WHITE PAPER

THREATCONNECT

6 Easy Ways to Advance Your Cybersecurity Program When You Have a Small Team

When You Lack People, You Have to Rely on the Process, or Better Yet, a Platform for Rapid Detection and Response.

INTRODUCTION

Cyber attacks are increasing.
Rapidly. For everyone.

Protecting your organization from threats is an ever-expanding and complicated process that requires an enormous amount of work.

Even though the frequency and severity of breaches are rising, many organizations still rely on a small team of talented individuals to protect their organizations from attacks. These **unsung heroes** of cybersecurity cover many job functions and work very long hours to keep their organization safe.

When your team is small, you have to do the mundane, manual tasks, from keeping spreadsheets and logs, to adding enrichment data and indicators before you can even think about incident response or proactive cybersecurity. You are asked to do so much, it wouldn't be surprising if they handed you a mop and bucket and asked you to clean the floors too.

In this paper, we outline six steps you can take to use a cybersecurity platform to enhance your ability to ingest, store, and prioritize threat data, develop intelligence-driven processes to automate manual tasks, and streamline your workflow. The right platform (and processes you drive with it) can be a force-multiplier for your small team. Now, your proverbial one-man (or one-woman) army can have the defensive power of an entire cybersecurity platoon.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

P 1.800.965.2708 F +1.703.229.4489

DEFINING A TRUE CYBERSECURITY PLATFORM

As the risk of cyberattacks increases, so does the need for significant changes within your organization's security program. Rather than buying additional tools to fill in the gaps, consider a cybersecurity platform. It doesn't just address a single facet of the problem, it unites all of your resources in one central place. A true platform allows you to spend more time on incident response, threat analysis, and proactive cybersecurity.

Cybersecurity platforms go by many names:

- Security incident response platform (SIRP)
- Threat intelligence platform (TIP)
- Security operations, analytics and reporting platform (SOAR)
- Cyber intelligence platform
- Actionable situation awareness platform (ASAP)
- Know another one? Let us know. We'll add it to the list.

All of these platforms are slightly different as far as what they emphasize, but for a small team, there's certain core functionality that's going to be important to help you reduce your manual work and increase efficiency through clear processes.

Here's what to look for in a cybersecurity platform:

- Aggregates open source and premium threat intelligence sources
- Stores threat campaigns, incidents, or IoC data records
- Enriches your data so you know of its quality, accuracy, and relevance
- Allows you to enter information for intel sources, threats, events, or indicators
- Provides a collaborative environment for your team
- Provides a means to securely share threat intel data with communities or partners
- Generates reporting and metrics to help data-driven decision making
- Integrates with additional tools and information sources via an open API
- Can be programmed by outside developers to extend the platform's features

So. You could continue to spin your wheels. Do mundane work. And constantly feel overwhelmed. Or, you can **implement these six steps** to utilize a platform that **empowers** your team and **accelerates** your threat intelligence program.

THREATCONNECT®

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com
P 1.800.965.2708 F +1.703.229.4489

THE SIX STEPS TO MAKING YOUR SMALL TEAM OPERATE MORE LIKE A LARGE PLATOON

Collect and Correlate Relevant Threat Data

You Are What You Eat

In order to start proactively protecting your organization from threats, you need information about what and who may be trying to attack your network.

Many small teams overlook one of the best sources of threat information: their internal data. Sources such as your log files or your endpoint protection device data can be a valuable source of information and a great starting point. Once you've looked at your internal data, you will want to begin correlating that information with data from external sources. The most common way to do this is through threat feeds.

Threat feeds can be either free or premium. Warning: It may be tempting to subscribe to every feed possible. Unfortunately, more data does not translate to a faster, more efficient security process. When you subscribe to feeds that aren't the right fit for your organization, resources, environment, or team, it could be detrimental. If you have too much information that isn't relevant to you, or, even worse, is bogged down with false positives, it will create more work for you later.

It is even more important for small teams to spend their time on what matters: protecting your organization from actual threats. Spending the majority of your time sifting through mounds of data to find what is relevant or truly malicious, wastes valuable hours that could be spent on more important – and relevant – tasks.

