How to Better Your Security Program with ThreatConnect

ThreatConnect™

Contact:

Mohammed Hamididdin
Director of Channel Sales | ThreatConnect®

mhamididdin@threatconnect.com | www.threatconnect.com

ThreatConnect™

ThreatConnect.com

ThreatConnect

About the ThreatConnect Platform

Designed by analysts, but built for the entire team, the ThreatConnect Platform has use cases for threat intelligence, security operations, incident response, and security management. With your entire team and all your knowledge in one place, you will drastically improve your ability to put security data in context with intelligence and analytics, establish process consistency with playbooks, workflows and a centralized system of record, and measure the effectiveness of your organization with cross-platform analytics and customizable dashboards.

With ThreatConnect, you are able to centralize your intelligence, establish process consistency, scale operations, and measure their effectiveness all in one place.

Make your security operations and analytics more efficient, while providing real-time insights to security leaders to enable better business decisions.

With ThreatConnect's intelligence-driven security operations platform, your teams have the ability to leverage threat intelligence, automation, and orchestration directly from one platform. Automation or orchestration informed by threat intelligence makes your pre-existing technology and your entire security team — including security operations and incident response — more efficient and more effective.

A complete solution, ThreatConnect enables you to gain visibility into threats and understand the relevance to your organization, as well as increase efficiency with automation, task management, and orchestration. With ThreatConnect, every member of your security team — including leadership — benefits from using the same platform. A centralized system of record, ThreatConnect measures the effectiveness of an organization with cross-platform analytics and customizable dashboards.

Product Features

- ✓ Open Source Feeds
- ✓ Ingest Premium Feeds
- ✓ Access to CAL™ Data
- ✓ TAXII Server
- ✓ ThreatConnect Intelligence Source
- ✓ Custom Dashboards
- ✓ Automated Email Import
- ✓ Manage Incidents and Tasks
- ✓ Create Threat Intelligence
- ✓ Orchestration
- ✓ Custom Indicator Types

ThreatConnect

The ThreatConnect Platform

Designed by Analysts, Built for the Team™

The ThreatConnect Platform supports a variety of use cases across the entire security team. Here are just a few examples of the processes that are supported:

Automated Phishing Reporting, Analysis, and Response

- Easy user reporting of emails to a central mailbox
- Automate email analysis to validate potentially malicious email components
- Quicker validation leads to faster response times

Automate Threat Hunting to Identify Threats Quicker

- Integrates with EDR solution to identify abnormalities quicker
- House all indicators and intelligence collected from external and internal sources
- Investigations that previously took days or weeks are now completed in minutes

Information Sharing Across People and Technology

- STIX and TAXII supports sharing of threat intel
- Collaborate with industry groups through strategic partnerships and integrations
- Enhance intelligence with global context provided through ThreatConnect's CAL™

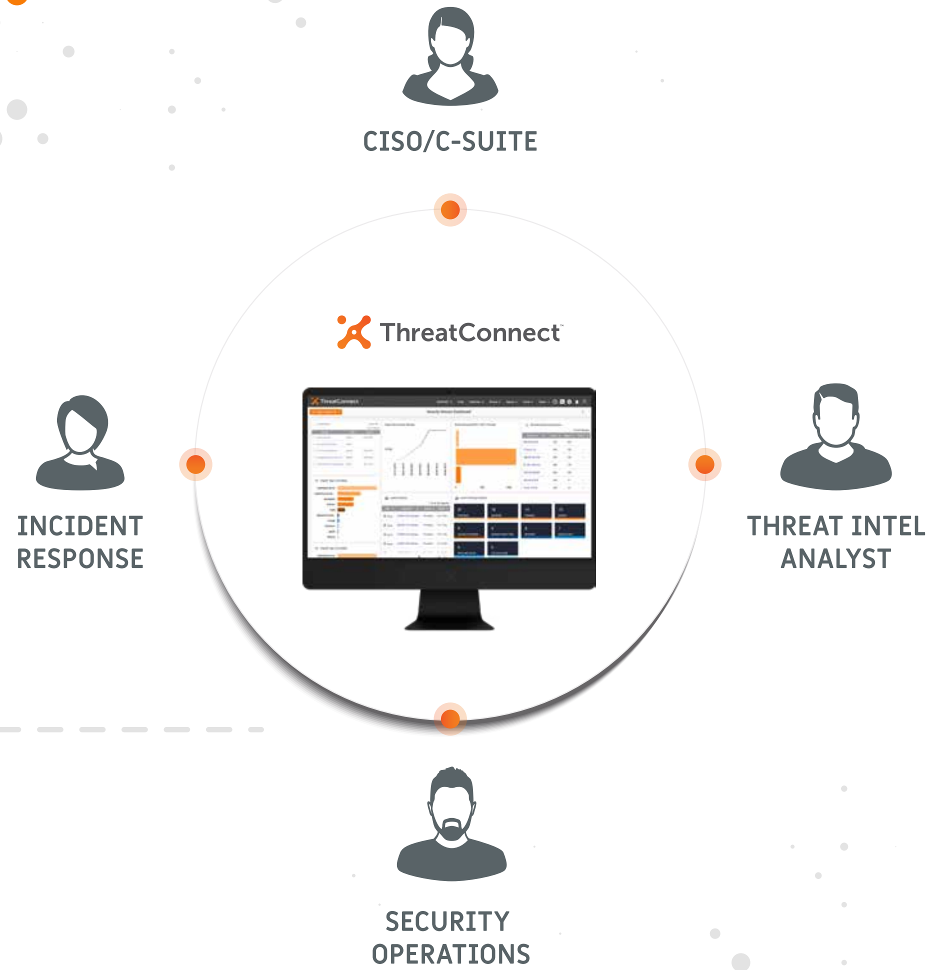
Provide Context to Cases with Integrated Intelligence

