INCIDENT RESPONSE TEAM

Transform Your IR Team From Reactive to Proactive

When your organization is attacked – and it's when, not if – it can take days to detect and weeks to resolve. Of course, that doesn't include the time it takes to rebuild trust in your brand. What's more, 40% of the time, attackers are using you to go after someone else. The likelihood is high that when you are breached, your customers, your peers, and your partners will soon find out.

ThreatConnect makes your IR team faster and more effective at protecting your network. The ThreatConnect platform unites your people, processes, and technologies within your IR team, and across your organization. The platform gives you the full context behind an incident. It integrates with your existing tools and processes, enabling you to leverage your current systems to their fullest potential.

With ThreatConnect, your SOC and IR teams are integrated and can work collaboratively. The platform provides a central place to store and contextualize data, eliminating barriers between the systems and processes that used to slow you down. Tasks that once took hours or minutes can be executed instantaneously, allowing you to focus on triaging incidents quickly and effectively.

www.ThreatConnect.com

Mobilization and Resolution

Overcoming Critical Challenges to Accelerate Response Time

When connectivity increases, vulnerability increases in turn. While your organization's SOC team is diligent about detecting and preventing attacks, it's not a matter of if, it's a matter of when you'll be breached. It's up to you and your team to perform damage control. There are a number of critical challenges that make it difficult to act fast when it matters most.

60%

OF BREACHES, NETWORK COMPROMISED WITHIN MINUTES.

– 2015 Verizon DBIR Report

Fragmentation

When people and tools don't communicate and there isn't a centralized place to store data, it is exceedingly difficult to mobilize a response. Fragmentation of internal systems and people can prevent IR teams from being effective, even if the team has the capability to resolve the threat.

Lack of Context

When threat intelligence is gathered as raw data from intel feeds, the sheer volume can become impossible to manage. Without tools to enrich the data and understand context, the IR team is left with little actionable intelligence to mount a coordinated defense.

Reactive Posture

Incident Response teams are often perpetually playing catch-up, maintaining a reactive posture that focuses only on repairing damage. Without a way to leverage historical data and intel from trusted communities, IR teams are constantly caught off guard by the latest attack.

HOW CURRENT IR CUSTOMERS USE THREATCONNECT

Example Use Cases from Drawn from Teams in the Real World

Proactive Posture

The most effective IR teams use ThreatConnect's leading analysis methodology, workflow features, and powerful API integrations to collect threat data from reliable external sources, compare it to in-house developed data. IR teams collaborate with SOC teams to proactively identify threats before damage can be done.

Improve Collaboration

ThreatConnect customers unite the Incident Response team with the SOC team, by using threat response workflows. Using workflows, teams can work together to conduct deep analysis into threat actors' capabilities, set up scheduling alerts, and enable automated actions for blocking and alerting.

Accelerate Detection and Response Time With ThreatConnect

## Transform Your IR Team from Reactive to Proactive Force
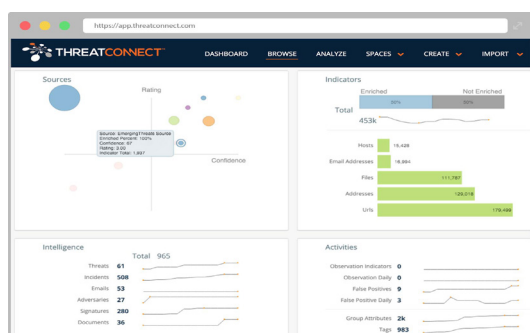
Prioritize Your Data

ThreatConnect works with your existing security products to help you prioritize threats within a SEIM to separate actual threats from common cyber noise. Working with your SOC team, you can easily determine what events you need to focus on and stop chasing false positives. You are finally able to focus on threats that could actually hurt your network.
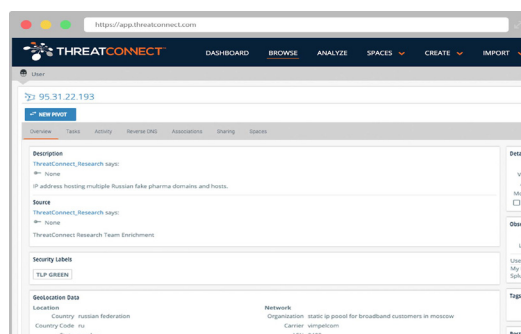
Have More Context