A platform provides a central place to automatically ingest all of your internal and external threat feeds. It normalizes the information so it is easily understood. It also provides a scalable way to generate metrics on the return on investment for each feed, such as how many priority tickets a feed has generated, or the average amount of observations or false positives a feed has.

Don't Limit Yourself

Feeds are an excellent resource for your cybersecurity program. But, they aren't the only resource, or even necessarily the best resource for your organization. Threat intelligence can and will come in a number of different formats. Everything that contains information about a threat, from an email to a text file, is a valuable resource that could help you improve your cybersecurity practice.

When you only have a few people on your team, finding time to locate, normalize, and store all of the various sources of threat intelligence is a challenge. A platform does this for you. It ingests all file formats, both structured or unstructured. Whether you work with DOCX, CSV, PDF, Yara, or just email, a platform will ingest that data and normalize it. More importantly, it will automatically parse the indicators out of these files for you.

With a small team, you shouldn't be spending your valuable time manually reading files, and copying and pasting indicators. Let a platform automate that process for you.

Gone Huntin'

It is also possible that you want or need more information on how to protect your network than a feed provides. Many small teams do not find value in free threat feeds, but do not have the budget for a premium feed. Instead, you read industry blogs about potential threats to your network. These blogs have a lot of valuable information, but manually pulling out the indicators is very tedious.

If you do a lot of blog reading, a platform can integrate with web browsers, streamlining these actions so they are done more efficiently. For example, a platform and web browser app can be written to automatically show you indicators on a web page. In one click, it will send the indicators to your platform for you. You can continue hunting without having to switch screens. When your team is small, every second counts.

Get the Context Behind Your Threat Data

A Place For Everything, and Everything In Its Place

Now you know how to find threat data and what to do with it, it is important to get the context behind that data. Cyber adversaries have tools, infrastructure, techniques, and processes. To better defend against all of this, it is important to get all of the information you possibly can, to determine when something is an isolated incident or part of a larger pattern that needs more attention.

To start gathering context behind data, it needs to be stored in one place. With a small team, you have to look for information in different places or wait for slow, manual spreadsheet querying. However, these tasks can be alleviated if you ingest all of your threat data into a cybersecurity platform. A platform will ingest your threat data, normalize it, index it, and store it so it is instantly searchable.

With all of your threat data in one place, you can now begin to create a threat repository, or knowledge base, for your organization. This allows you to retain the knowledge of your team. As your team grows and changes, the knowledge of the threats remains within the platform.

A platform provides a central location for you to quickly and easily search through your data to help create patterns or gather more information regarding a current incident. With a platform, you can eliminate manual querying and instantaneously search for any piece of information about a threat.

Every Little Bit Helps

Enriching your threat data from other sources is another important step to getting all of the context about a particular threat. You may have third-party tools that contain information about indicators, such as WhoIs or DNS record data. However, all of this information is stored in different tools. By pulling all of this information into one place, you can begin to see the full picture of a threat.

Because a platform integrates with other tools, you are able to gather all of this information in one place. When you view an indicator, you will have all of the information from your different tools, allowing you to make strategic decisions about how to act on the threat.

3

Prioritize Your Data

Tidy Threat Intel, Tidy Mind

Once all of your data is in one place, and you enrich it with additional information, it can be difficult to figure out where to allocate your time and resources. This is even more critical when your team is small. You need to address real threats to your organization and not waste time on information that really doesn't matter.

You need to organize your data in order to prioritize what matters most to your organization. **With a platform, you can prioritize information in the following ways:**

QUALITY

A platform has rating scales built right into the software configuration, giving you a quick and easy way to rate your data.

RELEVANCE

By integrating with third-party intelligence providers, a platform can record how often a particular indicator is observed on your network and tie it back to the source or integration in the platform.

