Building a Threat Intelligence Program

Version 1.7
Released: May 10, 2016

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author’s Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

This report is licensed by Anomali, Digital Shadows, and BrightPoint Security whose support allows us to release it for free.

All content was developed independently.

www.anomali.com www.digitalshadows.com www.bright-pointsecurity.com

Copyright

About our Licensees

Anomali delivers earlier detection and identification of adversaries in your organizations network by making it possible to correlate tens of millions of threat indicators against your real time network activity logs and up to a year or more of forensic log data. Anomali's approach enables detection at every point along the kill chain, making it possible to mitigate threats before material damage to your organization has occurred. To learn more, visit www.anomali.com and follow us on Twitter @anomalidetect.

www.anomali.com

Digital Shadows provides cyber situational awareness that helps organizations protect against cyber attacks, loss of intellectual property, and loss of brand and reputational integrity. Its flagship solution, Digital Shadows SearchLight™, is a scalable and easy-to-use data analysis platform that provides a view of an organization's digital footprint and the profile of its attackers. It is complemented with intelligence operations analyst expertise to ensure extensive coverage, relevant intelligence and frictionless deployment. SearchLight continually monitors the visible, deep and dark web and other online sources to create an up-to-the minute view of an organization and the risks requiring mitigation. The company is jointly headquartered in London and San Francisco.

www.digitalshadows.com

BrightPoint Security delivers immediate predictive insight and prescriptive responses to protect businesses from cyber threats. BrightPoint enables secure community-based threat intelligence sharing to achieve the most relevant visibility and awareness of current and emerging threats across enterprises, their digital ecosystems and infrastructures. Venture backed, the company is headquartered in San Mateo, Calif. For more information, visit www.brightpointsecurity.com.

www.brightpointsecurity.com

Building a Threat Intelligence Program

Table of Contents

Why Build a Program?

Security practitioners have been falling behind their adversaries, who launch new attacks using new techniques daily. Furthermore, defenders remain hindered by the broken negative security model: looking for attacks they have never seen before (well done, compliance mandates!), so they consistently miss new attacks. If your organization hasn't seen the attack or updated your controls and monitors to look for the latest new patterns, oh well…

Threat Intelligence has made a significant difference in how organizations focus resources on their most significant risks. Our [Applied Threat Intelligence paper]() highlighted how organizations can benefit from the misfortune of others, leveraging external information in use cases such as security monitoring/advanced detection, incident response, and even some active controls to block malicious activity.

These tactical uses certainly help advance security, but we ended Applied Threat Intelligence by pointing out that the industry needs to move past tactical TI use cases. The typical scenario goes something like this:

Furthermore, defenders remain hindered by the broken negative security model: looking for attacks they have never seen before (well done, compliance mandates!), so they consistently miss new attacks.

1. Get hit with attack.
2. Ask TI vendor whether they knew about attack before you did.
3. Buy data and pump into monitors/controls.
4. Repeat.

But that's not how Securosis rolls. Our philosophy drives a programmatic approach to security. The time has come to advance threat intelligence into the broader and more structured TI program to ensure systematic, consistent, and repeatable value. The program needs to address the dynamic changes in indicators and other signs of attacks, while factoring in the tactics the adversaries.

This *Building a Threat Intelligence Program* paper can serve as your map to design a program and systematically leverage threat intelligence. That's what this paper is all about: turning tactical use cases into a strategic TI capability to allow your organization to detect attacks faster.

The Value of TI

We have published a lot of research on TI, but let's briefly revisit the basics. What do we even mean by "benefiting from the misfortune of others"? Given the reuse of attack tactics, techniques and procedures, whether you are dealing with an opportunistic attack or something specifically targeting your organization, adversaries will likely use something that has been seen before. By leveraging the experience of those who were hit before you (likely government environments or large financials), you can recognize attacks the *first* time you see them — learning from these higher-profile targets. They (and their security vendors) figure out how they were attacked, and do the work to identify and remediate the attack. Another useful scenario for threat intel is when you didn't know about an attack because you were an early target, you can search *your* environment to see if this new attack has already been used against you, and reduce your detection time. Cool, huh?

If you haven't seen the malicious activity yet, it's likely just a matter of time; you can immediately start looking for the indicators within your active controls and security monitors. Let's briefly recap the use cases we have highlighted for Threat Intelligence:

- **Active Controls:** Threat intelligence gives you the information to block malicious activity using your active controls. When blocking traffic you need to be *very* careful, but some activities are clearly malicious and should be stopped immediately.
- **Security Monitoring:** An Achilles' Heel of security monitoring is the need to know what you are looking for. TI balances the equation a bit by expanding your view. You use indicators found by other organizations to look for malicious activity within your environment that has gone undetected or has not triggered a security alert yet.
- **Incident Response:** Our last major use case is streamlining incident response. Once adversary activity is detected within your environment, you have a lot of ground to cover to find the root cause of the attack and contain it quickly. TI provides clues to determine the business risk of an attack, by provide perspective on who is attacking you, their motives, what they are after and their tactics — enabling your organization to focus its response.