- Enrich data presented in ticketing system to maximize the application of threat intelligence
- Generate your own intelligence from existing cases to add back to the Platform

ThreatConnect

Get Smarter & Faster with Intelligence-Driven Automation

- ✓ ThreatConnect is an Intelligence-Driven Security Operations Platform
- ✓ Threat intelligence, automation, and orchestration from one Platform
- ✓ Action informed by threat intelligence makes your customers’ technology and people more efficient and more effective



ThreatConnect

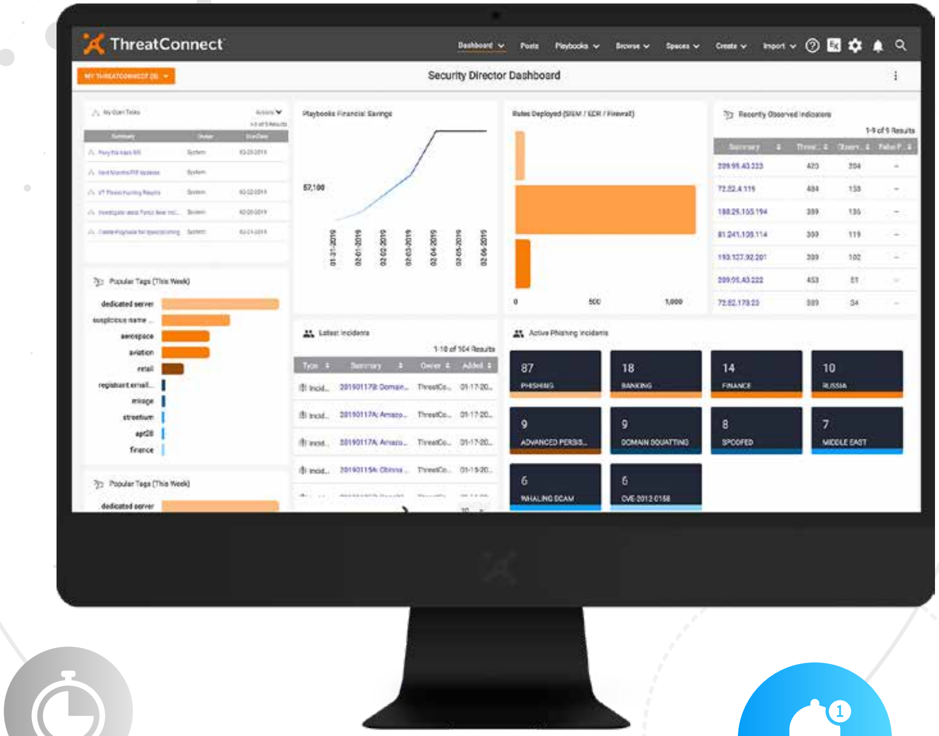
CISO/C-SUITE

INCIDENT RESPONSE

THREAT INTEL ANALYST

SECURITY OPERATIONS

With ThreatConnect, you are able to centralize your intelligence and automate processes out of one Platform, driving multiple benefits for your business:



Reduce False Positives and Focus Triage Efforts

You can automatically sort false positives in your SIEM and free your time to focus on triaging legitimate alerts. By cross-checking the data with ThreatConnect's CAL™ (Collective Analytics Layer) and external sources of threat intelligence — tech blogs, OSINT, and premium data feeds — you'll have the most complete information possible. You can determine where a deeper investigation is needed with customized workflows and playbooks.

