Threat Intelligence Platforms: The New Essential Enterprise Software

Due to the ever-increasing volume of cyber attacks and regulatory pressures, there is a need for a new type of enterprise platform – a platform that can support the entire security team from the CSO or CISO to the security and threat analyst teams in the trenches performing daily incident response, network defense, and threat analysis. The mature threat intelligence platform is used for operational day-to-day blocking and tackling, as well as strategic decision-making and process improvement. It should also facilitate the management of the Intelligence Lifecycle as it is used by intelligence organizations worldwide for a threat intelligence program.

What does a Threat Intelligence Platform do? As Rick Holland of Forrester Researchdescribes it, the TIP is like a quarterback for your operations: it calls the shots and runs the show (Holland, 2014). A threat intelligence platform (TIP) lets personnel throughout an organization manage security data and conduct processes, such as triaging events in the Security Operations Center (SOC), conducting incident response, or managing the threat team's processes for handling external feeds and intelligence. To meet the needs of managers, the platform must also reveal trends, supply real-time updates, support threat-driven long-term prioritization across the business, and enable real-time reaction to threat intelligence data. It should support integration of multiple types of data, as well as provide a way for all the stakeholders to work together as a team. The TIP should be customizable, as each organization has different processes and data customization needs.

The TIP will typically be closely integrated with the SIEM. Typically, aggregation of internal security event data is done in a SIEM, Log Correlation Engine, or other such application or platform; events that are involved in identified incidents, or otherwise directly relevant to threat activity, may be sent from a SIEM to the TIP for pivoting on threat intelligence, enrichment, and long term storage for knowledge management. Integrating the SIEM or other internal

intelligence sources with a TIP can be a powerful method of combining context from internal events with external threat intelligence data.

How Can a TIP Help Your Organization?

Organizations have different levels of maturity and capacity to leverage threat intelligence effectively. These factors are largely dependent on the organization's perceived need and resulting investments in threat intelligence and related personnel and processes. As an organization's capability to leverage threat intelligence grows, so do its threat intelligence use cases. An organization with low investment in threat intelligence will likely use it in a limited manner focused on purely tactical uses. A more mature organization will be able to use threat intelligence strategically to inform incident response and future investments in security. These more mature organizations become leaders, collaborating within their industry and sharing relevant threat intelligence with their trusted community.

Expected Capabilities of a Threat Intelligence Platform

The threat intelligence platform (TIP) has three primary functions: it must aggregate, analyze, and act. It should also integrate with network protection products, provide automated processes, and support workflow and roles.

Aggregation. Aggregation facilitates the *collection*, *processing*, and *exploitation* phases of the Intelligence Life Cycle. Both internal and external intelligence should be aggregated.

- **Aggregation of internal intelligence.** The TIP needs to be able to ingest and store selected events from SIEMs; select packet capture files; malware; incident response reports; and any internally derived intelligence reports.
- **Aggregation of external intelligence.** The TIP needs to ingest multiple sources of information, such as feeds of indicators (open source and premium; structured data with context (e.g. STIX, IODEF, OpenIOC); emails; and intelligence reporting. The TIP should also be able to query other repositories for indicator and file reputation, such as blacklists, VirusTotal, etc. It also should be able to gather information on indicator enrichment, such as IPGEO (geographical data). Analyst-driven and automated external pivoting is another powerful ability of a TIP. Pivoting is a way to place information in context by relating it to other threat activities, and external pivoting looks at outside information such as pDNS, malware repositories, and domain intelligence.

- **Normalization and parsing.** The TIP should be able to normalize and parse unstructured data**,** such as PDFs, Office documents, blogs, and text. It should also be able to normalize and parse structured data~~;~~. ~~there~~There are many languages and standards emerging today, with MITRE's STIX language becoming a potential leader among the financial, tech, and U.S. government sectors. Other types of structured data include CSV, Custom XML/JSON, IODEF, and OpenIOC,

Analysis

Most organizations know that they have to aggregate threat data. They also know they must act. But they often skip the analysis step. The analysis functions of a TIP facilitate the *Analysis and Production* and the *Planning and Direction* phases of the Intelligence Life Cycle.

