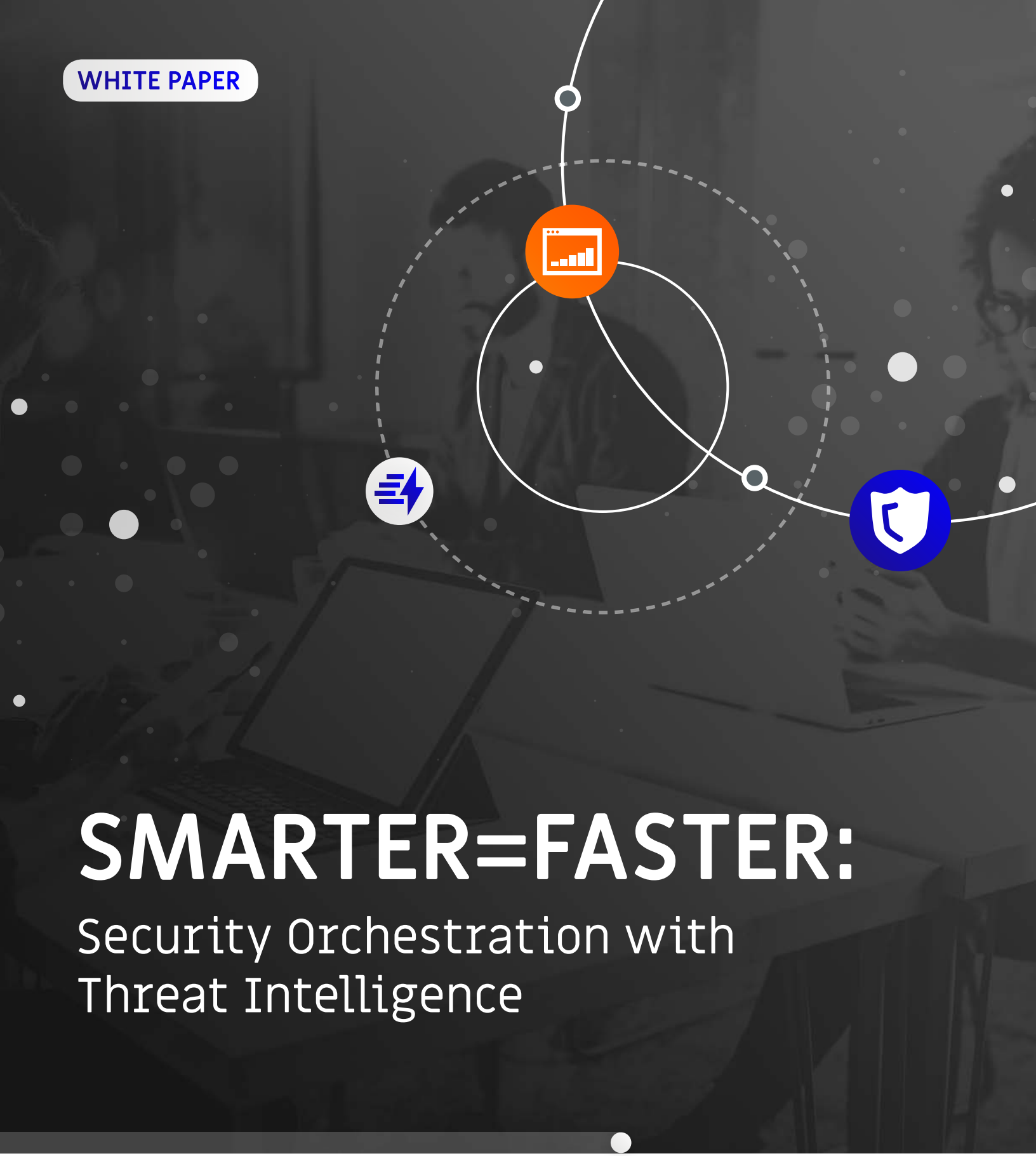
WHITE PAPER



SMARTER=FASTER:

Security Orchestration with Threat Intelligence

ThreatConnect™

ThreatConnect.com

Contents

Smarter=Faster: Security Orchestration with Threat Intelligence

Understand how you can make smarter decisions to move faster — both blocking an adversary and disrupting them altogether — by using orchestration with intelligence.

Executive Summary

The cybersecurity landscape moves at an incredibly fast pace. Analysts in security teams make decisions all day in their investigations that impact the security of the entire organization: Where should I look next? What should I do about this alert? Is this even dangerous? The better we can arm analysts with additional information, context, and situational awareness, the more informed their decision-making will be. But due to the dizzying scales of alerts and associated data occurring in a typical enterprise, decision making needs to scale. Generally, the faster you are at making decisions and taking action against a threat, the less likely you are to be breached and the more likely you are going to be able to stop merely reacting and move into a proactive approach with your team. Today, teams are automating mass amounts of data, but are not yet able to refine that data into intelligence suitable for decision making.

Even for the most skilled team, speed is not easy to achieve. Certain aspects of cybersecurity can be slow (think copying and pasting information from one tool to another — how long does your team spend doing that every day?). Instead of focusing on identifying threats and prioritizing response efforts, teams are scrambling to try to keep up with the ever-growing pile of simple, repetitive tasks. This, at best, slows your team down or frustrates them. At worst, it allows threats to fall through the cracks.

