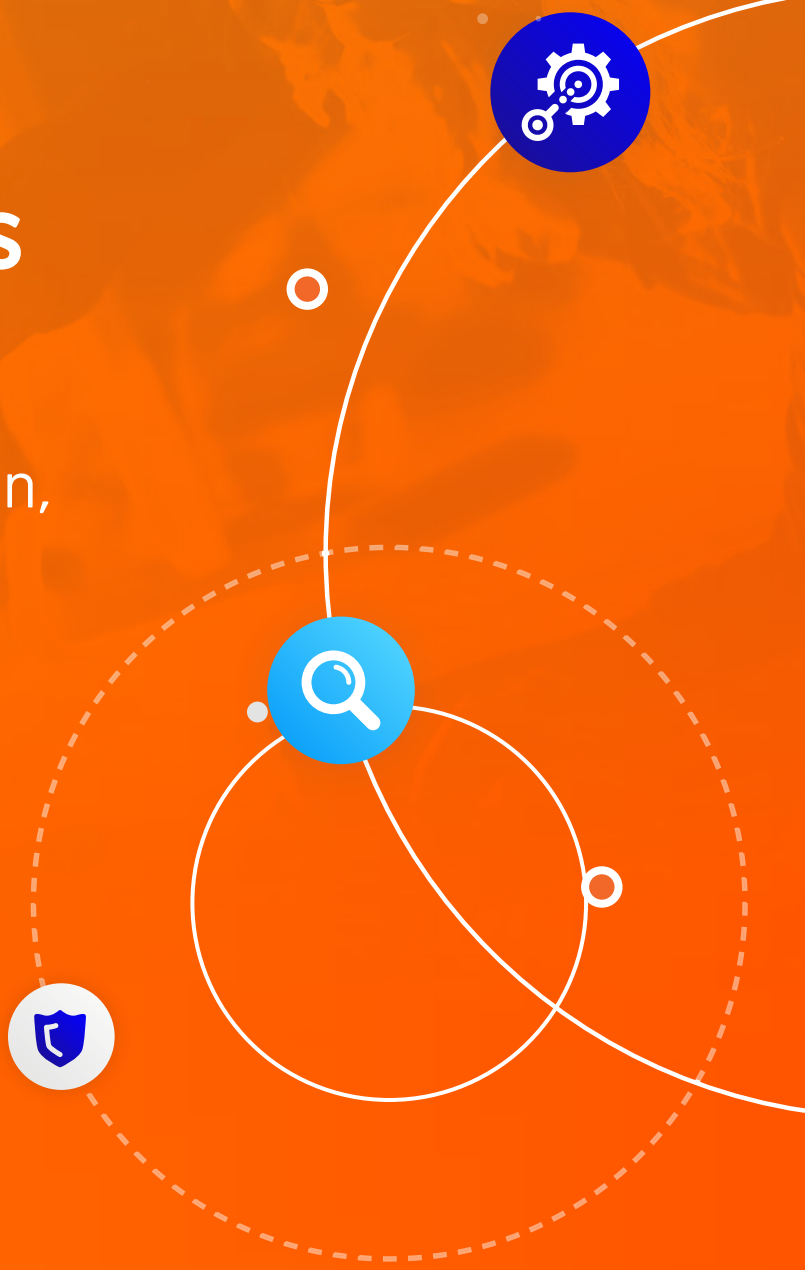
eBook

SOAR Platforms

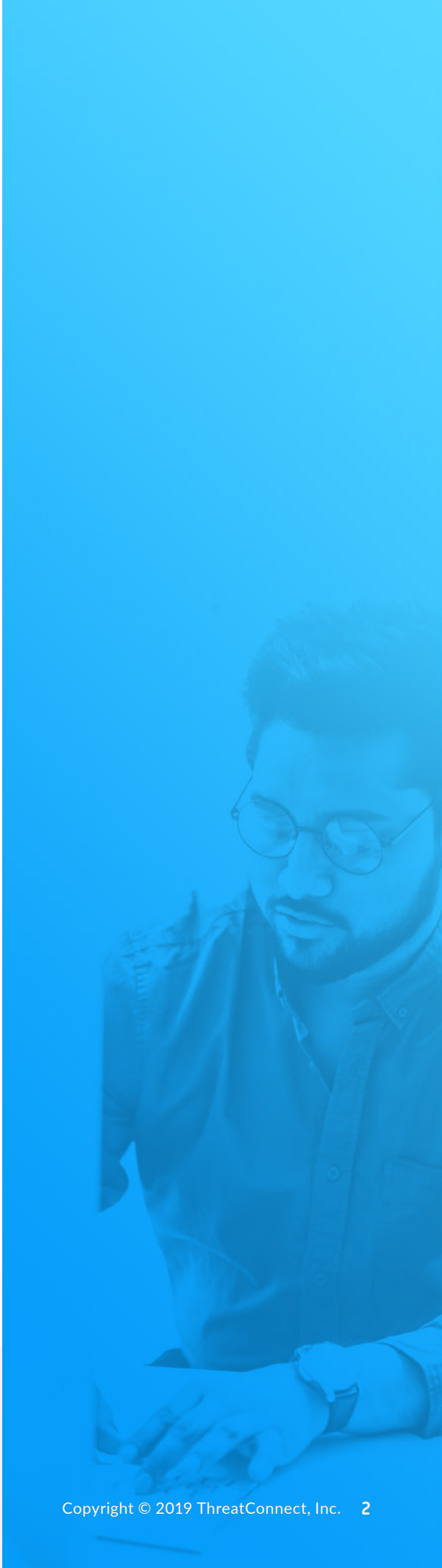
Everything you need to know about security orchestration, automation, and response



ThreatConnect™

ThreatConnect.com

Contents



Chapter 1

Too Much Data and Too Few Resources

We've heard it before; the cyber threat landscape is changing so rapidly that it's impossible for security teams to keep up. Everyday, analysts make multiple decisions that have the potential to impact the entire organization: What should I do about this alert? Is this even dangerous? Will I be able to triage everything? Can incident response act quickly enough?

Security operation teams are over-dependent on staff using manual processes to handle security alerts and data volume. According to a research survey by Enterprise Strategy Group (ESG)[1], organizations use somewhere between 20-30 individual solutions, most creating their own logs and creating an environment ripe for security alert overload and inconsistent triage.

This exponential increase of data and alerts means that quick decision-making and execution needs to find a way to scale. To counter this, many have turned to new solutions designed to automate and orchestrate some aspects of their cybersecurity operations – in real time – and bolster staff productivity through reducing workload. Where full automation is not possible or advisable, these same solutions are expected to present the relevant data and facts to enable responsible staff to make fast, informed decisions.

While the problem of "too much data" exists at all levels of decision making in the organization, it is felt most drastically at the operational level. While organizations are automating massive amounts of data (54% of those surveyed by ESG say that their organization collects, processes, and analyzes more than six terabytes of security data monthly), they are unable to refine that data into intelligence so that they can respond faster to active threats, as well as create and leverage internally-derived IoCs (indicators of compromise) and detection signatures for prevention, threat-hunting, and faster containment.

54%

of those surveyed by ESG say that their organization collects, processes, and analyzes more than **six terabytes of security data monthly**[2]

[1] Cybersecurity Analytics and Operations in Transition: Challenges, Plans, Successes, and Strategies. Jon Oltsik, ESG, July 2017. https://www.esg-global.com/

[2] Ibid.

Even for the most skilled team, keeping up with the threat landscape, increasingly complex IT environments, changing regulatory compliance mandates, and mounting security alerts is not easy to achieve, let alone do quickly. To address these challenges, many organizations have moved towards having multiple teams focused on various initiatives spanning the cybersecurity department.

Historically, meeting these objectives has necessitated coordination and manual labor across these various teams. Now, with the right solutions in place, you are able to codify and automate these objectives, yielding a faster time to completion via orchestration. Working off a single platform is critical to successful coordination of detection and response initiatives, as it keeps knowledge sharing across these teams fluid and instantaneous.