The TI Team

Threat Intelligence isn't new. Security vendors have been using dynamic data in their own products and services for a long time. The difference is in treating the data as a distinct product from other products and services. But raw data doesn't detect adversaries or block attacks, so mature security organizations have been staffing up threat intelligence groups, tasking them with providing context on which of the countless threats out there actually need to be dealt with *now* — and what needs to be done to prevent, detect, and investigate potential attacks. These internal TI organizations consume external data (both open source and commercial) to supplement internal collection and research efforts.

The TI Program

Organizations which build their own TI capabilities eventually need a repeatable process to collect, analyze, and apply the information on an ongoing, strategic basis, helping to align the business risk with appropriate threat measures and allocate scarce security resources in the most effective manner. We'll outline the structure of such a program here, and dig into each aspect of the process through this paper.

1. **Gathering Threat Intelligence:** This step focuses your efforts on reliably finding intelligence sources that can help you identify your adversaries, and determining the most useful specific data types — such as malware indicators, compromised devices, IP reputation, command and control indicators, etc. Then procure the data you need and integrate it into a system/platform to use TI. A programmatic process will cover identifying new and interesting data sources, constantly tuning the use of TI within your controls, and evaluating sources based on effectiveness and value.

2. **Using TI:** Once you have aggregated TI you can put it into action before the value of the data erodes. The key difference between tactical use of TI, and strategic use within a program, is the policies and rules of engagement that govern how and when you use it. Tactically you can be a bit less structured about using data, because you don't need to be consistent, but structure is a necessity to evolve a program and leverage the data in the most efficient manner.

3. **Defining and Communicating Success:** When building a tactical threat intelligence initiative you focus on solving a specific problem and then move on to the next one. Broadening the use of TI requires specific and ongoing evaluation of effectiveness and value by defining metrics and benchmarks to quantify the value of your program. The key here is to defining success criteria for the program, gather data to substantiate results, and communicate those results — just like any other business function.

4. **Sharing Intelligence:** If there is one thing that tends to be overlooked when focusing on how intelligence can help you, it is how sharing intelligence can help others… and eventually you again. This is more than a bit ironic, considering that the power of TI comes from organizations' willingness to share information both about the specific indicators as well as pointers as to disrupting adversaries and remediating attacks. But even assuming you want to share TI, it needs to be safe and secure, to protect your interests and control organizational liability.

Gathering Threat Intelligence

You begin building your program by digging into the mechanics, thinking strategically and systematically about how to benefit from the misfortune of others and make the best use of TI. It's hard to use TI you don't actually have yet, so the first step is to gather the TI you need.

Defining TI Requirements

After years of being unable to procure security data, you now have a ton of options for external security data. The threat intelligence market has exploded over the past year. Dozens of emerging companies offer various kinds of security data, and many existing security vendors are trying to introduce TI services to capitalize on the hype. We also see a number of new companies with offerings to help collect, aggregate, and analyze TI. But we aren't interested in hype — what new products and services can improve your security posture? With a wide variety of options, how can you choose the most effective TI for your needs?

As always we suggest you start by defining your problem, and then identify the offerings that would help you solve it most effectively. Start with your primary use case for threat intel. Basically, what is the catalyst to spend money? That's the place to start. Our research indicates this catalyst is typically one of a handful of issues:

1. **Attack prevention/detection:** This is the driver of most TI investment. You can't keep pace with adversaries, so you need external security data to tell you what to look for, and perhaps block. This budget tends to be associated with advanced attackers, so if there is concern about them within the executive suite, this is likely the best place to start.

2. **Forensics:** If you have a successful compromise you will want TI to help narrow the focus of your investigation. This process is outlined in our Threat Intelligence + Incident Response research.

3. **Hunting:** Some organizations have teams tasked with finding evidence of adversary activity within the environment, even if existing alerting/detection technologies don't spot anything. These skilled practitioners use new malware indicators and patterns from a TI service to search for malicious activity within the network, then can also use the latest adversary intelligence to recognize behaviors of specific actors before they act overtly (and trigger traditional detection).

Once you have identified primary and secondary use cases, focusing on potential adversaries can yield additional information about the types of attacks and tactics you are likely to see. Each TI provider — both platform and pure data vendors — specializes in specific adversaries or target types. Take a similar approach with adversaries: understand who your primary attackers are likely to be, and find providers with expertise in tracking them. To be clear, getting a heads-up on specific attacks is critical to protecting your environment, so that takes priority. But adversary-specific information can help refine your actions as a result of the threat intelligence.

The last part of defining TI requirements is deciding how you will use the data. Will it trigger automated blocking on active controls, as described in Applied Threat Intelligence? Will data be pumped into your SIEM or other security monitors for alerting as described in Threat Intelligence and Security Monitoring? Will TI only be used by advanced adversary hunters? You need to answer these questions to understand how to integrate TI into your monitors and controls.