Once data is aggregated, it has to be refined and placed in context before an effective action plan can be developed. This is where analysis comes in. Without analysis, the data has no meaning – it is useless.

Aggregated data can be analyzed manually or automatically. The pitfall of manual analysis is that it requires too many man-hours and humans can miss important connections. Therefore, analysis has to be automated whenever possible. Automated analysis generates results faster and therefore in greater quantity. The process is scalable and provides a greater level of technical detail.

Analysis features to look for in a TIP. To reduce false positives, a TIP should provide an automated or interactive process to validate indicators that are "bad", and to validate whether indicators that were "bad" yesterday are still "bad" today. This should include indicator reputation by correlating context and threat associations from the various sources. It should also validate any user-submitted indicator reputation.

Another aspect of analysis is Reputation Time To Live. This is the ability to set a time limit on the "evilness" of certain indicators whose association to specific malicious activity is not constant. This is also known within the security community as indicator deprecation or association half-life.

A good TIP includes the ability to create and highlight associations, perform indicator enrichment, and ranking. Each of these abilities is a prerequisite for effective pivot and grouping functionality. The association of indicators to each other or to contextual events, incidents, and

threats is needed to create the graph of relationships that are used to form activity threads and activity groups.

Indicator enrichment and ranking helps to determine the relevance and validity of an indicator as it is associated to a specific event, activity, or broader threat.

Pivoting, querying, and clustering serve to deepen knowledge about an indicator or set of activity. A TIP uses these capabilities to provides the ability to ask questions of the threat intelligence. These investigative capabilities of the TIP allow the discovery of other indicators known to be related by many factors such as threat, time observed, common incidents, common adversary TTP (tactics, techniques, procedures), similar infrastructure, common targeting, etc. They should also support the ability to discover relationships by common traits, artifacts, indicators, etc., that were previously unknown to the user. This directly benefits analysis-related activities, such as contextual alerting, incident response, and fusion analysis.

Contextual Alerting. One alert is often a sign of a larger set of malicious activity that was not alerted. A TIP should make related indicators, signatures, past incidents, adversary TTPs, and broader threats contextually linked (grouped) and "pivotable" so that it is easy to recognize the significance of alerts and what actions to take next.

Incident Response (IR). Similar to contextual alerting, IR can be served by a TIP's ability to pivot through indicators, threats, and the related courses of action

Fusion Analysis: Querying, clustering, and pivoting is crucial to fusing multiple sources of intelligence. A TIP should allow users to view intelligence on the same threat or indicator from multiple sources, contextualize it, and apply a confidence rating to each source.

The reporting features of a TIP are key to its usefulness. It should be able to generate executive, operator, and analyst-consumable reports and metrics. The TIP should support the creation of incident, threat, and adversary (actor) profile reports for executive decision makers, SOC or Operational Security team members, and threat intelligence analysts. The reports produced in a machine-readable format will become increasingly important to enable automated action on shared threat intelligence.

A TIP should be able to produce customizable types of metrics on the data within it. First, and most fundamental, it should be able to create relevant metrics on threat activity and capability. It should also allow the security team to ask specific questions of the data, such as "How many

zero day exploits has threat x leveraged in the past 18 months?" or "What are the CVE numbers for all exploits used by this threat?" or "What autonomous systems does a custom Remote Access Trojan (RAT) use for its callback infrastructure?"

The TIP should also be able to produce metrics on the effectiveness of mitigation actions. For instance, a metric might show whether adversary activity stopped after action X was taken.

The TIP should provide insight into the ROI for both security staff activity and TI data sources. Metrics can be provided on security and threat intelligence personnel actions and analysis provide the ability to measure task performance and ROI for various personnel's analysis activity. Metrics can also provide insight on the value of specific threat intelligence data sources by providing data on how frequently a source is used to thwart adversary activity, or how many false positives come from a particular source.

Another important feature of a TIP is visualization. Visualization is the ability to visually present the relationships between various infrastructures, malware-related indicators, incidents and timelines, and adversary profiles.

A TIP may include sensitive information that not everyone (even on the security team) may need access to, such as customers' or employees' personally identifiable information (PII) or details on sensitive data involved in an intrusion. Therefore, robust access control and data classification is essential. Likewise, being able to segment sharable and non-sharable data for external visibility is important to facilitate sharing processes and allow easy conformance to organizational sharing policies.