An Automated and Orchestrated Threat Detection & Response Framework

According to Forrester[2], 68% of security technology decision makers state that using automation and orchestration tools to improve security operations is a high or critical priority, and over half of enterprises are planning to or have already implemented such tools.

Security orchestration and automation integrates different technologies and allows you to conduct defensive actions: it increases your effectiveness in stopping, containing, and preventing attacks. Integration is important since your teams are likely to have little patience for point solutions that are difficult to implement or get value from.

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 automate decision making, often they can only do what you may call mundane tasks – those that require no intelligence.

[2] Forrester Data Global Business Technographics Security Survey, 2017

Differentiating Between Automation and Orchestration

Speed is not easy to achieve. Certain aspects of cybersecurity can be slow. Think copying and pasting information from one technology solution 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.

Meet **Automation** and **Orchestration**. These two will take care of getting your processes to the speed that they need to be in order to be effective. In the industry, you may see them used interchangeably, but dig deeper and their meaning is quite different.

Automation - Security automation is the handling of a task (such as querying logs or managing user privileges) that would otherwise be done manually by a cybersecurity professional. It makes things much quicker, but doesn't cover more complex operations that may involve multiple decision points or systems. Think of it as a road with no intersections; a straight shot with only one way to go.

Orchestration - Security orchestration is a coordination of multiple security tasks and decision points into an oftentimes complex process. It typically involves conditional logic to enable branched processes to enable connecting and integrating multiple security systems, applications, and teams together into streamlined workflows. It also correlates disparate data to help coordinate the right response. As a holistic solution security orchestration involves people, process, technology, and information.

Using orchestration to build an effective defense is still dependent on your knowledge of an attacker's methodology, and your ability to detect or mitigate it. Adversaries are adaptive. If one route to their objective is blocked, they will try others. If narrowly implemented, your orchestrated processes can be circumvented by a clever or persistent adversary.

How can you better avoid this situation? Keep reading.

Orchestration With and Without Intelligence: What's the Difference?

Orchestration informed by intelligence on threats and your environment is more effective, resilient, and adaptive. An intelligence-led approach will inform your strategy for orchestration in two key ways:

1. **Intelligence on adversary's capabilities, attack patterns, and intent will inform how you build and configure orchestration capabilities to defend your network better.**

2. **Orchestration playbooks can be built to be more adaptive to changing adversary capabilities, attack patterns, and infrastructure as both internal and external threat intelligence is available. In some cases, threat intelligence allows the process to automatically adjust itself and helps you drive further decision-making.**

When using intelligence and orchestration together, situational awareness and historical data determine when and how a task should be done. Intelligence allows the process to be adaptive to the changing environment. And, allows you to strategically plan for a better program.

When taking this idea of informed and adaptive orchestration, and practically applying it to security operations and incident response to dynamically solve problems, you're introduced to Security Orchestration, Automation, and Response (SOAR).

Chapter 2

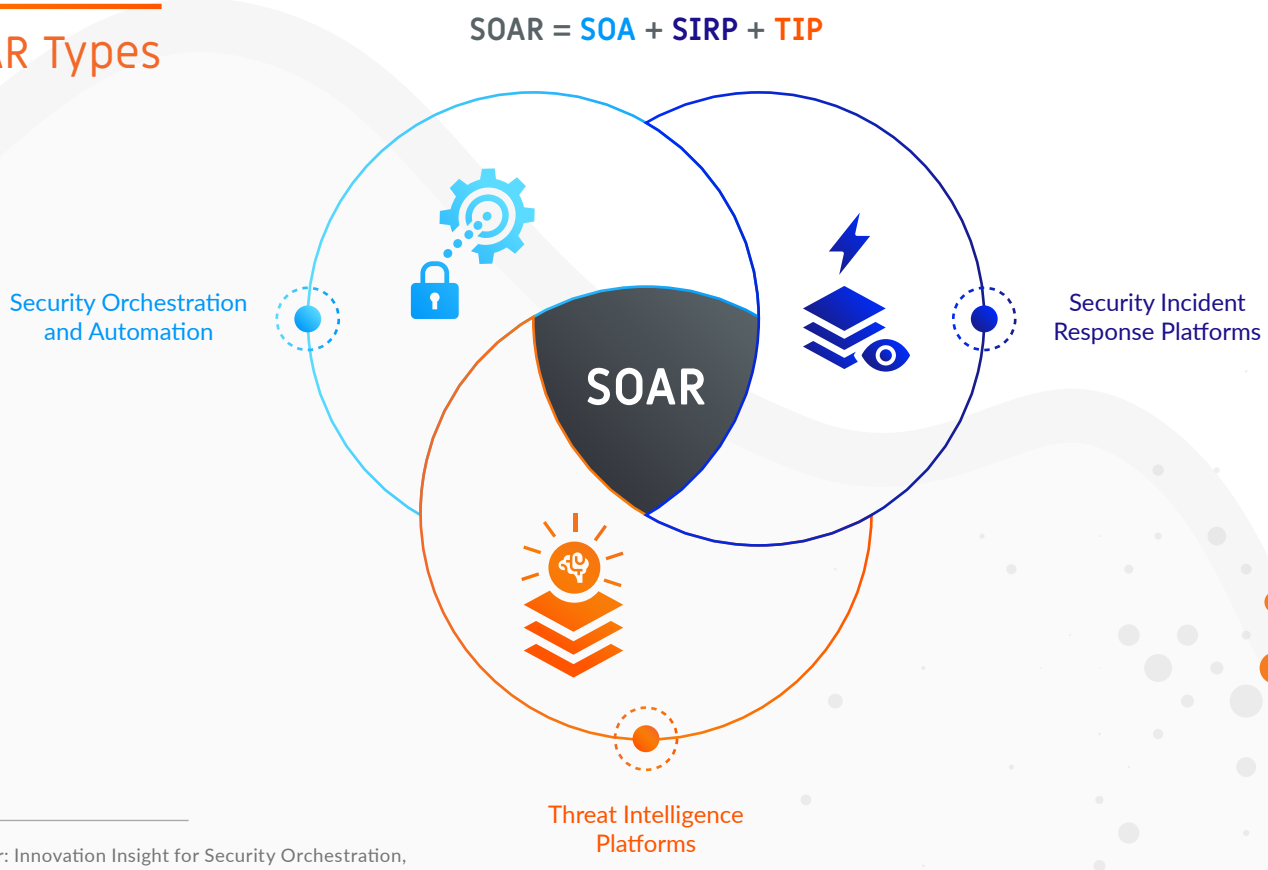
What is a SOAR Platform?

A SOAR platform represents an evolution in security operations driven by the vast amounts of data that must be processed.

It was the research and advisory firm Gartner that first coined the term SOAR as recent as 2015, then described as security operations, analytics, and reporting. Gartner stressed the need for machine-readable and stateful security data that could be used to provide reporting, analysis, and management capabilities to support operational security teams. Since then, its definition has evolved to address the convergence in the security orchestration and automation (SOA), security incident response platforms (SIRP), and threat intelligence platforms (TIP) technology markets.

The image below depicts Gartner's 2017 updated definition of SOAR[3].

SOAR Types



3 Gartner: Innovation Insight for Security Orchestration, Automation and Response, November 2017

Gartner stresses four key components of SOAR:

Orchestration — How different technologies - both security-specific and non-security-specific are integrated to work together.

Automation — How to make machines do task-oriented "human work".

Incident Management and Collaboration — End-to-end management of an incident by people

Dashboards and Reporting — Visualizations and capabilities for collecting and reporting on metrics and other information

SOAR vs SAO: What's the Difference?

SOAR and SAO Platforms have both emerged recently, and are oftentimes confused when it comes to their purpose.

Before Gartner coined "SOAR", the industry was already familiar with the term "SAO"- short for Security Automation and Orchestration Platform.

