WHITE PAPER

THREATCONNECT

Fragmentation: The “Silent Killer” of Your Security Management Program

How to close the detection deficit between attackers and defenders, eliminate silos, and build a cohesive defense.

Introduction

Fragmentation is the silent killer of your security program. Sounds serious, right?

Well, it is.

After more than a decade of research, innovation, and investment in the cybersecurity industry, the “Detection Deficit” between attackers and defenders is near an all-time high and trending wider. While many contributory factors exist, extreme fragmentation of enterprise security people, processes, and technologies is surely chief among them. In this paper we’ll take a look at the issues and lay out a path toward better security through better unity, one that cuts the detection deficit with a cohesive, intelligent defense.

Time is Definitely Not on Your Side

Before we delve into the characteristics and consequences of fragmentation, let’s take a look at the threat landscape, how it’s evolving, and how the defenders are doing, versus those that attack them.

In 2016, Verizon issued its annual Data Breach Investigations Report (DBIR)[1], a collection of real-world breaches and information security incidents from the prior year. The results for security teams was grim. Threat actors are getting better, faster, and more efficient at compromising networks, taking only minutes or less to compromise systems.

Organizations, meanwhile, are taking weeks to discover breaches – and often that alarm is sounded by customers or law enforcement, not their own security measures. As you can see from the chart on the following page, which is essentially a study of successful breaches, the defenders aren’t doing too well. In fact, not a lot has changed in 10 years. **Back in 2005, approximately 12% of breaches were discovered in days or less, and today that has increased marginally to just under 25%.** However, the gap between the time to compromise and the time to discover an attack is getting wider. The detection deficit isn’t closing. It’s getting worse.

[1] Verizon 2016 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

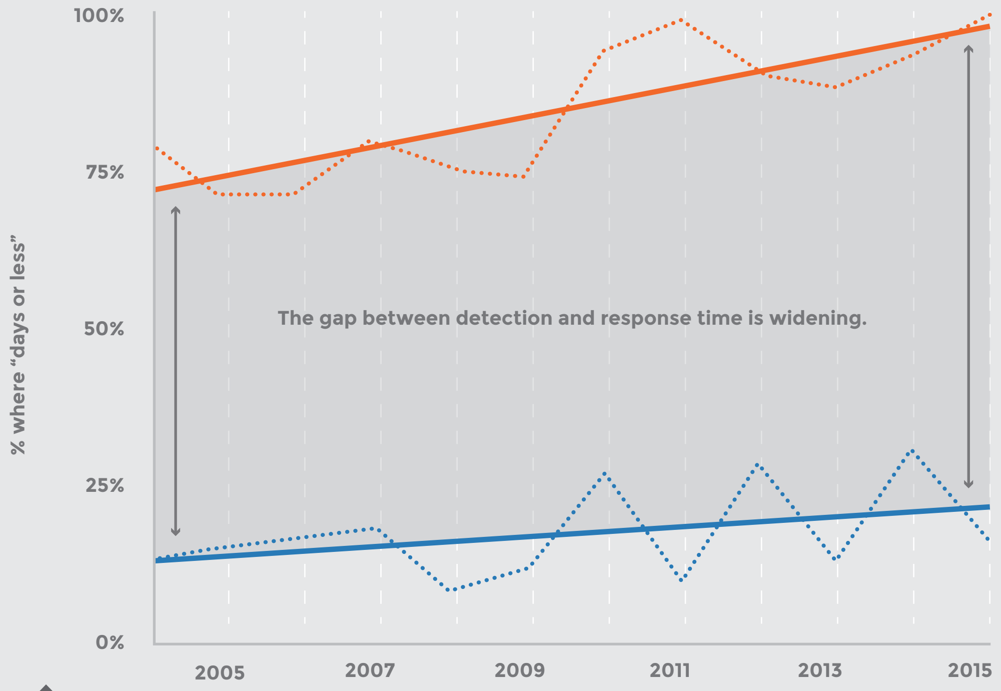


FIGURE 8.

Percent of breaches where time to compromise (orange)/time to discovery (blue) was days or less.

