ThreatConnect

Developer Partner Program

On-Demand Enrichment Integration

ThreatConnect.com

What is an On-Demand Enrichment Integration?

Information about existing or potential Indicators in the Platform is gathered from a remote source and made available in a Playbook.

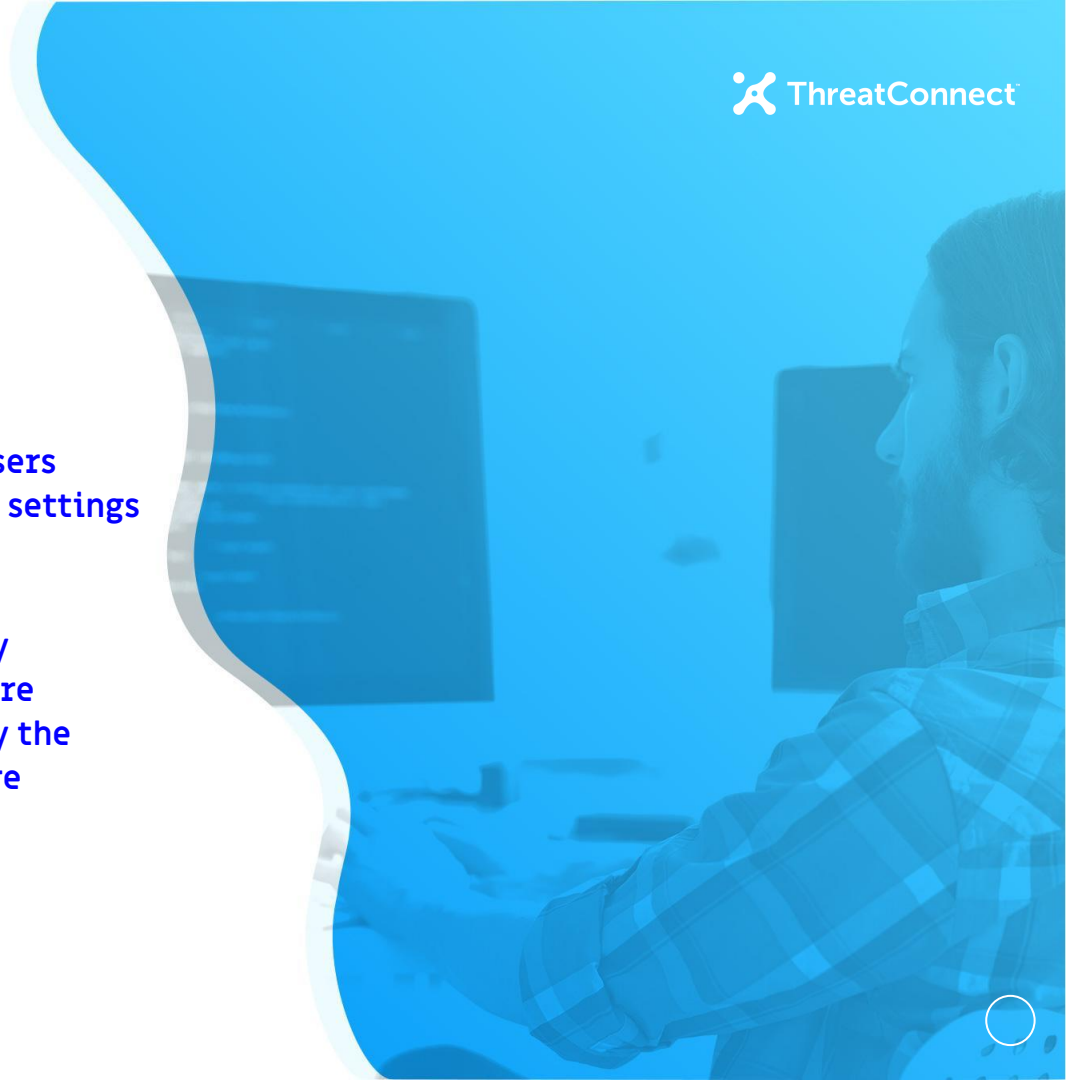
The enrichment App is triggered as part of a Playbook

