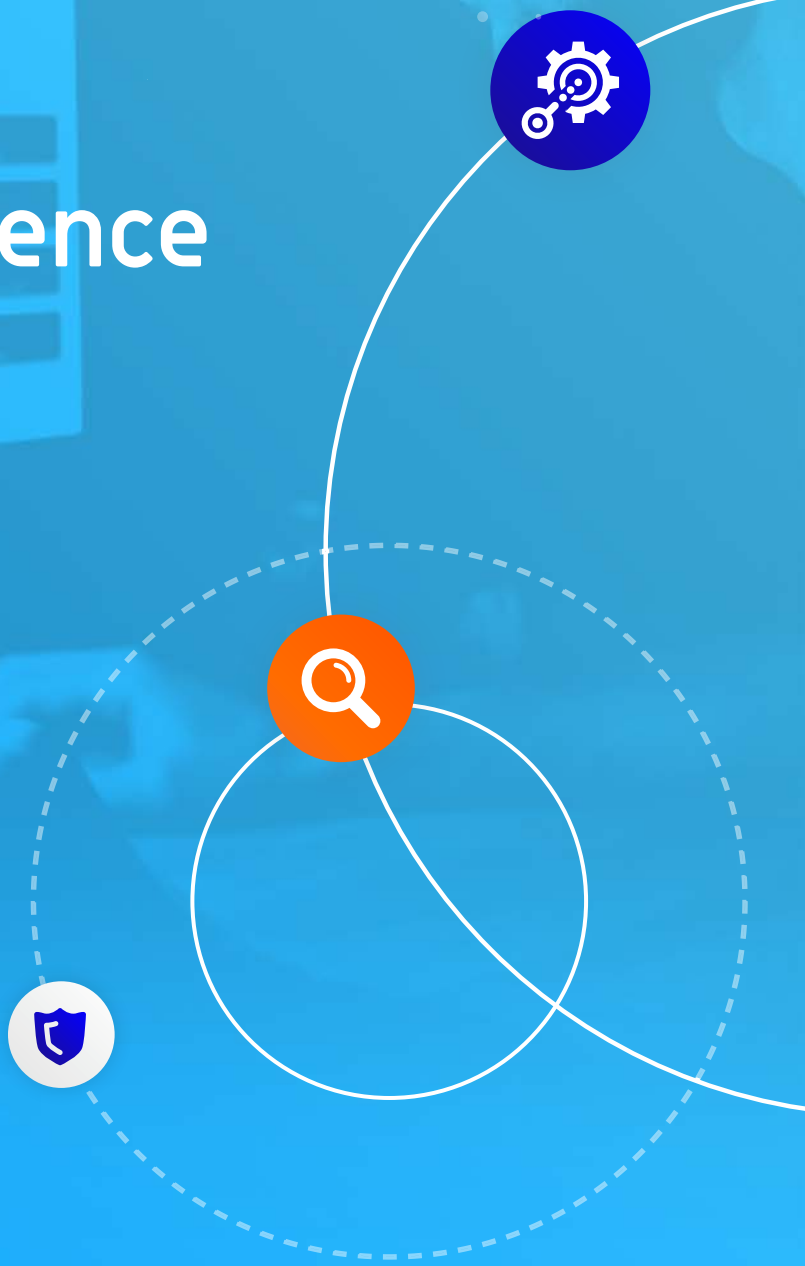
eBook

Threat Intelligence Platforms:

Everything You've Ever Wanted to Know But Didn't Know to Ask



ThreatConnect™

ThreatConnect.com

Contents

Chapter 1

Why Threat Intelligence Matters

FIRST AND FOREMOST:

Know Your Enemy

Yes, you have an enemy. It's highly probable you have more than one.

Today's threats are relentless and come in all shapes and sizes. While the internet has enabled a global economy to explode, it has also made it easier than ever to steal data. The internet was built for connectivity, not security. Approaches such as intrusion detection systems, anti-virus programs, and traditional incident response methodologies by themselves are no longer sufficient in the face of the widening gap between offensive and defensive capabilities.

30%

"By 2020, 30% of global enterprises will have been directly compromised by an **independent group of cybercriminals or cyberactivists.**"

– GARTNER

76%

76% of breaches were **financially motivated**.

– VERIZON DBIR 2018

87%

In 87% of network breaches, cybercriminals, compromise the network within minutes or less, **but only 3% of breaches are discovered this quickly.**

– VERIZON DBIR 2018

Cyberthreat actors are gaining more sophisticated tools, techniques, and procedures (TTP) which are outpacing stand-alone security solutions. It is not surprising they are able to get past disparate and uncoordinated defenses. Adversaries can be organized criminal or state-sponsored groups, known as Advanced Persistent Threats (APTs) – all of which have the tools, training, and resources to disrupt or breach most conventional network defense systems. These incursions are not conducted as isolated attempts. They are often multi-year campaigns targeting valuable, sensitive data.

Clearly, you need to react to threats. But if you are only reacting, you are playing a never-ending game of catch-up and clean-up. Having a threat-intelligence-led security program gives your company or agency a fighting chance to defeat these ever-changing threats. You need a holistic view of the threat landscape and a proactive posture to protect your institution from the multitude of threats you face every day.

To develop this holistic view and plan a proactive posture, you need to constantly harvest and process knowledge about the threat actors, not just the specific incidents. Knowing the who, what, where, how, and when of the adversaries' actions is the only way to decrease their chances of success. But the volume of intelligence is so massive that tracking and understanding adversarial actions can be overwhelming. A Threat Intelligence Platform (TIP) is the only way to manage the flood of data.

Effective threat intelligence management is an ongoing effort. The threat landscape is already large, and it's only growing, becoming more complex and getting more efficient as time passes. You have to constantly examine your defensive positions and adjust your operations and strategies to defend yourself against the evolving technologies and adversaries that endanger your assets. In the same way that an individual pays for a gym and attends it regularly to keep fit, your organization must make a continual investment and commitment to protecting your assets.

Any delay is a moment of risk. Your assets are being examined. Your vulnerabilities are being identified. Who are these adversaries? What do they want, how will they attack, and when will they do it? Have they attacked any of your partners or competitors, and, if so, what happened in those attacks? This is the breadth and depth of knowledge that you need to secure your assets today. The time to answer these questions isn't next quarter, next week, or tomorrow. The time is now.

How Threat Intelligence Platforms are Shaping Cyber Security:

In Chapter 3, we cover extensively what Threat Intelligence Platforms (TIPs) do, how they fit into your overall organization, and many potential use cases. In a nutshell, Threat Intelligence Platforms should:

Drive Security Process with Intelligence

First and foremost, a TIP should allow government agencies and large enterprises to aggregate all available threat data – both internal and external, structured and unstructured – analyze it rapidly, automate action, and then produce tactical, operational, and strategic threat intelligence all in one place.

Unite All Resources Behind a Common Defense

With well-defined data architecture, your TIP will unite intelligence analysts with incident response, security operations, and risk management in your common mission to defend the enterprise from modern cyberthreats. Then, through either public or private communities that you choose, your TIP will allow secure crowdsourcing to surface more than you could on your own. And, it should work with your other systems to automate action based on workflows you set.

