ThreatConnect.

Choosing the Right Platform for Threat Intelligence

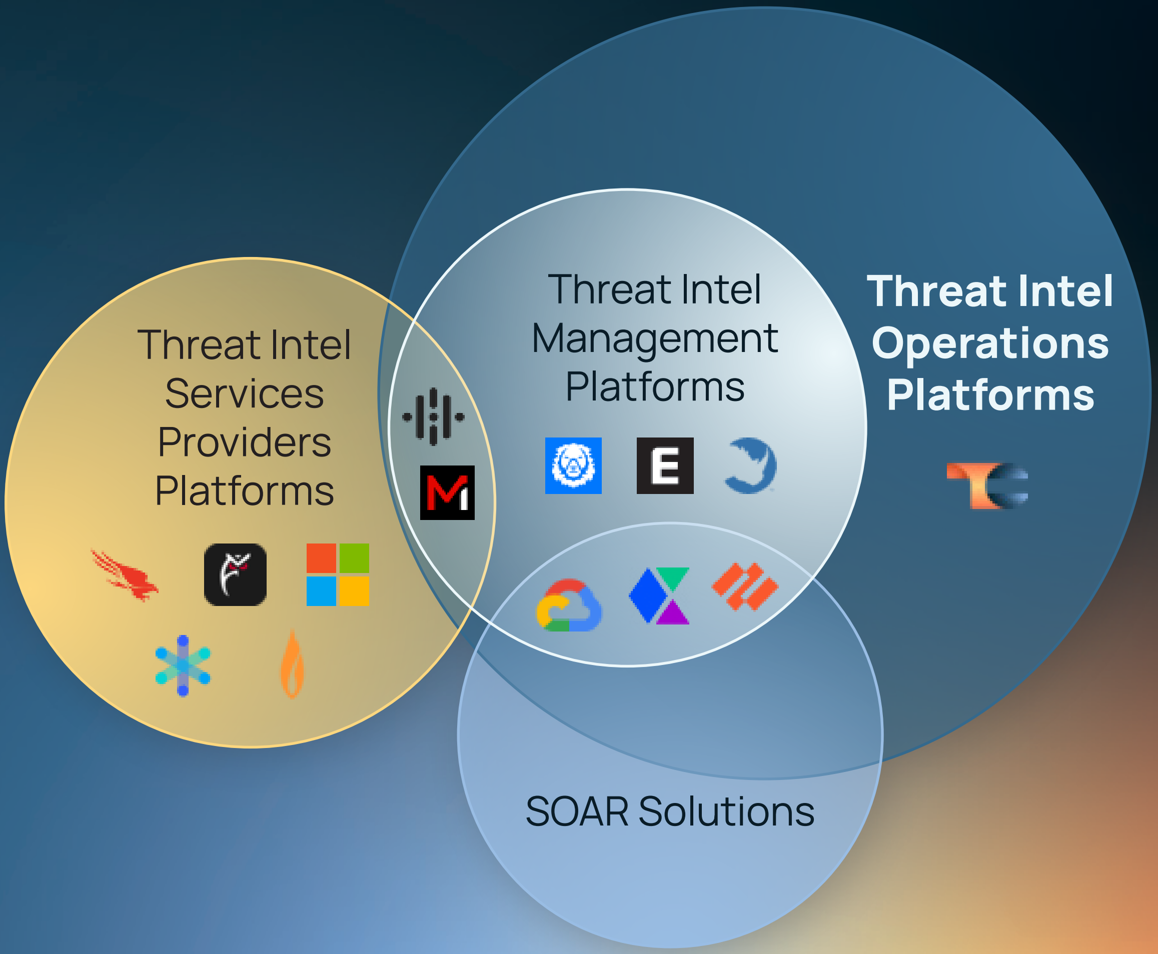
Use this short guide to cut through vendor confusion and hype, and choose the right platform for your organization's threat intelligence function.