When thinking about threat intelligence programmatically, consider not just how you can use TI today, but also what you want to do further down the line. Is automatic blocking based on TI realistic? This impacts what kind of threat intel you buy and how you use it. Aspirational thinking can drive flexibility, and produce better options moving forward. Don't get tied down to a specific TI data source, and ideally not even to a specific aggregation or threat intelligence platform. A TI program is about how to leverage data in your security program, not how to use today's data services and TI aggregation platforms. That's why we suggest focusing on requirements first, and then finding optimal solutions for this point in time.

Budgeting

After you define what you need from TI, how will you pay for it? We know that's a pesky detail, but it is important as you set up a TI program to figure out which executive sponsors will support it and whether that funding source is sustainable.

When a breach happens, a ton of money gets spent on anything and everything to make it go away. There is no resistance to funding security projects, until there is — which tends to happen once the road rash heals a bit. So you need to line up support for using external data and ensure you have a funding source who sees the value of investment, both now and in the future.

When a breach happens, a ton of money gets spent on anything and everything to make it go away. There is no resistance to funding security projects, until there is — which tends to happen once the road rash heals a bit.

Depending on your organization, security may have its own budget to spend on key technologies; in that case you just build the cost into the security operations budget, because TI is sold on a subscription basis. If you need to associate specific spending with specific projects, you'll need to find the right budget sources. We suggest you stay as close to advanced threat prevention/detection as you can, because that's the easiest case to make for TI.

How much money do you need? Of course that depends on the size of your organization. At this point many TI data services are priced at a flat annual rate, which is great for a huge company which can leverage all that data. If you have a smaller team you'll need to work with the vendor on lower pricing or different pricing models, or look at lower-cost alternatives.

As you build out your program it makes sense to talk to some TI providers to get preliminary quotes on their services. Don't engage in a sales cycle before you are ready, but you and any potential executive sponsor need a feel for current pricing.

While we are discussing money, this is a good time to start thinking about how to quantify the value of your TI investment. At some point the bean counters in Accounting will want to know what they are getting for the checks you are writing for data. You defined your requirements, so within each use case how do you substantiate value? Is it about the number of attacks you block based on that data? Or perhaps an estimate of how adversary dwell time or time to detect/remediate decreased once you were able to search for activity based on the TI? It's never too early to start defining success criteria, deciding how to quantify success, and ensuring you have adequate metrics to substantiate achievements. This is a key topic, so we will dig in later in this paper.

> It's never too early to start defining success criteria, deciding how to quantify success, and ensuring you have adequate metrics to substantiate achievements.

Selecting Data Sources

Next start to gather data to help you identify and detect the activity of potential adversaries in your environment. You can get effective threat intelligence from a variety of different sources. We divide threat intelligence data into five high-level categories:

- **Compromised Devices:** This data source provides external notification that a device is acting suspiciously by communicating with known bad sites or participating in botnet-like activities. Services are emerging to mine large volumes of Internet traffic to identify such devices.

- **Malware Indicators:** Malware analysis continues to mature rapidly, getting better and better at understanding exactly what malicious code does to devices. This enables you to define both technical and behavioral indicators across all platforms and devices to search for within your environment, as Malware Analysis Quant described in gory detail.

- **IP Reputation:** The most common reputation data is based on IP addresses and provides a dynamic list of known bad and/or suspicious addresses, based on things like spam sources, Torrent usage, DDoS traffic indicators, and web attack origins. IP reputation has evolved since its introduction, and now features scores to compare the relative maliciousness of different addresses, factoring in additional context such as Tor nodes/anonymous proxies, geolocation, and device ID to further refine reputation.

- **Malicious Infrastructure:** One specialized type of reputation often packaged as a separate feed is intelligence on Command and Control (C&C) networks and other servers/sources of malicious activity. These feeds track global C&C traffic and pinpoint malware originators, botnet controllers, compromised proxies and other IP addresses and sites to watch for as you monitor your environment.

- **Phishing Messages:** Most advanced attacks seem to start with a simple email. Given the ubiquity of email and the ease of adding links to messages, attackers typically use email as the path of least resistance to a foothold in your environment. Isolating and analyzing phishing email can yield valuable information about attackers and tactics.

These security data types are available in a variety of categories. Here are the main categories:

- **Commercial Integrated:** Every security vendor seems to have a research group providing some type of intelligence. This data is usually very tightly integrated into their product or service. Sometimes there is a separate charge for the intelligence, while other times it is bundled into the product or service.

- **Commercial Standalone:** We see an emerging security market for standalone threat intel. These vendors typically offer an aggregation platform to collect external data and integrate into controls and monitoring systems. Some also gather industry-specific data because individual attacks tend to cluster around specific industries providing a bundle of both data and the technology to analyze and use it.

- **ISAC:** Information Sharing and Analysis Centers are industry-specific organizations that aggregate data across an industry to share among members. The best known ISAC is for the financial industry, but many other industry associations are spinning up their own.

- **OSINT:** Open source intel encompasses a variety of publicly available sources for things like malware samples and IP reputation, which can be integrated directly into other systems.