Provide Enterprise-Level Intelligence for Strategic Decision Making

With all the tactical, operational, and strategic reporting in one platform, your C-suite should be able to get a full view of what's working and what changes need to be made to empower the cyber team to be successful in your threat-defense efforts. Furthermore, with the big-picture view made possible by enterprise-level reporting, you will be able to have risk, security, and mitigation discussions at a business level with the CEO and board.

Action Beats Reaction

CAPTURE AND DEPLOY INTELLIGENCE TO BUILD A STRONG DEFENSE

All organizations need to gather intelligence about the threats that endanger their systems. Intelligence provides private and government organizations with a means to fend off threats in progress and, in many cases, to prevent adversaries from infiltrating the network at all. The use of threat intelligence leads to a more holistic and a more focused approach to security.

All organizations need to gather intelligence about the threats that endanger their systems. Intelligence provides private and government organizations with a means to fend off threats in progress and, in many cases, to prevent adversaries from infiltrating the network at all. The use of threat intelligence leads to a more holistic and a more focused approach to security.

Holistic approach.

A company taking a holistic approach views security as more than a matter of mitigating risk by identifying and patching vulnerabilities on network assets. It also considers threat capabilities and motives against its assets. A holistic approach means that an organization is looking at every aspect of its threat management in relation to every other aspect.

Focused approach.

A company taking a focused approach concentrates its resources on concrete threats to its network. It directs and prioritizes the redundant multiple layers of information security that constitute Defense in Depth strategies (NSA). A focused approach does not replace the redundant layers of information assurance; rather, it strategically orchestrates the layers so that they can provide the most efficient defense.

Threat intelligence enables an organization to detect, recognize, and prevent attacks. A Threat Intelligence Platform strengthens security monitoring by delivering feeds of threat-related indicators and providing a single platform to analyze and act on those indicators. The result is a holistic view of the threats, adversaries, and tradecraft. By analyzing threats in relation to these indicators, you can proactively deploy network- or host-based detection indicators and signatures for threat-related activity, thus halting threats before the infiltration has become critical.

When an attack is discovered, incident-response investigations must be conducted more quickly because the threat intelligence has already exposed the adversary's tactics, techniques, and procedures (TTPs). Since the knowledge of the adversary has been revealed by the TIP, an organization can best align its overall security programs to real threats. Specific adversaries' motives, goals, objectives, and capabilities can be identified and tracked. When an adversary is known, his next move is predictable.

The use of threat intelligence enables you to prioritize your defenses around highly targeted assets, focusing on remediating vulnerabilities that adversaries are known to be capable of exploiting. Threat intelligence reveals which vulnerabilities are most likely to be targeted, while also revealing ways that the adversary activity can be mitigated. By examining where threats are coming from (sources) and the processes or business goals they are intended to act upon (functions), your organization can develop strong, actionable threat intelligence.

Chapter 2

What is Threat Intelligence

In the simplest terms, threat intelligence is the **knowledge of a threat's capabilities, infrastructure, motives, goals, and resources.**

The application of this information assists in the operational and strategic defense of network-based assets.

Internal and External Threat Sources

Threat data comes from several sources, both internal and external. Fusing the internal and external threat intelligence allows an organization to create the most relevant and accurate threat profile, and also to rate and rank the value of sources of threat intelligence.

Internal sources.

Your own network shows you which intelligence is truly relevant to your organization. By leveraging threat intelligence from your own network, such as log files, alerts, and incident response reports, you can recognize and stop threats. If you utilize a Security Information Event Management protocol (SIEM), this is an ideal place to start. Several raw sources of internal network event data (such as event logs, DNS logs, firewall logs, etc.) are already present in your SIEM. Maintaining historic knowledge of past incident-response engagements is helpful in leveraging more mature threat awareness based on internal sources. This includes retaining accessible data on the systems affected during an incident, the vulnerabilities exploited, the related indicators and malware, and, if known, the attribution and motivation of adversaries. Retaining malware used, relevant packet capture, and netflow can also be invaluable sources of intelligence.

External sources.

External sources can be quite varied, with many degrees of fidelity and trustworthiness. "Open source" intelligence, such as security researcher or vendor blogs or publicly available reputation and block lists, can provide indicators for detection and context. Private or commercial sources of threat intelligence can include threat intelligence feeds, structured data reports (such as STIX), unstructured reports (such as PDF and Word documents), emails from sharing groups, etc. Some of this data, particularly that from vendors, may be refined with context for a particular industry or government. However, it is ultimately up to your security team or someone with specific knowledge of your organization's threat landscape to determine its relevance.

Functional Threat Intelligence

Threat intelligence can also be gathered based on function. Functions can be operational (based on processes) and strategic (based on business goals).

Operational functionality.

At an operational level, threat intelligence identifies threat indicators that increase detection capability and provide warnings of attacks or potential attacks. It also exposes specific risks based on vulnerabilities within the network assets of the organization or personnel.

Sources of operational threat intelligence include vendor feeds of indicators, open source feeds of indicators, blog posts with indicators, and tactical reporting indicating attacks, capabilities, and infrastructure of adversaries.

Strategic functionality.

At a strategic level, threat intelligence spotlights the exposure an organization has to particular threats and allows those threats to be considered in relation to current and future financial risks, reputational risks, and continuity of operations. Types of strategic threat intelligence include threat assessments, intelligence summaries, and adversary profiles or assessments.

Assessing the Value of Threat Intelligence.

Threat intelligence must be useful to the defense of organizational assets to be of value. Sources that provide specific types of intelligence or threat-based intelligence focused on real threats to the organization are typically of more value than generic feeds of intelligence. **The general qualities of useful threat intelligence are relevance, variety, timeliness, and accuracy.**

Relevance

The most direct way to measure relevance is to measure positive hits or alerts in the environment when deployed. Relevance is enhanced by the volume or "completeness" of the threat data. However, the attribute of volume is hard to assess. Some threats or classes of threats are larger in scope than others and require more volume to be closer to "complete," so numbers by themselves cannot be the sole metric. In order to determine the relevance of data on active threats, you first need to understand the types of threats targeting your assets. This requires the mapping of business processes to specific geographic, political, and industry-focused threat classes. Once the classes are identified, then you must learn more about potential adversaries by focusing on threat intelligence sources that provide data on these particular types of threats. In practice, this is an iterative process. The more intelligence an organization has available to determine threat-based risk, the more it's possible to understand which intelligence is most relevant to it.

Accuracy

Accuracy is based on the number of false positive alerts or actions obtained from the threat intelligence. The lower the number, the more accurate the intelligence. Confidence ratings or certainty scoring may help in assessing the potential for false positives. Accuracy is also contextual. Hitting on actual "evil" is important for operational threat intelligence. Knowing what to do next is important for strategic threat intelligence. Context is the "glue" between operational and strategic threat intelligence, and it determines the next steps to take once there is an alert. When context correctly links the operational and strategic aspects of a threat, the activity can be accurately attributed and the motives and capabilities of the adversary can be assessed. Inaccurate context results in incident-response efforts that are misdirected, and strategic defenses that are misaligned with real threats.

Timeliness

Timeliness refers to the frequency of updates relative to new threat activity, changes, or evolutions in capability or infrastructure. Some types of threat intelligence are more subject to change than others. This attribute is called expiration frequency, and it depends on adversary resources, skill, and tactics; techniques; and procedures. When threat intelligence provides a way to detect adversary activity that persists through evolutions in capabilities and infrastructure, then that intelligence is less prone to expiration, is more reliable, and saves effort in making frequent updates.

