MORE IS NOT MORE

Busting the myth that more threat intel feeds lead to better security

ThreatConnect™

ThreatConnect.com

It's a common misconception that a large quantity of threat intelligence feeds leads to more effective security. Unfortunately, threat feed overindulgence can lead to confusion, disorganization, and inaccurate threat reports. Instead of adding more threat intel feeds, you should incorporate the feeds that provide the most value to your company's security operations.

Identifying Your Risk (or Learning How to Turtle)

To effectively evaluate a threat intel feed, as a security professional you should ignore the "more feeds, more intel" mindset. Instead, focus on the relevance of the intelligence provided to your security and business operations and the source from which the intelligence is gathered.

You need to first internally identify your organization's needs and priorities by understanding the various characteristics and personas of your own security operations. These can differ based on a variety of factors, such as threat landscape, maturity, risk tolerance, size, and budget.

Keep in mind, no two companies are exactly alike. Your organization's threat intelligence should be unique to your business. Once your company completes an internal review, you'll have the necessary information to evaluate the various threat intel feeds on the market and choose the ones that will best protect your business and security objectives.

So, what are your options when it comes to intel feeds?

- Open source feeds; sometimes called free feeds. Not to insult your intelligence, but free is not free. Ever. They cost your organization time and resources, and are often not relevant to your business and security objectives. Threat data does not equal threat intelligence.

- Ah, the premium feeds. Things to consider here: update frequency, context, timely information, and delivery format. Bottom line: trust, but verify.

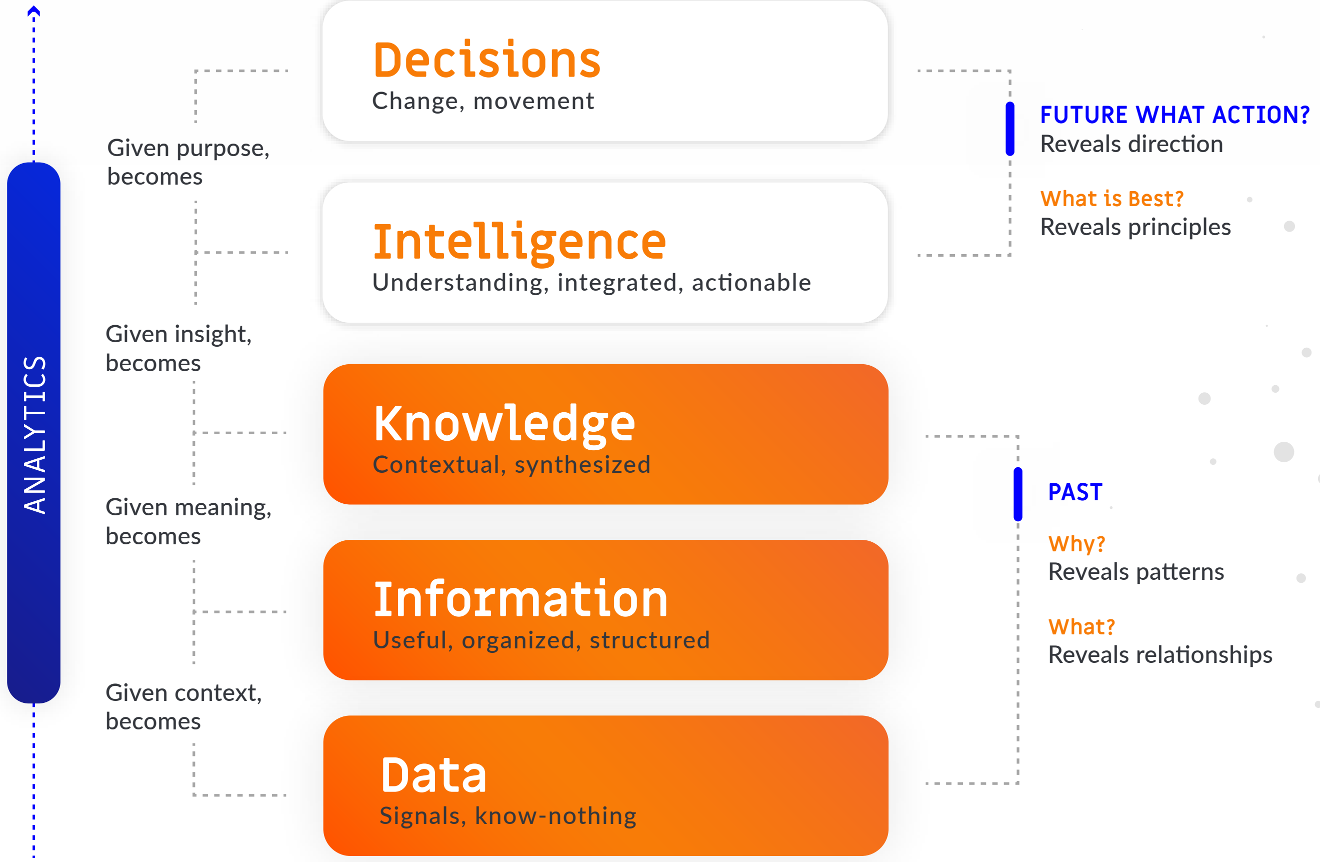
- Get all the feeds (premium and/or free) and hope that something sticks. There will be a lot (did we say a lot?) of chaos to go through with this option, but sometimes, you're Goldilocks and you find the one that is just right.