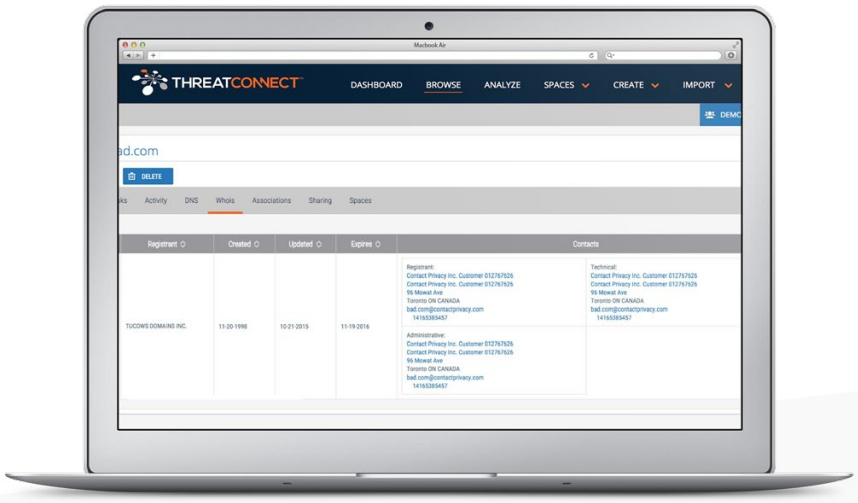
ACCURACY

A platform has false-positive reporting capability. You can see if an indicator is known as good, even if it is associated with an incident. This allows you to focus your time and effort on real threats.

Differentiating your sources by quality, relevance, and accuracy arms you with the knowledge of what sources are best for your organization. You can now strategically decide how to prioritize your team's time and resources.

Oooh! Shiny Object

Once you have enriched indicators, you can start to find patterns and trends in the data. An easy way to do this is through a visualization tool. A platform provides a place to look at all of your data in a graphical format, making it much easier to see connections and patterns in the data, giving you the context you need to thwart threats.



Collaborate and Share

You Are Not Alone

When you are a small team, validating your data and collaborating with your peers are crucial. Like yours, companies worldwide are experiencing similar threats daily. With a platform, you can securely share your data with your peers. You can ask them how they handled an incident, or even offer to share your own experience and expertise. By leveraging the knowledge of a community of experts in your field or vertical, you'll gain a comprehensive perspective of the threat landscape, and receive experienced guidance on how to act.

Keep Everyone In the Loop

Even the smallest teams usually have a leader or external stakeholder that needs to be updated on relevant security incidents or threats. If you don't have a central place for your data, or an easy way to present it to others, you will waste valuable hours gathering and compiling information on threats.

A platform makes this easy. It has export capabilities, allowing you to easily create and share intel reports of incidents, groups, adversaries, or threats. With a platform, you can even format your reports to display the most relevant information so it is easily seen.

THREATCONNECT MINI CASE STUDY

Organization: Confidential

Industry: Oil & Gas

CHALLENGE

The cybersecurity team could not sustain the enormous workload and manual workflow. They had no way of collaborating with industry peers on threats or solution development.

SOLUTION

The ThreatConnect platform eliminated manual processes and allowed collaboration with industry peers by providing access to industry and technology communities. It turned their one threat analyst into the equivalent of three.

RESULTS

- Eliminated manual analysis of 1 terabyte of data per day
- Automatic analysis of over 100 phishing emails per day
- Connected organization to peers in 70 countries

5 Automation is Key

Wash. Rinse. Repeat.

When your team is small, it is critical that you automate the mundane, repetitive tasks in your process to allow each team member to actually do the job for which they were hired: analysis, incident response, or IT security. Let's review: We've already talked about automatically ingesting, normalizing, and enriching your threat feeds. We will soon address automating tasks using platform integrations. But first, there are even more tasks that you can automate that can simplify your day.

One Phish, Two Phish, Too Many Phishing Emails

Email is one of the most popular methods for delivering targeted attacks, and represents a huge risk to organizations of any size. Phishing emails send a phony link that can lead to the installation of malware and viruses on a computer or on a network. To begin analyzing phishing emails, you need to analyze the data that is already in them. However, processing this information is often still a manual and tedious task. If your team is small, it is likely that someone spends hours collecting, compiling, and analyzing phishing emails.