Variety

Incident detection and prevention should not typically rely on one medium, technique, or capability. The threat intelligence used to enhance that incident detection and prevention should not do so either. Thus, for operational intelligence, it is essential to use a combination of host- and network-based indicators and signatures. Likewise, a combination of indicators or other detection techniques that find both adversary infrastructure and capabilities usage are critical. Finally, threat intelligence that enables you to detect or prevent activity at multiple phases of an intrusion, such as in kill chain tactics, will be more valuable (Hutchins, et al.).

How to Effectively Use Threat Intelligence

ALERTING AND BLOCKING.

This is the basic use case for leveraging threat intelligence. Use tactical feeds of threat- intelligence-derived indicators to block malicious activity at firewalls or other gateway security devices. Detection for indicators of compromise (IOC) can be deployed as alerts in SIEMs, as signatures on IDS/IPS, or host-based signatures on configurable endpoint protection products.

CONTEXTUAL ALERTING AND SIGNATURE MANAGEMENT.

Alerts with context provided by threat intelligence are useful in determining the severity and validity of alerts. Both host- and network-based detection signatures are made more useful in context from threat intelligence by providing confidence, priority, and appropriate next steps based on an adversary's known tactics, techniques, and procedures.

INCIDENT RESPONSE.

Threat intelligence directly supports incident-response processes by placing observed IOCs into context. This helps responders determine where to look next to observe an ongoing intrusion. Threat intelligence can also drive the prioritization of ongoing investigations based on knowledge of the adversaries involved.

FUSION ANALYSIS.

Threat intelligence fusion is the process of assessing intelligence from multiple sources and source types to create a more complete threat and risk picture for an organization. It is an underlying and critical function of any threat-intelligence analysis effort. It allows for the creation of comprehensive threat assessments and provides specific threat relevance by overlaying external intelligence sources onto internal ones.

SECURITY PLANNING.

This is the most strategic use of threat intelligence. By using threat intelligence that is relevant to your risk posture, security planning drives architecture decisions and refines security processes to better defend against known threats.

SHARING THREAT INTELLIGENCE.

Sharing is cited as one of the most productive sources of threat intelligence (Norse, 2013). The security community typically operates in tight trust circles, and giving is the best way to prove one is worthy to receive.

BENEFITS OF SHARING AND HOW IT CAN WORK.

Sharing your knowledge about threats that are relevant to other organizations opens up new sources and insight from others in your community for your security team. Sharing data allows organizations to get a more accurate understanding of the information they're collecting through community validation and expertise. The wider the pool of data that can be accessed, the better an organization can protect itself. Typically, making an investment in sharing relevant and usable threat intelligence yields wider access to data through deeper trust relationships with partners and access to more communities. As public and private organizations begin to collaborate, trust is established between partners, analytic work is conducted more broadly, working relationships expand, and collaboration occurs organically. The resulting communities and relationships are the essential non-technical elements that make threat intelligence sharing possible. Actively participating in and contributing to circles of trust lead to further opportunities to join additional private groups and benefit from the information shared within them.

Read more about Information Sharing and Analysis Organizations (ISAOs), Information Sharing and Analysis Centers (ISACs), and how they work with TIPs in Chapter 4.

78%

(78%) cybersecurity decision makers with threat intelligence programs said that their organizations have successfully used those programs in the last year to **block threats that otherwise would have cost the business a significant sum of money.**

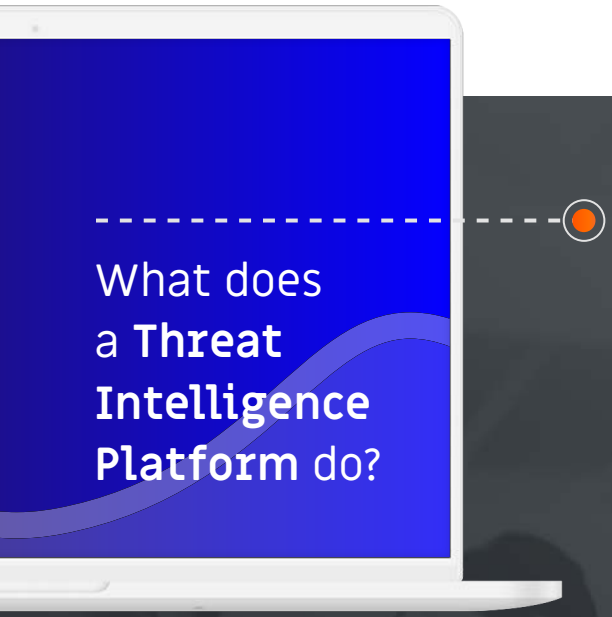
– BUILDING A TI PROGRAM

Chapter 3

Threat Intelligence Platforms: The New Essential Enterprise Software

Due to the ever-increasing volume of cyberattacks 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 (TIP) 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, formerly of Forrester Research describes it, the TIP is like a quarterback for your operations: It calls the shots and runs the show (Holland, 2014). A 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 typically is closely integrated with the SIEM. Ordinarily, 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. The use cases for threat intelligence grow as an organization's capability to leverage it grows. An organization with low investment in threat intelligence is likely to use it in a limited manner focused on purely tactical uses. A more mature organization is 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.

ANALYSTS

Pivot from one data point to another, uncover patterns, and gain a complete picture of your adversaries' TTPs.

CEO/BOARD

Better assess and mitigate risk when making strategic business decisions. Protect the integrity of your brand and data.

DIRECTORS

Manage a faster, more agile team. Get the most out of your existing tools and processes.

ISAC AND ISAO

Contribute to and draw from trusted communities to build a shared knowledge resource of common threat actors and tactics.

CISO

Make strategic security decisions with certainty and lead more informed, effective security operations.

MSSP

Provide greater value to clients by relying on a broader intelligence network to identify and counteract cyberthreats.

"The TIP is like a quarterback for your operations:
It calls the shots and runs the show."

– HOLLAND, 2014

Low Organizational Threat Intelligence Capability

PRIMARY USE CASES:

Consumption of threat intelligence for alerting and blocking.

Problem

Organizations that are just getting started with threat intelligence rarely have made a large investment in intelligence processes. In such organizations, there is likely no one person or group charged with the management of threat intelligence automation. It is tempting to turn on product-integrated feeds, and this will suffice for that product if the intelligence is properly refined and vetted by the provider. But problems typically arise when hooking threat intelligence directly into the products. The integration can cause as many problems as it solves, resulting in high false-positive alerts or blocks if the intelligence feed is "raw" or of low quality. The security team can be overwhelmed with data in multiple product and organizational silos. Often, these are spreadsheets buried in a shared drive's directory structure. Further, when underutilized threat intelligence sources are product-specific, security teams can potentially find themselves being asked to pay for the same feed for each product.

Benefits of a TIP:

A TIP provides aggregation and correlation of multiple external data sources. A TIP can help by aggregating multiple sources into one source of threat intelligence for analysis or API-based product integrations with security products. A TIP should help "sort the wheat from the chaff" from the various feeds through the use of automated analytics that lower the number of potential false positives from the various sources it is processing when the data is deployed. A good example of this is simple blocklist management, in which indicators are given time to live before they are dropped from the blocklist.

