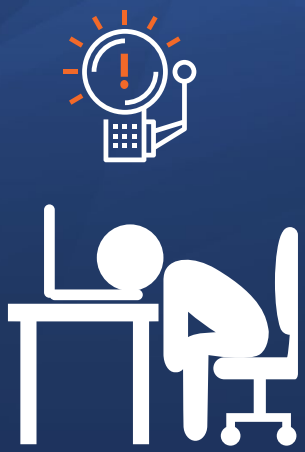
WHITE PAPER

THREATCONNECT

From Reactive to Proactive: How to Avoid Alert Fatigue

Take decisive action on the threats that are most critical and relevant to your organization.



Alert fatigue. As cybersecurity teams and technologies get better at detecting threats, they are also becoming more inundated with alerts, warnings, and notifications. As a result, IT and cybersecurity professionals become desensitized to alerts, and may be less inclined to address them. In fact, **80% of organizations that receive more than 500 critical alerts per day investigate less than 1% of them**[1]. Many refer to this issue as "alert fatigue" since the constant barrage leaves you with too many alerts and not nearly enough time to respond to them all.

If your team receives hundreds of alerts a day that are all labeled as the highest priority (or worse, not prioritized at all), how can they possibly know where to begin and which fires to put out first? Choosing incorrectly or not knowing where to begin wastes precious resources and may allow breaches to persist in your network for longer periods of time.

So how do you prioritize your alerts?

The goal is **active response**: the ability to respond to attacks and incidents as quickly as they are detected within your own environment. Ideally, active response is a combination of both automated activities and human-based actions. The response may be automatically blocking an IP on your firewall based on predetermined rules, or having a human take a final look at the IP and decide to block it themselves. With active response, your team will be able to leverage automation to free up time to focus on taking quick, decisive action on the threats that are most critical and relevant to your organization.

Stop drowning in alerts and spinning your wheels responding to alerts that aren't important to your organization. Implement a few easy changes and dramatically reduce false positives, have fewer alerts, and finally achieve active response in your organization.

[1] http://www.infosecurity-magazine.com/news/less-than-1-of-severe-critical/2016

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

P 1.800.965.2708 F +1.703.229.4489

HOW YOUR ORGANIZATION CAN ACHIEVE ACTIVE RESPONSE

Get Your S#*! Together

Look in the Mirror

The first step to achieving active response is arguably the easiest – assess what you already have. Organizations use a number of different tools to aid their cybersecurity program. As cybersecurity budgets increase, so do the options for tools. In 2016, there are well over 500 companies in the cybersecurity space.

Each of these tools is useful in their own way, helping protect the organization and also collecting some of the most important information for your cybersecurity program – your internal data. Each of your cybersecurity tools or systems collects valuable data. However, that's the problem: they collect their OWN data. They work on their own, collecting data and administering actions based on what they (separately) find in the network.

When it comes to maintaining the alerts, using multiple tools and logging into multiple portals can be overwhelming. The best way to reduce false positives and ensure that you are working with the most relevant data, with the most context possible, is to combine the data from all of your current tools and systems. When all of your data is in one place and in the same format, it is much easier to visualize what is occurring in your environment, prioritize it, and then decide how to address threats to your organization.

Teamwork vs. Isolation

There are a few ways to get all of the information from your tools in the same place. You could copy and paste all of the information into a central spreadsheet, but then never be able to find the information quickly again. Or, do what a lot of folks tell us they do now: start a massive email chain that no one takes the time to read.

Or, you could use a cybersecurity platform. A cybersecurity platform makes it easy to get all of your internal and external data in the same place. This is done through APIs (application programming interfaces). Open APIs are publicly available and give developers programmatic access to software. APIs are how different software programs and systems 'integrate,' or 'talk to each other' – basically, how they share data.

APIs allow data to flow in and out of one software program into another. That's why a platform is so important: you can construct it so that all of your cybersecurity data flows into the same place. With everything in one place, you can look at the data all at once.

Once all of your threat data is in the platform, it is enriched with all of the possible context gathered from your other tools and sources (which we will talk more about later). When your threat data gains more context and you can use it to inform decisions, it becomes 'threat intelligence.' Pushing validated, vetted threat intelligence back into all of your systems and tools allows each to work smarter and benefit from ALL of your data. Using threat intelligence helps yield the best results from all of your security investments.