The enrichment data is passed into the Playbook workflow

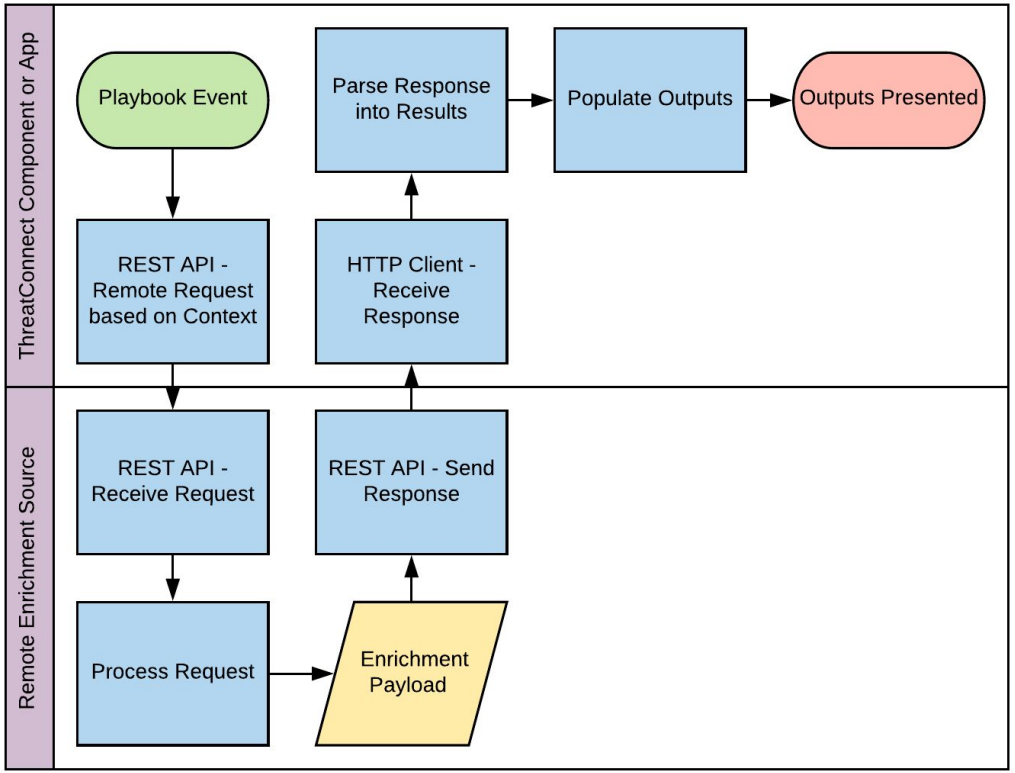
Playbook Apps are written in Python 3 using App Builder

Platform Installations

- 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



Integration Key Points

- Requests for external data should use our in-platform call within TcEx.
  - **This is a subclass of Request.**
- Output naming should follow our guidelines.
  - **Guidance in our Integration Cookbook.**
- Use Layouts functionality in most cases.
  - **This makes changes easier in the future.**
- Data should be mapped against our Data Model.
  - **This is included in the Solution Design.**
- Make use of in-platform Notes.
- Providing a Playbook Template helps people get started easier!

What deliverables are expected?