The Detection Deficit. This chart from Verizon's Data Breach Investigations Report shows the percentage of breaches where time to compromise / time to discovery was days or less. Note how the discrepancy gap is diverging. Defenders are struggling to close the gap, while attackers are increasingly proficient at their jobs.

Attackers are doing their job and doing it well far more often than defenders do, and that's a big problem. Given the heightened spotlight on security, the emergence of new technologies, and the growth in information security spending in the last decade, organizations must confront a difficult question – is that stuff actually making any difference?

Despite all the innovation and investment, the industry as a whole is, quite simply, ineffective at thwarting threat actors. Why is that? Why aren't we closing the gap and catching up with those who threaten our systems, data, and missions?

Threat Management is Merciless and Messy

To understand this, we need to understand the big picture. Cyber threats take many forms – malware, phishing, authentication attacks, application attacks, ransomware – and they come at you fast, often simultaneously. Then there's your security personnel (SOC teams, incident response teams, threat intelligence teams, risk managers, etc.) all of whom are trying to deflect the threats. Sometimes they work well together, but as they frantically try to study, respond and mitigate an onslaught of threats and attacks using different tools and controls, their efforts are often disconnected and lack coordination – prompting fragmentation. That's because threat management is merciless, it's unyielding, and it's messy.

Breaches Happen at the Seams Between Tools and Teams

Most breaches happen, not because a tool doesn't work or is inefficient, but because hackers find ways to penetrate your network in between the very tools and teams put in place to keep them out.

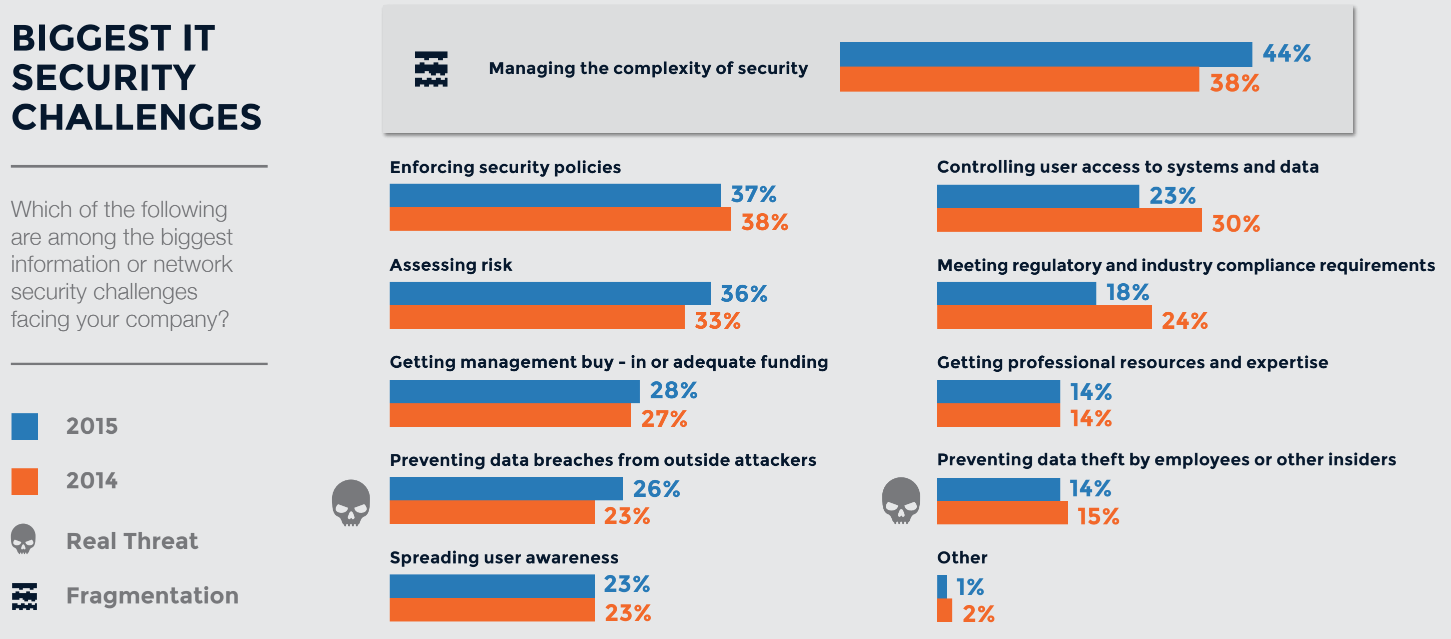
Despite efforts to stockpile the best technology that money can buy and assemble an army of defenders, today's security organizations struggle with inefficiencies. Deploying all those investments and human resources and making them work optimally, for the most part, isn't happening. We call it "death by inefficiency," and the data backs it up.