Don't Box Me In

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 (paid). **Warning: It may be tempting to subscribe to every feed available. Don't.** More data does not translate to a more efficient or effective security process. When you subscribe to feeds that aren't the right fit for your organization, environment, or team, it could end up hurting you instead of helping you. If you have too much irrelevant information, or even worse, information bogged down with false positives, it will likely create more work for your team.

It is important for cybersecurity teams to spend their time on what matters: protecting the 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 cybersecurity platform provides a central place to automatically ingest all of your internal data and external threat feeds. It normalizes the information so it is easily understood. Once everything is in the same place, a platform provides the context you need to start to prioritize the data and determine what is most important to your organization.

Connecting the Dots

The Alerts that Cried Wolf

As we stated earlier, alert fatigue is a very real problem that most, if not all, organizations face. In fact, IT professionals often ignore alerts because of the sheer volume they receive. They are receiving hundreds, if not thousands, of alerts per day. Even if they try to keep up, they usually find that, of this huge number of alerts, only a few are actual threats to their organization. So much time is wasted trying to manage their data and alerts, little time is left to actually deal with the threats themselves.

This provides a great opportunity for your organization's adversaries. It is much easier to slip through the cracks into an organization's infrastructure when they are drowning in alerts. The longer hackers are in your network, the better their attack. An attacker can sit dormant for months or even years, learning as much as possible about your infrastructure to craft the perfect attack. Speed is critical; the sooner you find malicious activity in your network, the sooner you can mitigate it.

As organizations look to lessen their alert fatigue, one thing becomes obvious: one size does NOT fit all. Different locations, companies, and industries attract different types of attacks. For example, health care organizations are concerned with security of patient information and APT groups, while oil and natural gas companies are concerned with protecting their critical infrastructures and supervisory control and data acquisition (SCADA) malware.

As organizations look to minimize and eliminate their team's alert fatigue, they must take a number of factors into consideration: their size, location, industry, and infrastructure. Each company's journey will be different. So that brings us to our next question – how do you decide which alerts are the most relevant to your organization?

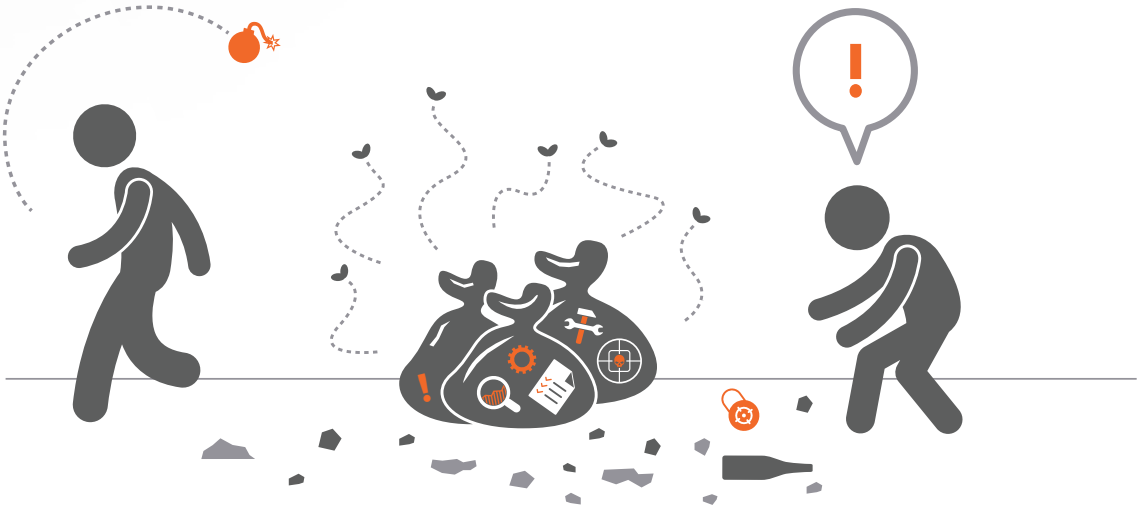
One Person's Trash is Another's Treasure

Organizations need to take a number of steps to determine how to prioritize their alerts and reduce alert fatigue. But it doesn't have to be a long or extensive process. A cybersecurity platform has many built-in features that are designed to do just that – help you find the context behind alerts and establish what your team needs to do first.