For a typical integration, we look for these deliverables:

Solution Design Document

Playbook App or Component Package

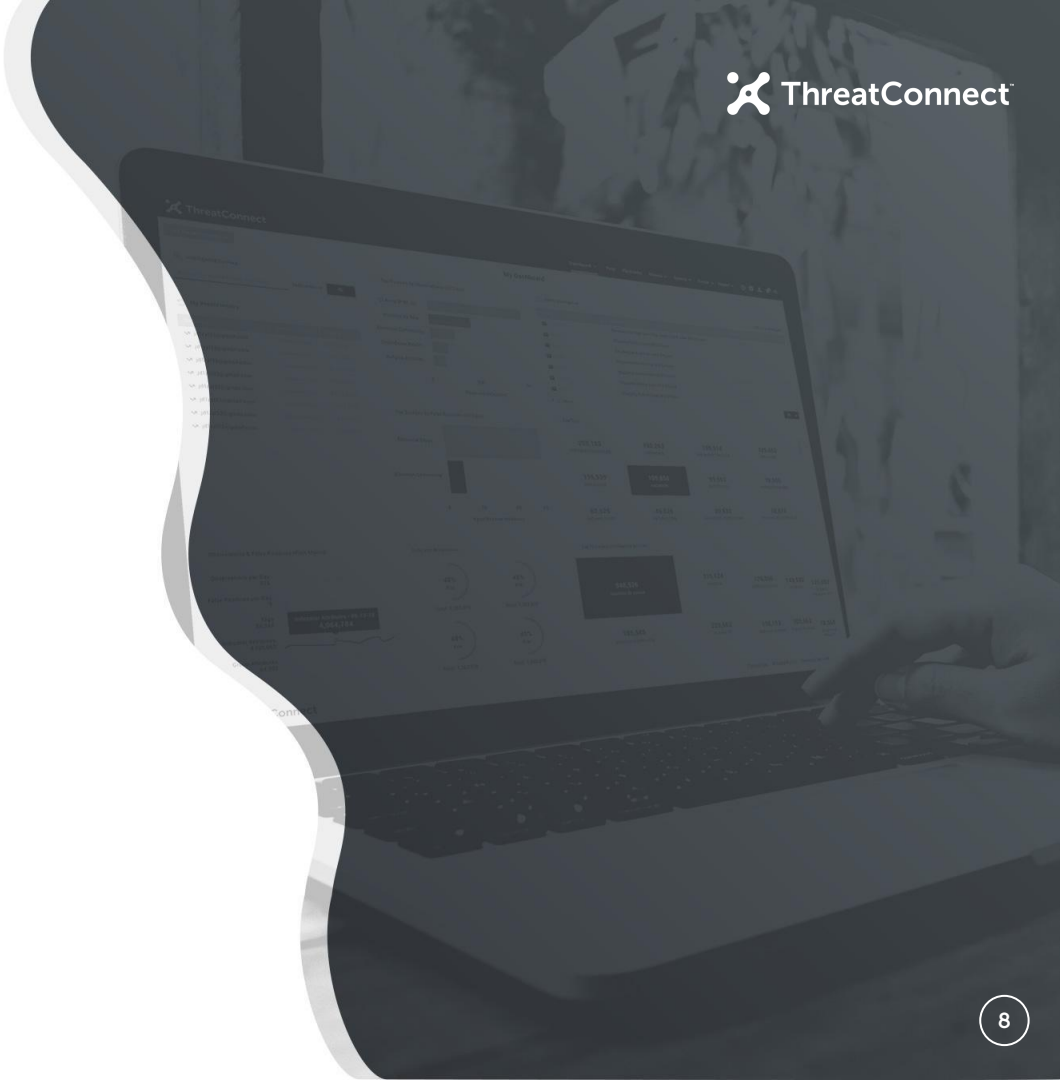
User Documentation and Media

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

- You create the your integration in-platform using either App Builder or Playbook Designer.
- In App Builder, you configure dependencies in requirements.txt, place code in the app.py (App class, run method).
- You create sample Playbooks and perform testing against your integration.
- Prepare User Documentation and Media.
- When ready for review, pass your downloaded project and documentation for review.
- Solutions Engineer installs and reviews.
- Upon approval, you post to your own GitHub and then submit PR to our GitHub.

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™