A 2015 survey by *Dark Reading* and *InformationWeek*[2] found that the biggest challenge faced by security teams was not preventing data breaches from outside attackers or data theft by employees, but **managing the complexity of security itself**. In other words, dealing with the outcome of fragmentation is more difficult than managing threats.

[2] 2015 Strategic Security Survey http://reports.informationweek.com/abstract/21/12549/Security/2015-Strategic-Security-Survey.html

BIGGEST IT SECURITY CHALLENGES

Which of the following are among the biggest information or network security challenges facing your company?



Source: Dark Reading / Information Week Strategic Security Survey

In essence, we've become our own enemy. With so many contingencies (funding, enforcement, regulations, etc.) and complexities, the average security organization is snowed under. Not only are the bad guys making life hard, corporate bureaucracy is too.

Ineffectiveness, inefficiency, and bureaucracy. All add to the ever-widening gulf between the proficiency of the attacker and the proficiency of the defender. And, so, the detection deficit grows.

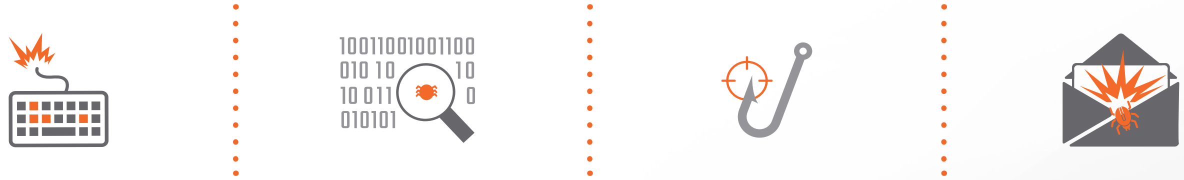
How Fragmentation Plays Out

1. Fragmented Threats

First, consider the threats you face. While your internal environment may be disconnected and fragmented, the external threat landscape is equally diverse. From adware to natural disasters, worms to programming errors, and everything in between, there are more than a hundred potential threat categories that organizations must deal with each day (160 to be precise).

One way to deal with threat fragmentation is to narrow down the threat environment by grouping threats into buckets. For example, adware, spyware, spam, and so on fall under "malware." Brute force, denial of service, use of stolen credentials, etc. fall under "intrusion and hacking." Other buckets include social engineering or environmental threats such as fire, flood, and power failure.

By introducing categorization, classification, and taxonomies to the vast array of threats, you can start to bring some method to the madness and defragment the landscape. But it's not enough, because you're also dealing with fragmented technology.



Unfortunately, the output is also fragmented. Threat actors are in the job of constantly adapting and changing their tactics, tools, and techniques. It's rare that an actor will use the same IP address over and over again. Instead, they employ hundreds of IP addresses over a period of time. **ThreatConnect's own research has shown that 50% of IP addresses used by threat actors are only used once, and 80% only resolve to that IP address for more than a day.**

Threat actors move on. If you trust those collected IP addresses as your knowledge of the threat, then your TI function is fragmented. Furthermore, if it takes you more than a day to discover a threat and enter it into your library of threat indicators and technology controls, that IP address is already rendered obsolete and useless.

Threat analysts need a better way to tie together their body of knowledge.

Achieving True Threat Intelligence: It's Time to Shift Your Approach

How do you break the pattern of fragmentation that makes managing the defense process and attack response so hard?

Here's how many organizations approach this today:

A SOC or threat analyst receives an email from a security colleague asking for more information about a threat affiliated with a particular IP address. The analyst responds by looking up the IP address and analyzing related TI. He or she finds a potential threat indicator, or not, and responds accordingly.

