

ThreatConnect TIP

Aggregate, Analyze, and Act
on Threat Intelligence with the ThreatConnect
Threat Intelligence Platform

The ThreatConnect Threat Intelligence Platform (TIP) centralizes the aggregation and management of all of your threat data. From one platform, normalize data from a variety of sources, add additional context, and automate manual threat intelligence-related security processes. ThreatConnect TIP provides you with a workbench to organize and prioritize your threat data and use it to drive actions across your security team.



“ThreatConnect provides our security team with a bigger picture view and a better understanding of the threat landscape, so that they can better prioritize the actions they take to defend the enterprise.”

— Security Intelligence Team Lead, Financial Services Company
ThreatConnect Customer

What You Get with ThreatConnect TIP

A Single Source of Truth for Intelligence & Processes

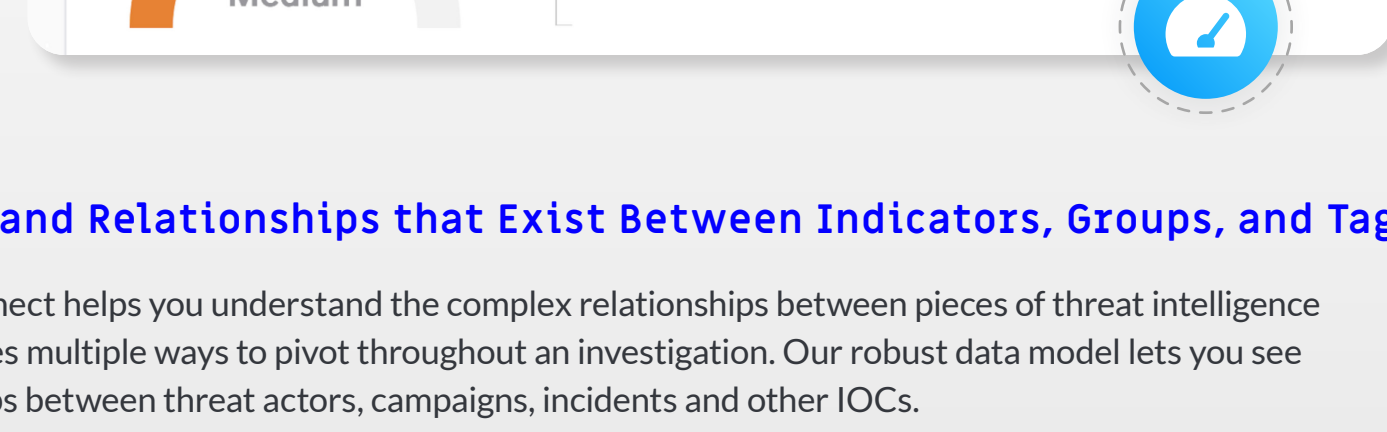
Enables the refinement of relevant data from cases, response engagements, threat investigations, shared communities, and external vendors into intelligence suitable for any analyst's decision-making and leverages that newly created intelligence to inform decisions across the security team.

Intel-driven Decision-Making Across the Security Team

Situational awareness and historical context are both provided by threat intelligence and are both key to confident decision-making. Apply threat intelligence to decisions being made across your security team and technology stack and improve processes over time based on new learnings.

Prioritize Response Based on Threat Ratings with ThreatAssess

With ThreatAssess, prioritize responses by assigning threat ratings to observed indicators. ThreatAssess distills multiple factors down to a single, actionable score based on an indicator's average threat and confidence rating across all sources, false positive votes, and recent activity. ThreatAssess also reports on why an indicator earned its particular score, providing valuable context.