While both are familiar in their vision when it comes to emphasizing a move away from a silo'ed approach to security operations and towards a more consolidated and integrated model, there are significant differences. What's absent from SAO Platforms are items such as threat intelligence and incident response-specific functionality; i.e. case management. Essentially, SAO is an automation engine which is completely reliant on integrations with other technologies to be of any use. **SOAR combines SAO with threat intelligence and incident response capabilities to offer a smarter and more complete solution for security teams.**

An evolution in security operations being driven by the vast amounts of data that must be processed is underway, and there's a need for the following:

- **Centralization and Normalization of Internal and External Security Data:** This will lead to better analytics for better decision-making. Decisions are informed by intelligence.
- **Automation and Workflows:** For cybersecurity teams to simultaneously address the pressures of attacks and maximize the efficiency of limited staff, they must have repeatable documented automation and workflows.

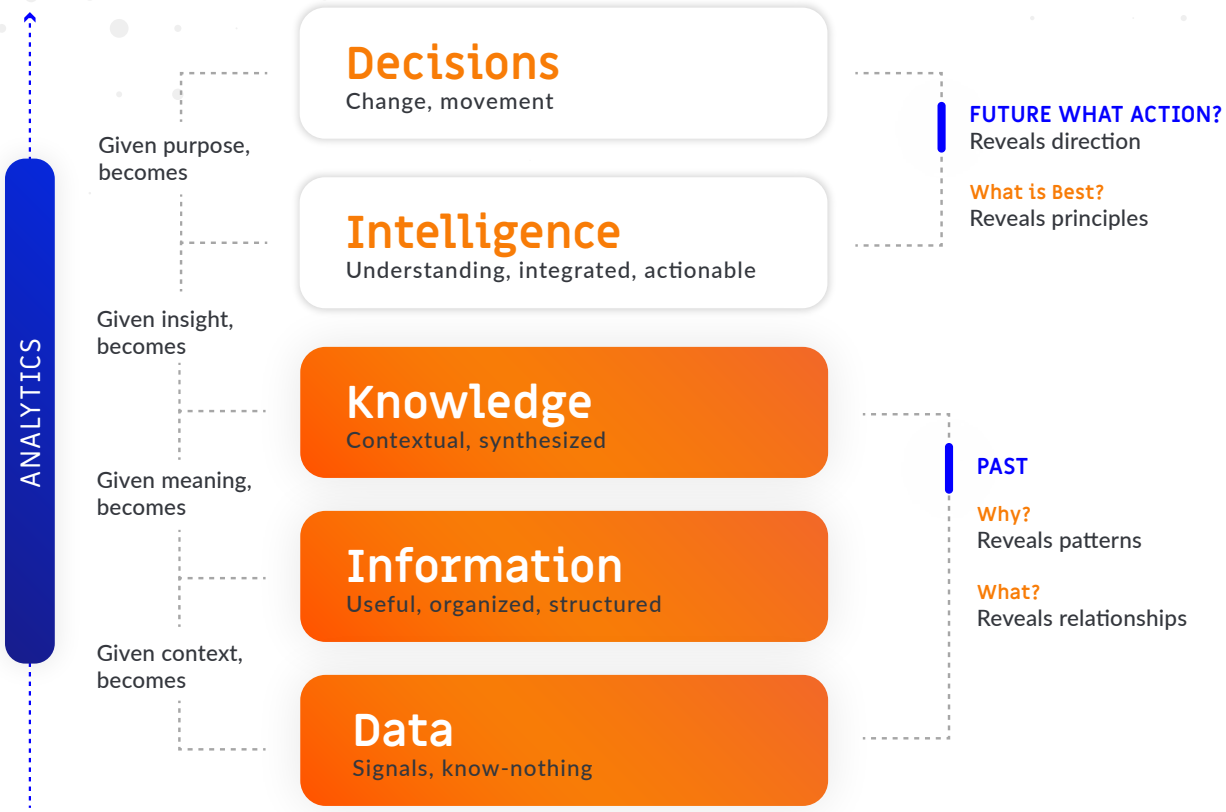
The great thing about SOAR is that, if deployed correctly, it gives your organization the platform required to implement an intelligence-driven security strategy. Let's break down exactly what this intelligence-driven security strategy is all about.

Intelligence Deconstructed

First, let's talk once again about what threat intelligence (TI) really is. The hype machine has put TI in a box. It's largely misunderstood as merely referring to Indicators of Compromise (IOCs) delivered via data feeds. These feeds are typically comprised of context-sparse information or data and have their place to support defensive operations, but they are far from a complete and accurate picture of what TI can be. Most IOC feeds are better characterized as information, not intelligence.

Intelligence is not raw data and it is not merely information - it is knowledge of threats you can use to inform decisions and possibly allows prediction of future circumstances or events.

[4] CSO Magazine, Goodbye SIEM, Hello SOAPA, Jon Oltsik, May 2016



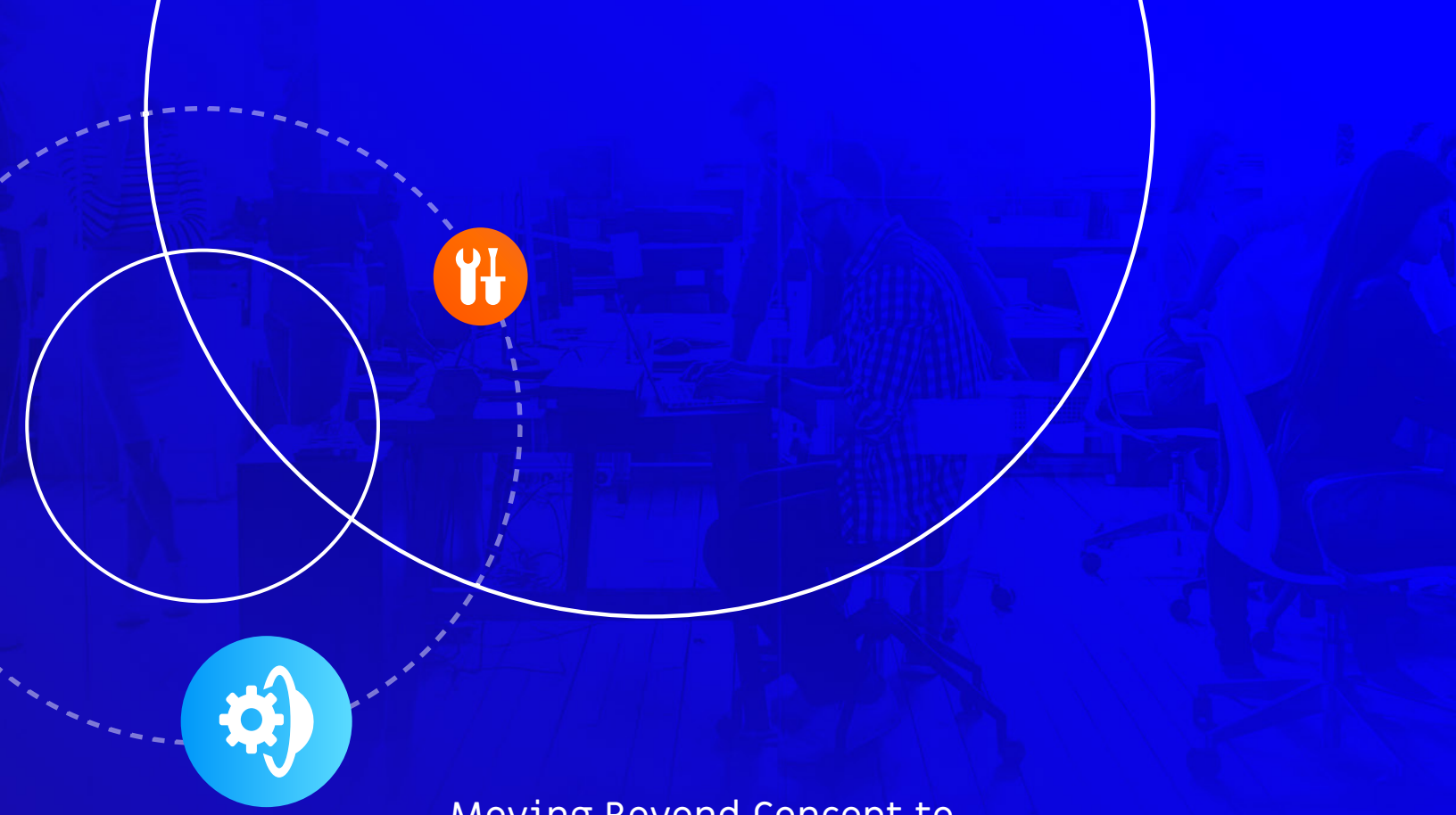
Intelligence Empowers Smarter Operations: Start a Feedback Loop between Intel & Ops

Intelligence does not exist for its own sake, intelligence, including threat intelligence, specifically exists to inform decisions for security operations, tactics, and strategy.