Establish Consistent and Repeatable Processes

With ThreatConnect, you can document processes more efficiently and consistently. Track metrics on completion, and time and dollars saved to demonstrate return on investment and the value of individual playbooks.

Streamline Communication Across Teams

You can set up Playbooks to trigger based on time or a specific action, which allows for extensibility and predictability across your security operations. Then you are able to notify your team members in the Platform or in a tool where you already communicate with multiple integrations, like Slack.

Quicker, More Efficient Onboarding

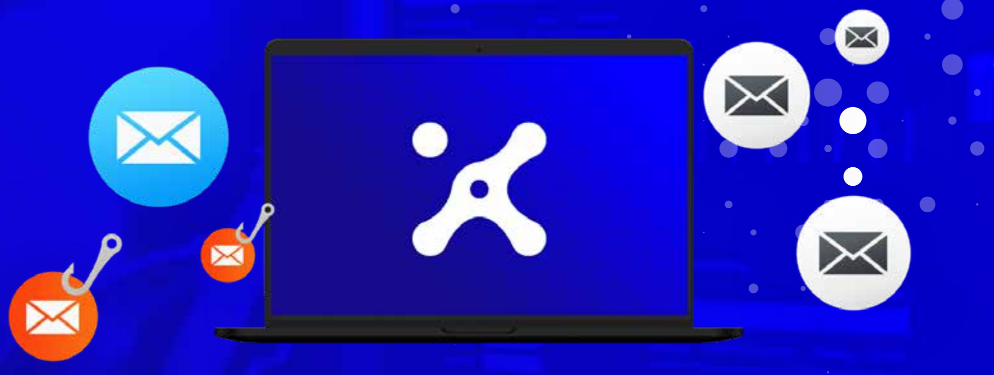
The most time consuming parts of onboarding a new team member are training on your specific products and processes. ThreatConnect enables the automation of many processes, and, with a built-in document repository, you can keep all pertinent documentation in one easily accessible place for everyone.

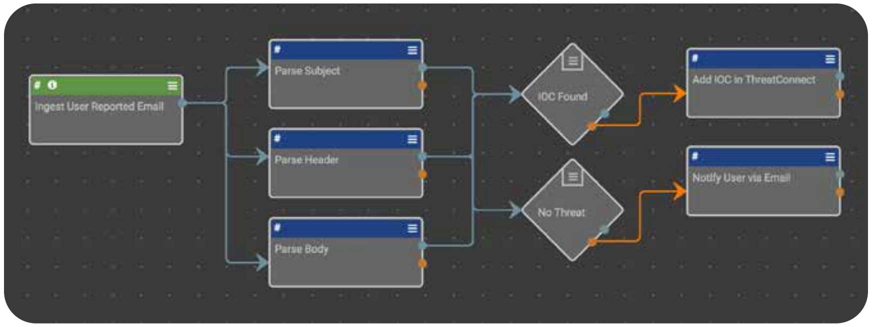
ThreatConnect

An Example of ThreatConnect in Action:

Automating Phishing Reporting, Analysis, & Response

Dealing with the management of user-reported phishing emails, sifting through the information to determine what's a legitimate threat and what's not, and acting accordingly is a necessary but extremely time consuming process. Do it in seconds with ThreatConnect.





Automated Email Analysis

Reported emails are parsed for indicators which are extracted from the email. Those indicators are automatically correlated against threat intelligence within ThreatConnect that has been aggregated by third party feeds and CAL^{TM}. If indicators are found to be malicious, appropriate response efforts are seamlessly kicked-off.

Easy User Reporting

In ThreatConnect, set-up a mailbox for centralized reporting of potential phishing emails from all sources, including both humans and technologies like Email Security Gateways. When the mailbox receives a message, the rest of the Playbook is triggered to automate the analysis and corresponding response efforts.