Today, more cybersecurity teams are turning to automating or orchestrating their processes to get the speed that they need to be effective. But, automation and orchestration have their limits when it comes to enabling speed and effectiveness at the same time. While automation can speed up a repetitive process and orchestration can carry it across tools, they typically can only do what you may call dumb tasks — those that require no intelligence.

Using threat intelligence and orchestration together, situational awareness and historical knowledge determine what and how processes should be handled. Threat intelligence allows the process to automatically adjust itself and helps you drive further decision making.

You ultimately want to be able to observe what is happening in your environment and across the greater security landscape. With threat intelligence, you can. Taken one step further, threat intelligence allows you to cross reference what you observe with historical knowledge and situational awareness. This trifecta of information provides insight that enables you to decide which action to take. And then, you can automate that action. Using threat intelligence to determine automation empowers you to be proactive in mitigating threats to your organization.

Threat intelligence allows the process to automatically adjust itself and helps you drive further decision making.

Using threat intelligence and orchestration, you can:

- Alert, block, and quarantine based on relevant threat intel
- Add context and gain insight to speed-up decision making
- Increase your accuracy, confidence, and precision
- Understand context and improve over time
- Adjust processes automatically as information and context changes

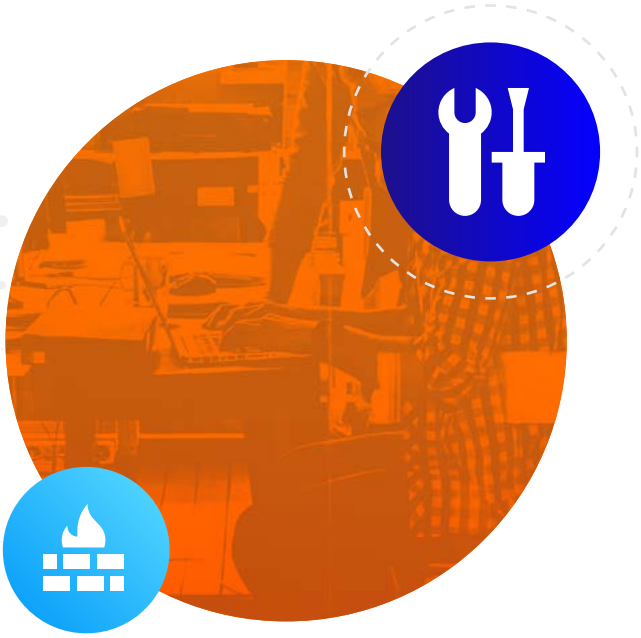
The Evolution of Orchestration and Automation

Orchestration and automation have evolved. Just a few years ago, companies were looking to automate some tasks through scripting and custom coding — a labor-intensive process that only the most mature teams could achieve. Lately, we've seen an emergence of security orchestration solutions in the marketplace. Security orchestration tools conduct automation of entire workflows across your existing security tools.

Automating certain repetitive tasks saves analysts time. When analysts have more time they can focus on context and accuracy, instead of just speed. Plus, with more time, they then can do higher-level work such as proactively hunt for threats. Orchestration is the greatest force-multiplier for time savings.

It helps teams maximize their current resources, get more out of the tools they have, and do more with less. Orchestration reduces the possibility for human error.

Unfortunately, there's much more to be done. Security orchestration, in its purest form, still has shortcomings. Automating tasks (like blocking on a firewall) can make people nervous — and rightfully so. Imagine trying a self-driving car for the first time. Odds are you would put your hands a few inches above the steering wheel, not sure if you could trust the machine to handle everything. Security orchestration presents similar trust issues.



The typical cybersecurity team **uses anywhere from 10 to 100+ tools to protect their network.**

The Changing Security Landscape

Because the cybersecurity landscape changes quickly, how do you know if the task you automated yesterday will still be relevant tomorrow? Is there any new information or intelligence related to this task that could affect how it should run? You can't always be sure that what you're doing now will still be the most efficient thing to do tomorrow, let alone in an hour, or the next time the task is due to be run.

Orchestration allows you to conduct defensive actions across technologies immediately, increasing your effectiveness in stopping, containing, or preventing attacks. However, even though you can be faster and take more complex actions with orchestration technologies, your ability to orchestrate an effective defense is still dependent on your knowledge of attacker's methodology and your ability to detect or mitigate it. Hackers, by definition almost, are adaptive. If one route to their objective is blocked, they will try others. If narrowly implemented, your playbooks can be be circumvented by a clever or persistent adversary.

How can you better avoid this situation? It takes an intelligence-led approach to inform your strategy for orchestration in two key ways. First, intelligence on adversaries attack patterns will inform how you build and configure orchestration capabilities to defend your network better. Second, orchestration playbooks can be built to be more adaptive to changing adversary capabilities and infrastructure as both internal and external threat intelligence is available.

Combining your threat intel **with your orchestration capabilities is key.**

Using Threat Intelligence

First, let's define threat intelligence (TI).

Here are two definitions currently used:

1

"**Threat intelligence is evidence-based knowledge,** including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

Gartner

2

"**The details of the motivations, intent, and capabilities of internal and external threat actors.** Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats."

FORRESTER

Though threat intelligence may mean different things to different people, there is one constant: It is meant to inform business decisions. Put simply, threat intelligence could be defined as “actionable knowledge of threats.”