The TIP enables action on the intelligence by providing APIs and connectors for out-of-the-box integrations with SIEMs, next-generation firewalls, endpoint protection devices, IDS/IPS, and other defensive products. The passing of structured, machine-readable threat intelligence, in a format such as STIX, allows immediate and flexible use of threat intelligence to generate alerts and blocking.

Finally, a TIP provides the capability to use threat intelligence in simpler, broader, and more strategic ways.

Moderate Organizational Threat Intelligence Capability

PRIMARY USE CASES:

Contextual alerting, signature management, and incident response.

Problem

When an organization has decided it needs to use threat intelligence to assist with incident response and SOC processes, it needs to move to intelligence-driven processes. This is the first step to a more proactive security posture. In addition to the aggregation of external threat intelligence, an organization needs a place to maintain knowledge of past incidents and related IOCs, apply context to detection signatures for the SOC team or monitoring staff, and correlate ongoing incidents with historic threat intelligence.

Benefits of a TIP:

A TIP enables knowledge management through the retention of threat intelligence and incident-related data. It also provides searchability. A TIP should index and/or normalize the internal and external threat intelligence coming into it to allow users to search for indicators, threats, incidents, malware, and adversary profiles. Another benefit is the ability to organize threat intelligence data and allow indicators to be linked together or associated with incidents, threats, or adversaries. Signature management is an important benefit at this level. Although individual signatures tend to be low context (meaning they provide little insight into the nature of a threat or sometimes even the alert that generates when they fire), signatures that are contextually linked to threats, threat indicators, intrusion phases, or other amplifying data become far more helpful in identifying the true priority of an alert and assisting with response actions. The TIP puts signatures into context which in turn speeds response, minimizes "alert confusion," and makes clear which activity they are detecting.

A TIP can enrich indicators in many ways, such as in the form of file, domain, and IP reputation, geographic mapping (e.g. IPGEO for IP addresses), Whois information for domain indicators, known past activity, threat type, etc. All of these can provide valuable context when alerts fire or when researching possible IOCs during an intrusion investigation.

The TIP is also able to add an organization's own context to threat intelligence in the form of personalized ratings and confidence, recommended courses of action upon detection, phases of intrusion, or other enrichments.

In addition, a TIP can maintain historic data on assets and personnel targeted or compromised to trend adversary intent and objective. This assists ongoing and future incident-response engagements.

TIPs can aid incident-response enhancement and metrics. During incident-response engagements, a TIP that is integrated with endpoint detection and response products can quickly detect and scope an intrusion with threat intelligence pushed to the device. A TIP can show ROI on feeds, personnel activity, and mitigation actions taken.

High Organizational Threat Intelligence Capability

PRIMARY USE CASES:

Threat intelligence fusion and creation, strategic security planning, and enabling the sharing of threat intelligence.

Problem

Once an organization puts external threat intelligence to work in its network and maintains historical and contextual threat knowledge derived from past incidents, a natural next step for that organization is to begin to create its own unique intelligence on the threats. The challenge in making strategic use of threat intelligence is that it requires sufficient processes to create and leverage the data.

Benefits of a TIP:

A TIP assists in fusing and creating threat intelligence by using its ability to pivot, draw correlations, and allow analyst and automated enrichments. The TIP can be the fundamental platform used in creating organizational intelligence. This fused intelligence is directly used in the next two capabilities: security planning and sharing. It enables an organization to create more accurate risk assessments based on real and observed threats.

A TIP enables strategic security planning by using its ability to act as a knowledge repository for threat intelligence, past incident-response engagements, and the effectiveness of courses of action taken. It can assist in identifying "centers of gravity" for adversary actions to pinpoint the most effective defensive actions against particular adversaries. This knowledge can then be used to direct security budgets, investments, and talent-resource needs within the security team.

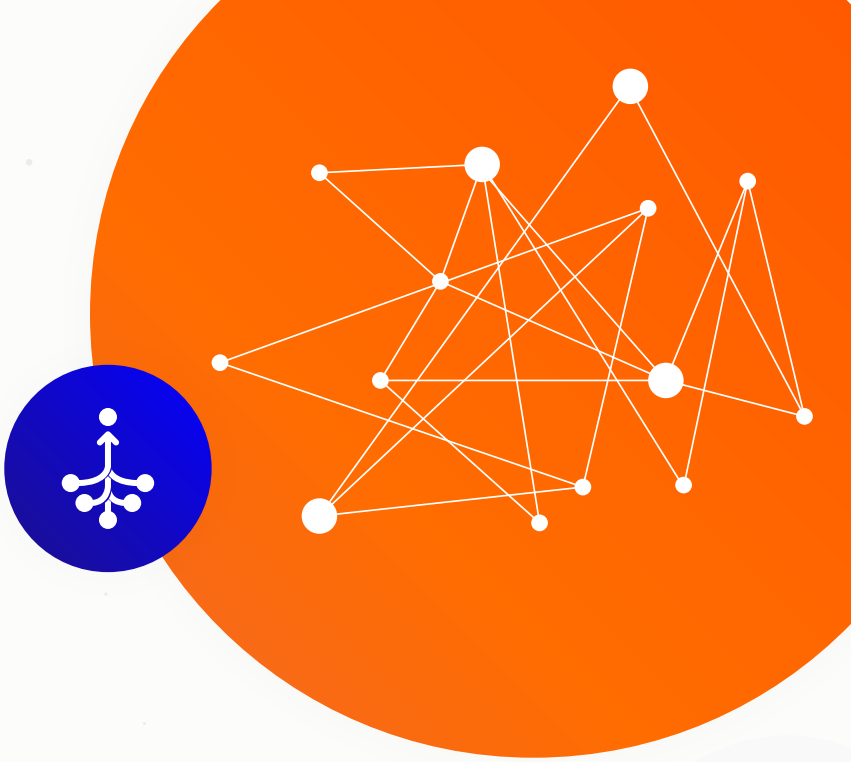
The TIP makes it easy to share threat intelligence, which assists in its creation and enables the sanitization of any sensitive or controlled data, thus making the threat intelligence safe to share.

If the TIP is a mature, extensible platform, a mature organization can also utilize its TIP to build its own applications based on its custom needs. A TIP that gives users the flexibility to build custom applications in an application runtime environment makes the TIP even more powerful for users. Those organizations can build upon their TIP as their security needs evolve, and take advantage of utilizing other apps built by the TIP's community, partners, and internal teams. Not only is sharing threat intelligence easy with a TIP, but as more apps are built and approved, they can be shared with other community members with ease directly in the platform. Smaller organizations, peers, and partners within your supply chain could also benefit from the applications you share.

Lastly, through its ability to automatically generate machine-readable threat intelligence, such as STIX formatted data, a TIP can speed and better enable the usability of the intelligence shared to external organizations.

Expected Capabilities of a Threat Intelligence Platform

The 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.



