# Developer Partner Program

Introduction to the ThreatConnect Platform
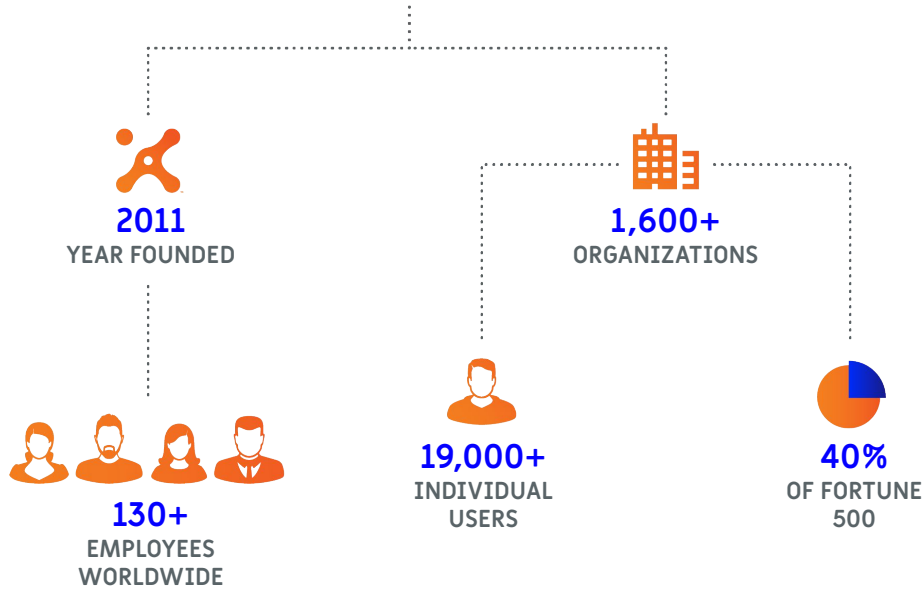
**ThreatConnect.com**

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:

How do I get all my intel sources 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**

**ThreatConnect**

# Team Collaboration

- Create custom dashboards by role:
  - **Visualize data based on role relevance**
  - **Interact and explore with data in tiles**
- Group data together to represent milestones:
  - **Create Events and Incidents and associate all relevant Indicators**
- Assign tasks to take action:
  - **Create Task items for additional human action required**
- Enhance data:
  - **Support for TLP, custom tags, and comments on Indicators and Groups**

# Take Action

- Use Playbook functionality to automate and orchestrate common functions:
  - **Drag and drop workflows with no code required**
- Use our ThreatAssess score:
  - **Base automatic decisions on our scoring**
- Create complex workflows easily:
  - **Support for incoming/outgoing HTTP as well as JSON parsing**
- Instantiate workflows in many ways:
  - **Inbound HTTP calls, timers, emails, user actions, or even data changes**

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

# 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 and trigger**
  - **Create reusable Components (Playbooks as a function) to use in Playbooks**
- In-Platform Apps
  - **Create Python-based Apps to run within the Platform.**

# 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.**
- 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.**