That's fine, but as we discussed earlier, threats evolve and IP addresses don't hang around long enough in the threat environment to be useful. If the threat actor has already moved on to another IP address, the threat is still out there. You've just conducted a wasteful and fragmented exercise.

A single IP address or malware hash is not TI. It's of limited use. But if you can piece it all together and use that IP address to better understand the threat actors' motives, the techniques they use, and the infrastructure that they're associated with, you're onto something. Only with this approach does the true definition of TI, i.e. empowered decision-making (such as where to tighten controls and close up vulnerabilities) and informed risk management, becomes possible.

This proactive approach, scuppers traditional parameter-based security practices, reactive fire-fighting, and fragmentation. Instead it gives you an intel-driven defense strategy that allows you to build a multi-dimensional picture of the underlying relationships between threat actors and their tools, techniques, and processes (TTPs) to help you gain a complete understanding of an adversary or event.

Enter the Cybersecurity Platform

As the risk of cyberattacks increases, so does the need for significant changes within your organization's security program. A key enabler and force-multiplier for your team in this regard is a cybersecurity platform. A platform like ThreatConnect can help you overcome fragmentation and the labor-intensive process of threat analysis that often exceeds the capacity of enterprise organizations.

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 TI. If you're trying to overcome fragmentation, 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.

For fragmented security organizations, ThreatConnect offers a number of benefits:

ThreatConnect unites all of your, previously fragmented, people, processes, and technologies in one place, making each of them work smarter and stronger.

2. Fragmented Technology

The market is awash with information security technology and vendors each with a point solution to “fix” your problems. Infrastructure security, endpoint security, application security, IoT security, threat intelligence, cloud security, risk and compliance, etc. – the brand names that address each of these functions are limitless.

It’s a marketplace that only serves to add to fragmentation. Today’s infrastructures are made up of multiple vendors, whose systems rarely work seamlessly together. Trying to make them interact, interplay, and integrate together is no easy task.

Security tools and controls are vital to the protection of your enterprise. But savvy adversaries are finding ways to bypass technology, quickly. They simply employ another technique, whether it’s spear phishing, spam, ransomware, or stolen passwords – they navigate the seams between technologies and teams. And they’re in.

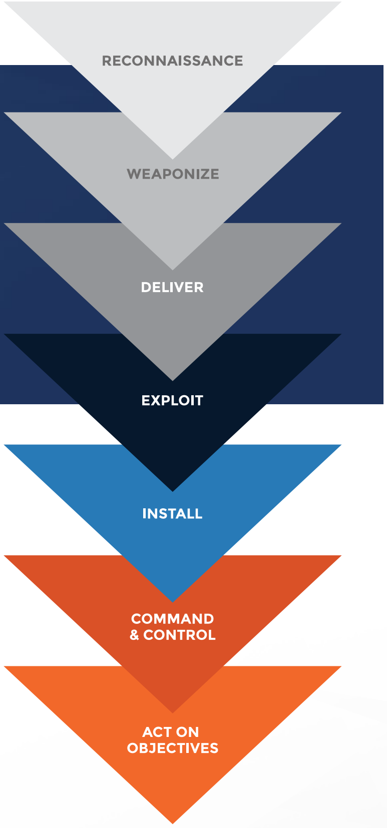
Another way that they bypass your controls is to infiltrate your assets. For example, an adversary may take over a web server that your database trusts and access your data that way. Again, despite your controls, which they’ve barely touched, they’re in.

3. Fragmented Processes

With changing threats and changing internal environments, managing your processes and responding to the attack progression is hard.

Today the attack process is widely understood, thanks to the seven steps of the Lockheed Martin Cyber Kill Chain® framework3, which is widely used as a model for the identification and prevention of cyber intrusions activity. But the scope of today’s attacks extends well beyond traditional intrusion-based attacks and emphasis on perimeter security that the Kill Chain model invokes. And this makes responding to each phase of the model a challenge, especially in a fragmented organization.

- What technologies do you have that let you see an attacker probing your network during the reconnaissance phase?
- How do you detect insider threats or non-malware threats? Something the Kill Chain doesn’t account for.
- How do you see them weaponize, deliver, and exploit?
- How do your teams work together to find that threat and respond to it?
- What processes tie those teams and tools together?