This relationship is not a one-way street. Intelligence and operations as functions of the security team should be cyclical and symbiotic. Intelligence informs decisions for operations resulting in actions being taken based on those decisions. Those actions (such as cleanups, further investigations, or other mitigations) will beget data and information in the form of artifacts such as lists of targeted or affected assets, identified malware, network-based IOC's, newly observed attack patterns, etc. These artifacts can be refined into intelligence that can thus inform decisions for future operations.

While some organizations do not have a formally defined intelligence function on their team, the concept of using what you know about the threat-space to inform your operations exists in all organizations. Regardless of whether an explicitly named threat intelligence analyst employee is on staff, the relationship between intelligence and operations is fundamental and present in all security teams.

Threat intelligence may be the catalyst for taking an action or starting a process and informing 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**.



Moving Beyond Concept to SOAR in Practice

Implementing an intelligence-driven defense isn't without its challenges. Fragmentation of information, people, processes, and technologies is a significant hurdle. At ThreatConnect, our objective has always been to help security teams get the most value out of that intelligence by enabling cross-team coordination and workflows.

While the industry analysts are defining the architectural concept of SOAR, we see a need for a platform to bring it altogether to automate, orchestrate, and break down fragmentation for seamless coordination. A centralized platform that enables the refinement of relevant data from cases, response engagements, threat investigations, shared communities, and external vendors into intelligence suitable for decision making by any analyst, and also leverage that newly created intelligence to inform decisions across the security team.

It's a practical application of SOAR that we'll discuss in the following chapters.

Chapter 3

Intelligence-Driven Orchestration

If there is so much value to be gained with implementing an intelligence-driven defense, why isn't everybody doing it? There are some significant challenges for organizations of all sizes to do it right. Fundamentally, fragmentation is the root of these challenges. This fragmentation is caused by varying levels of maturity across the different functions surrounding security that grew up separately and are now trying to work together without any friction.

Fragmentation is a natural occurrence in any organizational structure. It happens whenever groups get too big or processes get too complex. At ThreatConnect, we set out to help organizations implement an intelligence-driven defense by focusing on addressing the fragmentation problem across information, people, technology, and process. Let's discuss how you can address each with a SOAR solution:

Information: For relevant information to be refined into usable intelligence, it must be available to be correlated, enriched, and contextualized. You must remove the silos segmenting relevant data by creating a common source of record for it. A SOAR platform does this by aggregating internal and external information so that it can be refined into intelligence usable for informing decisions. Internally sourced information, details of an IR investigation, notable events from the SOC, or even curated intelligence from an in-house team is often the most valuable part of the feedback loop we enable.

People: Like data, the various functional teams within your security organization (IR, SOC, Intel, Risk, Executives, etc.) also need the silos taken down from around them. They need access to relevant information from other teams, and intel sharing communities outside your organization. They also need to be able to work seamlessly together with a dynamic workflow. A SOAR platform, like ThreatConnect, facilitates this by allowing teams to provide tips and tasks to each other, create and funnel intelligence to relevant functional organizations, and create reports for executive decision makers based on threats to the organization. It may also facilitate or automate sharing information with partners in your supply chain or intelligence-sharing communities.

Technology: Most organizations today have a very heterogeneous and disconnected set of point defensive technologies. For most, coordinating action across them means coordinating tickets between IT and various facets of the security team. ThreatConnect enables organizations to coordinate intelligence-driven action and automation across our ever-growing library of applications and integrations.

Process: Once you have removed the silos between information, people, and technology, a SOAR platform enables you to streamline your processes with playbooks that leverage both internal and external intelligence to inform action for your teams and your technology as well as learn from past experiences.

Many products perform some level of security automation and orchestration. However, they only incorporate intelligence to trigger certain workflows or to be used as enrichment for some context, and certainly do not enable adaption for future runs of their playbooks or the creation of new intelligence as one of the outputs of the workflow itself. This sets them up for struggles in the previously mentioned focus areas: information, people, technology, and process. Some TIPs allow for aggregation of external data feeds, creation of internal intelligence, and even have many connectors to defensive products for automation of detection and prevention with operational threat intelligence. This is a great first step, however organizations need a solution that focuses on getting the most value out of that intelligence by enabling cross-team coordination and orchestrating their workflows By creating one platform that includes threat intelligence, orchestration, automation, and response together, you create a holistic 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 memorize all of that information, you can strategically look at your processes to determine how to improve.

Orchestrate with more confidence

Native sense-making analytics on external threat intelligence allow for more accurate, less false positive prone alerting, blocking, and quarantine actions. It's not as simple as being able to ingest lots of threat intel feeds or take action from a shared Indicator of Compromise. Its making sense of them at scale with adaptable scoring and contextualization to know what action to take, if any, based off of it.

Organic intelligence creation from security operations and response

Your own team and data is the best source of intelligence you will ever have. Capture the insights, artifacts, and sightings from operations and response engagements that can be immediately refined into intelligence in the form of new IOCs, adversary tactics and techniques, and knowledge of gaps in your security.

Adjust processes automatically as information and context changes

Intelligence-driven orchestration is data first, while security orchestration is action first. When your orchestration capabilities are fully adaptable to new threat capabilities, tactics, techniques, and infrastructure as its available from structured threat intelligence, your processes automatically adjust as the threat landscape changes.

Chapter 4

Decreasing Time to Response and Remediation with SOAR

With increasing volumes of aggressive threats, where rapid response is measured in seconds, organizations need to reduce the time to respond. This is a core focus of SOAR solutions today. Automation and orchestration can help by delegating certain tasks to machines and removing unnecessary human roadblocks. When paired with real-time team collaboration functionality, your team will be able to reduce the response time, including containment and remediation, to seconds -- not days or weeks.

Using a SOAR platform can help incident response teams coordinate multiple streams of activity handled by different people, all with different roles and expertise, to support a comprehensive response to a security incident.

Working out of one single platform will enable teams to more effectively:

- **Perform Consistent and Collaborative Incident Response:** Using playbooks, you can organize, record, and structure these incident response processes, moving from a static incident response plan to a dynamic workflow-tracking platform.Through collaboration, security teams can then coordinate activities across team members. Incidents can be managed and tracked across your organization. While automating the configuration of compensating controls and threat countermeasure investigation through consistent best practice.

- **Speed Containment:** Leveraging integrations and connectors with endpoint and account security products, SOARs can speed containment of malware infections in the network.

- **Enrich Investigative Cases:** Incident responders can also use SOAR platforms to enrich investigative cases with additional data from sources like past or related incidents. Taking it one step further, SOARs have the ability to apply this intelligence and use advanced analytics to identify related cases, recommended playbooks, and apply best practices from within the platform to inform your response. SOAR platforms can also close an alert based on certain conditions, meaning it never develops into an incident or burdens incident response teams with false positives or duplicate alerts requiring human intervention.