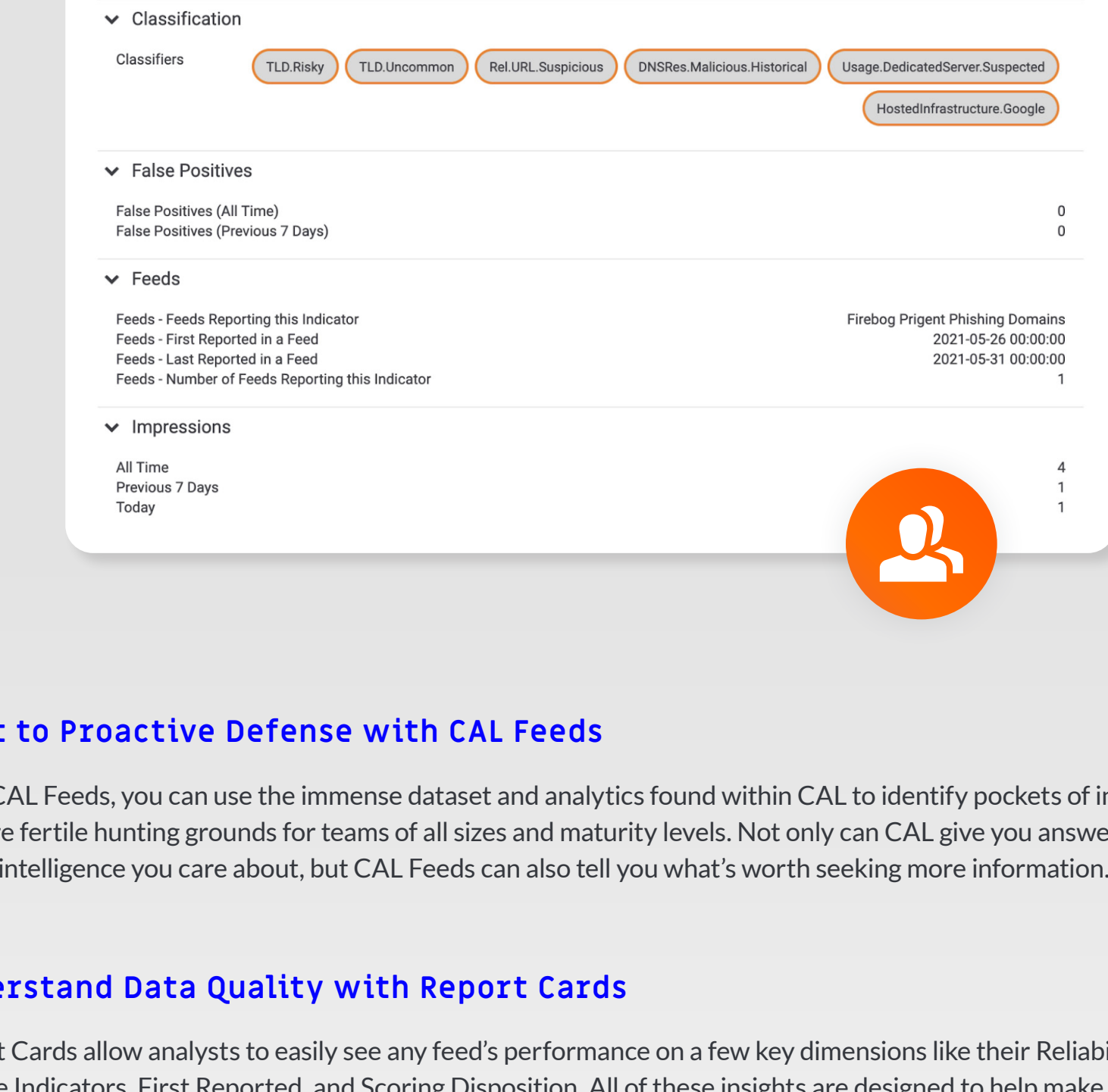


Understand Relationships that Exist Between Indicators, Groups, and Tags

ThreatConnect helps you understand the complex relationships between pieces of threat intelligence and provides multiple ways to pivot throughout an investigation. Our robust data model lets you see relationships between threat actors, campaigns, incidents and other IOCs.

Enhance Intelligence with Global Context

ThreatConnect's CAL (Collective Analytics Layer) anonymously leverages thousands of analysts worldwide who use participating ThreatConnect Platform instances and provides a way to learn more about potential threats. By distilling billions of data points, this innovative architecture offers immediate insight into how widespread and relevant a threat is, providing global context that has never before been available.

