WHITE PAPER

SIEM + THREAT INTELLIGENCE:

Quickly Identify the Threats that Matter to You

ThreatConnect™

ThreatConnect.com

Contents

SIEM + Threat Intelligence: Quickly Identify the Threats that Matter to You

Think before you dump unrefined threat intelligence into your SIEM and chase false positives. Learn how a threat intelligence platform can help you take control of the chaos and make sense of all that data.

Introduction

Security Information and Event Management (SIEM) systems are among the most versatile tools available for empowering your security organization. You might even say that they're the one security tool you can't live without. And, for many applications, you're right.

Yet, despite their many benefits, SIEMs are only as useful as the information you put in them. Inundate them with un-validated, raw threat data and the outcome is not pretty. In the face of hundreds, if not thousands of false positives, security teams must wade through the "noise" and try to piece together what's going on, wasting valuable time and resources.

SIEMs are a powerful tool for collecting and correlating event data and have a well-deserved place within your security infrastructure for centralized log management. But to truly shine they need to be supported by other technologies in your arsenal – most notably, a threat intelligence platform.

This paper will examine how security organizations can enhance their SIEM with a threat intelligence platform to take control of the chaos, gain a fuller understanding of threats, eliminate false positives, and form a proactive, intelligence-driven defense.

All About the SIEM

What is a SIEM designed to do?

SIEMs were designed to address the growing challenge that security organizations face when trying to spot trends and patterns produced in multiple locations across the enterprise. By collecting and analyzing security events from a wide variety of event and contextual data sources, SIEMs support threat detection and security incident response.

Benefits

Most enterprises use their SIEMs to collect log data and correlate security events across multiple systems (intrusion detection devices, firewalls, etc.), their internal security logs, and event data, and as such, SIEMs provide a number of benefits.

Centralized Analysis and Reporting

By bringing together log data from multiple disparate sources (including those that lack built-in detection capabilities), SIEMs provide centralized analysis and reporting of an organization's security events to identify malicious activity.

Attack Detection

Using this analysis, SIEMs enable security teams to detect attacks that otherwise would have gone undetected. Some SIEMs also deliver the capability to avert attacks that may still be in progress by communicating with other security controls, such as firewalls, directing them to change their configurations to block the attack.

Compliance Reporting

Because of their centralized logging capabilities, many organizations use SIEMs to streamline their compliance reporting efforts. By transferring log data from a host system, a SIEM aggregates all logged security events – helping an organization save time and resources in meeting security compliance requirements.

Speedier Incident Handling

By providing a single, centralized interface for aggregating and viewing event data, SIEMs increase the efficiency of incident response teams, speed containment of malicious activity, and limit any potential damage.

Limitations

SIEMs are a useful starting point for correlating internal data with ingested threat data feeds and beginning a process of automated alerts and blocking at the endpoint. However, as attackers continue to innovate and enterprises seek to gain more insight into the nature of threats, their intent, techniques, and capability to inflict damage, the limitations of SIEMs start to emerge.

Overwhelmed with "sensor fatigue" amid the increased noise and complexity of systems feeding into the SIEM, security operations teams are struggling to gain more value out of their SIEM deployments, for a number of reasons:

Too Much Raw "Noise"

A significant difficulty with SIEMs is that the data fed into them requires a good deal of filtering. Overfeed your SIEM with volumes of threat data and you risk creating an abundance of false positives, or increased security "noise," that results in unnecessary triage, and overwhelmed, unproductive security operations and incident response (IR) teams. Furthermore, when you begin incorporating invalidated, raw threat feeds into your SIEM, it can't distinguish between good and bad intel. If your SIEM can't, how can you?

Lack of Analysis Range

While SIEMs can correlate events and apply analytics to highlight suspicious or malicious activity, they lack the ability to focus on adversary intent or highlight what an intruder may do next based on past observed behavior.

SIEMs Only React to Identified Threats

SIEMs are typically designed to identify and flag threats that have already been identified, which becomes problematic when you're trying to stay one step ahead of malicious actors. If a persistent attacker deploys new techniques or tools to counteract your defenses, the SIEM, by itself, is unable to detect it because it's unfamiliar with this new method.

"By collecting and analyzing security events from a wide variety of event and contextual data sources, SIEMs support threat detection and security incident response."

The Benefits of Integrating Threat Intelligence into your SIEM?