The platform should have built-in rating features. With a built-in rating system, it will automatically take a piece of data, look for where it was seen in your network, the malicious activity it was associated with, and automatically give you a rating that shows how dangerous it is for your specific organization. The ratings are unique to your organization and its specific needs. And the ratings are adjustable. If a platform finds that something is dangerous, but you know that it is not, you can manually change the rating to reflect your analysis.

It is also possible that you aren't just concerned about where a piece of data has been seen in your network, but you also want to know what your teammates think as well. A cybersecurity platform should give you a place to 'vote,' or evaluate the relevancy of a piece of data. Having a quick, one-click response to indicate what you and your teammates think of a piece of data provides your analysts the information they need quickly and easily. If an alert or a piece of data has many relevancy votes, it is probably a high priority and should be looked into right away.

Finally, and arguably the most important: a cybersecurity platform should give you visibility into the relevancy of your sources and tools. Because all of your data goes into a central place, the platform is able to track which sources and tools detected the most alerts, and which detected the most *relevant* alerts. If you are paying for a premium feed that does not provide you any alerts, it is not relevant for your organization. And, if the feed only provides false positives, you know that the feed is literally not worth your time. A platform should allow you to mark data as a false positive, and also tracks how many times a piece of data is seen in your network. The ability to see how effective your tools and sources are provides you with the ROI metrics you need to make more informed budgetary decisions for your security team.



Keep It Simple, Stupid

As with most things in life, the simpler something is done, the easier it will be to do. The fewer alerts you have to deal with in your organization, the better. If you aren't drowning in alerts, you can take the time that is actually needed to learn about a threat, compare it to other data, and figure out the best way to mitigate it. The best way to have an efficient security program is to clear out all of the extra stuff you don't need – a.k.a. extra alerts that aren't relevant to your organization. Less is more.

Organizations struggle with a lack of cybersecurity staff, time, or adequate resources. They can't afford to have their talented, expensive analysts chasing after alerts that don't matter to their organization. By implementing a few of the processes we have mentioned above, security teams can finally take control of their alerts, refine their processes, and begin to build a proactive approach to their cybersecurity practices.

Now What?

Building a Proactive Approach

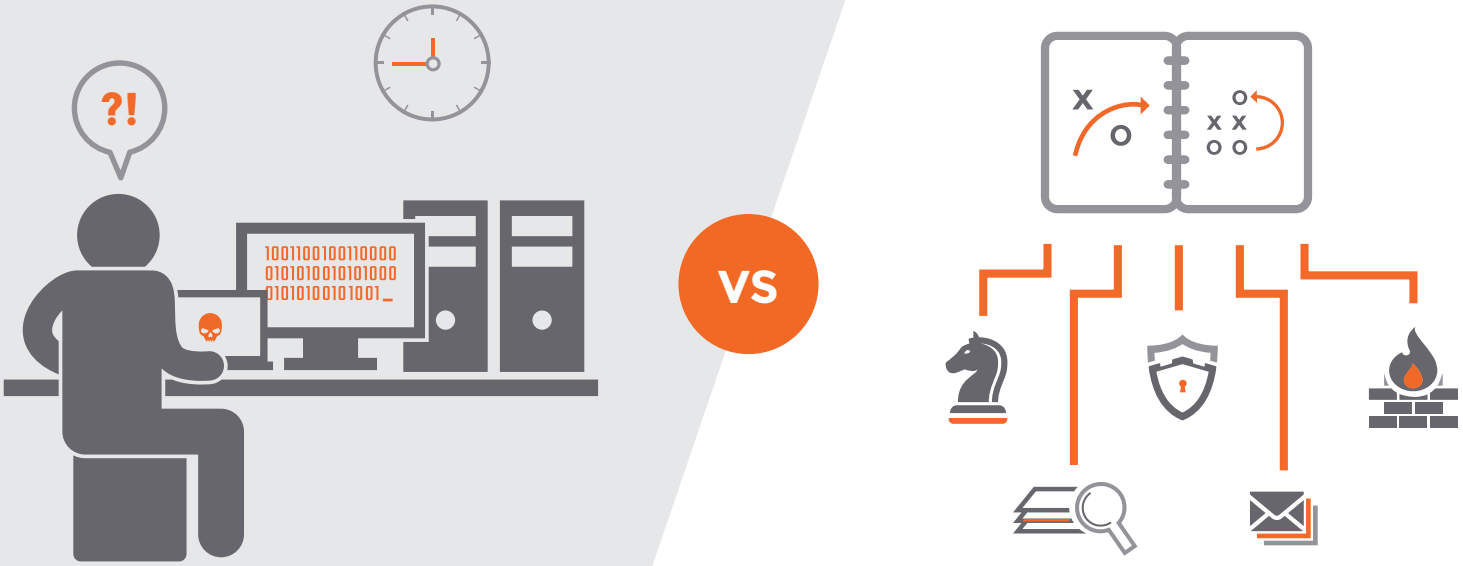
You've compiled your data into a central place – a cybersecurity platform. You've even analyzed the data for context to determine relevancy. Now what? How do you actually start to take action against alert fatigue? And, more importantly, how do you do this without using a large amount of time or resources?