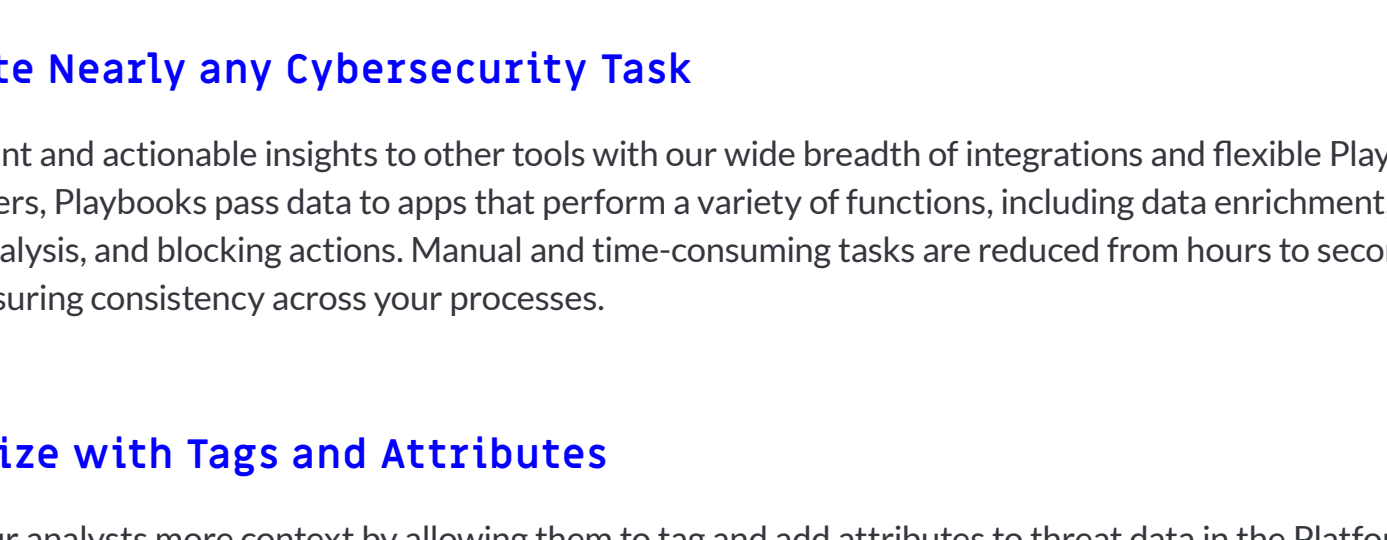


Shift to Proactive Defense with CAL Feeds

With CAL Feeds, you can use the immense dataset and analytics found within CAL to identify pockets of intelligence that are fertile hunting grounds for teams of all sizes and maturity levels. Not only can CAL give you answers about intelligence you care about, but CAL Feeds can also tell you what's worth seeking more information.

Understand Data Quality with Report Cards

Report Cards allow analysts to easily see any feed's performance on a few key dimensions like their Reliability Rating, Unique Indicators, First Reported, and Scoring Disposition. All of these insights are designed to help make better decisions during analysis and investigation.



Automate Nearly any Cybersecurity Task

Send relevant and actionable insights to other tools with our wide breadth of integrations and flexible Playbooks. Using Triggers, Playbooks pass data to apps that perform a variety of functions, including data enrichment, malware analysis, and blocking actions. Manual and time-consuming tasks are reduced from hours to seconds, all while ensuring consistency across your processes.

Categorize with Tags and Attributes

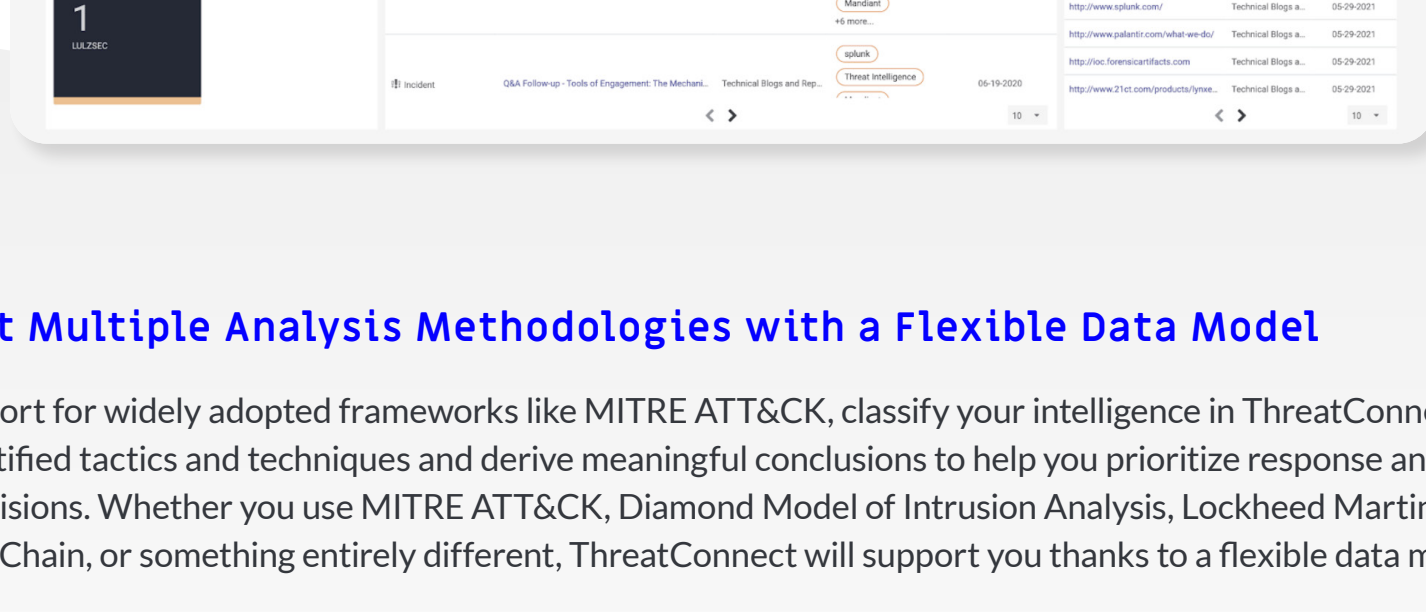
Provide your analysts more context by allowing them to tag and add attributes to threat data in the Platform. By adding tags and attributes, analysts gain a more holistic sense of the threat landscape and can improve their decision-making.