Cloud-based TIPS can enable community-driven analysis, allowing organizations to share analytical functions. This allows organizations to exchange mitigation techniques; detection signatures and capabilities; validate internal threat analysis; and add to the pool of indicators and knowledge on threats of interest to specific industries or groups.

Action

Once data has been aggregated and analyzed, it must be acted upon. The action features of a TIP facilitate the *dissemination*, *feedback*, and *requirements* phases of the Intelligence Life Cycle.

There are three primary classes of action a TIP should provide. They are deployment of indicators, creating a feedback loop, and dissemination of threat intelligence fusion.

Deployment of indicators or signatures is used for detection, alerting, & blocking in various network defense products. Receiving data back from these integrated products in a feedback loop allows for accurate metrics on actions taken and knowledge management of high-confidence threat-related events. This brings the cycle of aggregation, analysis, and action full circle as the TIP ingests new data based on threat intelligence it has disseminated to products. Lastly, the dissemination of fused threat intelligence, threat assessment, or other reports for either internal consumption or sharing allows an organization to participate in the greater security community, thereby strengthening its own defenses against adversaries.

TIP Integration with Network Protection Products

The TIP has to integrate with an organization's network protection products using an application-programming interface (API). An API is a set of routines, protocols, and tools that allows software products to interact. A good API is secure and also easy to learn, use, scale, and maintain. Above all, it must fulfill its purpose effectively. In order for a TIP to support the various integrations, it must provide the foundation for new software products to be built on top of it. This requires a very powerful API that must be:

Secure. The API must use HTTPS/SSL and, ideally, *keyed-has message authentication code* (HMAC) authentication.

Standards-based. The API must leverage the REST/Restful standard of architecture.

Static. An API cannot change quickly, given that others have built their own products and integrations to use it. Changing it necessitates all your partners to make changes in their products as well. Instead, new versions of the API that contain any new functionality should be made available. Partners are informed and can begin to leverage advanced functionality in their own time, and prior API versions are supported till all partners have been transitioned.

Versioned. Versioning is critical with an API. Improper or lazy versioning will very quickly result in compatibility issues with existing integrations and will ultimately result in inoperable integrations.

Documented. Due diligence with documentation is as important as proper versioning. Well-communicated use-cases and sample code for constructing queries make an API much more accessible. API query code should be intuitive and follow simple naming conventions in order to be easy to understand and use.

Useful. Support for various use-cases must be inherent within the API. For example, support for blocking/detection requires less detail (indicator, rating, basic context of usage), while Correlation or Threat Fusion would require much more detail (relational data between indicators, related attribution to threat actors). An API should not provide too much or too little information and should employ the fewest number of queries as possible. Ideally, an API has the ability to provide all required data within a single response.

TIP Process Automation

Automated processes can be executed or coordinated by a TIP to provide more seamless integrations with other network defense products. TIPs can coordinate dynamic defense processes on actions performed by integrated defensive products, such as sending a block action on an indicator to a firewall if a certain confidence level is reached or if it is associated with a particular threat.

Support for Roles and Workflow

Currently, security personnel throughout an enterprise use a variety of processes and tools to conduct incident response, network defense, and threat analyses. Integration among the teams supporting these functions, and between the teams and management, has been mostly manual efforts to this point.

Unless an organization had vast resources to build a proper platform, security team efforts either haven't been integrated, or were integrated only through rudimentary technologies like email, spreadsheets, or maybe a SharePoint portal or a ticketing system. These techniques, although better than nothing, do not scale as the team grows and the number of malicious events and security processes increases.

A TIP helps organizations move beyond the current disjointed workflow processes. It provides "a single pane of glass" to manage its various processes and perform threat intelligence tasks. A TIP can also assist in coordinating and directing the actions of the security team around threat intelligence. This allows an organization to prioritize response actions based on risk and to shorten response times for processing known threats.

