GuidePoint SECURITY
GOVERNMENT SOLUTIONS

WHITE PAPER

How to Effectively Use Threat Intelligence to Drive Better Security Outcomes

Threat intelligence (TI) has become a major focus of cybersecurity in the last several years. Threat Intelligence Units (TIUs), are being created and stood up to support Security Operations Centers (SOCs) and network defense teams in larger enterprises everywhere. There is good reason for this, as TI has evolved into more than signatures of MD5 file hashes and IP addresses seen in the wild used by adversaries.

Unfortunately TIUs have become more about collecting and combining as many sources as possible to throw at tools and SIEMs. A sense of accomplishment and security is achieved, but the TIU does not provide timely and relevant information for SOCs and CxOs to make informed decisions – and thus a different approach is needed.

This paper will:

- Break down the three operational focus areas
- Present the issues which typically hinder these areas
- Provide strategies to overcome the challenges

in partner with

CROWDSTRIKE

A disjointed and fractured approach leads to an overload of alerts for SOC teams to address. Rather than guiding and informing the organization proactively at all levels, the end result is a lack of quality and an overload of quantity TI with no big picture for clarity. This has caused confusion about what proactive actions need to be taken to protect the organization from threats and adversaries.

To understand threat intelligence completely, this paper will break down three operational focus areas, the issues which typically hinder these areas and some strategies to overcome these challenges – all with the goal of helping improve the use of threat intelligence within the organization to ultimately drive better security outcomes.

Understanding Threat Intelligence Focus Areas

Threat Intelligence is a complex discipline that spans across three operational focus areas:

1. **Machine-readable threat intelligence** or signatures are simply different artifacts that are known to be bad. Classic examples are malicious file MD5 hashes and attacker command and control (C2) IP addresses. If these are spotted on the network or endpoint, a SOC immediately knows that malicious activity is happening. More complex TI Indicators of Compromise (IOCs) include:

   - Snort rules
   - Bro/Zeek rules
   - Yara rules
   - SIEM correlations

   Some vendors add a different type of machine-readable threat intelligence IOCs that can go deeper into an endpoint system to find such things as registry keys, WMI changes and specific application behaviors.

What is a threat actor?

A threat actor is a known organization or person that has documented history of attacks. They can come in several different forms:

- Nation State
- Criminal Enterprise
- Politically Motivated Organization
- For Hire Free Lancer

2. **Predictive research** is when a TIU is able to identify a threat actor's intent before they strike the first time, or a reason to research if that threat actor has begun an attack before evidence is found within the organization's monitoring apparatus. There are three ways to acquire this predictive research intel:

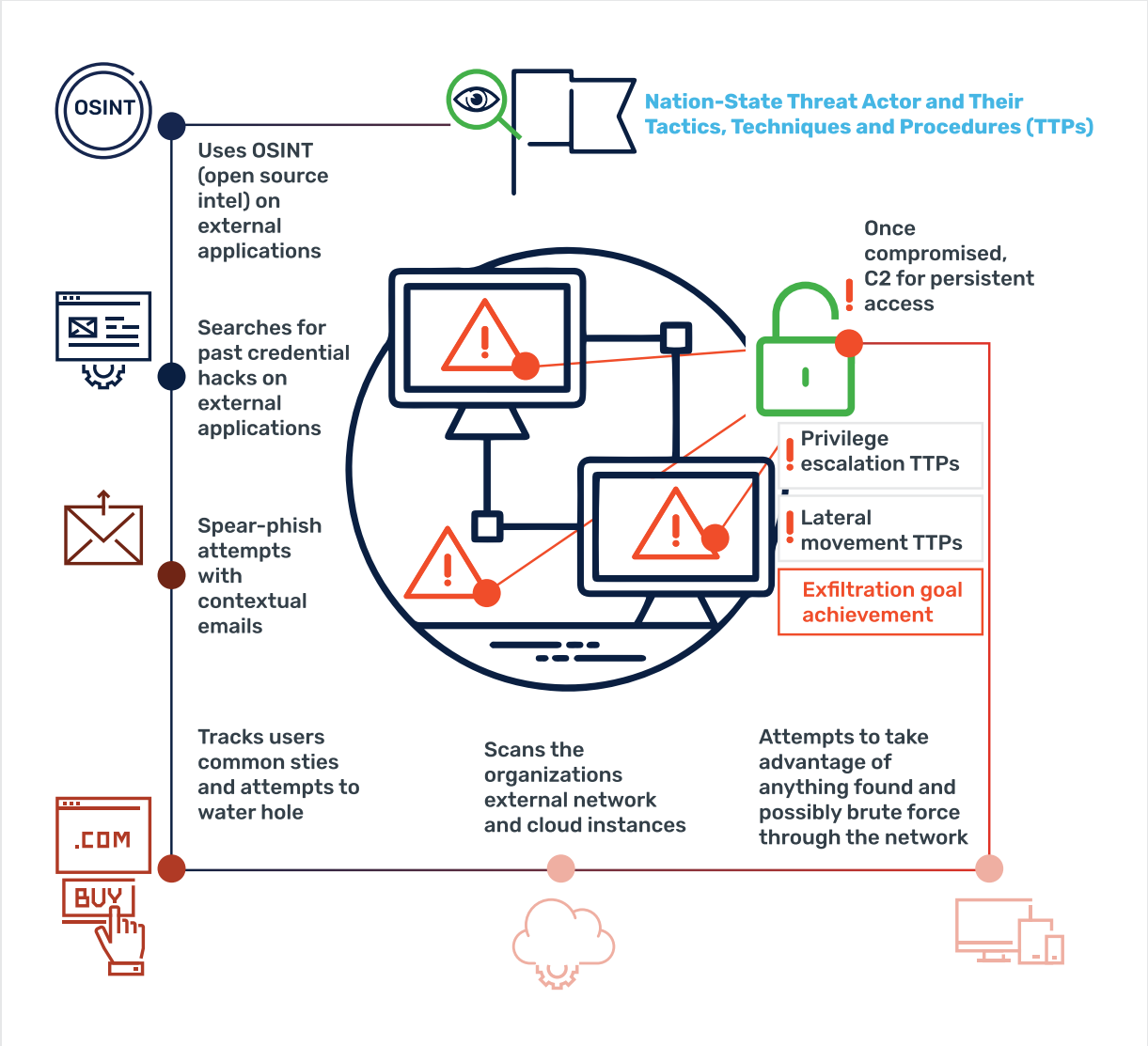
   i. An alert can come from several external sources, including services which monitor social media and dark web chatter and alert you when attackers are discussing your organization or agency.

   ii. Acquiring threat intel from attacks on partners and organizations similar to yours. Threat sharing agreements and workflows, whether manual or automated, can help you gather this intel. Manual sharing typically involves spreadsheets or PDF write-ups of seen attacks sent through email or some sharing process. Automation for threat sharing is accomplished through a Threat Intelligence Platform (TIP) that receives and processes the TI for consumption by a TIU, SOC and tools. The manual process has been around for years prior to automation options, but has proved to be quite slow and can sometimes result in being too late before the organization has received, normalized and consumed the TI. TIP threat sharing programs help automate this for quicker consumption and protection.

   iii. OEM mapping of partners and organizations that are similar to your organization. This can come in the form of a security OEM device TI feed straight to its product or from OEM mapping of TI for predictive research through high quality threat intelligence premium feeds.

3. **Adversarial context** or Human Focused threat intelligence is one of the most important and difficult aspects of threat intel. Very few offerings have the talent and resources to produce finished intelligence which illuminates adversaries behind TI along with their motives and tactics. Organizations that are building out TIU need this type of information to be effective, especially early on. Finding TI professionals that can build finished intelligence, at the level that some of the premium services can produce, is very difficult. Typically a TIU does not have anyone on the team that has that expertise, but has the potential to develop one or possibly two over time. In order to do that, being provided finished intelligence from multiple sources is important to learn from.