- **Document Activity for Governance, Risk, and Compliance:** When activities that spans across security teams are controlled and documented in one platform, it makes departmental reporting much more streamlined. Most SOAR platforms allow you to create, display, and export specific metrics and information to support items requested by your Governance, Risk, and Compliance (GRC) team. This includes basic proof that you do have an incident response plan in place and that you do have methodology for alert analysis, as well as specific metrics that show operational efficacy and capability gaps that can help justify needed technology, personnel, or training.

SOAR in Practice: Phishing Email Submission & Remediation

SOAR can also automate or semi-automate the processing of suspected phishing emails eliminating much of the manual and meticulous labor involved in investigating them. Using playbooks, security teams can automate much of the validation and investigation process to identify phishing emails that have evaded spam filters and other first line defenses, further they can take defensive action to terminate malicious emails so that they're automatically deleted from a user's inbox, extract network command and control indicators of compromise from any attached malware for further detection or blocking, and create suggested host based detection signatures for review, all with limited involvement by a security analyst.

Prior to the implementation of SOAR, this process was very tedious. Reputation checks and further analysis needed to be manually initiated across several systems, slowing confirmation and action. Now, orchestration provides enough information by automating data collection into a single place to either help the analyst to review and decide if the email is suspicious, or, if enough confidence is gathered, to take immediate automated action.

As an example of what steps of the subsequent workflow may be automated, if the investigation confirms an incident, it would initiate the playbook to respond to the incident. Integration with the email system, sandbox and ticket system would provide an automated process to look at the email system to find all messages with a suspicious link or attachment. Then, the system would quarantine email that was sent to other users, while waiting for the decision of deleting or allowing access to quarantined email.

In addition to reducing analyst workload, documenting these processes leads to a greater level of knowledge management and a better understanding of the adversary space. You're also able to continuously monitor efficacy of those workflows and processes and continue to improve. All good news!

Chapter 5

Achieving a Smarter SOAR

As we think about SOAR and how it's been defined and implemented so far, you can think of it as operating very much like an enabler, or a hub for decision making. It provides a centralized location that accepts numerous inputs which drive specific outputs. If you do not have a system that uses existing internal and external intelligence on threats and your operations as it orchestrates as part of all of its processes, you have an automation machine which can support various "if this,then that" type scenarios, but it's not necessarily improving efficiencies or efficacy after those experienced after it initial implementation. With the addition of engine that interprets and creates intelligence, the SOAR becomes smarter which makes the organization faster and stronger.

To see this theory in practice, let's apply it to vulnerability management. At any given time, an organization may have thousands of vulnerabilities across all of their software and devices. The key to vulnerability management is prioritizing those vulnerabilities based on risk and impact, and driving a remediation strategy that makes sense for your particular organization. A SOAR enables you to:

Collect information from your vulnerability scanner

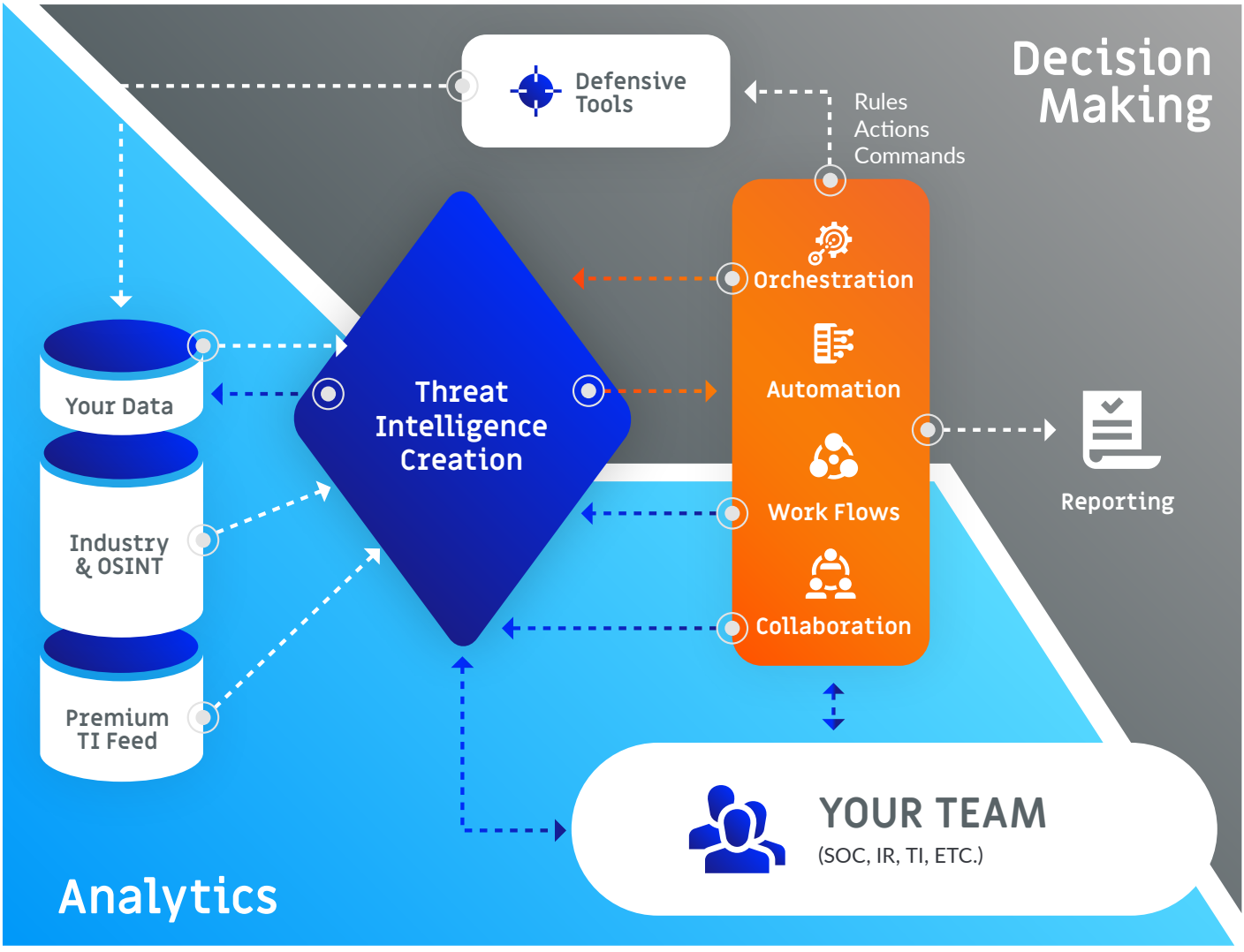
Perform a series of checks with internally derived intelligence and externally sourced vulnerability and threat intelligence to determine risk and priority:

1. Is there is known exploit code against the vulnerability?
2. Is the vulnerability being exploited "in the wild"?
3. Is the exploit being used by a threat in the organization's threatspace? What are those threats' capabilities and intent?
4. Has the organization been targeted by any threats using the exploit in the past?
5. What priority is already assigned to the vulnerable assets?
6. What controls are in place already that may mitigate the risk of the vulnerability?

Automate alerts for targeted mitigation techniques against the most critical vulnerabilities.

It may go without saying, but the aspect that makes this process possible is the capability to bring together multiple reliable sources of information from external sources on state of vulnerabilities and various threat groups, but also an internal understanding of what threats the organization has faced in the past, what they were after, and what they are capable of. That internal knowledge is not simply queried from a separate database, it must be intentionally created with context in the organization so that it is available to inform future decision making. With the right solution in place, this all takes place in a natural and cyclical fashion.

With analyst firms like Forrester, ESG, and Gartner laying the groundwork for technologies that cross solutions, the need for a platform to bring it altogether, make sense of the complexity, and provide security teams with a single place to get everything they need to make decisions is becoming more apparent.