The SANS Institute[1] defines threat intelligence (TI) as **"the set of data collected, assessed, and applied regarding security threats, threat actors, exploits, malware, vulnerabilities, and compromise indicators."**

TI gives security teams the ability to "recognize and act upon indicators of attack and compromise scenarios in a timely manner. While bits of information about attacks abound, threat intelligence recognizes indicators of attacks as they progress, in essence putting these pieces together with shared knowledge about attack methods and processes."

Pair your SIEM with threat intelligence and your organization has the power to scale and outwit evolving high-volume, high-impact threats in an agile and responsive way. Without that marriage, you're literally running blind and fighting chaos.

Many organizations make the mistake of thinking that SIEMs are a panacea for their security analysis woes, when in fact they are just a starting point. If you're throwing a bunch of unvetted, threat data feeds into your SIEM and hoping this is a sufficient "check the box" solution for threat intelligence to support detection, think again.

SIEMs aren't designed to handle the multiple formats, often unstructured, of threat intelligence that originate from numerous, disparate sources that are required for analysis. Overfed with unvalidated and uncorroborated data, which essentially clogs organizations' security arteries with garbage information, can quickly malnourish your SIEM and overwhelm your scarce security analyst resources.

Similarly, observing threats in your SIEM is like looking at the world through a microscope; the view is too constrained. Threat data, in all its forms – structured and unstructured – needs to be synthesized and looked at from a more "global" perspective. A SIEM will be great at illuminating potential security issues when refined threat intelligence is used for alerting within it. However, it isn't meant to provide you a deeper, holistic understanding of the threat and what they may be doing next. Only when you stop looking at threats at a microscopic level, on an alert-by-alert basis, can you begin to form a complete picture of a threat's capabilities (what they can do against you and how they might do it), infrastructure (where they're going to come from), motives (why they're doing what they're doing), and their goals and resources.

Make the most of your SIEM with TI

Security teams seeking to work smarter, take control of the data, build the bigger picture, and act as united force need a different set of capabilities to complement the SIEM.

This is where threat intelligence comes into play.

Tie Your SIEM to a Threat Intelligence Platform

Threat intelligence platforms (TIP) are a force multiplier that can help organizations overcome the laborintensive process of threat analysis that often exceeds the capacity of enterprise organizations. A TIP is a dynamic system for automatically ingesting threat data from many different sources, then correlating that data, enriching it, and seamlessly exporting it to other parts of your infrastructure to remediate threats.

With a TIP, you can aggregate and rationalize the threat data and create a "signal" to what would otherwise be "noise" if fed directly into your SIEM, automatically push refined Indicators of Compromise (IOCs) as Machine Readable Threat Intelligence (MRTI) into the system, and compare them with existing logs so you can easily spot trends or patterns that are out of the ordinary and act on them efficiently. By tying your teams, processes, and tools together, a platform gives security teams unprecedented visibility into where the threat is coming from and can track the entire incident from beginning to end – through reporting, blocking, and mitigation. The resulting productivity savings allow you to spend more time monitoring your network, rather than chasing false positives that SIEMs can propagate.