The best way to figure out which data sources are useful is to actually use them. Yes, that means a proof of concept. You can’t look at all the data sources, but pick a handful and start looking through their feeds. Perhaps integrate data into your monitors (SIEM and IPS) in alert-only mode, and see what you’d block or alert on to get a feel for its value. Is the interface one you can use effectively? Does it take professional services to integrate the feed into your environment? How often is the data updated? Can you use it to drill down into specific devices and identify compromised devices? Does a TI platform provide enough value that you would look at it every day, in addition to the 5-10 other consoles you need to deal with? Will the platform allow you to create a customized framework for your TI program? These are all questions you should be able to answer before you write a check.

Company-specific Intelligence

Many early threat intelligence services focused on general security data, identifying malware indicators and tracking malicious sites. But how does that apply to your environment? That is where the TI business is going. Providing more context for generic data, applying it to your environment (typically through a threat intel platform), and having researchers focus specifically on your organization.

This company-specific information comes in a few flavors, including:

- **Brand Protection:** Misuse of a company's brand can be very damaging. So proactively looking for unauthorized brand uses (like on phishing sites) or negative comments on social media can help shorten the window between negative information appearing and getting it taken down.
- **Attacker Networks:** Internal detection capabilities fail, so sometimes you have compromised devices you don't know about. These services mine command and control networks to look for your devices. Obviously it's late if you find your device actively participating, but better to find it *before* your payment processor or law enforcement tells you about your problem.
- **Third-party Risk:** Another type of interesting information is about business partners. This isn't necessarily direct risk, but knowing that you connect to networks with security problems can tip you to implement additional controls on those connections, or more aggressively monitor data exchanges with a partner.

The more context you can derive from TI, the better. For example, if you are part of a highly targeted industry, information about attacks in your industry can be particularly useful. It's also great to have a service provider proactively look for *your* data in external forums, and watch for indications that *your* devices are being used in attacker networks. But this context comes at a cost: you need to evaluate the additional expense of custom threat information, and your own ability to act on identified issues. Additional context is useful, but only if your security program and staff can take advantage of it by integrating it into your program in an automated fashion.

Managing Overlap

If you use multiple threat intelligence sources you will want to make sure you don't generate duplicate alerts. Key to determining overlap is understanding how each intelligence vendor gets its data. Do they use honeypots? Do they mine DNS traffic and track new domain registrations? Have they built a cloud-based malware analysis/sandboxing capability? You can categorize vendors by their tactics to make sure you don't pay for redundant data sets.

There is value in terms of finding common intelligence across providers and within your environment. But that also creates noise, so the data doesn't necessarily need to be discarded, rather the alerts consolidated to ensure you are focusing on the attacks presenting the most significant risks.

Be careful not to fall for marketing hype about proprietary algorithms, big data analysis, staff linguists penetrating hacker dens, or other stories straight out of a spy novel. Make sure you do your diligence by putting each provider through its paces before you commit.

This is a good use for a TI platform, aggregating intelligence and cutting out noise so you only see actionable alerts. As described above, you'll want to test these services to see how they work for you. In a crowded market vendors try to differentiate by taking liberties with what their services and products actually do. Be careful not to fall for marketing hype about proprietary algorithms, big data analysis, staff linguists penetrating hacker dens, or other stories straight out of a spy novel. Make sure you do your diligence by putting each provider through its paces before you commit.

Our last point on external data in your TI program concerns short agreements, especially up front. You cannot know how these services will work for you until you actually start using them. Many threat intelligence companies are startups, and might not be around in 3-4 years (or may be acquired by companies you don't want to do business with). Once you identify a set of core intelligence feeds that work consistently and effectively you can look at longer deals, but we recommend not doing that until your TI process matures and your intelligence vendor establishes a track record.

Scaling Context

One of the things to keep in mind is the sheer number of indicators that come into play, especially when using multiple threat intelligence services. You could be looking at thousands of new indicators every day and millions in the aggregate. Why does this matter? It's a scaling thing. Remember that when you are operationalizing the use of TI, every indicator is pretty much a signature. We all know what happens when you add millions of new signatures a day (AV fail, anyone)? So we need to make sure we aren't repeating the same issues we had with yesterday's security technologies.

Context is about knowing if the threat is relevant to the organization, but also about the behavior and severity of the threat as it relates to your organization. Thus, make sure you build a step into your TI process to provide context for these threat intelligence feeds before you add them to your monitors and/or active controls. Tailor what you feed into your TI platform (as we will discuss later in this paper), so that searching and indexing are only performed for intelligence sources relevant to your organization. As a trivial example, if you only have Macs on your network, a bunch of TI indicators for Windows Vista attacks will just clutter up your system and reduce performance.

It's a classic funnel. There are millions of indicators you can get via a TI service. Perhaps only hundreds apply to your environment. Do some pre-processing of the TI as it comes in to get rid of data that isn't relevant, make your actual alerts more actionable, and help you prioritize efforts on attacks that present real risk.

