Developer Partner Program
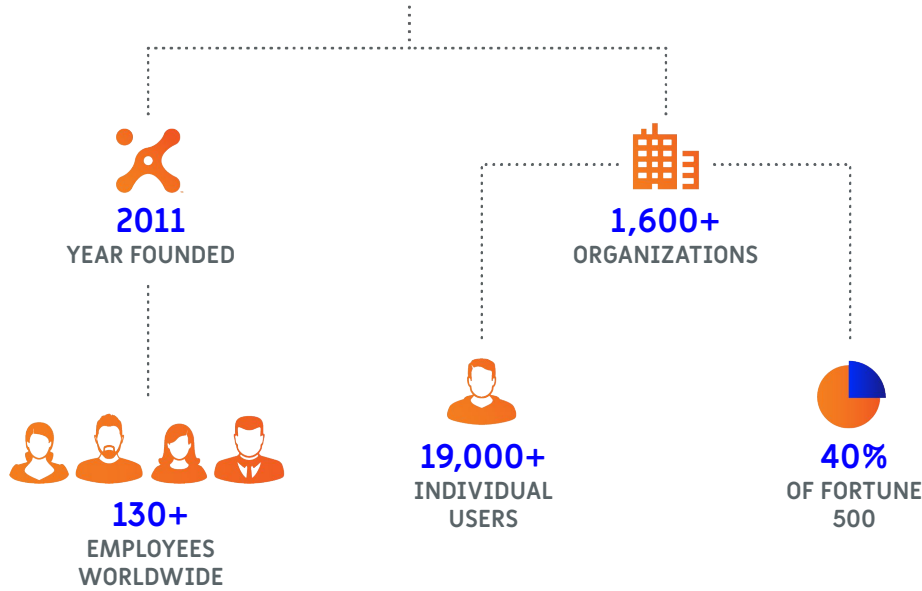
Introduction to the ThreatConnect Platform

ThreatConnect.com

ThreatConnect

Company

Since 2011, we've led the **threat intelligence** revolution, building the industry's most **comprehensive and extensible** security operations and analytics **platform** along with our large trusted cybersecurity community.

QUICK FACTS

2011
YEAR FOUNDED

1,600+
ORGANIZATIONS

130+
EMPLOYEES
WORLDWIDE

19,000+
INDIVIDUAL
USERS

40%
OF FORTUNE
500

What is ThreatConnect?

Intelligence-driven Security Operations Platform
We answer these questions for customers:

How do I get all my intelligence together?

How do my teams collaborate on this information?

How do I take action on my information?

Converged Intelligence

- Multiple intel sources:
  - **Industry, OSINT, and premium feeds**

- Normalization into our data model:
  - **All sources become uniform in nature**

- In-platform analytics:
  - **Simple, numeric scoring for an Indicator**

- Collective Analytics Layer:
  - **Anonymized data across multiple instances to improve value of intelligence**

- Artifact storage:
  - **Store artifacts as part of a Workflow Case**

Team Collaboration

- Create custom dashboards by role:
  - **Visualize data based on role relevance**
  - **Interact and explore with data in tiles**

- Group data together:
  - **Create Events, Incidents, Threats, and others to relate all relevant Indicators**

- Manage processes using Workflow:
  - **Define Templates to manage a process and instantiate these into Cases**

- Enhance data collaboration:
  - **Support for TLP, custom tags, communities and comments on Indicators and Groups**

Take Action

- Use Playbooks to automate and orchestrate common functions:
  - **Drag and drop assembly with no code required**

- Use our ThreatAssess score:
  - **Base automatic decisions on our scoring**

- Define complex operations easily:
  - **Support for incoming/outgoing HTTP as well as JSON parsing**

- Instantiate Playbooks in many ways:
  - **Inbound HTTP calls, timers, emails, user actions, data changes, custom App Services, or as part of Workflow Cases**