Cyber Kill Chain Model

For most organizations, there’s rarely a simple answer. The defense process is complicated. The tools, technologies, and processes (TTPs) are one giant hairball. Tied together, hard to unravel, and impossible to follow any process. Once you add people to the mix – your intel function, SOC, and incident response (IR) teams – each trying to share information, coordinate, and help each other respond to an attacker as they move through the Kill Chain, the situation gets messier.

Outside the threat management world, over on the governance, risk, and compliance (GRC) side of the building, things are equally problematic. The GRC function is often totally disconnected from the threat intelligence and IR functions. While GRC is busy assessing controls and risk, they do so with zero input from those dealing with frontline threats.

[3] The Lockheed Martin Cyber Kill Chain http://cyber.lockheedmartin.com/solutions/cyber-kill-chain

Threat Intelligence: Tying It All Together

How can you address threat management challenges, while tying all the fragmented components of your organization together? Enter threat intelligence (TI).

What is threat intelligence?

Let's start with what TI is not:

- TI is not about generating reports.
- TI is not about diagramming how malware works.
- TI is not about building catalogs of threat actors.
- TI is not about making libraries of indicators of compromise.

While each of these is part of TI, it's where these component parts leads you that's important. And that's towards making better decisions to protect your organization.

According to Gartner, threat intelligence is:

"Evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard."

- "How Gartner Defines Threat Intelligence," 23 February 2016,
Rob McMillan, (G00299526)

Forrester further refines this definition:

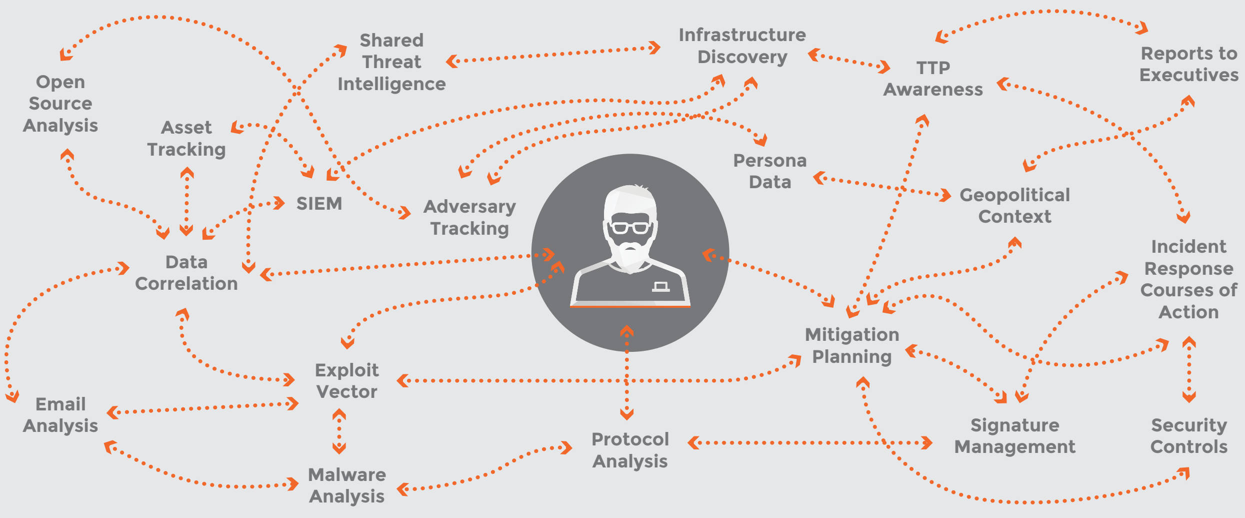
*"Threat intelligence's primary purpose is to **inform business decisions** regarding the **risks and implications** associated with threats."*

But Threat Intelligence is Fragmented Too

Although the overarching goal of TI is to bring unity to the process of threat management via enhanced decision-making and the inclusion of previously fragmented functions, such as GRC (hence Forrester's emphasis on the "risks and implications" associated with threats), it too is fragmented.