Quicker Response Times

Emails containing malicious indicators trigger response efforts such as user and administrator notifications, as well as communicating with other technologies such as firewalls and secure web gateways. If the email is deemed safe, the user is appropriately notified and can be marked as a false positive for future considerations.

Challenges We Solve

- Threat Data Relevance
- Lack of Alert, Incident & Case Context
- Manual Intel & SecOps Processes Long Collection & Analysis Time
- Gaps Between Intelligence & Operations

Deployment Models

ThreatConnect Cloud

AWS hosted public cloud: ThreatConnect Public Cloud gives the user the power to work with other trusted community partners to share structured threat intelligence, learn from each other's experience, and grow their knowledge of complex threats.

- The ThreatConnect Public Cloud is hosted at the us-east-1 AWS EC2 data center and follows the AWS redundancy schedule. Additional information available upon request.

Dedicated Cloud

AWS hosted private cloud: ThreatConnect Private Cloud gives the user the same granular access as the ThreatConnect Public Cloud, but on their own private instance. Ideal for organizations with privacy regulations and trusted groups that desire more control, with a Private Cloud instance the user has full administrative control with the convenience and accessibility of the cloud.

- Each ThreatConnect Private Cloud is hosted at the AWS EC2 data center nearest the customer and follows the data center's redundancy schedule. Additional information available upon request, based on customer's location.

On-Premises

ThreatConnect is available on-premises for customers who want the most advanced control and privacy of their network. The Platform can be installed and operated within their own environment and hosting facilities, allowing complete control, configuration and integration. Hardware is not provided by ThreatConnect, Inc. and is the responsibility of the customer.

ThreatConnect

Service Offerings:

Refer to the Training, Workshops, and Services, Catalog which is a complete listing of ThreatConnect administered training, workshops and service offerings. Constantly expanding, these offerings focus on kickstarting customers' experience with ThreatConnect to decrease the time to value and ultimately help master the ThreatConnect platform. All are delivered by experienced members of our Research and Customer Success teams.

Service Tokens

A Flexible Way to Purchase Training, Workshops, & Services

ThreatConnect now offers Service Tokens as a mechanism for flexible payment to support changing needs and priorities. Now more than ever, you are able to tailor the additional training workshops, and services needed to complement the team and allow them to make the most of their ThreatConnect subscription.

Benefits of Service Tokens

- ✓ Scalable for all enterprises and packages
- ✓ Courses can be held in-person on-site or virtually via webinar
- ✓ Flexibility to adjust training and professional services needs based on staffing or program changes

Additional Details

- ✓ Available to current customers only
- ✓ Valid during subscription period or 12 months from purchase, whichever is shorter

FAQs

What integrations do you have?

The ThreatConnect Platform was built to be open and extensible. With 350+ apps and Integrations, we strive to integrate the tools and technologies in our customers' existing ecosystem, and work with vendors across every category to make security easy and effective.

Can you integrate with ticketing systems?

Yes. Our workflow feature allows you to assign tasks to your team to keep track of your projects. In fact, one of our customers got rid of Remedy and has started to use our workflow features in its place entirely. ThreatConnect allows you to actually stop using a separate ticketing system.

Do you have alerting?

Yes. They come in the form of email notifications.

We have all of these feeds, we don't have time to sift through them all – can you help us?

Yes! ThreatConnect automatically aggregates and normalizes data from your feeds so you don't have to. Our false positive and observations feature lets you evaluate which feeds are providing the most relevant data for your particular security infrastructure.

Can you help us with phishing emails?

Yes! In ThreatConnect, you can set up a phishing email inbox that automatically ingests emails into it. ThreatConnect parses the emails for phishing URLs and information for them. Using this information, you can address the phishing campaign and figure out how to adequately stop it.

Can you aggregate structured or unstructured data?

Yes, we aggregate and normalize both structured and unstructured data.

Can you support STIX TAXII?

Yes.

Can my customers bring their listservs in?

Yes, they can. They can customize the platform by adding any feeds or listservs that they'd like.

Does ThreatConnect support MITRE ATT&CK?

Yes

How do you differentiate from your competitors?

Our approach is different from all of our competition. Traditional TIPs don't focus on what's next. They're aggregators. Traditional SAO or SOAR vendors don't focus on applying intelligence to processes to make them smarter. They're automation machines. We're both, and that's a powerful combination.