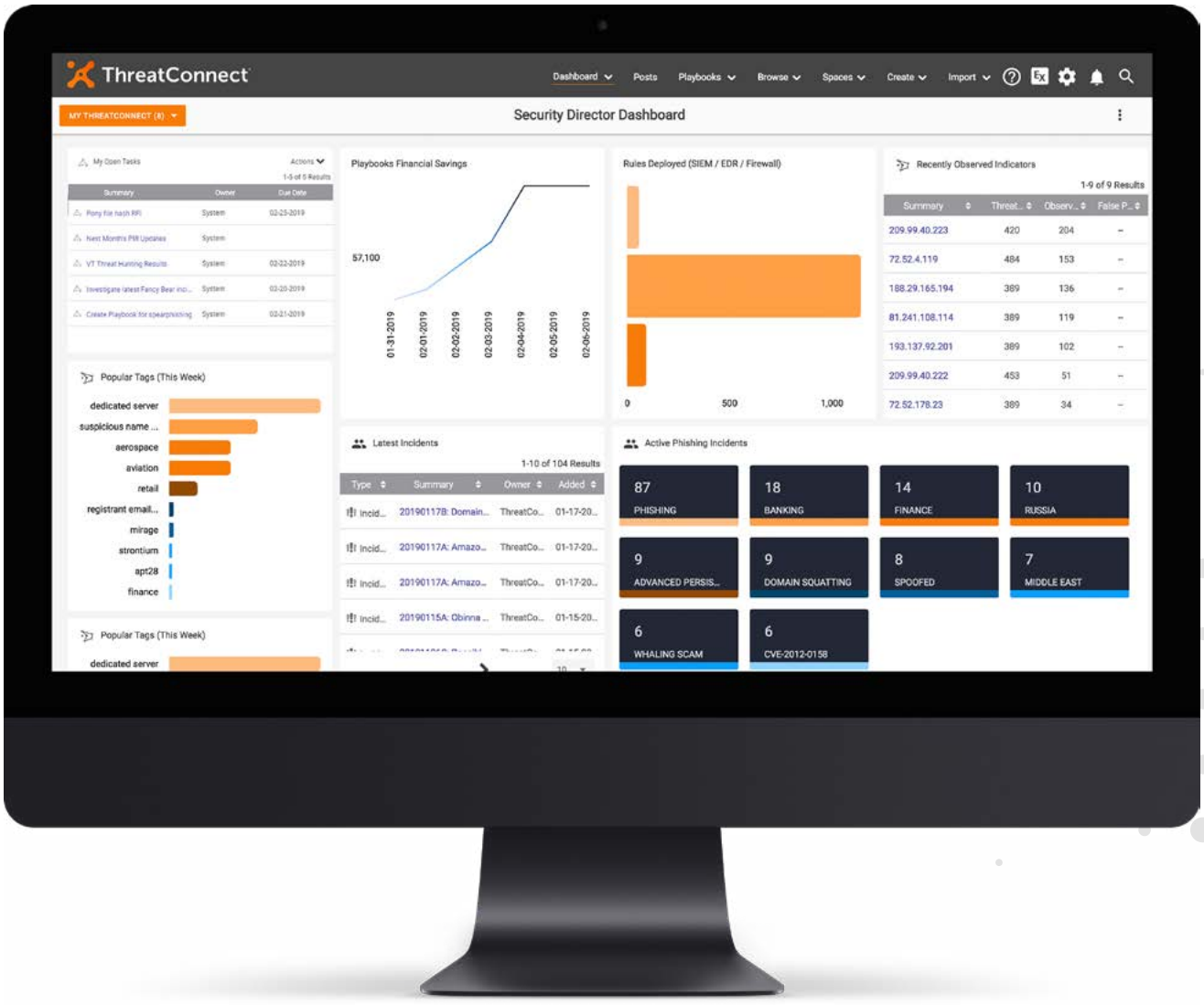
Executed properly, the convergence of threat intel with a platform and your organization's SIEM allows you to consolidate all your threat data, have control over it, validate it, measure the value of that TI, and mature the use of it in your SIEM for alerting and blocking – making it work better and smarter for you. With a threat intelligence platform you can be confident that your data is relevant and prioritized so that you can act on it more properly in your SIEM.

A threat intelligence platform provides immediate benefits to your SIEM, making it work smarter, not harder.

[1] Who's Using Cyberthreat Intelligence and How? SANS Institute, February 2015

SIEM + TIP:
How to Make the Most of Your TI

Implemented correctly, TI programs can sharpen your defenses, save time, and help you make better strategic security decisions. But to get the most out of TI, there are a number of best practices and workflows that a platform enables to unify your people, processes, and technologies.



Further Analysis of Logs, Events, and Data

Thanks to the bidirectional flow of data between the two systems (enabled by the platform), indicators from the platform are automatically sent to the SIEM for alerting, and telemetry and specific events from the SIEM can be sent back to the threat intelligence platform for correlation, analysis, and prioritization. The cycle can then start again as the platform uses this data to refine and update what is then sent to the SIEM for alerting. In the platform, the analyst can also see where the malicious indicators were observed. By identifying which sources or tools identified the indicator, analysts get a clear picture of which of their tools are finding relevant indicators in your network.

The Threat Intelligence Platform as a Knowledge Base

Comprehensive platforms can serve as a central threat repository for your organization giving you one place to store all your threat data, team's notes, and any related documents. Your team can find out about cybercriminals' tools, processes, victims, and intended goals. You can easily correlate information from past attackers' activity to current, and learn from past campaigns to proactively thwart an attacker's current and future attempts. TIPs also let you keep a record of false positives, so you can assign a level of confidence to incoming feeds and prioritize your response appropriately.

Align Your Security Investments

Leveraging built-in workflows, threat intelligence platforms also drive smarter practices back into your SIEM, intrusion detection, and other security tools thanks to the finely curated, relevant, and widely-sourced TI that the platform produces. Automatically share TI and logs correlated from your SIEM and TIP across your security infrastructure so that you can better align your security investments and understand the full health of your security operations.

