



# Developer Partner Program

External REST Integration



## What is an External REST Integration?

A remote application interacts with the ThreatConnect REST API to push or pull data



The entire workflow is maintained in the remote application



Retrieve a significant portion of the data model available



Commit external data for storage and enhancement

# Platform Installation Types

---

- Public Cloud
  - Multi-tenant mix of free and paid users
  - No Playbooks, cannot change system settings
  - REST API available via *api.threatconnect.com*
- Dedicated Cloud
  - Fully private instance maintained by ThreatConnect in cloud infrastructure
  - REST API available via *URL/api*
- On-Prem
  - Fully private instance maintained by the customer on customer infrastructure
  - REST API available via *URL/api* if exposed by customer



# Integration Key Points

---

- We require a SHA256 HMAC digest in our Authorization header.
  - **We provide an example of how to do this.**
- v2 Endpoints should be used for now.
  - **Most calls should still use this version.**
- Threat Rating and Confidence values must align with ThreatConnect best-practices.
  - **We have a blog post to assist.**
- Data should be mapped against our Data Model.
  - **This is included in the Solution Design.**
- You should support data owners.
  - **Our data model is oriented by owners.**
- Use ThreatAssess data when you can!
  - **This allows you to use our analytics.**

## What deliverables are expected?

---

For a typical integration, we look for these deliverables:



Solution Design  
Document



Integration  
Functionality



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 to provide a lot of detail to users on your implementation.**
  - **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.**
- One-page slide used for ThreatConnect internally.
  - **This provides a brief overview for our sales teams on the integration's value.**

# High-Level Development Lifecycle

---

- You prepare the integration in your platform based on the Solution Design.
- You perform all of the appropriate testing for the integration using the Sandbox.
- Prepare User Documentation and Media.
- When ready for review, you provide us with access to your integration for testing.
- Solutions Engineer reviews against your design and documentation.
- Upon approval, you release your integration using your normal channels.



# 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](https://ThreatConnect.com)