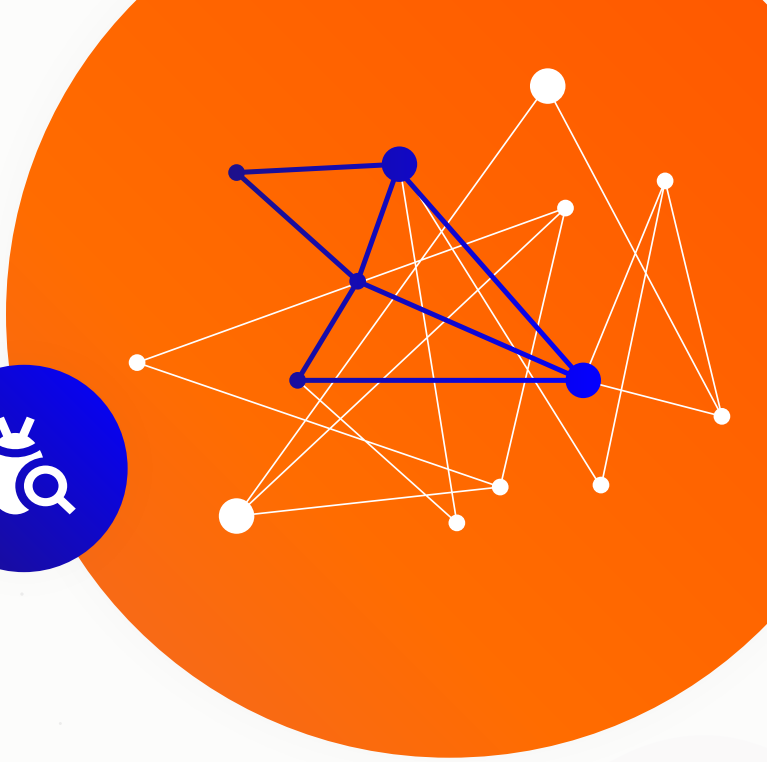
Aggregation

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

Aggregation of internal intelligence. The TIP must 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, such as STIX, IODEF, and 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 should be able to gather information on indicator enrichment, such as IPGEO (geographical data). A TIP enables analyst-driven and automated external pivoting. 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 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

You already know you have to aggregate threat data. You also know you must act. But, too often it's easy to skip the analysis step. The analysis functions of a TIP facilitate the analysis as well as production and the planning and direction phases of the Intelligence Lifecycle.

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. Human analysis using a proven methodology, like the Diamond Methodology, is key to effective analysis. 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 threatw 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 and to 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 activities. A TIP uses these capabilities to provide the ability to ask questions of the threat intelligence. These investigative capabilities allow the discovery of other indicators known to be related by many factors such as threat; time observed; common incidents; common adversary tactics, techniques, and 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.

ANALYSTS DIRECTOR CISO CEO/BOARD

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 tactics, techniques, and procedures; and broader threats contextually linked (grouped) and pivotable, so that it is easy to recognize the significance of alerts and determine 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 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.

Aggregation **Analysis** Action

A TIP should be able to produce customizable types of metrics on the data within it. First, and most fundamentally, 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?”

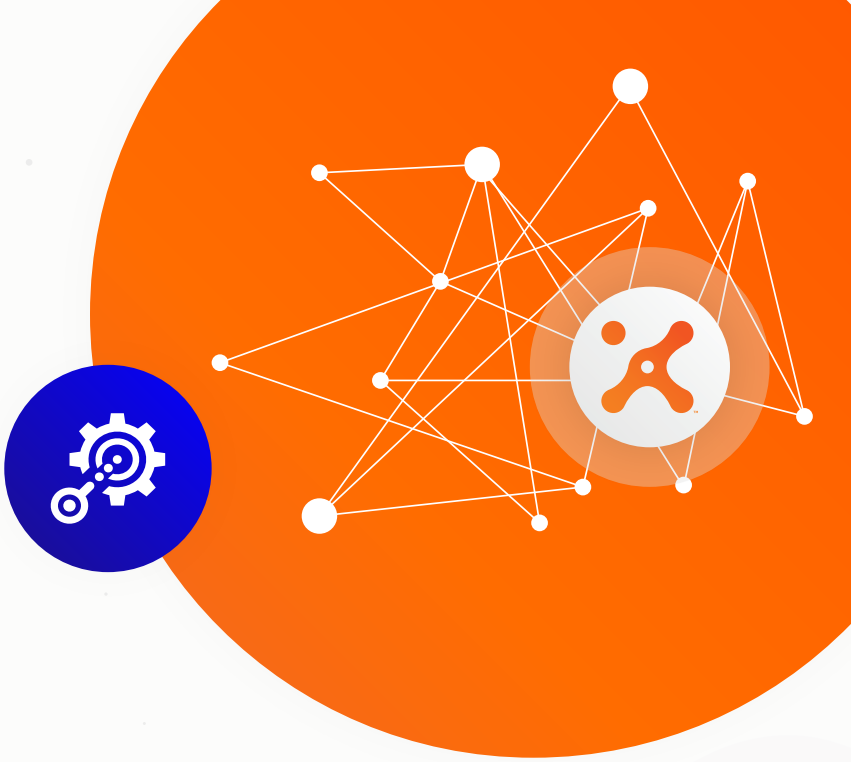
The TIP should also be able to produce metrics on the effectiveness of mitigation actions. For instance, a metric might show whether adversary activity stopped after Action X was taken.

The TIP should provide insight into the ROI for both security staff activity and threat-intelligence 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.

Visualization is another important TIP feature. 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. Then, you will be able 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, you and your systems must take action. The action features of a TIP facilitate the dissemination, feedback, and requirements phases of the Intelligence Lifecycle.

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

Deployment of indicators or signatures is used for detection, alerting, and 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.

Aggregation | Analysis | **Action**

TIP Process Automation

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 that all your partners 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 until all partners have been transitioned.

VERSIONED

Versioning is critical with an API. Improper or lazy v ersioning 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.

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.

Aggregation | Analysis | **Action**

TIP PROCESS AUTOMATION (CONT.)

A TIP should execute and coordinate automated processes 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 analysis. Integration among the teams supporting these functions, and between the teams and management, has consisted of mostly manual efforts to this point.

Unless an organization has 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 you move beyond the current disjointed workflow processes. It provides a single pane of glass through which 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 your 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.

Aggregation | Analysis | **Action**

TIP PROCESS AUTOMATION (CONT.)

As an advocate for these personnel, the decision maker must understand sophisticated cyberthreats, appreciate how an effective threat intelligence program works to mitigate risk, and ensure that the program is adequately resourced with people and tools. The strategic leader must be aware of threats and why threat actors are targeting the company in order to 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. This leader 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.

$8.8M

Organizations that have threat intelligence programs have **saved an average of 8.8 million dollars in the last twelve months.**

– BUILDING A TI PROGRAM

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.

70%

70% of C-Suite leaders in organizations surveyed said they plan to invest more in their organizations' threat intelligence programs in the next twelve months.

– BUILDING A TI PROGRAM

78%

78% of companies experiencing significant revenue growth plan to invest more in their threat intelligence programs over the next twelve months.

– BUILDING A TI PROGRAM

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.

Chapter 4

In Support of Sharing: A TIP Should Enable Communities, ISAC and ISAO

A 2014 STUDY BY THE PONEMON INSTITUTE:

"Exchanging Cyber Threat Intelligence: There Has to Be a Better Way," identified enhanced situational awareness and improved security posture of both organizations and the nation as benefits associated with shared Cyberthreat Intelligence (CTI). Also, it positioned internal data, data shared from industry peers, and feeds purchased from commercial vendors as the most valuable sources of shared CTI, in that order. **While this study highlights the need for better cooperation and sharing between cyber defenders, is this reality?**

41%

41% of cybersecurity decision makers with threat intelligence programs in place, report that sharing information with governments and other NGO groups is integral to their program development.