- You don't want to hear this, but it needs to be said: create your own. Your organization's information is the most relevant to you. It isn't easy, but it's yours; and it's reliable.

- The combination. This is an advanced move, but also a good goal. In this situation, all of the data is aggregated into a Threat Intelligence Platform (TIP), and analytics are used to pare down what you need to address by sorting out the false positives, adding context, and elevating the threats that are real to your organization.

DIKI DIKI DIKI Can’t You See? Sometimes TI Hypnotizes Me

One useful resource to help you decide which threat intel feeds are relevant to your organization is the DIKI pyramid (Data, Information, Knowledge, Intelligence), adapted from the well-established DIKW (Data, Information, Knowledge, Wisdom) hierarchy. Specifically, the DIKI pyramid can help you use analytics to add context that turns data into information, information into knowledge and — finally — use that knowledge to make an intelligent business decision.



ANALYTICS

Decisions
Change, movement

Given purpose, becomes

Intelligence
Understanding, integrated, actionable

Given insight, becomes

Knowledge
Contextual, synthesized

Given meaning, becomes

Information
Useful, organized, structured

Given context, becomes

Data
Signals, know-nothing

FUTURE WHAT ACTION?
Reveals direction

What is Best?
Reveals principles

PAST

Why?
Reveals patterns

What?
Reveals relationships

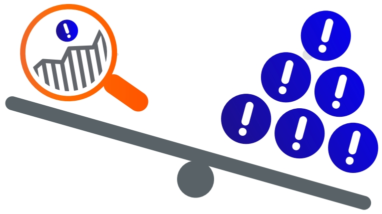
Let’s start at the bottom of the pyramid with data. In layman’s terms, data is the initial beacon or signal that a company may receive when something isn’t quite right on their network. It’s the rawest component that your organization will obtain, and it needs to be contextualized in order to be useful further down the road. For example, if you notice a lot of login attempts from the same IP address, this is the initial signal, this is data. There is no context behind these IP login attempts... yet. This is what you get with open source feeds.

Let’s move to the information portion of the DIKI pyramid. Simply put, information is contextualized data. Maybe you notice that the IP login attempts are all coming from the same location, somewhere you wouldn’t normally expect. This small piece of context has transformed the original data into information. Now what?

With knowledge, maybe you’ll recognize that these IP login attempts look like a credential stuffing attack (someone is trying to access accounts by overloading the system). This knowledge provides you with the context necessary to make a decision on how you’d like to handle the influx of IP login attempts.

When you’ve contextualized data to provide information that leads to the knowledge of how the attack was occurred, you have the intelligence you need to take the appropriate action.

Quality Over Quantity: Size Doesn’t Matter



At ThreatConnect, we know that security operations and threat intelligence are not one size fits all. No matter how many feeds a company claims to have, at the end of the day the quality of your threat intelligence will make all the difference. That’s why it’s so important to choose a TIP that brings together all of your intelligence sources.