This illustrates how intelligence flows through every aspect of your security program; that your entire team is connected to the intelligence, each other, and the tools; and that a feedback loop from the people and tools is built-in to improve the intel.

Chapter 6

Enter ThreatConnect – Fusing Intelligence, Automation, Orchestration, and Response in One Platform

As we alluded to earlier, it's been our philosophy since our founding that we would incorporate intelligence in all aspects of security operations including orchestration and workflow, as functionality within the ThreatConnect platform. ThreatConnect is security orchestration, automation, reporting, analytics, and more that facilitates the creation of insights to not only speed and scale operational processes but enables better decision making. An intelligence-led defense benefits organizations by enhancing detection, shortening response and remediation engagements, and allowing more predictive and proactive strategic decision making.

Flexibility and Extensibility as Core Principles

Leveraging multiple SDKs and an App Framework for community development, the ThreatConnect Platform today incorporates more than 100 intelligence sources and more than 350 enrichment, processing, and integration apps that can be used to leverage intelligence and drive operations across any process in the security team's technology stack.

Our focus is not simply to take feeds of data from the internet and fire hose them into our customers' networks, but rather to refine data a customer has from any relevant source into an intelligence service for various security teams. Each of these services enables the business to integrate data, analyze it to add context and determine relevance, provide insights and recommendations, or most powerfully - to take immediate action when appropriate.

A true platform should allow you to grow the technology to suit the needs of your people and processes. The alternative is a software tool that forces you to adopt its processes and methodology, which may or may not suit the needs of your team. Our SDKs and App Framework have enabled our customers to grow far beyond our hundreds of supported out-of-the-box applications to ensure that ThreatConnect works the way they want.

Of course, these user-built apps and Playbooks shouldn't serve only the individual who built them. If someone solves a difficult security problem, we believe that the entire infosec community should benefit. To that end, we've provided some mechanisms for sharing. One is a GitHub repository. The other is a Slack channel in our customers-only Slack workspace[5]. Both resources allow ThreatConnect users and engineers to contribute and collaborate on apps and Playbooks built using our Platform.

5 For an invitation, please contact your Customer Success representative.

Using Analytics to Understand Platform and Team Performance

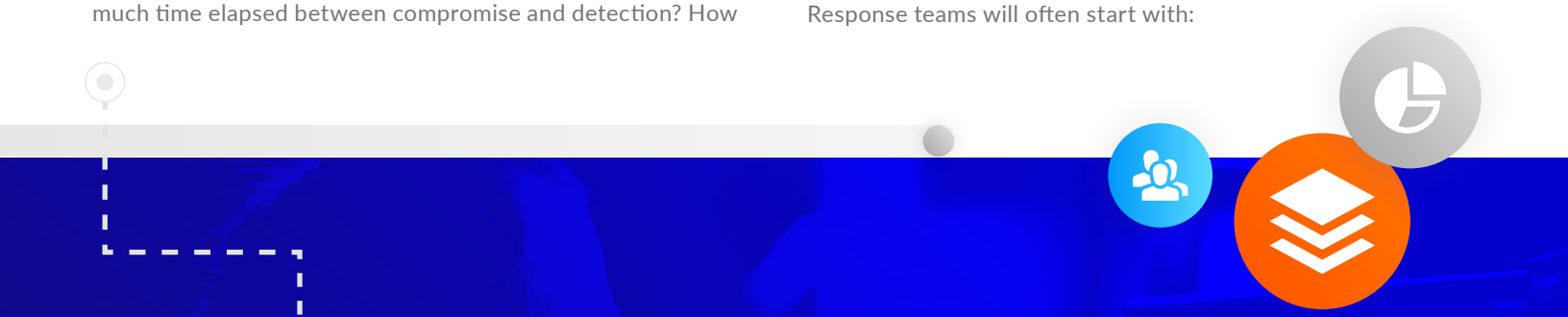
Orchestration turns automation into a force multiplier. Those enrichments that you got by pushing that button (or that happened behind the scenes while you slept) can now drive SOC or incident response investigations faster and more effectively. Artifacts and insights gained from those investigations yield new intelligence, and the cycle can continue to feed itself. The entirety of that lifecycle can be captured, recorded, and measured so that you prioritize risk and drive team and process improvements.

Today, with our range of integrations and automation capabilities, customers are using ThreatConnect to facilitate use cases as broad as intelligence-led patch management, phishing email triage, infected host containment, detection and alert enrichment in the SIEM, and intelligence report creation and sharing, to just highlight a few. But how to optimize?

One of the most basic ways to optimize is around time: how much time elapsed between compromise and detection? How much time has elapsed between detection and remediation? Which processes or tasks are taking up the most time, and where can efficiencies be gained?

To start looking those time-based efficiency optimizations, the first step is to baseline and record the key milestones you want to measure. This can be done using ThreatConnect's Metrics capability. Once you've started recording the time between your key milestones, you can analyze those metrics in aggregate on any number of custom dashboards.

Once you've baselined, you can start looking for ways to improve fairly easily because the data has already been collected and made available for querying.Your next step is to simply start with a hypothesis: for example, dwell time on phishing investigations undertaken by Alice is lower than dwell time on phishing investigations undertaken by Bob, **and then test**. There are several basic metrics that SOCs and Incident Response teams will often start with:



- **Dwell time by affected system.** This can be calculated as a **Mean Time to Detect** (MTTD) for all incidents. Hopefully, your infrastructure has adequate support for breach detection. Even so, there will likely be differences in the time it takes to detect intrusions attempts based on what's been targeted, techniques, tradecraft and capabilities used by the adversary. Understanding where these "time gaps" are can you help you prioritize your efforts and invest in closing gaps in your detection.
- **Time from Alert to Triage.** Similar to "Dwell Time" above, but instead measuring the mean time it takes from detection or alert to be triggered to it be validated and initial response to begin.
- **Time to Mitigation/Containment.** How long it took for the bad thing to actually be brought under control. This is also known as Mean Time to Respond (MTTR).
- **Time to Close.** That is, from the case being opened to it being closed.

More than just tracking the time between certain milestones in a case or response effort, performance analytics need to focus on both the specific values that matter to you as well as the knobs you're able to turn. It might be worthwhile considering tracking the following values to optimize your performance:

Time to collect artifacts/evidence broken down by source or origin.

If you understand where your information is coming from and how long it takes to get to you, you can work to optimize your tools. E.g. are gathering event logs from endpoints a bottleneck?

New intelligence created from operational or incident investigations.

A key aspect of the intel cycle involves generating new intel from your boots on the ground. Understanding how much new insight is gained from those activities can help inform whether processes or policies need changing.

False positive ratio on Alerts.

Are wild goose chases more common on certain teams than others? With certain types of incidents? These time wasters can lead to loss of morale and less effort devoted to true threats.

Most Active Playbooks.

This is just good situational awareness. Where are my automations kicking off and providing value? Is there any anomalous activity, e.g. broken or overly active Playbooks?

Team Workload and efficiency.

Understanding who is working on what (and how effectively) can help you uncover bottlenecks on your team. Are we hitting our due dates and SLAs? Is anyone overworked? Are we understaffed?

Of course, this is just a sampling. We encourage you to understand where your own teams, tools, and processes can go off the rails so you can start measuring and improving.

With many of these measurements, you're also introduced to the ability to understand how all of your investments are performing. By investments, we specifically mean your organization's people, data, process, and technology. How efficient are the people you hired, when using the technology and data you've acquired, to carry out the desired processes you've identified?

ThreatConnect provides built in return-on-investment calculators and activity management capabilities for various security personnel's key workflows, as all are either consuming, creating, or processing intelligence. Build these capabilities on metrics that are applicable to your organization to have a clear view into cost savings since implementing intelligence-driven orchestration.

Your Adversaries are Adaptive. Your Processes Must be too.

