WHITE PAPER

Making a Case for Threat Intelligence Platforms

GUIDEPOINT®
SECURITY

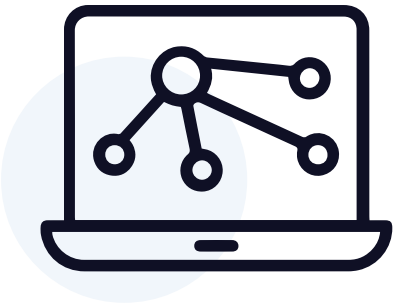
This paper is written with the goal to help walk you through:

The threat intelligence landscape

A conceptual threat intelligence workflow

The expected benefits

The barriers to successful redesign



The security industry began with two vectors of defense.

IP routing tables in the form of Firewalls and a list of “bad files” in the form of Anti-Virus (AV), which were updated often. This created a reputation of what files and IPs not to trust. Over the years, those AV and IP reputation databases have matured into what now is a deluge of threat intelligence that includes attack signatures, registry data, IP addresses, domain names, and a host of other pieces of information often referred to as “artifacts” or “Indicators of compromise.” Additionally, now threat intelligence (TI) will add information about how adversaries operate and behave during an attack, often called Tactics, Techniques and Procedures (TTPs).

This information overload of TI data reflects the advancements of adversaries. The monetization of hacking – both by criminal enterprises and advanced nation states – led to an increase in innovation by attackers. Polymorphic malware overwhelmed MD5 hash AV signature databases, while information sharing structures that malicious actors have created assisted in forming a complex infrastructure to adapt and hide at machine speed.

In response to this evolution of threats, organizations began to develop teams that would take in threat intelligence from like-minded organizations and sources, such as professional feeds, to cull into usable information.

Unfortunately, there are two primary problems with the current way that cybersecurity infrastructures deal with TI:

1. **Most threat intelligence comes from siloed sources to specific tools**
2. **The wide selection of threat intelligence feeds rarely are brought together into one place to maximize analytical value and speed decision-making**

Security teams are usually overwhelmed from running the many defensive tools that receive threat feeds.

It is also a daunting and expensive endeavor to hire enough analysts to manually combine the threat feeds together for analysis, make the intel relevant, and then push the insights to all other tools. Enter Threat Intelligence Platforms (TIPs), which can absorb threat intelligence at machine speed.

Understanding the Threat Intelligence Landscape

Most enterprise security environments pull in multiple threat intelligence sources, but oftentimes that intel is old or irrelevant. A common source of threat intelligence already available comes from products such as Endpoint Protection Platforms (EPP), network security tools, vulnerability management, and even some SIEMs. The problem with these threat feeds, however, is that they're product-specific and must be shared with other tools.

Understanding the various sources of threat intelligence, the quality, timeliness, and relevance is critical. Large enterprises with mature information security teams typically leverage product-specific intel as well as from these additional intel sources:

- **Trust Circles –** Trust Circles follow NIST guidelines to ensure safety of the member organizations. Since Trust Circles are designed for like organizations, they allow for ingestion of threat intelligence that has a higher likelihood of applicability. Threat actors targeting banks probably will look and be different than threat actors targeting a power grid network. Receiving timely threat intelligence from an attempt on a like organization is of great value to the SOC.

- **Threat Intel Sharing –** Feeds provided by DHS US-CERT, ISACs, and other organizations involve passing threat intelligence between members, often doing research and analysis of the threat landscape and adding new threat intelligence. The difference between these feeds and paid threat intelligence feeds is that typically, there is a low (or no) charge, only a signed agreement if the organization qualifies to participate.

- **Paid threat intelligence feeds –** These come in either the form of threat intelligence aggregation, threat intelligence research, or sometimes both. Feeds that come in the form of threat intelligence research are considered high quality and come with a higher cost. Typically, the firms providing this type of feed offer more than simple artifacts, such as full reports on threats and threat actors. A mature threat intelligence team can not only add to their artifacts and apply them, they can learn about a threat actor's TTPs, allowing for next attack predictions.

- **Locally gathered threat intelligence –** Often when an alarm or correlation rule fires in a tool or SIEM, not all the artifacts of the attack were known previously. Sometimes none of them were known. Locally gathered threat intelligence provides new intel that can be shared with like organizations, applied locally and immediately to the entire infrastructure. However, in current architectures, the application of the intelligence often is manual and slow.

The Threat Intelligence Workflow

To realize the best scenario of threat intelligence consumption and usage, four key areas need to be automated: Access, Augmentation, Curation, Operationalization. Each of these builds on the other to create a greater benefit. The greatest advantage to automating these areas is adding new feeds from all four sources.

The four feeds are:

1

Access

- Vendor threat intelligence
- Free threat intelligence
- Paid research and threat intelligence
- Locally created threat intelligence

✓ Brings all the external sources of data into one repository. This must be the first step because it enables the other three areas. Additionally, it allows for unified searching during Incident Response (IR) and mitigation.

2

Augmentation

✓ Allows for local and partner threat intelligence to be added and used to supplement external data sets. Augmentation includes both local tool alerts that create the most urgent threat intelligence and partner threat intelligence from like organizations that can come in forms such as PDF, XLS and SharePoint.

3

Curation

- IP addresses
- MD5 hashes
- File artifacts
- Registry keys
- Snort rules
- TTPs
- Vulnerabilities

✓ Involves multiple sources to identify pieces that can be put together with context, creating a full picture of a threat. When threat intelligence comes in, it sometimes has duplicates from local and external sources and is incomplete with all vectors. Commonly, it will include an MD5 hash, an IP address, or domain names, but rarely does it include all these and other artifacts such as registry keys.

