THREATCONNECT™

SECURITY OPERATIONS CENTER

Unite People, Processes, and Technologies Across Your SOC with ThreatConnect

As an analyst or director in your organization's Security Operations Center (SOC), it's your job to stay one step ahead of threats to your network, and have a solid plan of action to respond.

ThreatConnect helps you broaden and deepen your threat intelligence, validate it, prioritize it, and act on it. The platform brings together the people, processes, and technologies that comprise your SOC team, and the other teams you partner with on a daily basis. It's a single place for everyone, from the analysts to the CISO, to work together to proactively defend your network.

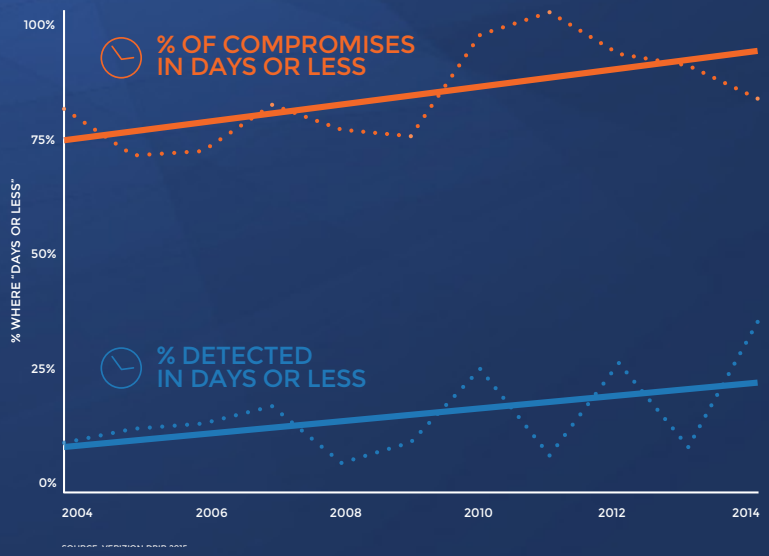
ThreatConnect integrates with the security products your team is already using, and helps you make the most of these existing tools. You can automate the mundane tasks that slow you down, so you can triage events faster, spend more time on analysis, and unite your SOC around an intelligence-driven defense. With ThreatConnect, your team works as a single cohesive unit, reinforced by a global community of peers.

www.ThreatConnect.com

Your Job Isn't Getting Any Easier

It's Time to Stop Playing Catch-Up, and Start Being Proactive

More than 1,200 organizations around the globe use ThreatConnect to get better intelligence to run their security operations. Our customers use our platform to collaborate across internal and external teams, to automate actions, and to get the most out of existing security products.



Fragmentation

Incidents happen at the seams, between tools and teams. When critical roles and systems within your SOC are not aligned and not collaborating, it slows and even halts detection and response efforts. Unfortunately, fragmentation is a constant across organizations in all industries. This costs companies dearly, and requires countless hours to clean up.

Ability to Respond

When a breach happens, every second counts. But many organizations measure response time in days, weeks, or months. In fact, a recent Verizon* study showed it takes organizations an average of 256 days to even detect an attack. In 60% of these attacks, networks are compromised within just minutes. When it's your responsibility to prevent, detect, and mitigate damage, you can't afford to respond to threats manually.

Data Overload

Endless streams of raw data make it nearly impossible for organizations to sort information in a timely manner, let alone turn that data into actionable intelligence. While your organization is busy being overwhelmed with information, threats are penetrating fragmented defenses. Your SOC team needs to be able to enrich data, understand context, and pivot between data points to uncover patterns.

"Our intel guys are sending us [the SOC], 100s of IOCs every week, basically made up of IP addresses, every IP address represents an event, and we have to look into every event because compliance makes us, and we are dying. We understand that we need to collaborate with the other teams to understand context for the IOCs, and we need an intelligence Platform like ThreatConnect to enable this."

– Fortune 500 Financial Services Organization

HOW CURRENT SOC CUSTOMERS USE THREATCONNECT

Real-World Use Cases

Identify Threats

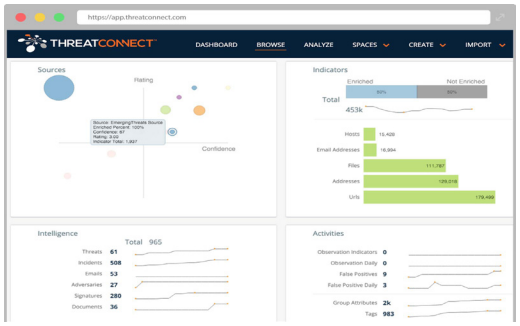
The most effective SOC teams use ThreatConnect's leading analysis methodology, workflow features, and powerful API integrations to collect threat data from reliable external sources and then compare it to in-house developed data. Using these intelligence-driven processes, SOC teams proactively identify threats before damage can be done to their organization.