ThreatConnect

Let's Explore the Platform

ThreatConnect.com

ThreatConnect™

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**

ThreatConnect

Integrating with ThreatConnect

Partner Resources Available

Sandbox environment with up-to-date OSINT data

Developer Community Site

Support via Partner workspace on Slack and email

Platform Integration Points

- REST API
  - **Comprehensive API to interact with our data model**

- Playbooks and Components
  - **For simple to mildly complex operations, design a Playbook as a Template**
  - **Create reusable Components (Playbooks as a function) to use in Playbooks**

- In-Platform Apps
  - **Create Python-based Apps to run within the Platform**

- Workflow Templates
  - **Create process templates combined with Playbook Templates to guide customers**

Integration Milestones

- Integration Training
  - **We'll discuss the specifics of the integration type chosen.**
- Solution Design
  - **You will complete our design document template and we'll review.**
- Solution Development
  - **Once design is approved, you build the integration according to our guidance.**
- Integration Vetting
  - **We'll review your deliverable and documentation.**
- Integration Release
  - **We'll approve your integration for release.**

ThreatConnect™

Next Steps

- Request access to our Sandbox environment.
  - **Use this to get familiar with our platform in a hands-on fashion.**
- Plan an integration type.
  - **You propose an integration type that you'd like to pursue based on our discussions.**
- Schedule Integration Training.
  - **We'll discuss the details of the specific integration type and getting started.**
- Collaborate together on an integration design.
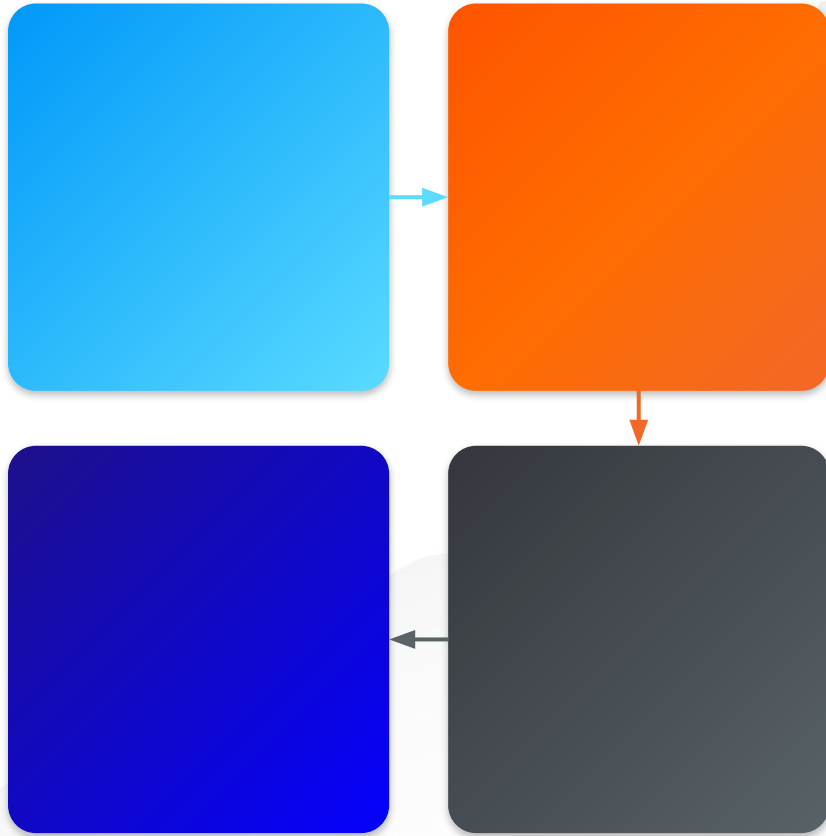 - **We supply a Solution Design Document template to complete.**

ThreatConnect.com

ThreatConnect.com

ThreatConnect™

ThreatConnect.com

ThreatConnect.com

ThreatConnect™