– BUILDING A TI PROGRAM

Until recently, many companies feared consequences – political, financial, insurance, and others, associated with admitting they had experienced a cyberattack, so they opted to remain discrete. Isolation prevented valuable CTI data from getting to organizations who may have benefited – preventing additional attacks. But, this is a fight that cannot be won alone. Criminal organization and advanced persistent threat groups are working together – sharing malware and other tools. To change the game and get ahead of those groups, organizations must work with one another and leverage the force of the community. Fortunately, the ethos for CTI-sharing is starting to change.

In early 2015, President Obama announced and signed an executive order to encourage companies to share their CTI and launched the Cyberthreat Intelligence Integration Center (CTIIC). This draws comparisons and criticisms to the current Information Sharing and Analysis Centers (ISAC) models and more, but overall is a great thing for the security industry. Sharing critical data can lead to uncovering related tactics and threats targeting specific industries or organizations, and private-sector organizations are seeing financial incentives emerge to encourage sharing.

The 113th Congress 2nd Session proposed legislation to provide incentives in the form of a tax credit to organizations who share cyberthreat intelligence. The chairman of the Senate Commerce Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security is leading the Cyber Information Sharing Tax Credit Act, which proposes "to amend the Internal Revenue Code to provide a refundable credit for costs associated with Information Sharing and Analysis Organizations" (ISAOs).

While CIOs, CISOs, and their threat intelligence and response teams are proponents of sharing threat intelligence data, this legislation speaks directly to private-sector management teams by providing financial incentives.

Financial incentives should increase private-sector awareness and the adoption of TIPs to encourage the implementation of CTI production best practices, and simplify and make sharing more secure through data classification, filtering, and controlled access. However, before an organization can begin sharing, it needs to mature its CTI capability. NIST, the National Institute of Standards and Technology, offers some practical guidance and building blocks to help organizations create a more mature CTI program.

In October 2014, NIST released their Special Publication 800–150, "Guide to Cyber Threat Information Sharing." This publication covers a variety of topics related to CTI sharing and can be a valuable resource to organizations regardless of their maturity. It specifically endorses the acquisition of external data and sharing relationships while recognizing that this is a more mature CTI capability. NIST states, "An organization should move from informal, ad hoc, reactive cybersecurity approaches where the organization operates in isolation to a formal, repeatable, adaptive, proactive, risk-informed practice where the organization coordinates and collaborates with partners" (p. 12). It goes on to recognize that basics like "establishing information sharing rules" and "joining a sharing community" are important first steps (p. 19).

A THREAT INTELLIGENCE PLATFORM:

Driven by Communities

A good TIP enables collaboration amongst cyber defenders as an out-of-the-box experience. It must be more than a simple information exchange or data feed, and the result must be threat intelligence which is timely, relevant, accurate, specific, and actionable.

A TIP should provide users the ability to match their personal and organizational interests to various communities of interest, whether by industry, threat, short-term events (like the World Cup or Olympics), geography, or more. This concept aligns very nicely with the ISAO (Information Sharing and Analysis Organization) concept that was mentioned in the Executive Order, because it aims to facilitate the creation of private-sector communities to collaborate around threat intelligence themes. Organizations who belong to an ISAC may find their ISAC is using a TIP for its analytic and sharing capabilities. Analysts want relevant intelligence to make smarter data-driven decisions, and a TIP that offers à la carte intelligence sources, collaborative communities, and defense integrations is ideal. CTI-sharing can be a complicated business, so a TIP should have communities that are provisioned to support member attribution or anonymity, while fine-grained access controls enable role specialization for each community user. A TIP community empowers organizations with the ability to create custom security labels and attributes, and provides automated redaction (stripping) when sharing data into a community. Each community member has the ability to receive automatic notifications when something of interest changes within the community, while activity logs capture historical information and threaded comments with hyperlinked context. This makes navigation through complex threat data easy.

Since the threat doesn't discriminate, having a TIP with secure community collaboration brings together the very largest and smallest of organizations to collaborate around common threats that they are facing.

Think of a TIP's communities as an analyst's early warning system. The ability to track infrastructure movements via community collaboration can create defensive actions that are dynamic, and in many cases, predictive. Sharing with the community effectively increases the number of analysts who are looking at the problem – potentially growing the dataset.

Another important, but not so obvious benefit, is analyst learning. Often, community members will share techniques on how to conduct analysis and find adversaries operating in their networks. Less-skilled analysts can develop new skills through community participation and collaboration.

Less-mature organizations should consider community participation. Gains made through the consumption of community data can help analysts secure permissions needed to support sharing into a community or enriching community data. Sometimes, getting management and/or legal permission to share can be easily obtained if some clear guidelines can be established.

Get Started Sharing

A TIP will have many communities that range from the most sophisticated to just getting started with CTI. Very sophisticated and mature organizations may regularly contribute threat intelligence data and can serve as role models for newcomers. Other less-mature organizations can learn from what these organizations are sharing as well as contribute their own data to support the community. Perhaps the following best practices provide some general guidelines for organizations who are just starting to share their threat intelligence.

Open Sources (Reports and Blogs):

Share reports and published articles as soon as they are uncovered. If the content is analyzed, it is helpful to have enrichments contributed too.

Spear Phish:

With a spear phish email, consider sharing the indicators associated with it along with any enrichments to an external or ThreatConnect ISAO/ISAC, private, and/or industry-themed communities. Consider redacting target or victim information before sharing.

Threat Groups:

After analysis related to a threat group is completed, share the data with the TIP's ISAO/ISAC, private, and/or industry-themed communities. In general, most tracking is done on an adversary using registrant email addresses and C2 nodes. However, sometimes tracking can be done using a target entity – a conference, geography, a conflict area, or an oil field as examples.

Historical Data as Enrichment:

Share historical indicators as enrichments whenever possible. Historical data, as illustrated in this community collaboration case study, can be quite useful in understanding patterns and trends.

As a general rule, share indicators whenever possible. Also, enrich community data whenever possible and share back into the community.

Organizations are stronger when they work together. Like the old adage, one stick is easy to break, BUT a bunch of sticks together are hard to break.

“All that is necessary for the triumph of evil is that good men do nothing.”

– EDMUND BURKE

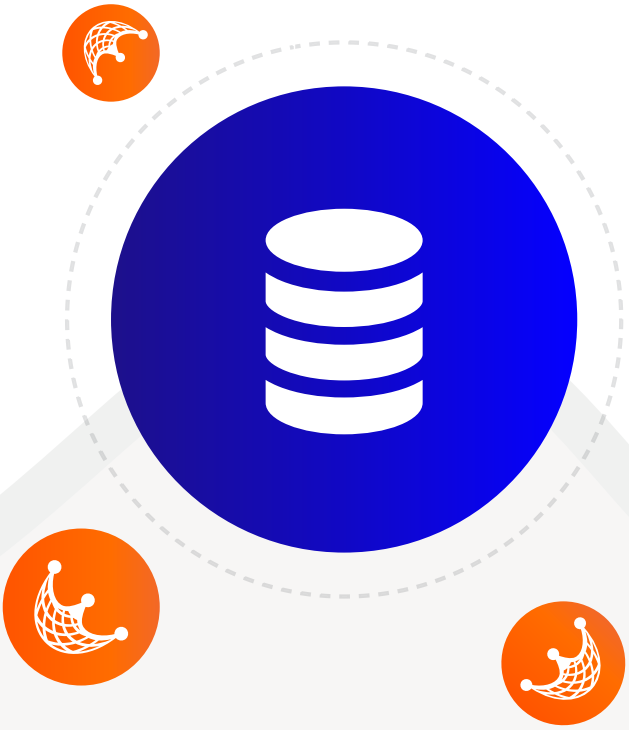
Chapter 5

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.