Generate and Refine Intel Based on What's Happening Within Your Network

Rather than look at a series of events and identifying the inconsistencies as SIEMs do, a platform adds contextual and relationship-rich indicators so that organizations can better understand the nature of the threat, the risk they present to the enterprise, and inform an overall response more effectively. In doing so, you're able to strategically thwart the attacker instead of playing a random game of whack-a-mole.

Form a Proactive Defense

Threat intelligence platforms allow IR teams to look beyond their own network for clues and connections that may suggest relationships between the threat that's attacking the organization and where else it may exist and uncover new intel that may be relevant. Using this acquired knowledge, security teams are transformed from a reactive to proactive defensive force.

Automate and Orchestrate to Tie Your Teams, Processes, and Tools Together

Far too often, security products and solutions are designed to be independently managed, an unfortunate norm that enables the fragmentation of people, processes, and technologies. Because it handles these tasks automatically, a threat intelligence platform enables a security analyst to orchestrate many of the sophisticated duties normally reserved for specialist threat analysts. With a TIP, workflows are automated and multiple kinds of TI from a multitude of sources can be processed automatically.

TI can be quickly visualized (by security teams, the organization as a whole, and wider communities) and pivoted to provide a richer picture of threat actors so that action can be taken. With TIPs, your entire security infrastructure is integrated – from your teams to their processes to their tools and systems. You can automatically share IOCs to the relevant tool, or system, right in the platform. You don't have to use a different system to set up a rule or enrich your data – everything you need is in one central place. Proper workflow ensures that everything moves smoothly through your security organization and that team members are addressing the most important jobs.

TI can be quickly visualized (by security teams, the organization as a whole, and wider communities) and pivoted to provide a richer picture of threat actors so that action can be taken.

A SIEM is Vital to Any Security Arsenal, But Needs Help in Order to Maximize its Potential.

It's simple: SIEMs work best when supplemented with a threat intelligence platform. A threat intelligence platform is the ideal workspace for an analyst to ingest data from any source, fuse internal and external data, prioritize data for faster analysis, and form a complete picture by synthesizing that data together for a fuller understanding of threats.

By uniting your SIEM with a threat intelligence platform, you can unite all of your people, processes, and technologies behind an intelligence-driven defense and achieve powerful results:

Identify the Threats that Matter to You

Aggregate your internal logs and combine them with your threat intel to quickly identify which feeds are most applicable to your environment.

Gain Confidence in Your Threat Vetting

Keep a record of false positives, so you can assign a level of confidence to incoming feeds and prioritize your response appropriately.

Better Understand the Nature of the Threat

Go beyond the capabilities of your SIEM to add contextual and relationship-rich indicators to alerts and events for a better understanding of risk and a more informed response.

Enrich Your Intel with New Sources

Share threat data for further enrichment from other data sources and intelligence communities.

Share Data and Store

Use the TIP as a knowledge repository for historical threat data and help combat re-emerging or persistent threats.

Leverage Workflows and Orchestration

Use platform workflows to drive actions via integrations with the rest of your security infrastructure, turn your own incident data into internal threat intelligence (the most valuable). And, eliminate fragmentation and manage your security infrastructure from one central hub.

How ThreatConnect Can Help

Unite your cybersecurity people, processes, and technologies behind a cohesive, intelligence-driven defense.

ThreatConnect® is built to bridge incident response, defense, and threat analysis. Designed for security teams at all maturity levels, companies and agencies worldwide use ThreatConnect to maximize the value of their security technology investments, combat the fragmentation of their security organizations, and enhance their infrastructure with relevant threat intelligence. Make better decisions based on your TI using ThreatConnect.

Once an organization has leveraged a threat intelligence platform like ThreatConnect to automate its TI workflows and establish a feedback loop between TI, the platform, and the SIEM, it is now empowered to make tactical and strategic decisions based on that TI.

Aside from discovering patterns in the chaos and driving smarter practices into your SIEM, ThreatConnect is a powerful platform that gives you a broader understanding of the evolving threat landscape, and delivers experienced guidance on when and how to act based on what's hitting your environment.

No longer confined by the data gathered solely within your department, or within your organization, you have the power to share information with response teams, vendors, trusted partners, and your supply chain.

Make better decisions based on your TI using ThreatConnect.

No longer confined by the data gathered solely within your department, or within your organization, you have the power to share information with response teams, vendors, trusted partners, and your supply chain.