Breakdown Silos & Increase Collaboration

Remove silos by sharing the intelligence generated during investigations with your SOC and IR teams. This new Threat data can then be used to inform broader security decisions.

Gain Insight and Situational Awareness with At-a-Glance Dashboards

Get an at-a-glance view of priorities, including priority intelligence requirements (PIRs) with highly flexible Dashboard capabilities. Monitor recent history, open cases, open tasks, active incidents, observations, false positives, and more with pre-built and configurable cards.



Support Multiple Analysis Methodologies with a Flexible Data Model

With support for widely adopted frameworks like MITRE ATT&CK, classify your intelligence in ThreatConnect using identified tactics and techniques and derive meaningful conclusions to help you prioritize response and make better decisions. Whether you use MITRE ATT&CK, Diamond Model of Intrusion Analysis, Lockheed Martin's Cyber Kill Chain, or something entirely different, ThreatConnect will support you thanks to a flexible data model.

Flexible Deployment Options

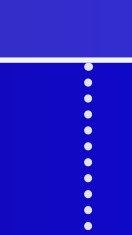
Flexible deployments in Cloud or On-Premises get you up and running the way you want quickly. Multi-Environment Orchestration allows for orchestration across multi-cloud or hybrid on-prem and cloud environments. Wherever your security controls reside, we can connect them seamlessly.

How it works

Automatically ingest and deduplicate data from various sources



Premium Feeds



Logs & Data from Security Tools



OSINT

Continuously collect, normalize, and analyze threat data in your existing threat library to organize and make sense of it



What Makes ThreatConnect TIP Better



High Confidence Intelligence Baked-In



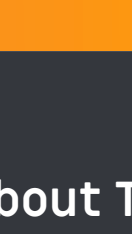
Bi-Directional Integrations With 100's of Products



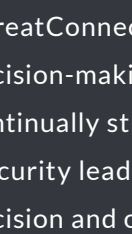
Reduce False Positives and Automate Threat Intel Security Processes



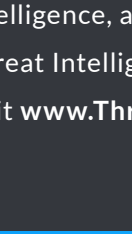
Deployment Support for Cloud and On-Premises



Leverage Insight From Other ThreatConnect Users



Make Better Decisions Using Intel Feed Report Cards



Dedicated Customer Success Team



Scale Incrementally Without Affecting Performance

About ThreatConnect®

ThreatConnect, Inc. provides cybersecurity software that reduces complexity for everyone, makes decision-making easy by turning intelligence into action, and integrates processes and technologies to continually strengthen defenses and drive down risk. Designed by analysts but built for the entire team (security leadership, risk, security operations, threat intelligence, and incident response), ThreatConnect's decision and operational support platform is the only solution available today with cyber risk quantification, intelligence, automation, analytics, and workflows in one. To learn more about our Cyber Risk Quantification, Threat Intelligence Platform (TIP) or Security Orchestration, Automation, and Response (SOAR) solutions, visit www.ThreatConnect.com.