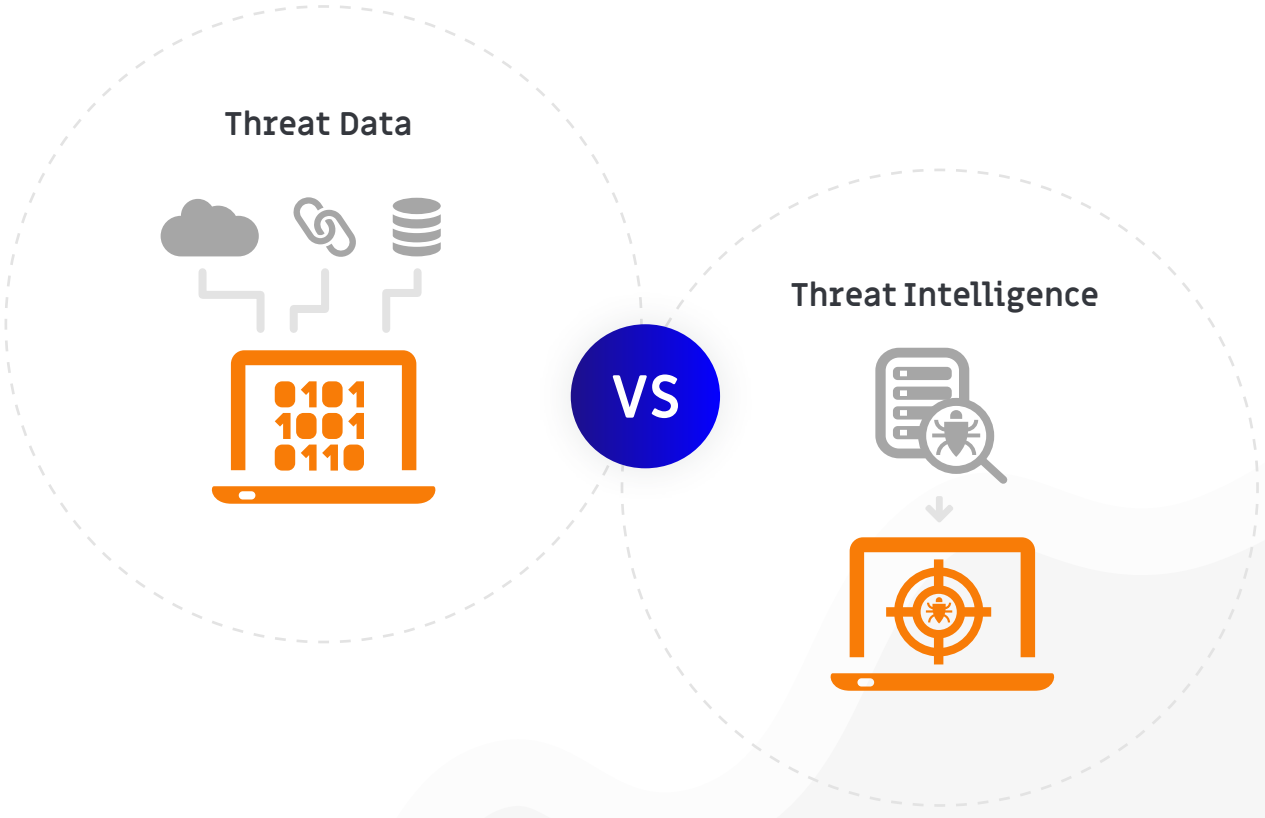
Organizations can use threat intelligence in many ways. Some use TI to enhance detection and prevention, increase their speed and efficacy of response, inform security or corporate policy, or all of the above. No matter the size of the organization, threat intelligence is an essential part of their cybersecurity program.