What market segment and/or vertical does your company operate in?

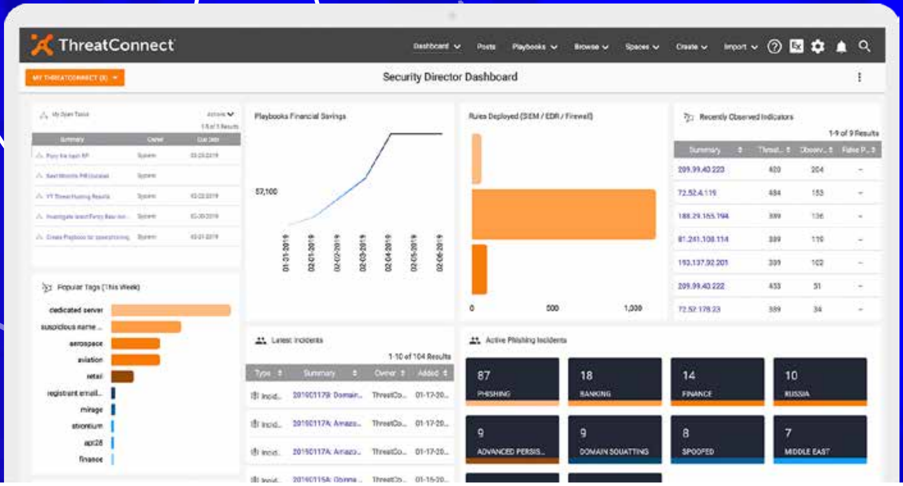
ThreatConnect sells to mostly corporate, Fortune 1000 customers.

ThreatConnect

Integrations

Make the most of your existing tools

ThreatConnect easily integrates with an organization's existing security products to make them more effective. Users are able to take advantage of multi-sourced data within the ThreatConnect platform to push threat indicators and context back out to partner-integrated products.



My Open Tasks — 1-5 of 5 Results

Summary	Owner	Due Date
[illegible]	System	02-23-2019
[illegible]	System	
VT Threat Hunting Results	System	02-22-2019
Investigate latest Fancy Bear Act...	System	02-20-2019
Create Playbook for spearphishing...	System	02-21-2019

Latest Incidents — 1-10 of 104 Results

Type	Summary	Owner	Added
Incid...	20190117B: Domain...	ThreatCo...	01-17-20...
Incid...	20190117A: Amazo...	ThreatCo...	01-17-20...
Incid...	20190117A: Amazo...	ThreatCo...	01-17-20...
Incid...	20190115A: Gmma...	ThreatCo...	01-15-20...

Recently Observed Indicators — 1-9 of 9 Results

Summary	Threat...	Observ...	False P...
209.99.40.223	420	204	–
72.52.4.119	484	153	–
188.29.165.194	389	136	–
81.241.108.114	389	119	–
193.137.92.201	389	102	–
209.99.40.222	453	51	–
72.52.178.23	389	34	–

Threat Intelligence:

- **Open source feeds:** Publicly available threat data from many sources vetted by the ThreatConnect Research team to enhance your customer's ability to respond to threats to your network
- **Premium threat intelligence feeds:** gather, filter, normalize, and analyze threat data for easy enrichment and action

Security products:

- **Endpoint detection & response:** automatically send threat intelligence to devices to detect and block malicious behavior
- **SIEM (security information & event management):** aggregates internal logs and combines them with your customers' threat intel, so they can easily spot trends or patterns that are out of the ordinary and act on them efficiently
- **Risk and vulnerability management:** enhances ability to identify, remediate, and mitigate vulnerabilities or risk in network with threat intelligence vetted in threatconnect
- **Network defense:** with threat intelligence from threatconnect, enhance ability to detect, monitor, and protect networks or host against infiltrations from threats
- **Malware analysis:** efficiently detect, analyze, and defend organization against malware and indicators of compromise
- **Incident response & ticketing:** receive full context behind an incident to allow prioritization and triage investigations faster
- **Orchestration:** enrich your automated security processes with threat intelligence and conduct defensive actions across technologies
- **Deception:** gain additional insights and context behind an attack on network for stronger analysis

Enrichment & analysis

- **Analysis:** visualize data to quickly see relationships or patterns
- **Enrichment:** automatically enrich data for stronger analysis