreatConnect Platform.
ThreatName	Group	Any text string	Each related Address, Host, or File becomes associated with this Group.
ThreatScore (1-10)	Threat Rating (1-5)	Numbers 1 - 5	The ThreatScore field is divided by 2 and rounded by the Score Rounding value (up/down).
ThreatConfidence	Confidence	Numbers 1 - 100	
FirstObservation	Attribute - First Seen	ISO 8601 Timestamp	

LatestObservation	Attribute - Last Seen	ISO 8601 Timestamp	
Category	Custom Attribute - SecuLast Category	Any text string	

Requirements

Malware Threat Intelligence has the following requirements:

- ThreatConnect paid subscription (you cannot use TCOpen).
- At least one ThreatConnect API user.
- SecuLast Malware Threat Intelligence API Key (this is available in the SecuLast portal).
- SecuLast Custom Attributes (noted above) configured in the ThreatConnect instance to be used. This is handled automatically when Feed Deployer is used.

Design Assumptions

This design has the following assumptions:

- Indicator deprecation is handled automatically by the ThreatConnect Platform using the Deprecation Rules configured for the owner of SecuLast Malware Threat Intelligence indicators.
- There is no retry logic built into the SecuLast Malware Threat Intelligence Runtime App. Failures will be logged and must be investigated by an organization administrator.
- The owner for SecuLast indicators on systems where the feed was deployed with the Feed Deployer Wizard will be “SecuLast Malware Threat Intelligence”.