The Difference between Threat Data and Threat Intelligence

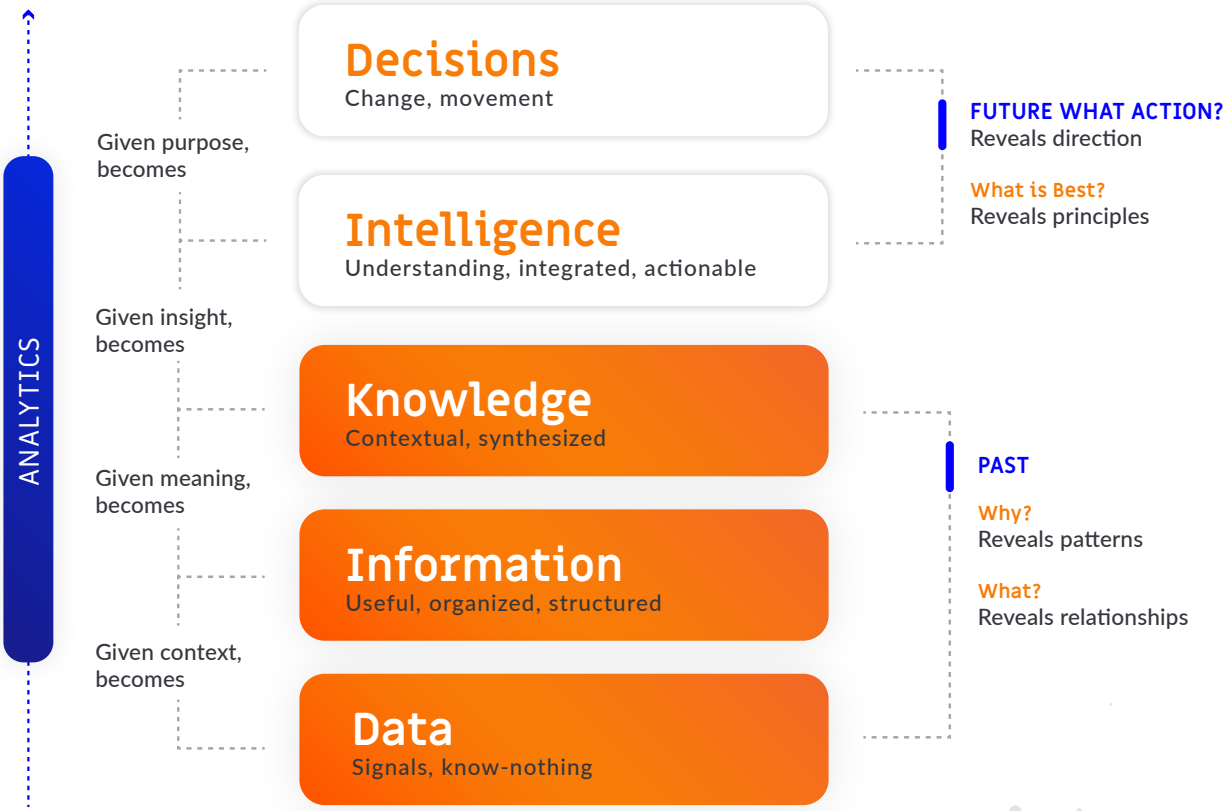
You may be thinking that you already have both orchestration and threat intelligence covered in your current infrastructure; that threat Intelligence ‘feeds’ can be integrated with security operations tools. It’s not that simple, though.

Feeds typically contain threat data or threat information at best. Threat data must be refined, enriched and/or correlated to provide additional context and meaning. This allows data and information to be promoted to knowledge. Knowledge that conveys understanding, is integrated with the organization’s processes and systems, and is actionable such that it can be used to make decisions qualifies as intelligence. Of course, not all external “intelligence” is really masquerading low fidelity “data.” Many commercial threat intelligence vendors put rigor into providing enriched and relevant information into their products.

Still, some context such as how some given intelligence affects you specifically, whether or not a given threat has targeted you before, how vulnerable you are to a given technique may only be answerable by you and your organization directly. To address this problem, some platforms such as ThreatConnect, integrate with commercial intelligence providers as well as your own internal tools, giving you a way to assimilate external intelligence to ensure it is truly integrated and actionable in your environment.

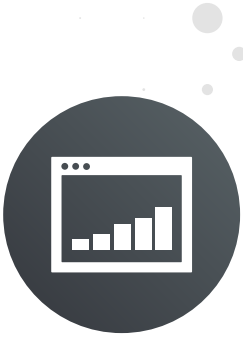


Using Threat Intel to Make Informed Decisions



Intelligence fuels decision-making for taking action against a threat.

Once you make contact with an adversary, you have an opportunity to collect information and store it as knowledge of their attack patterns. This can drive your knowledge of the adversary so you can block them better in the future. Knowledge of your adversaries allows you to ask better questions and find gaps in knowledge.



With threat intelligence in the complete sense of the term, you go beyond knowledge to being able to predict where an adversary is likely to attack next.

As a result, you can make decisions to defend against or mitigate an attack. So, as you begin to automate your processes, it is essential that you use threat intelligence to drive your decisions. Orchestration can continue to block where an adversary has been before, but using your threat intel to drive orchestration enables you to determine where the attacker will most likely go next — allowing you to become proactive.

Orchestration with and without Threat Intelligence:

What's the Difference?

As mentioned above, orchestration is facilitating human and automated processes by integrating multiple security tools and systems. It should be the connective tissue that facilitates efficiency and scale across people, processes, and technology. Orchestration informed by threat intelligence is more effective, resilient, and adaptive. It uses available relevant information on threats and information about your own environment to adjust and improve your processes dynamically.

Let's use an analogy to explain the difference: Say you want to automate taking out your trash.

Using an orchestration tool for simple automation, you set it to automatically empty into the dumpster when the trash can is full. You set the parameters and the end destination, and then leave it alone. This task can only be changed if you go in and change the parameters.

Threat intelligence-driven orchestration goes a step further — it takes things like environment, situational awareness, and circumstances into account. What if you throw away food that will rot and smell bad? You'll want to take out the trash before it is full. What if the dumpster is already overflowing? Maybe you want to wait a day to take out the trash so you don't add to the mess. What if someone brings your trash can into a different room to use? What if it is knocked over?

Even with something as simple as emptying a trash can, there are numerous circumstances that can alter the outcome. Using threat intelligence and orchestration together, situational awareness and historical data determine when and how a task should be done. In this example, the trash can would be emptied at different times and in different ways depending on the circumstance. Threat intelligence allows the process to be adaptive to the changing environment.

Now that we've explored different ways to automate a chore like taking out the trash, let's focus again on cybersecurity. To reiterate, threat intelligence may be the catalyst for taking an action or starting a process, and also informs how the process and decision-making are done throughout. As threat intelligence drives your orchestrated actions, the result of those actions can be used to create or enhance existing threat intelligence. Thus, a feedback loop is created — threat intelligence drives orchestration, orchestration enhances threat intelligence.