Using Threat Intelligence

Now let's document a programmatic approach for using TI to improve your security posture and accelerate your response & investigation functions. To reiterate, TI enables you to benefit from the misfortune of others. It is likely other organizations will get hit by any attack before you, so you might as well learn from their experience. This is the basis for the classic quote, "Wise men learn from their mistakes, but wiser men learn from the mistakes of others." But knowing what's happened to others isn't enough. You must be able to use TI in your security program to benefit.

We have plenty of security data available today. So the first step in your program is to gather the appropriate security data to address *your* use case. That requires a strategic view of your data collection process, both internally (collecting your own data) and externally (aggregating threat intelligence). As we described earlier, you need to define your requirements (use cases, adversaries, alerting or blocking, integrating with monitors/controls, automation, etc.), select the most useful sources, and then budget for access to the data.

Aggregating TI

When aggregating threat intelligence, the first decision is where to put the data. You need it somewhere it can be integrated with your key controls and monitors, securely and reliably. Even better if you can gather metrics regarding which data sources are the most useful to optimize your spending. Start by asking some key questions.

- **Platform:** To platform or not to platform? Do you need a standalone platform or can you leverage an existing tool like a SIEM or an advanced endpoint detection offering? Of course it depends on your use cases, the scale of the number of TI sources you want to include, and the amount of manipulation and analysis you need to make your TI useful.

- **Portal:** Should you use your provider's portal? Each TI provider offers a portal you can use to get alerts, manipulate data, etc. Will it be good enough to solve your problems? Do you have an issue with some of your data residing in a TI vendor's cloud? Or do you need the data to be pumped into your own systems, and how will that happen?

- **Integration:** How will you integrate the data into your systems? If you need to leverage your own systems, how will the TI get there? Are you depending on a standard format like STIX or TAXII? Do you expect out-of-the-box integrations? Is there a well documented API to build these integrations?

Obviously these questions are pretty high-level, and you may need a couple dozen follow-ups to fully understand the situation.

Selecting the Platform

In a nutshell, if you have a dedicated team to evaluate and leverage TI, have multiple monitoring and/or enforcement points, or want more flexibility in how broadly you use TI, you should probably consider a separate intelligence platform or 'clearinghouse' to manage TI feeds. Assuming that's the case, your key selection criteria when selecting a stand-alone threat intelligence platform are:

1. **Open:** The TI platform's task is to aggregate information, so it must be easy to get information into it. Intelligence feeds are typically just data (often XML), and increasingly distributed in industry-standard formats such as STIX to make integration relatively straightforward. But make sure any platform you select will support the data feeds you need. Be sure you can use the data that's important to you, and not be limited by your platform.

2. **Scalable:** You will use a lot of data in your threat intelligence process, so scalability is essential. As described before, you can be looking at 1000s of new indicators *every day*, and will inevitably have to process and analyze millions of indicators. But computational scalability is likely more important than storage scalability — you will be processing the indicators on the way in to provide proper context and also intensively searching and mining aggregated data, so you need robust indexing. Unfortunately scalability is hard to test in a lab, so ensure your proof of concept testbed is a close match for your production environment, and that you can extrapolate how the platform will scale in production.

3. **Search:** Threat intelligence, like the rest of security, doesn't lend itself to absolute answers. So make TI the beginning of your process of figuring out what happened in your environment, and leverage the data for your key use cases as we described earlier. One clear requirement for all use cases is search. Be sure your platform makes searching all your TI data sources easy.

4. **Scoring:** Using Threat Intelligence is all about betting on which attackers, attacks, and assets are most important to worry about, so a flexible scoring mechanism offers considerable value. Scoring factors should include assets, intelligence sources, and attacks, so you can calculate a useful urgency score. It might be as simple as red/yellow/green, depending on the needs of your security program.

5. **Workflow:** Does the platform offer a structured way to investigate an attack, processing both the TI and leveraging internal security systems to streamline the detection process? You want the TI platform to provide as much help in both hunting and detection.

Key Use Cases

Our previous TI research focused on how to address these key use cases, including preventative controls (FW/IPS), security monitoring, and incident response. But a programmatic view requires expanding the general concepts around use cases into a repeatable structure to ensure ongoing efficiency and effectiveness.

The general process for integrating TI into your use cases is consistent, with some variations we will discuss under specific use cases.

1. **Integrate:** The first step is to integrate the TI into your tools for each use case, which could be security devices or monitors. That may involve leveraging the management consoles of the tools to pull in the data and apply the controls. For simple TI sources such as IP reputation this direct approach works well. For more complicated data sources you'll want to perform some aggregation and analysis on the TI before updating running rules. In that case you'll expect your TI platform for integrate with your tools.

2. **Test and Trust:** The key here is trustable automation. You want to make sure any rule changes driven by TI go through a testing process before being deployed for real. That involves monitoring mode on devices, and ensuring changes won't cause excessive false positives or take down any networks in the case of preventative controls. Given the general resistance of many network operations folks to automation, it may be a while before everyone trusts automatic changes, so factor that into your project planning.