A traditional threat intelligence platform (TIP) can put your data into one place, provide some context for prioritization, and maybe even connect to some of the other devices in your infrastructure. But, how do you actually take action on minimizing the number of alerts, or automating certain tasks so you can spend your time on actual threats?

This is where a cybersecurity platform can help. A top-notch cybersecurity platform will have orchestration capabilities that provide automated and configurable 'playbooks' – or automated chains of events that are triggered by an event in your network. For example, you can set up a playbook for when an IP address is seen in your environment. Once the IP is in the platform, it is assigned a rating based on the other information in the platform. The playbook then contains an 'if/then' statement. If the IP is higher than a certain threat rating, you will be sent an email and assigned a task to investigate it or even take automated blocking actions. If it is not, it is added to the platform for a historical record.

That is just one of the infinite possibilities of playbooks. Using your cybersecurity platform's APIs, you can loop in any of your other existing tools. Or, loop in any of your teammates by adding a task in your cybersecurity platform. You can send yourself, your boss, or even your grandma an email based on almost any action in the platform. As a result, you no longer need to constantly monitor or scramble to react to alerts. When a threat comes into your environment, you will have a series of events pre-determined to decide whether you investigate or mitigate a particular threat instantly. Playbooks gives the power back to security teams, so you can finally eliminate alert fatigue and achieve active response.

Having your aggregated and enriched data in the same place as your orchestration capabilities gives you a more focused, efficient, and effective response to threats – all without having to expand your team or buy more tools.



Automation Magnifies Efficiency

Automation, coupled with human intervention, is key to the success of your cybersecurity program. Cybersecurity employees today are highly skilled – the last thing you want to be doing is comb through PDFs for indicators or cut and paste indicators into a spreadsheet. When you start to automate the smaller tasks, it frees up your time to do more important tasks, like analyzing malware, patching vulnerabilities, or even building new defenses.

Often, with automation comes hesitation. There is concern that if a playbook is set to automatically perform a task, a million things could potentially go wrong. A cybersecurity platform will solve this problem by allowing you to weave in human intervention with your automated playbooks, looping in humans at critical decision points, or aligning to your policies for approval of things like blocking actions.

Cybersecurity platforms often have built in 'tasks' that allow you to see what your team is working on, assign tasks, and create an organized workflow. Because your playbooks are created in the same place as your tasks (in the platform), you can bring in a human element. So you don't want to automatically block an IP on a firewall? No problem. You can set up a playbook to automatically assign you a task to tell you to block an IP on a firewall. Then, you can make the final decision, while still automating much of the process.

Another important aspect to think about is not just automating playbooks for your team – but how you can set them up. Do the actions require a lot of custom coding? If so, you'll probably need to allot more time and resources than you can afford. That's why it is important that your orchestration capabilities are easy to use for anyone on your team. Cybersecurity platforms should allow you to create a series of automated actions at the touch of a button – no coding needed.

Having an easy-to-use orchestration feature helps you to finally automate your team's tasks and get one step closer to a proactive cybersecurity program.

From Reactive to Proactive (Finally!)