Introduction

Organizations at the beginning of, or in the process of maturing, their cyber threat intelligence programs, need a platform that enables them to leverage and disseminate their threat intel. Depending on the specific needs of the threat intel team, and broader cybersecurity and operations team, there are different available solution paths:

- Threat Intel service providers may offer a platform with some operational capabilities to leverage their proprietary intel.
- Some SOAR solutions offer threat intel management functionality.
- Threat intel platforms focus (TIPs) primarily on the aggregation, management, and analysis of intel.
- Threat Intel Operations platforms are a modern solution that goes beyond TIPs enabling the operationalization of threat intel analyst work and their outputs.

There is a wide variation between these platforms. One thing is common, they can help manage threat intelligence, but most struggle to operationalize it. Let's learn more about these platform options and which is the best fit for your threat intel needs.


Threat Intel Services Providers Platforms
Threat Intel Management Platforms
Threat Intel Operations Platforms
SOAR Solutions
E

Comparison of Platforms

Capability / Feature	TI Ops Platform	Open Source TIP	TI Provider Platform	Commercial TIP	SOAR
Manage TI	●	◕	◑	●	◔
Centralized Threat Repository	●	●	◑	●	○
Supported Intel Sources	●	◑	◔	●	◔
Scalability	●	◔	◑	◑	◑
Flexibility	●	◕	○	◑	◕
AI & ML	◕	○	◕	◕	◑
Support PIRs	◕	○	○	○	○
No/Low Code Automation	●	◔	○	◑	●
Workflows	●	◔	○	◑	●
Threat Visualization	◕	◕	◑	◕	○
Automated Enrichment	●	○	◔	●	○
Native Reporting	●	◔	◑	◔	○
Case / Incident Management	●	○	○	●	●
Support for ATT&CK	●	●	●	●	●
Tech Integrations	●	◔	◔	●	●
Sharing TI	●	●	◔	●	○

○ Lacks feature/capability ◔ Basic ◑ Average ◕ Above Average ● Comprehensive

The chart above is an average across various vendors that have an offering in each column.

- Open Source TIPs generally are strong at aggregating OSINT and intel shared amongst trusted partners, and being used to produce and share operational intelligence. They support fewer threat services and security technologies. They are also highly customizable given they are open source software and can be customized if the organization has developers.

- TI Provider Platforms are the portals to access the intel produced by a provider. Increasingly these Platforms are offering TIP features, such as integrating with downstream security tools, like SIEM, XDR, EDR, firewalls, etc. to share IOCs.
- Commercial TIPs are oriented to the production of operational, tactical, and strategic intel, but are less mature in their operational capabilities, like the use of AI, automation, workflow, and knowledge capture and management. They are also primarily used by threat intel analysts with less utility to other roles across security operations, e.g, SOC analysts.
- Security Automation tools generally have basic TI management capabilities given their primary focus on orchestrating and automating processes and activities, sometimes along with case management and workflow features.

Threat Intel Platforms and Capabilities

Threat intelligence platforms/tools are software solutions designed to facilitate the collection, analysis, and management of threat intelligence data. These platforms offer a centralized and organized environment for analysts to collect, process, and analyze threat intelligence.

To enhance its efficacy, threat intelligence tools often integrate with tools to detect and/or prevent threats, like SIEM, XDR, endpoint, and network security solutions, to help analysts with prioritizing alerts and determining urgency. Moreover, these tools support basic triage and investigation processes for alerts generated by threat detection, prevention, and response tools. Finally, threat intelligence platforms foster information sharing primarily through the exchange of indicators with other teams and external parties. The table below explains the operations and capabilities possible with threat intelligence management tools/platforms:

Operation	Description
Data Aggregation	Collecting threat intelligence data from multiple sources.
Data Enrichment	Enhancing raw data with additional context and metadata.
Threat Analysis	Analyzing collected data to identify trends and patterns.
Indicator Management	Organizing and managing indicators of compromise (IOCs).
Threat Intelligence Sharing	Sharing intel feeds for consumption by downstream security technologies. Collaborating and sharing threat intelligence with trusted partners or industry peers. Several ISAC portals offer similar capabilities.
Dashboards	Useful for displaying charts and tables related to collected intelligence, e.g., indicators with a specific tag.

TI Management vs. TI Operations: What's the Difference

Let's explore how requirements and deliverables differ between managing and operationalizing TI.