3. **Tuning via Feedback:** In our dynamic world the rules that work today and the TI that is useful now will both need to evolve. So you'll constantly be tuning your TI and rulesets to optimize effectiveness and efficiency. You are never done, and will constantly need to tune and assess new TI sources to ensure your defenses stay current.

See our Applied Threat Intelligence research for granular process maps for integrating threat intelligence with each use case.

> We want to use TI to block recognized attacks, but not cause an explosion of false positives or adversely impact availability. You only get one opportunity to take down your network with an automated TI-driven rule set, so make sure you are ready before you deploy blocking rules.

Preventative Controls

The goal when using TI within a preventative control is to use external data to determine what to look for before it impacts your environment. By 'preventative' we mean any control that is inline and can prevent attacks, not just alert. These include:

- **Network Security Devices:** This category encompasses firewalls (including next-generation models) and Intrusion Prevention Systems. But you might also include devices such as Web Application Firewalls, which operate at different levels in the stack but are inline and can block attacks.

- **Content Security Devices/Services:** Web and email filters can also function as preventative controls because they inspect traffic as it passes through, and can enforce policies to block attacks.

- **Endpoint Security Technologies:** Protecting an endpoint is a broad mandate, and may include traditional endpoint protection (anti-malware) and newfangled advanced endpoint protection technologies such as isolation and advanced heuristics.

We want to use TI to block recognized attacks, but not cause an explosion of false positives or adversely impact availability.

The greatest sensitivity, and the longest period of testing before trust, are needed for preventative controls. You only get one opportunity to take down your network with an automated TI-driven rule set, so make sure you are ready before you deploy blocking rules.

Security Monitoring

Our next case uses Threat Intelligence to make security monitoring more effective. As we have written countless times, security monitoring is necessary because you simply *cannot* prevent everything, so you need to get better and faster at responding. Improving detection is critical to effectively shortening the window between compromise and discovery.

Why is this better than just looking for well-established attack patterns like privilege escalation or reconnaissance, as we learned in SIEM school? The simple answer is that TI data identifies attacks happening right now on other networks. Attacks you otherwise wouldn't see or know to look for until too late. In a security monitoring context leveraging TI enables you to focus validation/triage efforts, detect faster and more effectively, and ultimately make better use of scarce resources which need to be directed at the most important current risks.

- **Aggregate Security Data:** Internal security data is the foundation of any security monitoring process. Before you can worry about external threat intel you need to enumerate devices to monitor in your environment, scope out the kinds of data you will get from them, and define collection policies and correlation rules. Once this data is available in a repository for flexible, fast, and efficient search and analysis, you are ready to start integrating external data.

- **Security Analytics:** Once the TI is integrated, you let the advanced math of your analytics engine do its magic, correlating and alerting on situations that warrant triage and possibly deeper investigation.

- **Action/Escalation:** Once you have an alert, and have gathered data about the device and attack, you need to determine whether the device was actually compromised or the alert was a false positive. Once you verify an attack you'll have a lot of data to send to the next level of escalation — typically an incident response process.

Your margin for error is a bit larger when integrating TI into a monitoring context than a preventative control, but you still don't want to generate a ton of false positives and have operational folks running around chasing then. Testing and tuning processes remain critical to ensure that TI provides sustainable benefit instead of just creating more work. We keep repeating this last point because it's important.

Incident Response

Similar to the way threat intelligence helps with security monitoring, you can use TI to focus investigations on the devices most likely to be impacted, help identify adversaries, and lay out their tactics to streamline your response. To revisit the general steps of an investigation, here's a high-level view of incident response:

- **Phase 1: Current Assessment:** This involves triggering your process and escalating to the response team, then triaging the situation to figure out what's really at risk. A deeper analysis follows to prove or disprove your initial assessment and figure out whether it's a minor issue or a raging fire.

- **Phase 2: Investigate:** Once your response process is fully engaged, you need to get the impacted devices out of harm's way by quarantining them and taking forensically clean images with a documented chain of custody. Then you can start to investigate the attack more deeply to understand your adversary's tactics, build a timeline, and figure out what happened and what was lost.

- **Phase 3: Mitigation and Cleanup:** Once you have completed your investigation you can determine the appropriate mitigations to eradicate the adversary from your environment and clean up the impacted parts of the network. The goal is to return to normal business operations as quickly as possible. You'll want a post-mortem after the incident is taken care of, to learn from your issues and make sure they don't happen again.

The same concepts apply as in other use cases. You'll want to integrate the TI into your response process, typically looking to match indicators and tactics against specific adversaries to understand their motives, profile their activities, and get a feel for what is likely to come next. This helps you determine the level of mitigation necessary, and whether you need to involve law enforcement.

> The final aspect of the program is optimizing which data sources you use — especially the ones you pay for. Your system should be tuned to normalize and reduce redundant intelligence, so you'll need a process to evaluate the usefulness of your TI feeds.