4

Operationalization

✓ Allows for the collected, augmented and curated data to be applied to all of the security defenses (including employee training and alerting) in the environment. The tools that apply TI should span multiple information security disciplines such as endpoint, network, data protection, SIEM, cloud, and DNS.

TIPs for Gaining Situational Awareness

Threat intelligence delivers information about the behavior and tools that adversaries are using to give you external situational awareness that can be used to detect advanced adversaries on the network.

Below we walk through how to use a TIP to gain situational awareness in the context of the Threat Intelligence Workflow:

1. **Access**
2. **Augmentation**
3. **Curation**
4. **Operationalization**

FIRST TIP

Access

A Threat Intelligence Platform (TIP) aggregates the hundreds of intel sources into a single repository for analysts to more easily and effectively identify threats. Unfortunately, threat intelligence often becomes stale quickly, losing its value within hours or days. Without a TIP, early warning signs of an attack may be missed because of the volume of data and the inability to apply the threat intelligence fast enough.

In classified environments, without a TIP, analysts do not have a way to view open source threat intelligence (OSINT) without creating a spillage by searching classified data on an unclassified network. OSINT is extremely relevant in a classified environment because it allows the analyst supplement their classified data publicly known intel.

To gain access to threat intel that provides situational awareness, the TIP must integrate actionable sources including:

- Open Source
- Commercial Feeds
- Collaboration
- Sync open source intelligence into a classified environment

SECOND TIP

Augmentation

Organizations and agencies often share intelligence in a variety of forms including documents and email. While the intelligence that is produced by an organization and shared from like organizations can provide critical situational awareness, analysts are often unable to easily leverage the TI because it's stored in multiple formats and locations.

Your TIP should import:

- Your own internally-created intelligence
- Unstructured intelligence from documents and PDFs
- Intelligence shared by partners

THIRD TIP

Curation

OSINT sources produce millions of indicators that require curation to remove false positives and prioritize the most critical threats. Open Source data frequently include false positives (like shared infrastructure that cannot be acted on) and result in wasted analyst resources. Without curation, you risk missing serious threats due to these false positives.

Not all OSINT indicators are equal, so you need additional context to prioritize the most serious threats to your organization. Analysts must understand the confidence level in an indicator to determine what's most actionable for detection and avoid wasting time on low fidelity alerts.

Analysts also need to know the behavior of indicators to identify the impact that intelligence can have on a network. The combination of the confidence in, and behavior of, indicators quantifies the most impactful threats.

Your TIP should:

- Remove false positives from Open Source Intelligence
- Provide a confidence score for Open Source Intelligence
- Provide the impact type of Open Source Intelligence

Operationalization

Threat intelligence really becomes valuable when it is integrated into all of your organization's security controls, not just the SIEM. When TI is integrated with the SIEM, it identifies malicious activity by correlating the intelligence with your log sources, however this is detection only, not prevention.

- With Integration: Gain full value of TI and proactively stop threats on the network by blocking connections to malicious attackers
- Without Integration: Miss out on the biggest value of TI because it won't be able to detect and prevent known threats on your network before they get in

Many vendors provide APIs that rely on customers to develop and maintain integrations, thus increasing your level of effort to deploy and sustain integrations. An enterprise TIP should include a software binary to manage integrations so when an integration API changes, it is updated by the provider and therefore, no action is needed by you. This significantly reduces the level of effort required to maintain integrations and ensures no impact to your operations or security risk when new updates are released by integration targets, even SIEMs such as Splunk.

Without this capability, you'll have to devote significant resources to update API integrations each time a point product releases an update. As the enterprise improves its security posture by integrating TI with more products on the network, maintaining these integrations without a TIP will be resource-intensive and could become unsustainable.

Threat Intelligence changes constantly because new intel is added and must be integrated with devices and older intelligence must be expired so it doesn't generate false positives. A TIP that manages the full TI lifecycle adds new intelligence to integrations and automatically expires old intelligence.

Many products have limitations on the number of indicators they can ingest. For example, there are over 100 million public indicators in a typical TIP at any given time. Endpoint products may only be able to ingest 10,000 indicators, while SIEMs may be able to ingest 2 million. Your TIP should includes logic to manage the destination device limitations and ensure that, out of the millions of indicators, the high-priority threats are detected and prevented.

Your TIP should:

- Manage the full lifecycle of intelligence in integrations
- Provide software binary to manage integrations
- Integrate with SIEMs
- Offer destination device management

Conclusion

Cybersecurity teams today have many tools and resources available to them, which is both a blessing and a curse. Leveraging relevant and timely threat intelligence can be a significant challenge without automation and integration that TIP solutions provide. With adversaries creating infrastructures to work at machine speed to attack and hide, defenders need to adapt with infrastructures that can respond at machine speed.

By gaining access to premium threat intelligence products, augmenting with local and partner threat intelligence, curating the information to make it not only relevant but consumable, and finally operationalizing the information in a timely manner, cybersecurity analysts can now catch up with the latest adversary advancements. Doing this at machine speed with a threat intelligence platform significantly changes the landscape for the defenders.

Finally, by reducing the amount of time spent on responding to incoming threat intelligence and threat news feeds, analysts can become more proactive, hunting in the environment, armed with the relevant intelligence required. This allows them to fight back offensively rather than simply responding defensively.

GUIDEPOINT®

SECURITY

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

WP-TIP-082020-02