Improve Collaboration

ThreatConnect customers unite their SOC and Incident Response teams by using threat response workflows. Using workflows, teams can conduct deep analysis into threat actors' capabilities, set up scheduled alerts, and enable automated actions for blocking and alerting.

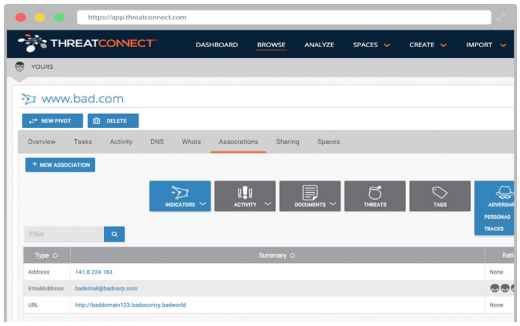
Transform Your SOC With ThreatConnect

Discover Immediate Benefits



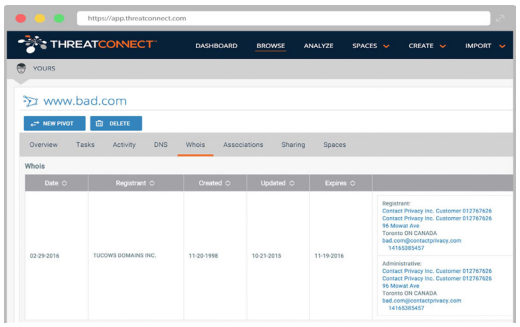
Make Strategic Decisions

You can use ThreatConnect to quickly and easily find out more about the context of an event. You're able to automatically normalize and enrich data. You have the option to add even more information to that data to ensure you have all of the context you need in the future. Once you know more information about the events, you can easily prioritize them and work through your queue more quickly.



Gain More Awareness

ThreatConnect serves as a central data repository for your organization. It is a place to store all of your threat data, team notes, and any related documents in one central place. Your team can learn from similar events and incidents, estimate the kill chain stage, and proactively block future threats. Your team can build tactical playbooks based on data, incident and event response history, as well as your successes and failures.



Focus on What's Important

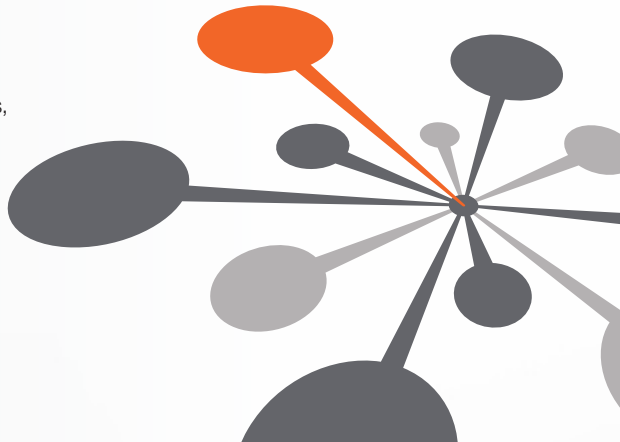
Using our indicator and confidence rating, and correlation of data from multiple sources, ThreatConnect customers can hone in on which threats are most important to their business. You'll be able to automate response actions and shift your focus to prevention instead of clean-up.

Improve Reporting

Based on data collected and analyzed in ThreatConnect, security teams can build adversary reports for organizational stakeholders that identify threat actors, their capabilities, infrastructure, and intended goals, along with specific details on how the team thwarted the threat.

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 SOC Benefits of the ThreatConnect Platform

SOC Team Favorite Features

- Leadership can ensure that resources are used effectively
- All structured and unstructured data are 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
- Built-in workflow features allow tracking of team progress to make sure no task is left behind

Unite Your SOC Behind an Intelligence-Driven Defense

Join more than 1,200 companies and 9,000 individual users worldwide

With ThreatConnect, your entire security team – from the analysts, to the tools they use, to the directors and your CISO – has a single place to store, analyze, and use threat intelligence proactively. You can maximize the value of your technology investments while fighting fragmentation and enhancing efficiency. You'll understand context, leverage historical data, and benefit from a global peer community. In short, ThreatConnect helps you be more effective at your job.

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