Optimizing TI Spending

The final aspect of the program is optimizing which data sources you use — especially the ones you pay for. Your system should be tuned to focus on the most actionable intelligence, so you'll need a process to evaluate the usefulness and effectiveness of your TI feeds. Obviously you should avoid overlap when buying feeds, so understand how each intelligence vendor gets their data. Do they use honeypots? Do they mine DNS traffic and track new domain registrations? Have they built a cloud-based malware analysis/sandboxing capability? Categorize vendors by their tactics to help find the best fit for your requirements.

Once the initial data sources are integrated into your platform and/or controls, you'll want to start tracking effectiveness. How many alerts are generated by each source? Are they legitimate? The key here is your ability to track this data, and if these capabilities are not built into your platform you'll need to manually instrument the system to extract this data. Sizable organizations invest substantially in TI data, and you want to make sure you get a suitable return on your investment.

At this point you have a systematic program in place to address your key use cases with threat intelligence. But taking your TI program to the next level requires you to think outside your contained world. That means becoming part of a community to increase the velocity of your feedback loop, and become a contributor to the TI ecosystem rather than just a taker.

At this point you have a systematic program in place to address your key use cases with threat intelligence. But taking your TI program to the next level requires you to think outside your contained world. That means becoming part of a community to increase the velocity of your feedback loop, and become a contributor to the TI ecosystem rather than just a taker.

Success and Sharing

As we wrap up program development, let's briefly jump back to the beginning. How do you define success for your program? More important, how can you kickstart your program with a high-profile success to show the value of integrating external data into your defenses, and improve your security posture? Get a quick win, and then publicize it.

Quick Win

The lowest-hanging fruit in threat intel is finding an adversary already in your environment who you didn't know about. Of course it would be better if you *didn't* have an active adversary inside your defenses, but that scenario is frankly unlikely. The reality is that some devices in your environment are already compromised — it's just a question of which.

> The lowest-hanging fruit in threat intel is finding an adversary already in your environment who you didn't know about.

You are already doing security monitoring (you can thank compliance for that), so it's just a matter of searching the existing repository of security data for indicators from your threat feeds. Any log aggregation or SIEM platform can perform a search like this. Of course it's a manual process, and that's fine for right now — you're just looking for a quick win.

Once you complete the search, one of two things happens. Perhaps you found an active adversary you didn't know about. You can drop the proverbial mic at this point — you have clearly proven the value of external threat intel. But before you spend a lot of time congratulating yourself, you have an incident response to get moving. Obviously you'll document it, and be able to tell a compelling story of how TI was instrumental in identifying the attack earlier than you would have discovered it otherwise.

If you don't find a smoking gun you'll need to be a bit more creative. We suggest loading up a list of known bad IP addresses into your egress firewall and looking for the inevitable traffic to those sites, which may indicate C&C nodes or other malicious activity. The value here isn't as pronounced as finding an active adversary, but it illustrates your new ability to find malicious traffic sooner using a TI feed.

Keep in mind that a Quick Win is just that. It shows short-term value from an investment in threat intel. This should take place during any proof of concept you run with TI vendors during procurement. If you aren't getting immediate value, either you are using the wrong data source or tool, or you already had a strong security posture and might get better short-term value from another project.

Sustained Success

We didn't call this paper "Getting a Quick Win with TI," so we need to expand our aperture a bit and focus on turning your quick win into sustainable success. There are three main aspects of building out the program from a quick win:

1. **Operationalizing TI:** We suggested earlier in this paper that you start by integrating TI into your security monitoring environment. Once that is operational you can add additional use cases, such as integrating into your perimeter gateways and egress filters for proactive blocking, and further leveraging the data within your incident response process.

Executing on a successful security program requires significant planning and consistent execution. You cannot afford to focus only on the latest attack or incident (although you also need to do some of that), but must also think and act strategically.

2. **Evaluating TI Sources:** This is key to optimizing your program. You cannot just assume the data source(s) you selected will continue to provide the same impact. Things change, including adversaries and TI providers. You are under constant scrutiny for how your security program is performing, so your TI vendors (actually *all* your vendors) will be under similar scrutiny. You should be able to close the loop by tracking TI, to alerts, to blocked or identified attacks, by instrumenting your security environment. Some commercial TI platforms offer this information directly, but alternately you could build it into your SIEM or other controls.

3. **Selling the Value:** Senior executives, including your CIO, have a lot of things to deal with every day. You cannot count on them remembering much beyond the latest fire to appear in their inbox today. You need to systematically produce reports that show the value of TI. This should be straightforward using your instrumentation for evaluating TI sources. This is another topic to cover in your periodic meetings with senior management. Especially when the renewal is coming up and you need to keep the funding.

Executing on a successful security program requires significant planning and consistent execution. You cannot afford to focus only on the latest attack or incident (although you also need to do some of that), but must also think and act strategically. Here a programmatic approach pays huge dividends. To really magnify your impact you'll need to move beyond tactical day-to-day security battles, and implement a program for both TI and security activities in general.