If you look at a threat analyst's job and his or her daily activities, it's another giant hairball. Your average analyst deals with multiple tools and tasks (some of them documented, some not). Intuition also comes into play, as they scour intelligence sources and use their smarts to determine risk and loop in other security teams, as necessary. It's a complex process. All of which adds time and slows down the defense process.

It's a fragmented method that looks a lot like this:



Threat analyst's day-to-day activities, tasks, and processes are fraught with fragmentation.

DEFRAGMENTED INTELLIGENCE	DEFRAGMENTED PEOPLE	DEFRAGMENTED TECHNOLOGY	DEFRAGMENTED PROCESSES
Quickly Identify and Prioritize Threats ThreatConnect allows you to automatically ingest all of your threat data (from any source), normalize it, and enrich it with data from your partners and intelligence services.	**Eliminate Silos** Having one place to work together, whether you're a threat analyst, IR, a security director, or CISO, is critical. Without it, teams are scattered, knowledge transfer is problematic, and process and hand-offs between teams is limited (believe us, you don't want to be doing that stuff over email).	**Connect Intel Data and Feeds** It doesn't matter which tools or systems you use, ThreatConnect can tie in different intel providers, data, and feeds. No need to log into multiple vendor portals.	**Manage in One Place** Build processes to manage your security infrastructure from one central hub. Keep track of workflows and tasks.
Determine Relevance You'll also get a high-level overview of how relevant your intel sources are for your organization by recording how often particular indicators are observed on your network and by enabling false positive reporting. Focus on the real and most harmful threats.	**Be Better at What You Do** ThreatConnect is also great at boosting a security analyst's capabilities. With ThreatConnect you can perform many of the sophisticated duties normally reserved for specialist threat analysts – such as understanding an adversary's TTPs and exploiting them to your advantage.	**Enrich Your Data** With all your data in one place, you can enrich it with additional threat information and prioritize information by quality, relevance, and accuracy so that you know where to allocate your time and resources.	**Leverage Built-In Workflows** Build cyber threat analysis and response processes based around ThreatConnect's built-in workflow features and integrations with leading security products.
Be a Detective You can even automate the normalization of data and don your Sherlock hat to uncover patterns by analyzing and pivoting between different data points.	**Share Threat Intelligence** With ThreatConnect you can securely share your data with your peers. You can ask them how they handled an incident for a comprehensive perspective of the threat landscape.	**Integrate Your Entire Security Infrastructure** ThreatConnect drives visibility across your security products. 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.	**Automate** Automate parts of the cybersecurity process to establish a faster, more streamlined process for a quicker response and reduced detection deficit.

Defragmentation Best Practices

In addition to implementing a cybersecurity platform, there are a number of best practices that can help your security organization get more from your defragmentation initiatives:

1. Defragmenting Your Intelligence

- **Identify a process/framework. Don't wing it.** A platform can help with this. Not only can you build processes to manage your security infrastructure from one central hub, you can leverage built-in workflow features and integrations with other leading security products to build automated cyber threat analysis and response processes.
- **Select the best intel feeds.** Your teams need to find the right mix of sources to correlate the best threat data for your organization. The best data is a combination of intel feeds, open source, and paid sources that suit your organization's particular issues, infrastructure, and security posture.
- **Work up the stack.** Don't just stop with operational indicators of compromise, strive for tactical and strategic information about adversarial actions. This can help inform wider teams and the use of and investment in security tools. Use your platform to quickly visualize and pivot to provide a richer picture of threat actors so that action can be taken.
- **Work inside-out.** Many 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.
- **Connect threat intel to vulnerabilities, controls, and risk.** Don't just focus on intelligence about threats. Determine if you are susceptible to it, if it specifically targeted at you, and then tie that knowledge into your risk management practice.

2. Defragmenting Your People

- **Create clear roles and responsibilities.**
- **Centralize knowledge and workflow.** This is ultimately what's going to crack the nut of defragmented people.
- **Concentrate on smooth interactions.** Remember "breaches happen at the seams between tools and teams," so it's critical that you ensure that hand-offs between your teams are defined. Study them. How do they work? What happens if they break down? Would you even know if they had?