Orchestration informed by threat intelligence is more effective, resilient, and adaptive.

Understanding OODA

You need both orchestration and threat intelligence to make informed decisions. To further demonstrate this, let's take a look at the OODA loop. A decision making cycle, the OODA loop stands for: Observe, Orient, Decide, and Act. It was created for the military by James Boyd, but it has been widely used across other business verticals and law enforcement. Originally designed to explain how to defeat an adversary and survive in airborne dogfights — it also applies well to cybersecurity.

OODA Loop for Cybersecurity

Observe

Security monitoring and detection to identify certain activity, anomalies, or events that may require a second look or further investigation.

Orient

Analyze the current threat landscape both internally and externally. Combine this information with context, associations, and patterns to determine relevance and prioritization for your organization.

Decide

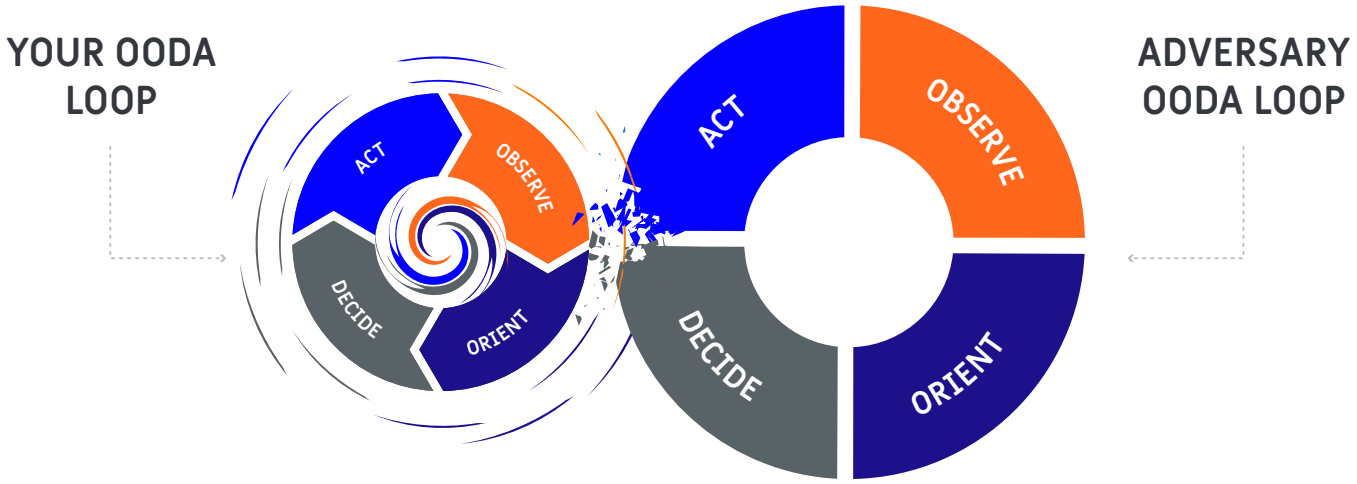
Use what was learned from Observe and Orient to determine the best course of action to take to respond to and mitigate, the potential threat or incident.

Act

Take action on the identified threat or incident based on what was determined in Decide. Record the results of the action and what the end result was.

The OODA loop is a recurring cycle. Both attackers and defenders are constantly making decisions based on their own OODA loop. Observations are the information that fuel the decisions and actions. The second O, orient, is a sense-making function that filters out irrelevant information, and creates focus based on all presently observed information and all of the knowledge and previous experience the decision maker has. This is a very important part of the loop, as it will fuel how we decide and act.

In order to defeat an adversary, in physical battle or in the cyber landscape, you must have a faster OODA loop than they do. Faster, more accurate actions on your part break (or get inside) an adversary's OODA loop.



Without effective observation and orientation, it is extremely difficult (if not impossible) to make a decision and know how to appropriately react. Just like in battle, if you know a cyber adversary's capabilities, intent, and infrastructure, you can effectively shrink the attack surface. Your ability to anticipate the adversary's next move is dependent on the ability to access available information and leverage it.

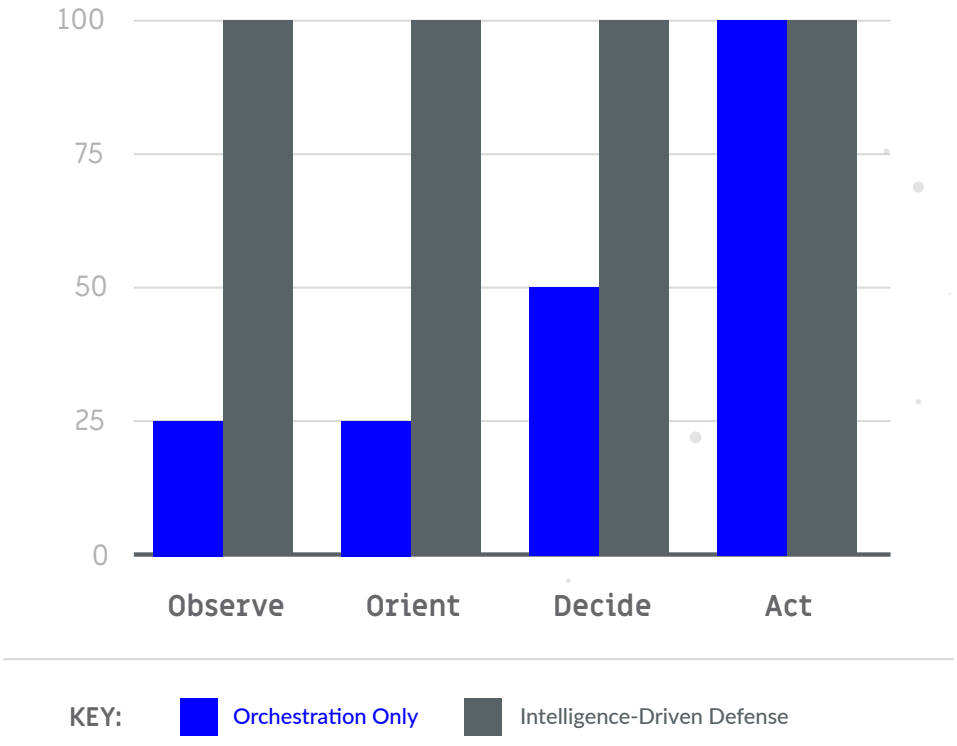
Threat intelligence provides a wider aperture for observation and provides insight to assist in clearer, more accurate orientation to a decision.