Sharing

Threat intelligence hinges on organizations sharing information about adversaries and tactics, so everyone can benefit from survived attacks. For years this information sharing seemed like an unnatural act to enterprises. A number of threat intelligence vendors emerged to fill the gap, gathering data from a variety of open and proprietary sources. But we see gradual growth in the willingness of organizations to share information with other organizations of similar size or within an industry. Of course threat information can be sensitive, so sharing with care and diligence are critical.

The first decision point for sharing is the constituency to share with. This can be a variety of organizations, including:

1. **ISAC:** Many larger industries are standing up their own Information Sharing and Analysis Centers (ISAC), either as part of an industry association or funded by the larger companies in the industry. ISACs are objective, exist to provide a safe place to collect and share industry threat information, and offer value-added data analysis. If there is an ISAC for your industry we recommend you participate.

2. **Commercial Vendors:** We increasingly see threat detection vendors asking customers to share information about what they see to make their products and services more accurate and useful. This is usually opt-in (ask if it is not specifically mentioned) and we see very little risk in sharing data with vendors. Not because we *enjoy* the idea of a vendor monetizing your data without compensation, but because it helps make their product or service better, and *you* benefit from others doing the same.

3. **Trading Partners:** If your industry doesn't have a formal ISAC, or you cannot afford to participate, you will likely need some kind of semi-formal means of sharing information. This can be challenging due to both the technology platform requirements (threat information must be shared securely) and legal agreements required to establish a sharing partnership (lawyers are fun!). That doesn't mean you won't do it, but understand that it's not easy and requires a 1:1 agreement with each trading partner.

4. **Informal Contacts:** Many security practitioners share information informally with friends and colleagues — we call this water cooler TI. If you are plugged into your local community, you probably send a note to a buddy when you find something interesting, and *vice-versa*. It's a bit like hanging out at the water cooler, sharing indicators with pals. As long as there isn't anything proprietary or possibly damaging to your organization, sharing with contacts can provide excellent value on both sides. But this requires a lot more manual processing because you don't get a machine-readable feed. Unless your pals talk STIX and TAXII — and yes, that was a TI joke.

Sharing Securely

Once you figure out who you will share threat intelligence with, you need to figure out how you'll do it securely. Each of the various types of TI can be useful when shared, so there are plenty of data types in play. You will likely want some kind of platform you can use to aggregate threat intel and provide secure access. Perhaps it will be handled through a secure web service which ensures only authorized partners have access. Or you might be able to host a subset of your threat intelligence where a trading partner can access it directly from your TI platform.

Either way there are a couple key considerations to ensuring this kind of sharing is done securely, and below are a few questions to answer before embarking on a sharing initiative. Yes, we know they read like Security 101.

1. **Authentication:** Who will access the system? How will you manage entitlements? Is this something you need to use existing identity and access management systems to provide? Will you require multi-factor authentication? What about machine-to-machine sharing via APIs and/or standard protocols? What is the process to deprovision a partner and remove access?

2. **Authorization:** What types of data/TI sources can each partner access? How will you manage entitlements, including new partners and changes in authorization?

3. **Data Protection:** How is your data anonymized and/or protected? Is it encrypted so unauthenticated or unauthorized users cannot access it?

4. **Logging Activity:** How will you track which partner looked at what information? You should be able to see which partners contributed content to make sure you have some balance — especially in an informal situation.

Sharing information securely between trading partners is complicated, so make sure you ask the right questions before you start sharing information.

As you can see, sharing information securely between trading partners is complicated, so make sure you ask the right questions before you start sharing information. As with the rest of developing a TI program, it is critical to develop feedback loops and a mechanism for evaluating the value of your information sharing partnerships. You should have objective criteria for deciding whether sharing threat intelligence makes sense for your organization over time, whether you are paying for it or not.

Summary

The only truism in threat prevention is that *you can't*. The attack surface you need to protect is too vast. The tools your adversaries use have been optimized to evade detection. And you can't find enough skilled security resources to keep pace with the attacks. So you need to be much smarter about what you do, and much more diligent about responding quickly to attacks in progress.

But you still largely need to know what to look for in order to detect malicious activity. The value of threat intelligence is in peeking outside your little corner of the world, seeing attacks and patterns being used against other organizations. The increasing pervasiveness and maturity of threat intelligence data, and the ability to quickly integrate into your detection and hunting tools, make security efforts more efficient and effective.

> Executing consistently and effectively doesn't just happen. You need a structured plan and process to perform the right security activities systematically.

Executing consistently and effectively doesn't just happen. You need a structured plan and process to perform the right security activities systematically. This paper covers what's involved in both gathering threat intelligence and using it to improve your security program.

No collection of threat intelligence sources or tools can ever replace a skilled team of security professionals. But you can make your professionals much more effective by establishing the right processes, and giving them tools and support to do what they do best. Whether it's giving them a head start by identifying IP addresses typically associated with malicious activity, or looking for indications of adversary activity on devices, you can supercharge their efforts by benefiting from the misfortune of others who have already been hit by attacks.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com.

About the Analyst

Mike Rothman, Analyst and President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.