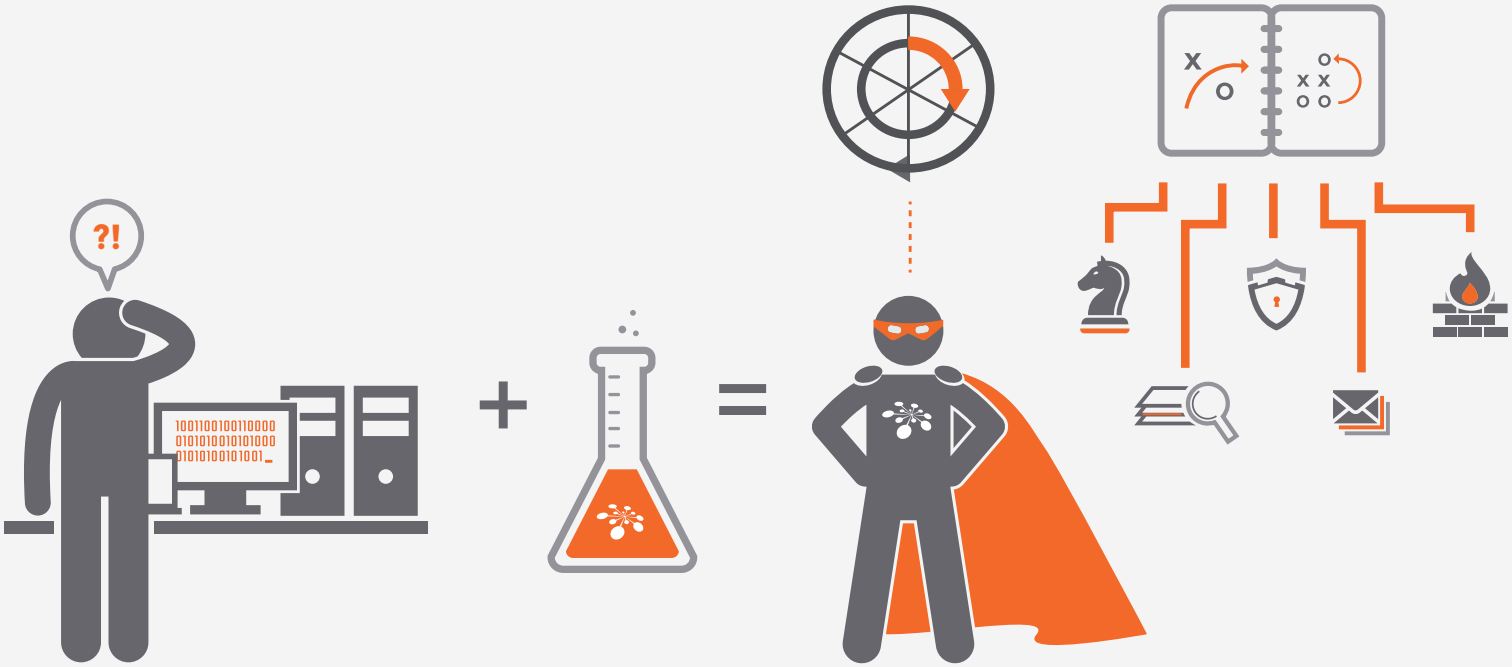
Using automated playbooks allows you to step back and examine your current processes. Each playbook records whenever it runs, giving you a list of exactly what actions happened and when. For example, a cybersecurity platform will show you when a malicious IP was seen in your network, when you received the alert email, when it was automatically enriched with data from your third-party tools (like DomainTools), when a task was created for your employee, and when they sent the IP to your firewall for blocking. And, it will show you exactly when this process was done, *every time*.

When your processes are memorialized, it becomes extremely easy to look at them strategically. What worked? What didn't? What can you improve? With a cybersecurity platform, it is all laid out in front of you. There is no guessing. Using data from the platform, you can finally make strategic, well-informed decisions about your security processes.

In the End

Active response is easier to achieve than you'd think. The more time attackers are in your network, the more advanced their attack will be. It is critical to take control of your alerts so you can detect threats faster and better protect your organization. If you are looking to achieve active response, a cybersecurity platform can be particularly helpful as you begin to get your data in one place, prioritize it, and take action using automated playbooks.

That's where ThreatConnect comes in. ThreatConnect has all of the capabilities of a traditional TIP, but is much more. If you just need to aggregate and normalize your data, ThreatConnect can do that. If you need to conduct deep threat analysis, you can do that in the platform as well. You can even set up automated playbooks to perform some of your tasks for you. The cybersecurity platform is built to help you through the entire lifecycle of a threat – from aggregation, to analysis and prioritization, all the way through taking necessary action to defend your network. ThreatConnect bridges threat intelligence and orchestration, allowing security teams to fully utilize their current tools and existing team's talents by automating simple tasks, prioritizing critical events, and putting time back on the clock to do what matters most – protect your organization from attacks.



THREATCONNECT

ABOUT THREATCONNECT

The ThreatConnect platform helps organizations identify, manage, and block threats by using threat intelligence, automation, and orchestration. 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