ThreatConnect's comprehensive TIP serves as a central threat repository for your organization. It is a place to store all of your threat data, your team's notes, and any related documents in one central place. Your team can find out about cybercriminals' tools, processes, victims, and intended goals. You can easily correlate information from past attackers' activity to current, and learn from past campaigns to proactively thwart an attacker's current and future attempts.
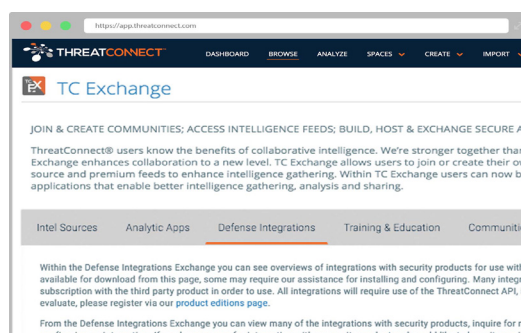

Tie Your Team, Processes, and Tools Together

ThreatConnect integrates your entire security infrastructure, from your teams to their processes to their tools and systems. You can automatically share IOCs to the relevant tool or system, right in the platform. You don't have to use a different system to set up a rule or enrich your data – everything you need is in one central place.

Build on the Platform

ThreatConnect customers leverage bi-directional integrations with firewalls, SIEMs, endpoint protection devices, and other security products to efficiently monitor and act on any security incidents that might occur. Using TC Exchange™, teams can build, host, and share secure, customized applications right in the platform.
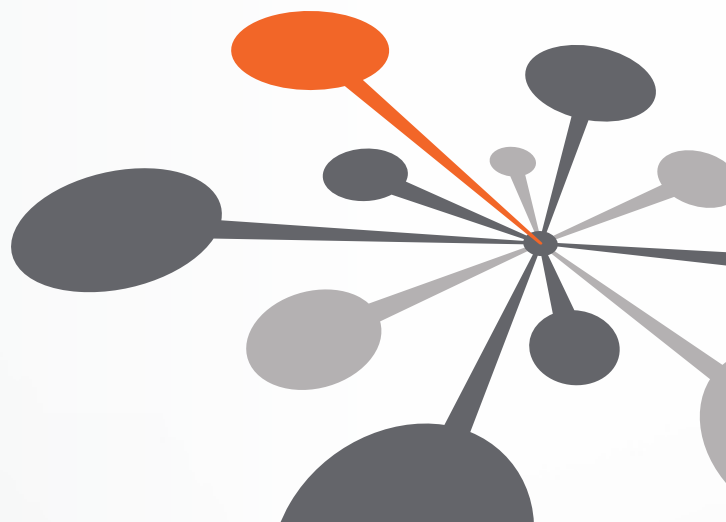
Key IR Benefits of the ThreatConnect Platform

IR Team Favorite Features

▸ Leadership can ensure that resources are used effectively

▸ All structured and unstructured data is collected in a central place

▸ Automated normalization of data allows teams to efficiently analyze patterns

▸ Flexible API allows integration between products already in use

▸ Automation reduces or eliminates manual labor

▸ Use TC Exchange™ to build, host, and share secure, customized applications in the platform

▸ Share threat intelligence with vendors, partners, and communities

Intelligence Feeds

Firewalls /UTM

Web Proxy

SOC, IR, TI Teams

IPS/IDS

Private/Public Communities

CISO/CIO C-Suite/Board

Network Controls

SIEM

ISAC/ISAO

Vulnerability Scanner

End-Point Protection

Form a Faster, More Efficient IR Team

Unite Your People, Processes, and Technologies Behind an Intelligence-Driven Defense

Worldwide, cybersecurity incidents are growing in frequency and sophistication at an exponential rate. It's only a matter of time before the challenges you face when responding to attacks will outweigh your capabilities. With ThreatConnect, you can unite all of the people and systems across your security team, and leverage internal, and externally gathered data. You'll understand the full context behind an incident, and be able to act rapidly and precisely to keep your business' and your customers' data secure.

SCHEDULE A FREE THREATCONNECT DEMO TODAY.

CALL US AT 1.800.965.2708

ABOUT THREATCONNECT

ThreatConnect unites cybersecurity people, processes and technologies behind a cohesive intelligence-driven defense. Designed for security teams at all maturity levels, ThreatConnect enables organizations to maximize the value of their security technology investments, combat the fragmentation of their security organizations, and enhance their infrastructure with relevant threat intelligence.

THREATCONNECT™

THREATCONNECT, INC.
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

E: sales@threatconnect.com
P: 1.800.965.2708
www.ThreatConnect.com