	Threat Intel Management	Threat Intel Operations
Primary Focus	Production of TI	Production and Consumption and use of TI
Users	CTI team	Cyber offense and defense, incident response, and risk management teams
Primary Use	Collecting and analyzing threat data	Understanding and utilizing threat intel data to inform decisions and actions; leveraging automation to aid in the production of intel
Deliverables	Collections of IOCs, reports, briefings, and alerts on emerging threats	Insights, recommendations, motivations, and automation-powered actions based on threat intel
Common use cases	Building a central threat library, threat detection and prevention, generating strategic intel	Building a unified threat library, threat detection and prevention, generating strategic intel, threat hunting, incident response, vulnerability prioritization, informing red/purple teaming, and risk management

TI Operations Platforms

Given the differences between managing and operationalizing threat intelligence, different capabilities are needed. The following capabilities are critically different from TIPs focused primarily on the management of threat intel.

- **Managing, organizing, and enabling intel requirements:** In order for intel teams to be successful, threat intelligence requirements are vitally important. Having a single location where these are collected, organized, and enabled removes the overhead of manually managing requirements, e.g., in a spreadsheet or documents. It allows requirements to be measured and validate the value from intel.
- **Collection depth and breadth from a variety of structured and unstructured threat intel sources:** A wide-aperture of the threat landscape is needed to have the best situational awareness on threat actors. The ability to support a variety of structured (e.g., commercial, open source, and shared threat feeds) as well as unstructured intel (e.g., reports, blogs, news websites).

- **Ability to scale to hundreds of millions of indicators:** Having the coverage and history of indicators needed per requirements and use cases can be a challenge for many TIPs that are unable to support the volumes needed by some CTI teams.
- **Customizable and flexible low to no-code automation:** Automation is vitally important to improve the efficiency and effectiveness of intel producers and to support the requirements from consumers (e.g., enrichment of alerts, real-time sharing of indicators, on-demand reports). Every team has different ways of working and processes, so the ability to customize automated actions is necessary.
- **AI and machine learning:** AI, like natural language processing and recommendation engines, and machine-learning, e.g., for detecting domain generation algorithms, reduces the manual burden of TI producers when processing and analyzing threat intelligence.
- **Automated enrichment of threat intel:** Threat intelligence needs context. The ability to automate the enrichment of intel lets intel analysts focus on high value work, like analysis.
- **Support for MITRE ATT&CK:** ATT&CK has become a common language across cybersecurity monitoring, detection, prevention, and response. It can take the form of automatically identifying and tagging tactics and techniques to visualizing threat intelligence on the ATT&CK Navigator.
- **Native reporting:** Reports are a common product of intel teams, but can be tedious and waste precious resources. The ability to centrally create, store, update, and distribute reports from within the same platform analysts do their work saves significant time and effort.
- **Ability to visualize and respond to threat intelligence and context:** Visual analysis allows analysts to see patterns and find connections that may be difficult in other mediums like tables of data. This is not enough however. The ability to take action on intelligence directly within a dynamic visual environment is critical to making analysts more efficient and effective when doing their analysis.
- **Case management:** Teams need the ability to capture and memorialize knowledge across security operations activities about threats and actions taken, and be able to leverage that historic knowledge as part of daily activities, process improvements, etc.
- **Customizable and dynamic dashboards:** Dashboards tell a story to a variety of users and stakeholders, but it must be adaptable to the different personas. Static dashboards are not sufficient. The ability to custom design dashboards, interact with the dashboards, and share those with peers and stakeholders is required.

Identifying the right platform for your cyber threat intel program is critical.

A TI Ops platform approach will allow you to achieve the most efficient and effective aggregation, processing, analysis, and dissemination of your cyber threat intelligence. To learn more about the market's only TI Ops Platform, take a tour of the ThreatConnect Platform, or reach out to speak with one of our experts.

Reach out to learn how the ThreatConnect Platform can make you and your team more effective, decisive, and collaborative.

+1 (800) 965.2708 -or- **ThreatConnect.com/Request-a-Demo**

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

+1 (800) 965.2708