The LIfecycle of an Attack



With finished intelligence, a TIU can connect internally caught TI to threat actors and make predictive decisions about what that adversary might do next. This ability may also be connected to a partner organization's predictive research or could be the first notification that an attacker has begun a campaign against the organization. With that the TIU can prioritize and build a defense against that attack that would be much more targeted and effective than broad brush TI pushes and defense.

Knowing the adversary more clearly can help TIU and SOC analysts determine where in the process this attacker is in their campaign. With an established adversary and knowledge of their normal process and where they are, the organization can significantly improve targeted defenses and identification of additional attacks or attempts. Specifically, the most difficult defense is social engineering done in person, on the phone, or by personal email that is not monitored by the organization. Organizations cannot technically defend against all these attacks, so understanding that they might be a part of a campaign, can contribute to a notification to employees with relevant information to add to their awareness.

In order to make those notifications, a detailed understanding and confidence needs to be established through a well-informed TIU.

Overcoming Challenges of Relying on Different Types of Threat Intelligence

Machine Readable Threat Intelligence

To many organizations this means gathering as much threat intelligence from a variety of sources and applying all of them to all the tools possible, such as a SIEM, endpoints, IPS, firewalls and web network tools. This hoarder mentality does not always serve the organization well for several reasons:

- The reality is that most open source TI is not timely and thus cannot assist in defense against current threats.
- Timely TI indicators that are found in a specific business sector often will not be relevant as a threat to a different sector because it's not common that highly advanced threat actors cross sector lines. The most relevant TI will be that from the same industry sector as the organization being protected. For example, if an organization is in finance sector, they should be focused on indicators associated with actors attempting to access other finance organizations, as opposed to pharmaceutical companies.
- The overwhelming amount of threat intelligence that is available is costly to manage and can overwhelm SIEMs and security tools.

Acquiring machine readable TI that is specifically timely and relevant will help reduce the amount ingested and enhance the effectiveness of the TI acquired.

Predictive Research

This type of intel is often focused on social media monitoring and dark web intelligence because they are the easiest to acquire. This type of predictive research TI is often not effective nor timely because if attackers are talking about your organization, they probably have already penetrated it. While it can be a warning to look for a breach in progress, before an outside organization finds the breach and notifies you, the goal of TI is to prevent a breach in the first place.

The most effective predictive research is identifying partner or like organizations being attacked by adversaries and acquiring the TI that was used to discover the attempt or successful breach. Having this TI from the partner or like organization would alert if that actor had begun to attack the enterprise. While threat sharing programs can be highly effective when automated, they require quite a bit of expense and lift to establish and maintain. It is recommended to put the time, effort and cost into doing this method. One way to speed the ROI using a TIP is to acquire an OEM premium feed intelligence with predictive research.

OEM mapping inside the proprietary tools is also recommended, but will be limited as there are very few premium feeds through OEM tools and there are no premium feeds that would be applied to a full platform suite of all the pillar security tools necessary to run an enterprise. There will always be a need to apply this TI to third party security tools.

When it comes to predictive research, the best first step is acquiring the aforementioned high quality threat intelligence premium feed that identifies files, IPs and IOCs specific to your type of organization and can be sent to the entire organization's security enterprise.

Adversarial Context

Also known as Human Focused TI, this is most often focused on particular outcomes that an organization wants to avoid, such as ransomware, Business E-mail Compromise (BEC), phishing and "downloaders." Most threat intelligence providers are unable to provide a full threat actor lifecycle, so in order to provide some higher value than simple machine readable threat intelligence, TI providers take the extra step of attaching attribution. Providing that full threat actor lifecycle, from initial attack, landing, expanding, to actual exfiltration takes a higher functionality and data that is not common in the marketplace. That is, however, what is needed to protect an organization.

Solutions Approach

In order to bring value to the organization through threat intelligence, a solutions approach that does three things are needed.

