ThreatConnect™

Developer Partner Program

Threat Intelligence Feed Integration

ThreatConnect.com

What is a Threat Intelligence Feed Integration?

Threat Intelligence from an external source is made available in the ThreatConnect Platform

Data maintained externally is brought into the Platform

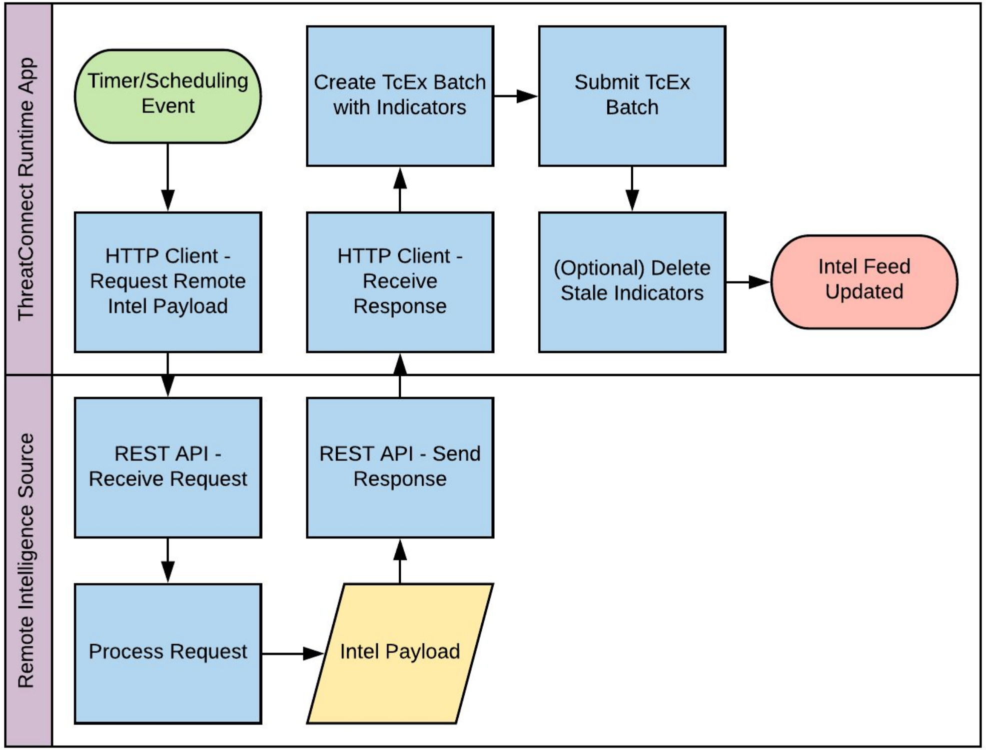
In-platform Runtime Apps (Python 3) are used in Jobs

Jobs run on a pre-defined schedule

Platform Installation Types

- Public Cloud
  - Multi-tenant mix of free and paid users
  - No Playbooks, cannot change system settings
- Private Instances (majority)
  - Fully private instance maintained by ThreatConnect in cloud infrastructure
  - Fully private instance maintained by the customer on customer infrastructure

Integration Flow Diagram


ThreatConnect Runtime App
Remote Intelligence Source
Timer/Scheduling Event
HTTP Client - Request Remote Intel Payload
REST API - Receive Request
Process Request
Intel Payload
REST API - Send Response
HTTP Client - Receive Response
Create TcEx Batch with Indicators
Submit TcEx Batch
(Optional) Delete Stale Indicators
Intel Feed Updated

Integration Key Points

- All subscription management must be done outside of the ThreatConnect Platform.
  - **We do not manage third-party subscriptions.**
- Data brought into ThreatConnect will have a unique “owner”.
  - **This represents your organization’s data in our data model.**
  - **In our Public Cloud, there will be multiple instances of your data.**
- Threat Rating and Confidence values must align with ThreatConnect best-practices.
  - **We have a blog post to assist.**
- Differential updates and indicator deletions are desired but not required.

What deliverables are expected?

For a typical integration, we look for these deliverables:

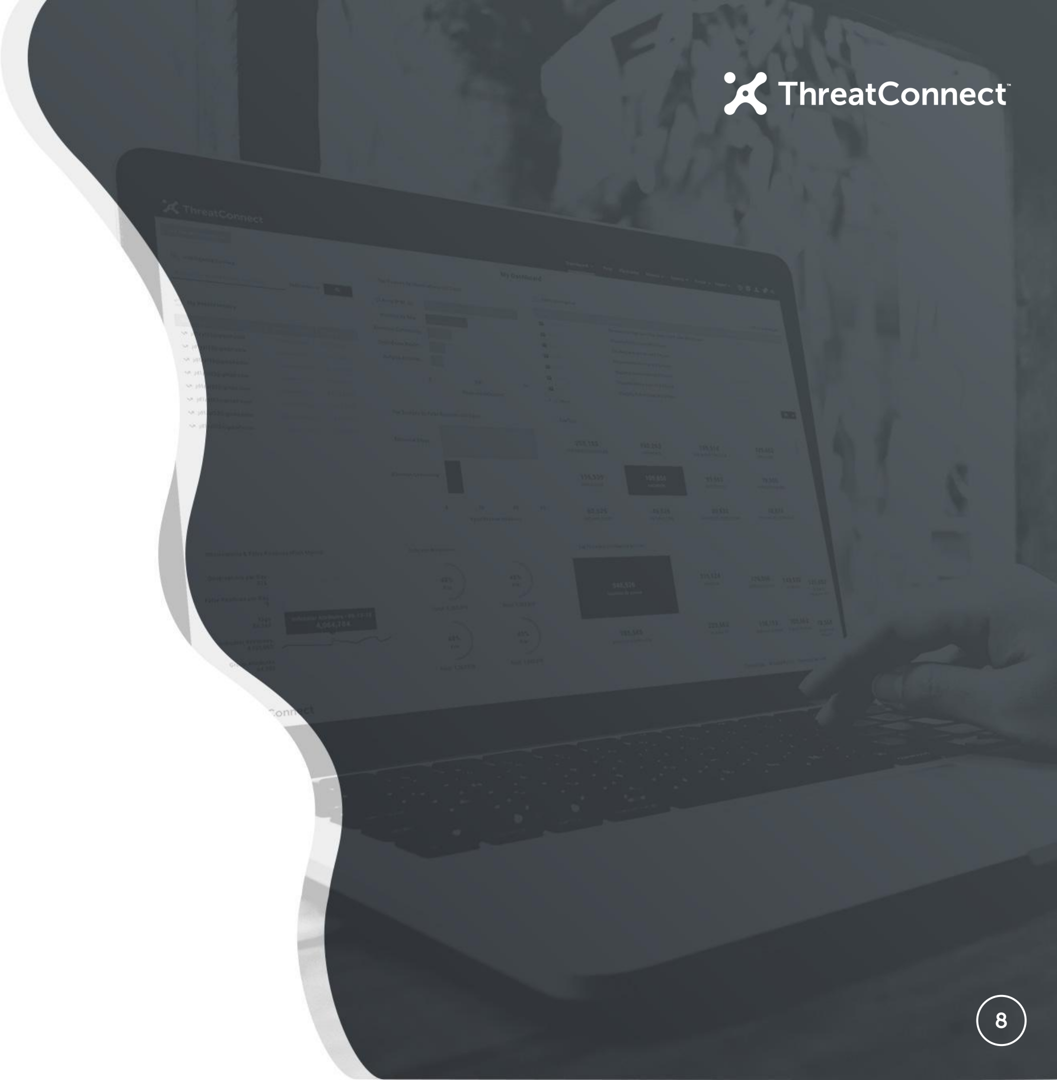
- Solution Design Document
- Runtime Package
- User Documentation and Media

Solution Design Document

- We provide a Solution Design Document template.
    - **You complete this template.**
    - **Document is meant to remain concise.**
- We'll review together and reconcile any concerns.
    - **We'll provide input on the design and try to guide you towards best-practices.**
- Once reviewed and approved, this document serves as a reference.
    - **Only minor updates are typically required.**
- This document is not published at this time.

User Documentation and Media

- Documentation delivered to customers and ThreatConnect teams.
  - Primarily used for setup and configuration.
  - A lot of information can be taken directly from the Solution Design Document.
- Brief video of the integration is used for ThreatConnect internally.
  - Our internal teams use this for a high-level overview of your solution.
  - You may choose to publish this video with your documentation.



High-Level Development Lifecycle

- Install and/or use a Python 3.6 environment.
- Install the ‘tcex’ module using pip3.
- Create a project directory.
- Run the ‘tcinit’ command with the template ‘job_batch’.
- Update the code appropriately and unit test within your own environment.
- Package the app using ‘tcpackage’ and pass to your Solutions Engineer.
- Solutions Engineer installs into the Sandbox and you perform in-platform tests.

ThreatConnect

Next Steps

- Your Solutions Engineer will provide you with documentation:
  - **Integration Documentation**
  - **Solution Design Document Template and Example**
- You will begin working through your design and completing the Solution Design Document Template
  - **We're here to support you via Slack and email and can stay up-to-date this way.**
  - **We can schedule calls as needed.**
- You will complete work on your project and then we'll review together.
  - **We may ask for changes during this process as we iron-out our program.**

Questions?

ThreatConnect.com

ThreatConnect™