Closing the OODA Loop:

How Orchestration and Intelligence-Driven Orchestration Compare

Most security orchestration tools today can fully support the 'Decide' and 'Act' part of the OODA loop. You can automate processes to do things like enrich indicators with information from third party tools, ingest and parse emails, block on a firewall, or maybe even empty the trash. By using threat intelligence to drive your orchestration, you can greatly enhance the 'Observe' and 'Orient' components of the OODA loop.

You can observe what's happening, both in your environment and in the greater security landscape. You may then orient by cross reference that information with historical knowledge about the threat and awareness of the current landscape. This can be done easily by referencing all of the threat intelligence and additional context. From there, you can decide on which action to take based on all relevant input. Finally, you can take that action across your teams and technology.



Using Threat Intel in Orchestration:

How to Complete the OODA Loop

One of the key, often overlooked, tenets of the OODA loop is that it's a loop. That means it feeds back on itself. Actions taken are themselves data points for observation. In the paradigm of data, information, knowledge, and intelligence, the results of actions can be refined into intelligence to better inform the next decision. To do this correctly you need to be able to quickly and succinctly access relevant knowledge fused from past events, Incident Response engagements, and external threat intelligence.

The best way to do this is to use a system of insight. Forrester's Brian Hopkins defines this term as "closed loop systems [that] 1) discover the insights that matter most; 2) embed them into the software their customers and employees use to engage; and 3) continuously measure and learn from the results." Systems of insight combine people, process, and technology by combining systems of record, automation, and engagement into one tool, system, or platform.

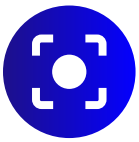
With Systems of Insight, you can:

1. Discover the insights that matter most
2. Embed them into the software their customers and employees use to engage
3. Continuously measure and learn from the results

By using one platform that includes threat intelligence and orchestration together, you create a system of insight, enabling:

Alert, block, and quarantine based on relevant threat intel

Even for lower level tasks like alerting and blocking, having relevant threat intel is important. You can automate detection and prevention tasks. Having multi-sourced, validated threat intel can help ensure that you are alerting and blocking on the right things.



Increase your accuracy, confidence, and precision

Situational awareness and historical context is key to decision making. Working directly from threat intelligence allows you to work quicker and prevent attacks before they happen. The more you can automate up front, the more proactive you can be. By eliminating false positives and using validated intelligence you are increasing the accuracy of the actions taken. This accuracy leads to confidence and improves speed and precision.

Understand context and improve over time

When you automate tasks based on threat intelligence thresholds such as indicator scores, and memorialize all of that information, you can strategically look at your processes to determine how to improve.

Adjust processes automatically as information and context changes

Intelligence-driven orchestration is data first, while security orchestration is action first. When your threat intelligence is stored in a data model (with threat scores), you can set your processes to automatically adjust if the threat landscape changes.

A Practical Example of Intelligence-Driven Orchestration

Now, let's say that a security team is on the lookout for whaling scams. There is a Security Operations Center (SOC), an incident response (IR) team, and a cyber threat intelligence (CTI) team. The CTI team has been gathering intel on several possible adversaries, and the SOC has several monitoring inboxes for collecting email data.

Without threat intelligence you can only use orchestration to:

- ✓ remediate those suspected whaling emails
- ✓ perform checks to see if they've made it to the Users' inboxes, and if they've been opened
- ✓ generate tickets for remediation, or;
- ✓ even take action to quarantine the email and associated attachments or dropped files.

This is an effective decision and action based on available observed data-points filtered for relevant orientation. However, your ability to convict suspected targeted whaling attacks is greatly enhanced by operational and dynamic threat intelligence providing information on malicious senders, mail servers/relays, and other characteristics of the email header or attachment itself that can trigger action. You're going to let things slip through if you don't have intelligence plugged in to your orchestration capability at the operational level. This gives you the ability to more dynamically observe and orient to relevant facts that will inform your decision.