3. Defragmenting Your Technology

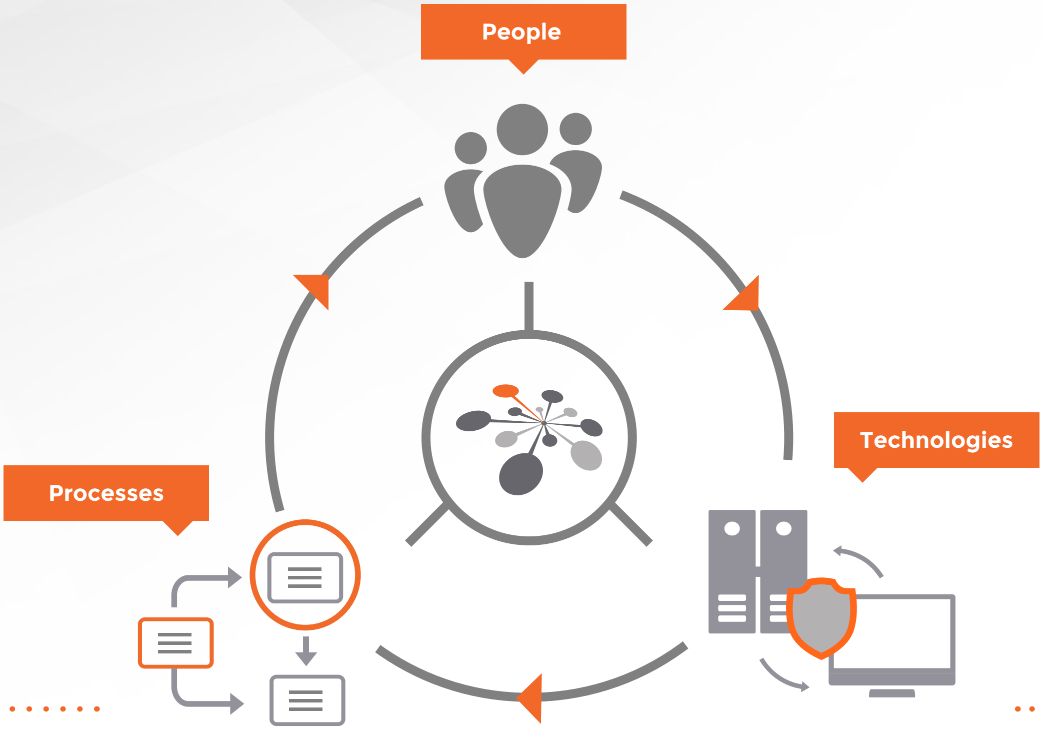
- **Improve visibility.** See what's going on in your environment – in a centralized place.
- **Build and share knowledge across technologies.** Eliminate the ineffectiveness and inefficiency of operating in silos. For example, add to knowledge gained at the endpoint, translate it to the network layer to take an action, and so on.
- **Control.** Do something based on shared knowledge at the appropriate control point. Whether it's the network layer or host layer or in between, take the appropriate measures, at the right time.
- **Orchestration.** Improve response times by taking automated, coordinated, adaptive action across technologies.

4. Defragmenting Your Processes

- **Decompose and document critical processes.**
- **Identify key tools and teams.**
- **Eliminate the seams via automation, integration, or (at least) documentation** (so that someone who's trying to do this can follow the process and figure out what's going on).
- **Test and review periodically.** As processes change, continually test and edit your workflows accordingly.

In the End

The best way to cut the detection deficit is with a cohesive, intelligent defense that unites your technologies, people, and processes, protects your assets, and narrows the detection deficit.



Using ThreatConnect and the best practices described in this paper, your organization can seamlessly leverage all of your tools and systems in unity to fight fragmentation, integrate your existing investments, run seamless, intelligence-driven security teams, and provide a central place for all of your threat intelligence.

Without it, fragmentation will continue. When nothing works together, and a bunch of discombobulated processes and technologies are thrown together, the lines between your defenders and your attackers will never converge, and the disparity between the time taken to compromise systems and your ability to discover and act on a breach will continue to widen.

THREAT CONNECT®

ABOUT THREATCONNECT

ThreatConnect, Inc.® 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**.