1. **Holistic Understanding of TI** To gain a holistic understanding of threat intelligence, you must have timely and relevant machine-readable TI that can be compared to predictive research from partner organization sources, along with the proper adversarial context to understand what defenses need to be ready. Machine readable TI sources need to provide high quality and time sensitive data relevant to threat actors, which can be achieved through automated threat sharing directly with partner organizations or through previously mentioned OEM TI structures. Once that data flow is established, connecting that TI to a predictive flow for prioritization is key.

2. **Source Understanding of TI** This solution focuses on where the TI is coming from as opposed to desired outputs, such as reports, indicators, etc. Intelligence that comes from sources which provide less relevance to the specific enterprise being protected, will provide less value. Focusing specifically on threat intelligence that comes from either inside the organization or from inside relevant types of organizations, will be of most value. Threat intelligence collected from non-relevant organizations, or even the egress of relevant organizations and especially from the external internet will likely provide little value to defending the enterprise.

   Threat intelligence specifically from an endpoint inside the organization or a relevant organization is the closest to finding truth about threats and should be used to augment intel from other sources. Endpoint intelligence can provide the organization with an understanding of how adversaries will attack your endpoints as well as their ultimate goals. Deprioritizing dark web chatter, open source research and overlapping sources of network attack telemetry will reduce focus on information that may not have any actionable conclusions.

3. **Understanding the Stakeholders** Knowing who in your organization will use this threat intel will drive the value of the intelligence. The value of intelligence is a direct measurement of its usefulness to its stakeholders, which include:

- **Tactical Stakeholders:** these personnel are focused on functional defensive cybersecurity systems including examples like SIEMs, Firewalls, EPP and IDS/IPS. Their priority is maintaining the functionality and defense of these systems in an administrative capacity, and their expertise is often not specific to cybersecurity, but more infrastructure that maintains security tools. Because of the nature of their function, these team members will want static and behavioral threat indicators as well as the ability to perform malware analysis and enrichment.
- **Operational Stakeholders:** classic cybersecurity professionals found in the SOC, Information Assurance (IA) and Incident Response teams. They are focused on understanding threats and prioritized cybersecurity operations and are not distracted by running the infrastructure.

When it comes to having a holistic understanding of threat intelligence, you should be able to answer these 5 questions:

1. Do we know the adversaries that operate in this space and do we understand why we care about them?
2. Do we understand exactly who and what adversaries are targeting our specific organizations, agencies and industries?
3. Do we understand the psychology and the strategy of those who send the phishing emails?
4. Are we able to see the bigger adversarial picture as opposed to just reactively responding to a series of discrete events?
5. Are we able to map TI to the full MITRE ATT&CK kill chain visibility of adversarial TTPs?

Their goal is to form knowledgeable understanding of adversaries while conducting targeted and prioritized cybersecurity defenses, which include understanding goals and TTPs that drive behavior that needs to be monitored.

- **Strategic Stakeholders:** these are the management and business teams - CISO, CIO, CTO and executive board - that drive decision making across the organization. Their value gained from threat intelligence will be macro trends and adversarial motives which can be used to drive how strategic security and infrastructure decisions are made to benefit the business.

Conclusion

As organizations begin to build threat intelligence practices and TIUs, there is a temptation to simply acquire and combine as much threat intelligence from as many sources as possible. However, this is not a strategy for success. By ensuring that the threat intelligence collected provides a holistic understanding from several angles, the entire organization can be provided actionable information for the specific needs of their role.

The most common gaps in the TI holistic understanding is both predictive research and adversarial context. By leveraging threat intelligence from like partner organizations and successfully understanding the adversaries behind the threats, the technical threat intelligence can be made more valuable. With this focus, the massive amount of threat information can be focused into what is important specifically to the organization being defended.

In addition to completing the TI understanding across the three focus areas, the threat intelligence must be timely and relevant, while providing adversarial context that informs stakeholders at all levels on exactly how to defend the organization. When these goals are combined for a complete TI strategy, the entire organization can all respond with appropriate, timely and proactive actions.

GuidePoint SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132

CORPOV-fWP-THREATINTEL-CS-072020-01