Action to Take Now:

Building Threat Intelligence Capabilities and Processes

IDENTIFY NEEDS

Get started by understanding your organization's specific needs for threat intelligence. This first step is perhaps the most difficult. Your organization should be asking this question again and again, as your needs, budget, and risk posture evolves.

LEVERAGE FRAMEWORKS

Leverage frameworks such as The Diamond Model for Intrusion Analysis and the Kill Chain to assist in planning your organization's processes.

IDENTIFY RESOURCES

Identify associated resources that will be required to collect, manage, analyze, act on, and refine usage. Resources include personnel, infrastructure, platforms, tools, and vendors.

TAKE ACTION

Establish means for acting on threat intelligence indicators through operational integrations in your defensive ecosystem, as well as making strategic changes to fill gaps in your security posture identified by the threat intelligence.

BUILD AND CONFIGURE

In order for a TIP to be considered a true platform, it should be extensible and mature enough to allow for customization and expansion. You should be able to build custom applications with ease directly within your TIP. You may possibly even take advantage of applications that others have built, or be a leader and share your custom applications with partners or the larger TIP community. With application development, hosting, and sharing within the platform, your analysts will spend more time on analysis and less time coding or manual processes.

REPEAT

Repeat the process as your organization's risk posture changes. Assets, business processes, opportunities, and threats evolve, and adversaries alter their tactics. Organizations must continually evolve with the landscape.

UNDERSTAND YOUR ORGANIZATION'S DATA AND ENVIRONMENT

Understanding your organization's data and environment helps you evaluate the information about emerging threats against your organization's data and operations. It also helps to identify sources of internal threat intelligence that can be collected.

COLLECT DATA

Perform data collection from identified sources. Aggregating your internal and external intelligence data will enable easier analysis.

ANALYZE DATA

Once data has been collected, analyze it with automated tools that identify the data that needs further scrutiny, including trends and red flags.

COLLABORATE

Collaborate with others within your organization, as well as with trusted partners, and industry peers to fill gaps in knowledge and build a picture of the threats you may face. Consult. If necessary, consult with experts in threat intelligence to help identify patterns and associations, which may not be immediately evident. These experts may exist within your industry, within your peer group, or within commercial intelligence teams focused on emerging threats.

AUTOMATE

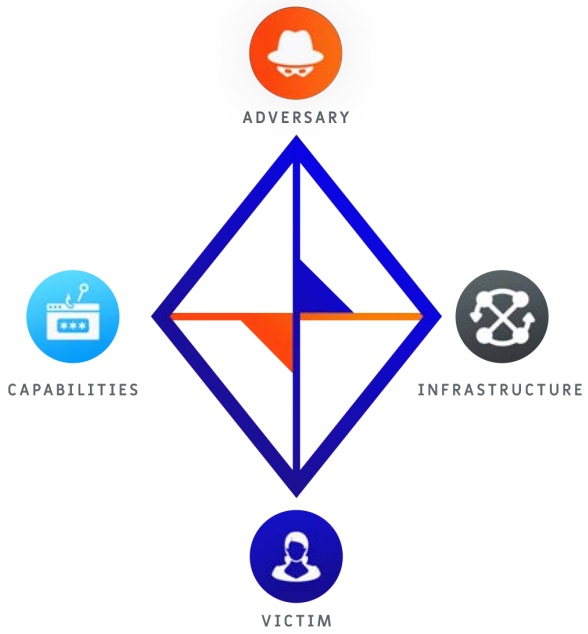
Many of these steps, particularly those relating to operational threat intelligence, can be automated using the right platform. The right platform should save an organization's time, money, and staffing resources while better equipping the organization with usable threat intelligence. Selecting the best threat intelligence platform for your organization is crucial to your ongoing success in defending your assets from adversaries.

SHARE KNOWLEDGE

Contributing insight back to the global community helps all TIP-based organizations become more resilient against threats. By sharing reports, indicators, and historical data as enrichments whenever possible, organizations with challenges similar to yours are better able to take action against existing threats. Sharing threat intelligence with ISAOs and ISACs enables better, faster adversary tracking.

Appendices

The Diamond Model for Intrusion Analysis



Overview

The Diamond Model for Intrusion Analysis is a methodology for carrying out intrusion analysis that focuses on hypothesis generation and testing to ask questions of intrusion-related data to inform decision makers of the best approach for mitigation. Since its goals as a methodology and framework are so closely aligned with that of a Threat Intelligence Platform (TIP), it is quite ideal as the inspiration for a TIP's data model. Analytic techniques defined by the Diamond Model can then be performed as a natural aspect of the mature TIP.

What is it?

The Diamond Model looks at each relevant "cyber" event and breaks it into four vertices or nodes. These vertices represent an adversary, capability, infrastructure, and victim. The edges between the vertices form a baseball-diamond shape; this is how the model got its name. Typically, an event can be described such that an adversary deploys a capability over some infrastructure against a victim.

Events do not typically happen by themselves but are part of a larger set of activity. Within the Diamond Model, each event can then be linked, based on a causal relationship, to the next to form a chain of diamond events. These chains are known as activity threads within the model and typically correlate to an incident.

The Diamond Model is flexible to work with existing or emerging ontologies of cyberactivity. The Diamond Model was not built to be an ontology or taxonomy itself, but rather a framework to enable analysis independent of the structure of the data. Each node on the diamond can be further characterized with knowledge about it, or the edges can be characterized to describe the relation between nodes on the same event or correlations between separate groups of activity.

Activity groups can be established in just this manner, by correlating nodes from events across incidents or knowledge of infrastructure or capabilities prior to them being used operationally. Once an activity group is established, it can be used for gaming and planning mitigation options.

Practical Uses of the Diamond Model:

PIVOTING:

Pivoting from knowledge you have for discovery of related data is naturally supported in the Diamond Model. Possibly related events and data can be formally tested with hypothesis generation and establishment of grouping functions to allow links to be established in a formal manner.

IDENTIFYING KNOWLEDGE GAPS:

Diamond nodes that are not populated within events, or even missing events in an activity thread, can be articulated with the Diamond Model and can help focus efforts for incident response where there are unknowns, or more broadly against a threat's capabilities and infrastructure.

"CENTERED" APPROACHES:

Centered approaches extend the concept of pivoting using the Diamond Model. There are six centered approaches. The first four focus on the nodes of the diamond: adversary centered, capability centered, infrastructure centered, and victim centered. The next two focus on meta-features of the diamond: social-political centered and technology centered.

- Victim-centered approach. Most organizations take this approach through network- and host-monitoring, detection, and defense operations. In the victim-centered approach, data related to a victim is used to learn about an adversary. Threat activities against a victim reveal the adversary's capabilities and infrastructure. In some cases, analysts have watched an attack in action in order to see how the adversary operates; this can allow organizations to predict who might be targeted next.