In a platform, you can create structured, actionable threat intelligence from emails. Automatically forward suspected phishing emails into a phishing inbox for analysis and correlation. The platform will know to parse the email for indicators based on rules you define. This translates into easy transporting, correlating, and vetting, which, in turn, enables the extracted intelligence to be pushed into a sensor for alerting, and monitoring and blocking.

6 Tie It All Together

Better Together

Many small teams tend to have a number of security tools and systems that help them with their day-to-day tasks. However, they tend to work in silos, generating valuable information, but with no way of combining it with the other tools.

A true platform unites all of your tools and systems in one place, making each of them work smarter and stronger. With an open application program interface (API), it can be programmed by outside developers. A platform allows you to integrate all of your existing tools and systems, and completely customize the platform to your needs.

Mo' Value. Less Money.

Each of your current security investments has a specific function. A platform aggregates each tool's data and combines it with your threat intelligence data, so you can easily spot trends or patterns that are out of the ordinary and thus act on them efficiently.

Using this information, you can quickly identify what data is most useful for your organization. A platform makes this information easily shareable, either within your own team or across a community of your peers. By bringing all of your current investments together, you maximize the value you get from each investment.

IN THE END

Using a cybersecurity platform to unite your people, processes, and technologies is key to establishing or advancing a solid detection and response program, based on valid threat intelligence. With cyberattacks on the rise, using a platform to leverage all of your tools and systems not only saves time, but helps mitigate your risks more quickly, and provides a central place for all of your threat intelligence. If you are a small team, a platform is particularly helpful as you build your security processes, from ingesting and normalizing your threat data and automating tasks, to collaborating with leadership and industry peers and integrating all of your current investments.

That's where ThreatConnect comes in. Built for security teams at all maturity levels – and of all sizes – the ThreatConnect platform helps organizations build a cohesive intelligence-driven defense. With ThreatConnect, your team has a central hub from which to work and develop processes to identify, protect, and respond to threats. And it's scalable. As your team grows, so can the platform.

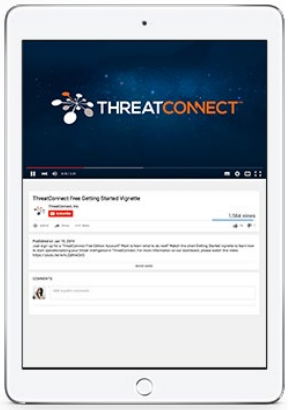
You don't need to have a big team or a large suite of products to benefit from using a threat intelligence platform. You can start today, with your team of only a few individuals (or team of one), to improve how you ingest, store, and prioritize threat data. Then, you can develop intelligence-driven processes to automate manual tasks and streamline your workflow.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

P 1.800.965.2708 F +1.703.229.4489

GET STARTED TODAY

ThreatConnect has created some materials to help you get started accelerating your detection and response program.



Watch some of our short **how-to videos** on how to get started with ThreatConnect on the ThreatConnect YouTube channel. We highly recommend the **'Getting Started'** vignettes.

LEARN MORE

Watch now on YouTube: www.youtube.com/c/threatconnect1
Visit our Knowledge Base: kb.threatconnect.com

Head back to the **ThreatConnect Knowledge Base** and learn how to conduct analysis in ThreatConnect and how to enrich data in ThreatConnect.

If you are interested in one of our editions (or if you just need help along the way), please email us at **accounts@threatconnect.com** or tweet us **@ThreatConnect**.

THREAT CONNECT®

ABOUT THREATCONNECT

ThreatConnect unites cybersecurity people, processes and technologies behind a cohesive intelligence-driven defense. Built for security teams at all maturity levels, the ThreatConnect platform enables organizations to benefit from their collective knowledge and talents; develop security processes; and leverage their existing technologies to identify, protect and respond to threats in a measurable way. More than 1,200 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. **To register for a free ThreatConnect account or learn more, visit www.threatconnect.com**.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

P 1.800.965.2708 **F** +1.703.229.4489