Here are just two use cases that can help you derive more value and drive ROI from your TI activity:

1 Create an Intelligence-Led IR Process

With ThreatConnect, you can leverage any number of metrics gathered by a global community of intelligence experts, including our own research teams, to gain a broad understanding of the evolving threat landscape and receive experienced guidance on when and how to act based on what's hitting your environment.

Given the fragmentation and silos prevalent in today's security organizations, measuring the ROI in threat data and TI hasn't always been apparent or accessible, until now. Using ThreatConnect's reporting capabilities, you can gain some simple measures of relevance and accuracy (and quash those false positives) and use this insight to drive more informed decision-making about the intelligence you are currently using (or thinking about using) based on the value it brings to your organization.

Examples of ROI uses cases that ThreatConnect enables include:

- ✓ **Understand Where Intel Originates:** ThreatConnect's Observations and False Positives capabilities allow you to see which of your security tool integrations are actually reporting the data. Track observations per integration and achieve a better picture of where potential threats (and false negatives) are appearing in your network and what your team is saying about them. This lets you hone in and prioritize your response.
- ✓ **Download PDF Reports:** ThreatConnect lets you share information about incidents, adversaries, and threats quickly and easily with a one-click export to PDF. They can even be stored in ThreatConnect as PDFs for easy retrieval later. This makes it easy to loop in leadership, partners, or outside parties of relevant intelligence pertaining to security events and incidents.
- ✓ **Achieve Global Awareness:** When you view an IOC in ThreatConnect, you can see information on all of the other feeds, sources, and communities in which the indicator appears. ThreatConnect also includes data on the indicator's rating and confidence so that you can have the full puzzle in front of you.
- ✓ **Evaluate Your Intel:** Users can up-vote or downvote intelligence that they feel is relevant and useful (or irrelevant and useless!), so that only the most criticalor important items rise to the top. That way you can coordinate around the biggest problems and ensure that your team stays on course, even in the chaos.

2 Establish and measure the ROI of threat intel for informed decisions

According to a 2018 Verizon DBIR Report, in 87% of cases, networks are compromised in a matter of minutes. The pressure on IR teams' need to accelerate response times is significant, and ThreatConnect can help.

The most effective IR teams use ThreatConnect's leading analysis methodology, workflow features, and powerful integrations to collect threat data from reliable external sources, compare it to in-house developed data, and collaborate with SOC teams to proactively identify and prioritize threats before damage can be done. No more chasing false positives!

Using threat response workflows, teams can work together to conduct deep analysis into threat actors' capabilities, set up scheduling alerts, and enable automated actions for blocking and alerting. When faced with a threat, security professionals can leverage ThreatConnect to immediately connect critical dots and make data-driven decisions, within a central interface.

Q: What is the threat and do I have any intel on it?
A: Fueled by threat intelligence, the IR team finds an artifact during an investigation and can access the dataset in ThreatConnect to learn more about the adversary and how to more effectively combat him.

Q: Have we seen this threat elsewhere? Is this threat limited to one of many machines?
A: IR teams can look into a database of past incidents to understand similar threats, their scope, if the threat has appeared before in a similar fashion, what the intended goal of the adversary might be and have been. From here they can estimate, based on past threat interaction, what stage in the kill chain the threat might be and can proactively estimate what the future threat activity might be, thus improving response times by taking targeted action.

Q: I need to report to management monthly / quarterly on our activities. Where do I get this data from?
A: The IR team can pull incident report data from ThreatConnect. This includes blocks of descriptive summaries of adversaries (including their tools, infrastructure, and goals), and statistics on types of incidents, and more. Data and reports can showcase vulnerabilities and how additional investments might improve network protection.

Q: How can I take advantage of other security pieces of my security infrastructure to better respond to incidents?
A: ThreatConnect allows IR teams to act earlier in the kill chain so that investigation and remediation can take place side-by-side. For example, you can use an Cisco Umbrella integration to block communications quickly to the adversary's command and control infrastructure. You can monitor what they are doing overtime, or you could send indicators to Tanium for alerting and blocking of actions on the host machine.

Are you ready to use threat intelligence to enhance your SIEM?

Whether you are getting started or are a mature enterprise organization in need of a cloud-based or on-premises platform, ThreatConnect is available in a variety of deployment editions to suit your requirements, local data security regulations, and your team's preferred operational methodology.

To Register For A Free Threatconnect Account Or Learn More, Visit Threatconnect.com

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