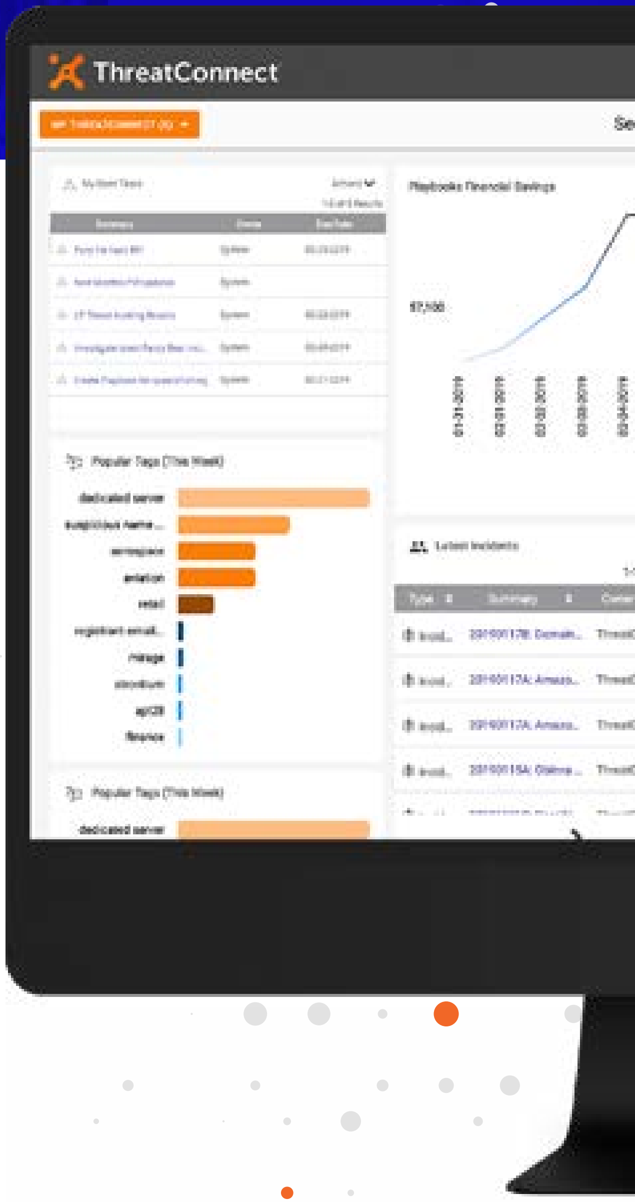
The ThreatConnect Platform doesn’t stop at aggregation. It gives you the situational awareness you need to know when to take action, help your team prioritize indicators, and validate your findings with other Threat Connect users. And the Platform allows you to automatically share indicators to all relevant tools or systems in your security arsenal so you will immediately be able to distinguish true threats from false positives.

Our latest threat intel Report Card feature utilizes the ThreatConnect CAL™ (Collective Analytics Layer) to help users more effectively manage and evaluate intelligence in the ThreatConnect Platform. Report Cards are context-packed, objective ratings of open source threat intelligence feeds that include crowdsourced classifications for reliability, unique indicators, indicators first reported, and the average threat score of indicators. Customers can now immediately evaluate the effectiveness and quality of open source intel feeds and minimize the number of false positives and irrelevant data.

For any company scouring the market for the best threat intelligence platform, we recommend taking the above information to heart. Be careful not to be tempted by something that appears too good to be true, because it probably is - and will cost you in the long run. You win when you invest the time needed to really know and understand your organization so you can confidently approach the problems at hand.

Know and understand your organization so you can confidently approach the problems at hand.

ThreatConnect intelligence is a **premium intelligence source** created and contextualized by our in-house Research Team.



More than a typical threat feed, ThreatConnect Intelligence is actionable intelligence that provides real insight for your organization, building out additional information about a threat, from adversary activity, country of origin, phase of intrusion, and more.

Also, our team is constantly adding more data types to our threat intel feeds, such as tech blogs. This diversifies the type and style of data we can use to help customers identify and mitigate threats. The ThreatConnect Research Team is dedicated to the trade. Using the ThreatConnect Platform, we scrutinize trends, technology, and socio-political motivators to develop comprehensive knowledge of the cyber landscape. Then, we share what we've learned in the Platform so you can protect your organization, and your team can take precise action against threats.

ThreatConnect Intelligence Includes:

- Enriched indicators
- Context about the impacts on your particular organization
- Consolidated open source intelligence on adversaries
- Downloadable, shareable reports
- High-quality data about relevant threats
- Access to the expertise of the ThreatConnect Research Team

ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708