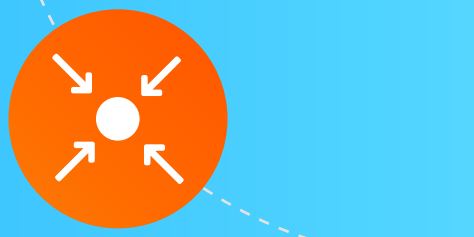
More importantly, there is a huge opportunity being missed and that is using the speed and scale provided by orchestration capabilities to learn and adapt from attacks as they occur by creating intelligence as you orchestrate.

Let's continue with the example with an intelligence-led approach: Your orchestration capability was able to act on intelligence based on an Indicator of Compromise match against a known email address recently used in a campaign against a partner in your industry with whom you share intelligence. Great, you completed the OODA.

Your ability to convict suspected targeted whaling attacks is greatly enhanced by operational and dynamic threat intelligence providing information on malicious senders, mail servers/relays, and other characteristics of the email header or attachment itself that can trigger action.

Now for the loop.

Your orchestration capability gathers other artifacts on the email that could have also led to detection, but didn't. Facilitated by orchestration, you perform an initial automated triage of the malware, recognizing the backdoor malware family and new command and control domains. Other artifacts are gathered from the email itself; and the email is also stored along with the new artifacts in a knowledge repository for future analysis if necessary. The orchestration capability then runs correlation checks on the new artifacts and shows that the detected email was actually part of a campaign targeting a specific group within your organization.



Orchestration informing Intelligence

Your orchestration capability gathers other artifacts on the email that could have also led to detection, but didn't. Facilitated by orchestration, you perform an initial automated triage of the malware, recognizing the backdoor malware family and new command and control domains. Other artifacts are gathered from the email itself; and the email is also stored along with the new artifacts in a knowledge repository for future analysis if necessary. The orchestration capability then runs correlation checks on the new artifacts and shows that the detected email was actually part of a campaign targeting a specific group within your organization.

Operationally

Intelligence created from the newly gathered artifacts extracted from the campaign. And the artifacts have been dynamically vetted and scored to be sent to defensive sensors.

Tactically

Orchestration, through Playbooks, may be modified to account for newly observed adversary attack patterns or techniques.

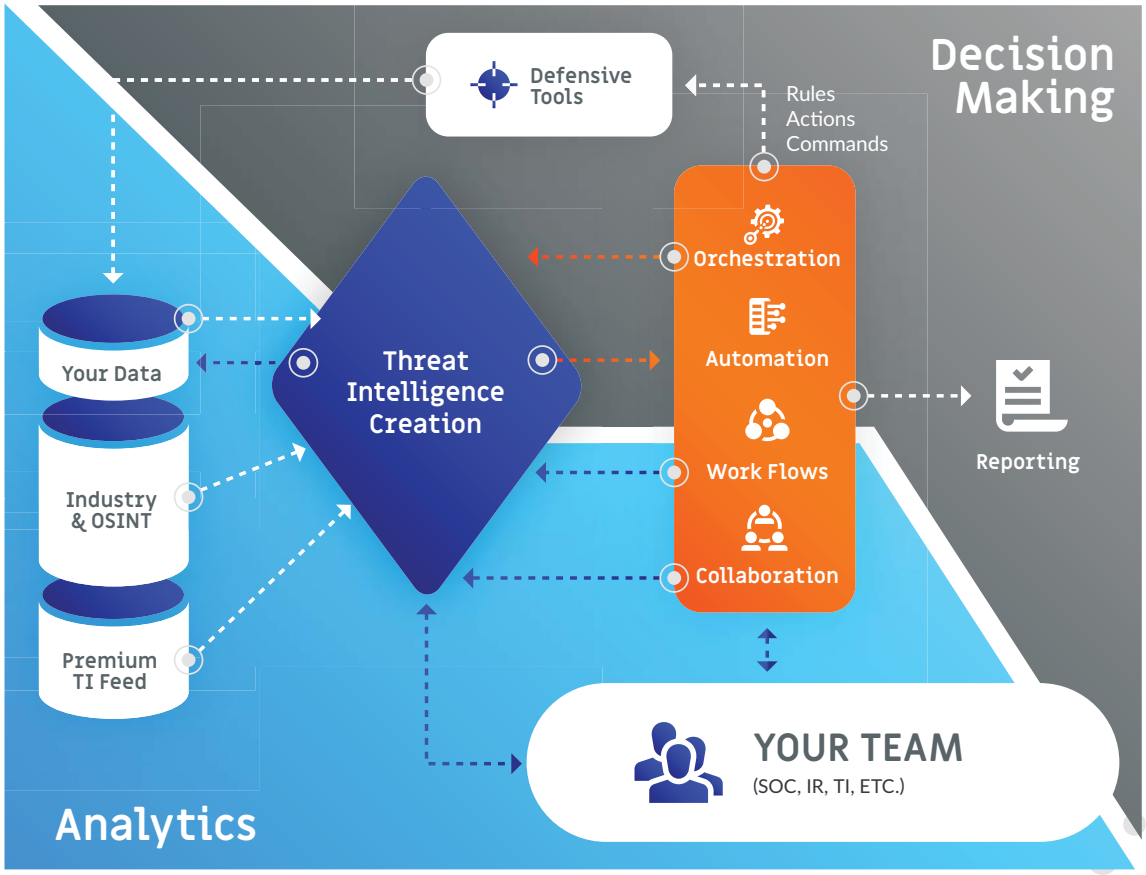
Strategically

With orchestration, you are able to check against historic intelligence, and then tie this campaign to a previously known threat group. Targeting analysis also shows trends in users targeted and actions taken by the adversary once inside. Orchestration enables technical attribution, adversary intent, and observed capabilities that scale to better determine security policy and inform defensive technology allocations.