Decision-makers. Decision-making executives need to serve as threat intelligence program advocates, supporting their organization's consumers of strategic threat intelligence. This group includes the roles of Chief Security Officer (CSO) and security directors and managers (SOC

leads). These are the personnel who are responsible for corporate expenditures, future budget decisions, and corporate strategy.

As an advocate for these personnel, the decision-maker must understand sophisticated cyber threats, appreciate how an effective threat intelligence program works to mitigate risk, and ensure that the program is adequately resourced with people and tools. He must be aware of threats and why threat actors are targeting the company so he can communicate the risk to other stakeholders. If a breach occurs, the decision-maker can direct the corporate response more quickly by having prior knowledge of the intentions behind a specific threat, as established by consumption of strategic threat intelligence. He is also responsible for notifying corporate governance groups and company shareholders in the event of an incident.

The lead executive must understand security ROI. The return on a security investment is indirectly related to maintaining the growth in profit for the company, so the threat intelligence program should not be seen as a “black hole” in which the investment never sees a return. Instead, it should be viewed as something similar to a gym membership; if used properly, a gym membership can prevent future doctor visits and health risks. Similarly, a well-run threat intelligence program reduces risks posed to the company.

Analysts and operational staff. The roles of the analysts and operational staff involved in threat intelligence usage and production vary between organizations. The roles are largely dependent on the level of investment in threat intelligence processes. Often, there is no dedicated threat analyst; instead, the role is shared by one or more IRs, SOCs, or malware analysts.

Regardless of the actual job titles associated with their roles, staff members typically use threat intelligence to some extent in the same way that a threat analyst does. Each of the other traditional security roles also has its own usage or contribution of threat intelligence.

Threat analysts. The job of a threat analyst is to build a big-picture view of the threats and trends that his or her organization has to deflect. The threat analyst discovers and analyzes threat information by actively monitoring threat groups worldwide. These groups include major nation-state hacking groups responsible for attacks on major media outlets, energy infrastructure providers, and large financial institutions.

Threat analysts perform many types of work. They are responsible for threat intelligence fusion; this requires them to analyze internally-collected threat data and fuse the results with

threat information obtained from incident reports created by the Network Defense staff. They also perform technical research about threats and adversaries, forecast potential attack activities by analyzing existing knowledge about current threats and adversaries, and create reports to keep the organization's leaders informed about the current and potential threat landscape.

SOC or security analysts. These analysts add signatures or detection to sensors and security products provided from threat intelligence. They monitor logs and SIEMs (if present), correlating with threat intelligence data for alerts.~~,~~ They also fix vulnerabilities, triage alerts, conduct initial response, and prioritize activities based on related threat intelligence data.

Information assurance staff. The information assurance staff deploys new technology based on prioritization from strategic threat intelligence. They implement new logging solutions, also based on prioritization from strategic threat intelligence.

Incident responders. Incident responders provide context and direction in investigations of threats that have been escalated to them. They examine, analyze, and document the findings in easily-read formats that can be understood by everyone, since the reports might be used as evidence in legal or regulatory proceedings. Incident responders also work with business departments to develop incident remediation solutions.

Malware analysts. Malware analysts correlate similar malware from threat intelligence to save time, identify related threats, refine detection methods, and provide previously-unknown related indicators.

Summary of Threat Intelligence Platform Key Points and Benefits

In order to protect assets against adversaries, organizations have to know who, how, why, and when those adversaries are likely to attack. The volume of threats is so great that there is only one way to manage that firehose of information. That way is a Threat Intelligence Platform (TIP).

A TIP works because it aggregates, analyzes, and enables action. The TIP has to be able to handle massive amounts of information from different sources, including shared data from other organizations. But collecting data from internal and external sources is just the first step; raw data is useless until it is refined and placed in context in the analysis phase. The analysis phase identifies relationships among countless pieces of information, thus developing a panoramic

view of the threat landscape. The resulting picture has to be easy to understand and share; visual analyses provide an at-a-glance overview, and plain-language reports help decision-makers communicate risks to stakeholders. Action is most easily planned and taken when the TIP integrates with network defense products and includes workflow features that let security professionals at all levels have the proper level of access required to perform their functions.

The threats are not going away. They're only getting bigger, stronger, and more numerous. Protect your organization's assets by taking a proactive stance against the bad actors.