- **Learn from your failures,** and from your successes. The system should recommend human actions and playbooks based on likely adversary techniques being leveraged, context from past incidents or sightings, and measures of efficacy from previous actions.
- **Adapt together.** Any insights gleaned as you build, measure, and tune your processes can be shared with your peers. Come together to model the threats, identify the effective workflows and playbooks, and help us all improve. Adversaries aren't used to fighting all of us at once.
- **Tailor prioritization to your organization.** Automatically curate your own scoring for IOC's, threat groups, campaigns, and malware families based on relevance to your organization. What techniques or motives do you care about? What are peers in your industry seeing? Our ThreatAssess scoring and CAL analytics help aggregate and normalize all of that information so you know how to treat a piece of intelligence.
- **Breaking the IOC barrier.** Playbooks use inputs from intelligence on adversary techniques, malware families, and vulnerabilities exploited, not just IOC's. This means that your defensive posture takes into account what the adversary can do holistically, not just the disposable tools they're using to do it.
- **Understand your enemy, understand yourself.** Modeling and analyzing adversary capability and intent can help you drive decision making. It can help you prioritize **your human and technological** investments, and better understand risk.
- **Accelerate along the maturity curve.** Correlate ongoing cases to past incidents to drive quicker, more effective response actions. Find your formula for success and easily replicate it across teams regardless of geographical, organizational, or expertise boundaries.
- **Optimize your investments.** Measure efficacy of your intelligence, detection, and mitigation spending versus your newly-understood threat space. Where are your biggest risks, how are your investments performing, and are you mitigating as much risk per dollar as you can?

Capabilities for Scale and Efficiency

How do we enable these use cases? ThreatConnect's playbooks capability allows a sequence of tasks, arranged as a process, to be configured as a playbook, executed to incorporate automated analytics or human workflows, and measured to support continuous improvement. The processes, playbooks, dashboards, and apps can be built, shared, and utilized by anyone in the ThreatConnect community, or organizations can create private iterations to only be shared within their own organization.

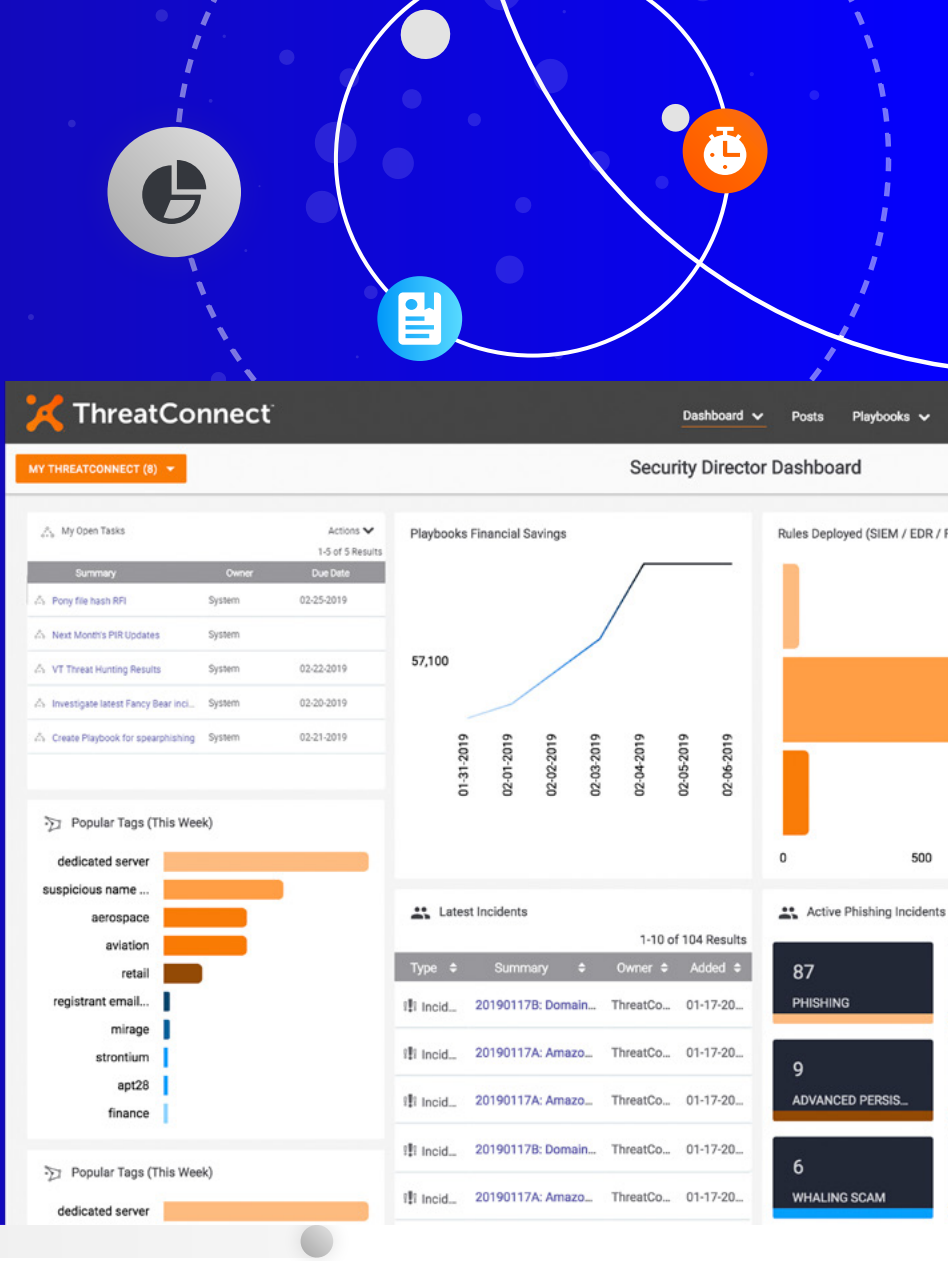
Our Playbooks and other automation capabilities enable the refinement of data into intelligence suitable for decision making, and also leverage that newly created intelligence to inform decisions across the security team.

Tying critical security operations to orchestration can be pretty nerve-racking initially. Having real-time insight into which Playbooks have run, are being run, and what's queued up is critical to understanding that things are working as intended. ThreatConnect provides an Activity Dashboard which provides users with:

- ✓ CPU Metrics
- ✓ Memory Utilization Metrics
- ✓ Counts of Top Playbooks Running
- ✓ Duration of Playbooks Running
- ✓ Most Popular Executed Apps
- ✓ Playbooks Currently Running

This Real-time Playbooks Activity Monitoring gives users:

- ✓ An instant status check to ensure things are running smoothly
- ✓ Improved visibility and control over actively running Playbooks; making troubleshooting problematic Playbooks easier; and actively managing them much simpler
- ✓ Quick checks for reporting on metrics like Top Executed Playbooks and Total Playbooks Executed



Of course, knowing what's happening is only half the battle. If your volume of activity suggest a need to scale, ThreatConnect customers can roll out additional Playbook Servers that allow them to easily and effectively scale ThreatConnect to handle thousands of Playbook executions per day, while prioritizing what's important. Each Server is its own machine, and once the Playbook Server is deployed, customers can set up multiple Playbook Workers to handle and monitor concurrent Playbook executions.