Fusing Intelligence and Operations in One Platform

A security operations and analytics platform combines threat intelligence, analytics, and orchestration into one place. These platforms are the perfect technology to create your own system of insight. It enables team members to assign each other tasks, work from the same data, and easily collaborate about the threats they are seeing. A security operations and analytics platform can also become your system of record, because they store every piece of threat data, all of the additional context added to it, and all of your processes in one place. Plus, the platform enables automation by incorporating advanced orchestration capabilities, which allow a user to connect to any other tool in their environment.

By using a security operations and analytics platform, you can start to build a system of insight and make more informed decisions about your security operations and strategy.



In The End

Once you've aggregated and stored your threat intelligence, you can begin to build out your system of insight and expand knowledge for everyone in your organization. You can then start to run and adjust your orchestrated playbooks on your threat intelligence. The best way to do this is to have both capabilities in one place. A security operations and analytics platform combines threat intelligence, analytics, and orchestration into one place. Once you have one in place, you can start to make more informed decisions about your security operations and strategy.

ThreatConnect bridges threat intelligence and orchestration, allowing security teams to fully utilize their current investments by automating repetitive tasks, prioritizing critical events, and providing the situational awareness and additional context needed to inform decision making that will better protect your organization from attacks.

If you want to start aggregating and normalizing your threat data, you can do that in ThreatConnect. If you need to conduct deep threat analysis, you can do that in the Platform too. You can orchestrate tasks based on your stored threat intelligence. The ThreatConnect Platform is built to help you through the entire lifecycle of a threat — from aggregation, to analysis and prioritization, all the way through taking necessary action to defend your network.

The ThreatConnect Platform was specifically designed to help organizations understand adversaries, automate workflows, and mitigate threats faster using threat intelligence. Because there are organizations at every maturity level, ThreatConnect built a suite of products designed for teams at any of these levels. And because each of the products is built on the ThreatConnect Platform, it will adapt with an organization as it grows and changes.

The ThreatConnect Platform is built to help you through the entire lifecycle of a threat — from aggregation, to analysis and prioritization, all the way through taking necessary action to defend your network.

Further Reading

eBook

What is a SOAR Platform?

The cybersecurity space is evolving more rapidly than any other business function before it. This is where the Security Orchestration Automation and Response platform comes in.

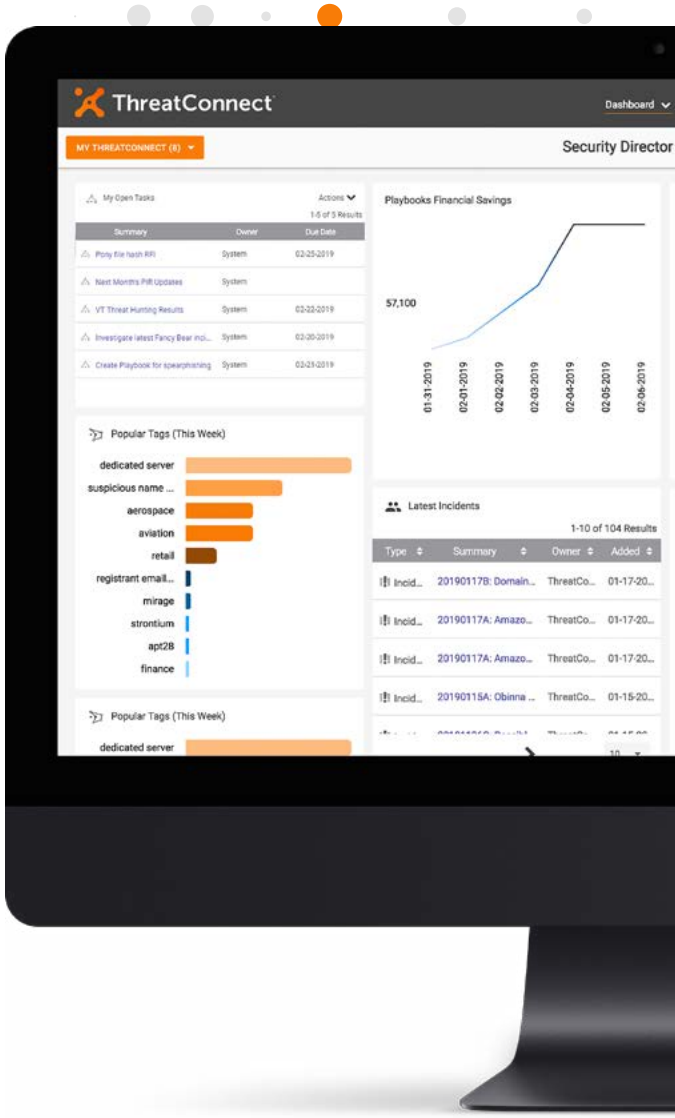
https://www.threatconnect.com/download-SOAR-ebook

Webinar

Mitigate Threats Faster with an Intelligence-Driven Defense

Learn how to understand adversaries and mitigate threats to your network faster using threat intelligence and orchestration.

https://www.youtube.com/watch?v=WnEVEDGEsjI



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