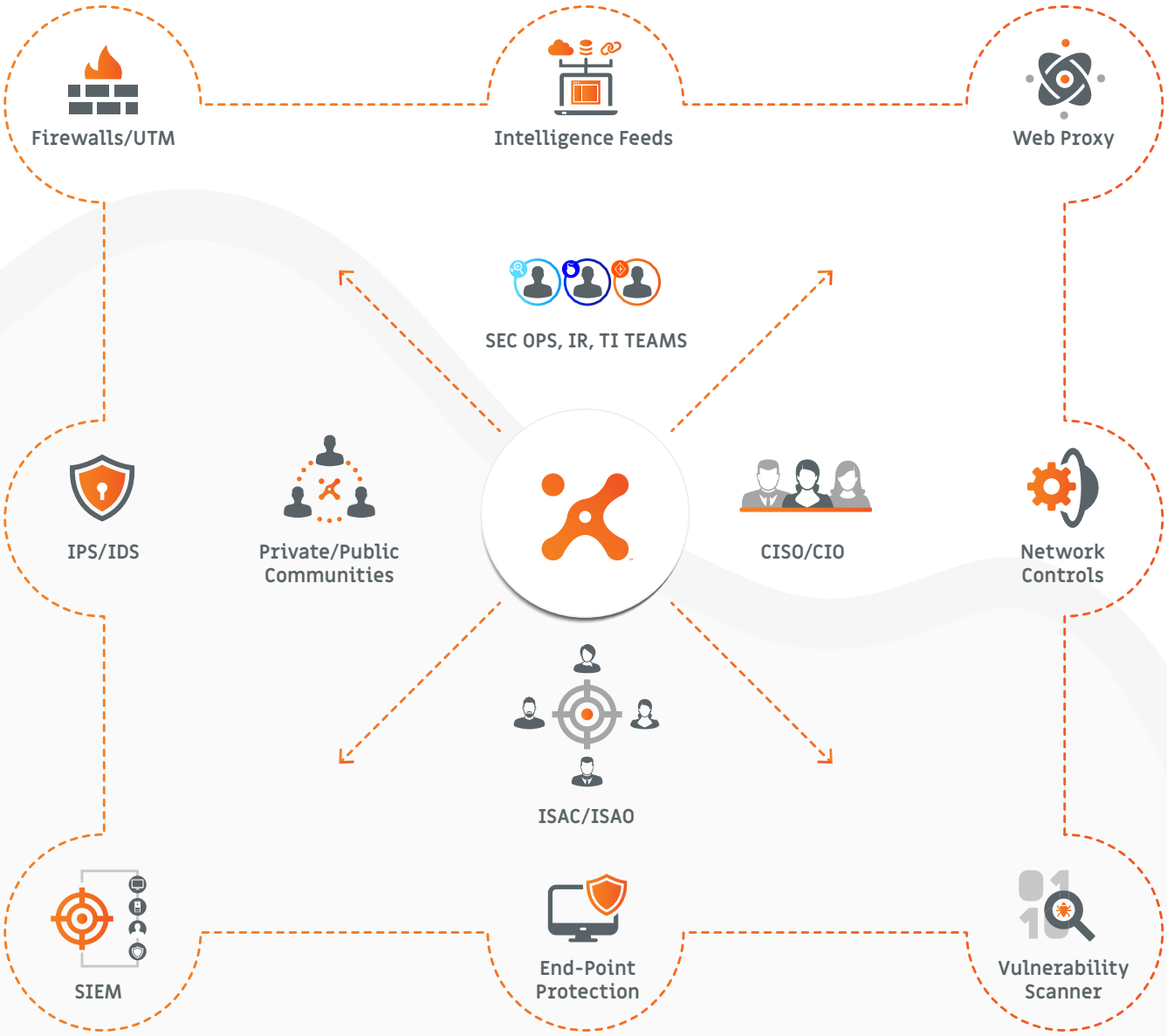
Not all Playbooks are created equal. Some Playbooks perform basic enrichments and send routine notifications, while others hunt for mission critical intel and loop in the entire security team about potential major incidents.

Users can assign a High/Medium/Low Priority setting to each Playbook. Playbooks deemed "High Priority" essentially jump the queue when an action triggers it. If additional resiliency is required, users can allocate Private Servers to an Organization for the highest priority Playbooks to get ahead of the queue. You can also enable high availability (HA) by deploying multiple Playbook Servers. If at any point a Playbook Server crashes, the remaining servers take over responsibilities. There is no single point of failure!

We all want to make sure the important things are getting done first. We run through prioritization exercises daily, and it becomes even more critical when dealing with security operations. The ability to set Playbooks at different priorities enables the most important things to get done first.

Establish a More Intelligent Security Program with ThreatConnect

The ThreatConnect Platform contains all the functionality you need to drive informed decision-making based on the power of your organization's threat intelligence. For the first time, you can orchestrate your security processes, analyze your data, and proactively hunt threats in one central place. We provide not only the ability to orchestrate your security functions, but also the confidence that you are basing your tasks and decisions on vetted, relevant threat intelligence.



Chapter 7

Checklist for a Complete SOAR Solution

With SOAR concepts gaining steam, we've put together a checklist of what to look for in a complete SOAR solution.

Feature	Details
Management and Sharing of Intelligence	Look for a solution that provides the following: ✓ The ability to heavily leverage a REST API and represent data in a way that can be shared among multiple teams and tools ✓ Relationships with Information Sharing and Analysis Centers (ISACs) to aid in collaboration with your respective industry. ✓ Secure flexibility around who can see what information, for example using the TLP protocol ✓ STIX/TAXII support ✓ Integrations with multiple OSINT and paid intelligence providers
Team Collaboration	Collaboration features that are a must include: ✓ Role-based access control ✓ Team-based notifications and tasking ✓ Commenting and markdown support ✓ Escalation management ✓ Integrations with communication tools like Slack
Document & Artifact Storage	✓ Document indexing, for example using ElasticSearch ✓ Extensible storage to meet growing needs ✓ The ability to link documents and artifacts to relevant intelligence or other information
Investigative Case Management	Cybersecurity investigations are complex with huge amounts of digital evidence. Look for features that reduce complexity, foster collaboration, and speed up investigatory timelines. Specific capabilities a SOAR solution should include are: ✓ Reconstructed timelines of actions taken and decisions made to provide up-to-date progress reports and to support post-incident reviews ✓ Ability to assign tasks to specific team members or groups of users to allow collaboration and management ✓ Ensure consistency and repeatability of investigations through the use of customizable workflow templates ✓ Reduction in false positives and dwell time by integrating threat intelligence directly in case reports ✓ Quickly link cases and investigations to historical or other ongoing cases

Checklist for a Complete SOAR Solution Continued

Feature	Details
Automated Phishing Handling	Eliminate the burden of manually analyzing and remediating the growing volume of phishing emails with feature capabilities that support the following: ✓ The automated collection of potentially malicious emails from end users ✓ Automated analysis of email with available threat intelligence ✓ Integration with the email system, sandbox, and ticketing systems to provide process for finding all emails with suspicious link or attachments to enable quarantining any email that was sent to other users while waiting for decision of deleting or allowing access
Feedback Loop	Leverage the feedback loop to enable faster, more accurate actions as you anticipate and thwart a threat actor's next move. Focus on solutions that: ✓ Reduce false positives and determine level of risk and prioritization based on historical data ✓ Help you derive meaningful threat intelligence from operational data
Robust Integration Capabilities	Scale integrations across security tools and processes with solutions that offer: ✓ Flexible playbooks to support integration workflows ✓ REST API to allow flexibility in integration development ✓ Mature, bidirectional SIEM integrations to help with false positive issues ✓ Integration can be built directly in a playbook without the need for custom development or code
Automation and Orchestration	✓ No limits on executions ✓ Ability to prioritize mission-critical playbooks ✓ Additional servers can be rolled out to meet demand for resiliency and performance ✓ Performance can be easily monitored from a central location
Collective Analytics Layer	✓ "Ground truth" telemetry from other analysts around the globe is provided anonymously and automatically.
Dashboards	There's no such thing as a one-size-fits-all dashboard, so ensure that the solution allows you to: ✓ Create multiple, custom dashboards tailored to different teams ✓ Query the data using a variety of parameters to ensure the right information is bubbled up ✓ Use your own, custom metrics to measure the key performance indicators you care about
Data Model	✓ Flexible data model that supports bespoke indicators ✓ Admins can create their own attributes to ensure the data they care about is properly modelled and memorialized ✓ Associations can be formed between different objects, for example between threat actors and their capabilities

Request A Demo

Call **1.800.965.2708** or visit **threatconnect.com/request-a-demo**

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 www.ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708