- Capability-centered approach. This approach, most commonly used by anti-virus manufacturers, looks at a specific capability. By focusing on a known capability, analysts can determine potential new victims, as well as the infrastructure and technology that support the capability. Also, analysts can gather clues to related capabilities and possible clues to the adversary's identity.

- Infrastructure-centered approach. Focusing on the adversary's infrastructure reveals the victims that are in contact with the infrastructure, the capabilities controlled by the infrastructure, any related infrastructures, and possible clues to the adversary.

- Adversary-centered approach. This is possibly the most difficult of the centered approaches to utilize. It requires direct monitoring of an adversary's activities in order to learn about their infrastructure and capabilities, so it's limited by the need for access to their operations.

- Social-political-centered approach. This approach does not lead directly to new elements or indicators. Rather, it uses an expected adversary-victim relationship to hypothesize who might be a victim and who is likely to attack that victim, or who might be an adversary and who that adversary might attack. For instance, organizations in one country might be targeted by a rival country with which it is at war.

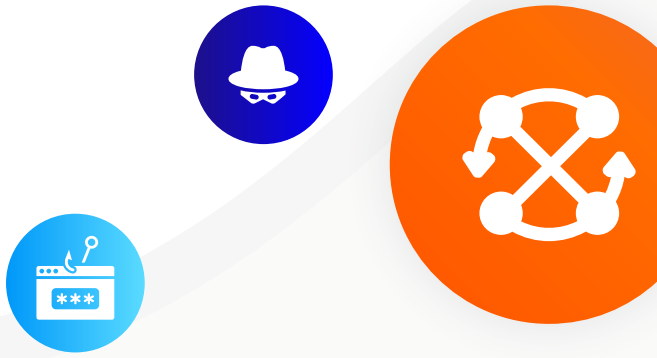
- Technology-centered approach. This approach looks at potential misuse or peculiar use of a technology. For instance, peculiar activity might indicate that adversaries are trying to find and exploit a vulnerability. The techniques they deploy can then be used to deduce which infrastructure and capabilities will be used to conduct a future attack.

CREATING ACTIVITY GROUPS:

The Diamond Model allows for the creation, growth, and ongoing testing of activity groups using the processes described in the overview.

SUPPORT COURSE OF ACTION DEVELOPMENT:

Course of action development or mitigation planning and execution can be facilitated using the Diamond Model. The model can be integrated easily with almost any planning framework. Further, measures of effect from actions taken against an adversary can be characterized in real-life or gaming scenarios.



Threat Intelligence Platform (TIP) Checklist

This handy list defines the key features of an effective TIP and provides a series of questions that make it easy to understand if a TIP will be able to keep your organization's assets secure.

1 Does the TIP have the ability to aggregate threat intelligence from multiple sources for alerting and blocking?

Your TIP should be able to ingest structured and unstructured sources of indicators and related context to streamline and automate the delivery directly into your security infrastructure for action. Some detailed questions to ask about this process include:

- Will the TIP support all of the various sources you need ingested, both structured (STIX, OpenIOC, IODEF, XLS, CSV, etc.) and unstructured (PDF, Office documents, email, etc.)?
- Do you need the TIP to ingest all of these sources in an automated manner?
- Does the TIP maintain the fidelity of relationships and context within the data imported?
- Can the TIP support trusted communities for receiving community-sourced threat intelligence?
- Does the TIP have an API for integration into the existing security environment?
- Does the TIP have out-of-the-box connectors or integrations into the security products within your network (SIEM, firewall, IDS/IPS, endpoint protection, etc.)?

2 Does the TIP have the capability to support signature management?

The TIP you select should be able to provide additional and necessary context around alerts from your various signature-based security devices. It should be able to work with all the signature types relevant to your security ecosystem (Snort, Yara, Bro, etc.). Maintaining context is critical here, and the TIP should be able to tell your team if a signature is related to a specific threat group or actor, what phase of an intrusion it is related to, and where the team should look for the next signature hits.

- Does the TIP support signatures?
- What signatures does the TIP support relevant to my security network?
- What does the TIP do with the signatures, how does it store them, and what can you do with them once imported?

3 Is the TIP capable of supporting Incident Response (IR)?

The TIP should assist your IR teams in coordinating tasks around their investigations, especially in relation to leveraging and building relevant threat intelligence. Some specific questions to ask about how a TIP will support your IR processes are:

- Does the TIP have the ability to notify your team when new information about an ongoing incident has become available, a new IOC has been discovered, or a mitigation recommendation has been made?
- Does the TIP allow for selected events from a SIEM or other network security endpoint product to be ingested, correlated with existing threat intelligence, and processed by the team?
- Does the TIP integrate with a ticketing system or otherwise provide a ticketing capability?
- Can you task others on your team to act on threat intelligence to quicken response times?
- Can you communicate with team members using messages in the TIP? If so, through private inbox, email, or chat functionality?
- Can you create customized context for incidents that you're tracking, such as what courses of action are or should be taken?
- Can you store knowledge of assets affected and exploits used along with the relevant threat intelligence indicators involved within your TIP?

4 Does your TIP fuse threat intelligence and enable threat research?

The TIP should allow your team to retrieve the knowledge stored there in an intuitive manner. Robust search and filtering capability is a must. If your organization will be performing fusion analysis to further refine knowledge of relevant threats and their capabilities, then the ability for your TIP to draw connections between indicators and incidents, threats, threat actors, and other elements will be paramount. Some specific things to look at while making your selection of a TIP are:

- How does the TIP handle information on the same indicator from multiple sources? Does it show the criticality ratings or indicator reputations and associations from each of the sources?
- Does the TIP allow for the deprecation of an indicator or its associations as the intelligence becomes stale or no longer relevant?
- Does the TIP allow you to pivot in ways that show otherwise non-obvious relationships, such as the Diamond Model-defined associations?
- Does the TIP support a visualization capability to view complex relationship graphs?
- Does the TIP allow for the creation of customized intelligence reports for management or sharing with other stakeholders? Does it have the ability to produce these reports using a structured language (such as STIX)?

5 Does the TIP enable intelligence-led decision making around your security?

Your TIP should allow the CSO or CISO to have situational awareness of current network-based threats to the organization. By acting as a historic knowledge base for security incidents and response engagements with detailed information on the threats behind those incidents, a TIP can allow your organization to be better informed when making risk decisions, taking mitigation actions, and making additional investments in security around the data or assets that threat actors are trying to steal. Some specific capabilities in this category to consider when selecting a TIP are:

- Does the TIP allow the generation of reports with metrics on threat actor trends and past behavior?
- Does the TIP allow you to characterize the effectiveness of response engagements?
- Can the TIP characterize observed threat actor capabilities; vulnerabilities exploited; hacker tools used; and tactics, techniques, and procedures (TTPs) leveraged?
- Can you create customized context for incidents that you're tracking, such as what courses of action are or should be taken?
- Can you store knowledge of assets affected and exploits used along with the relevant threat intelligence indicators involved within your TIP?

6 Does the TIP collaborate with trusted communities?

Collaboration within a trusted community can be the most effective source of threat intelligence you have, if managed appropriately. A TIP should allow your security team to collaborate with other trusted teams – whether across industries or within your organization. One or both of two sharing models will typically be supported.

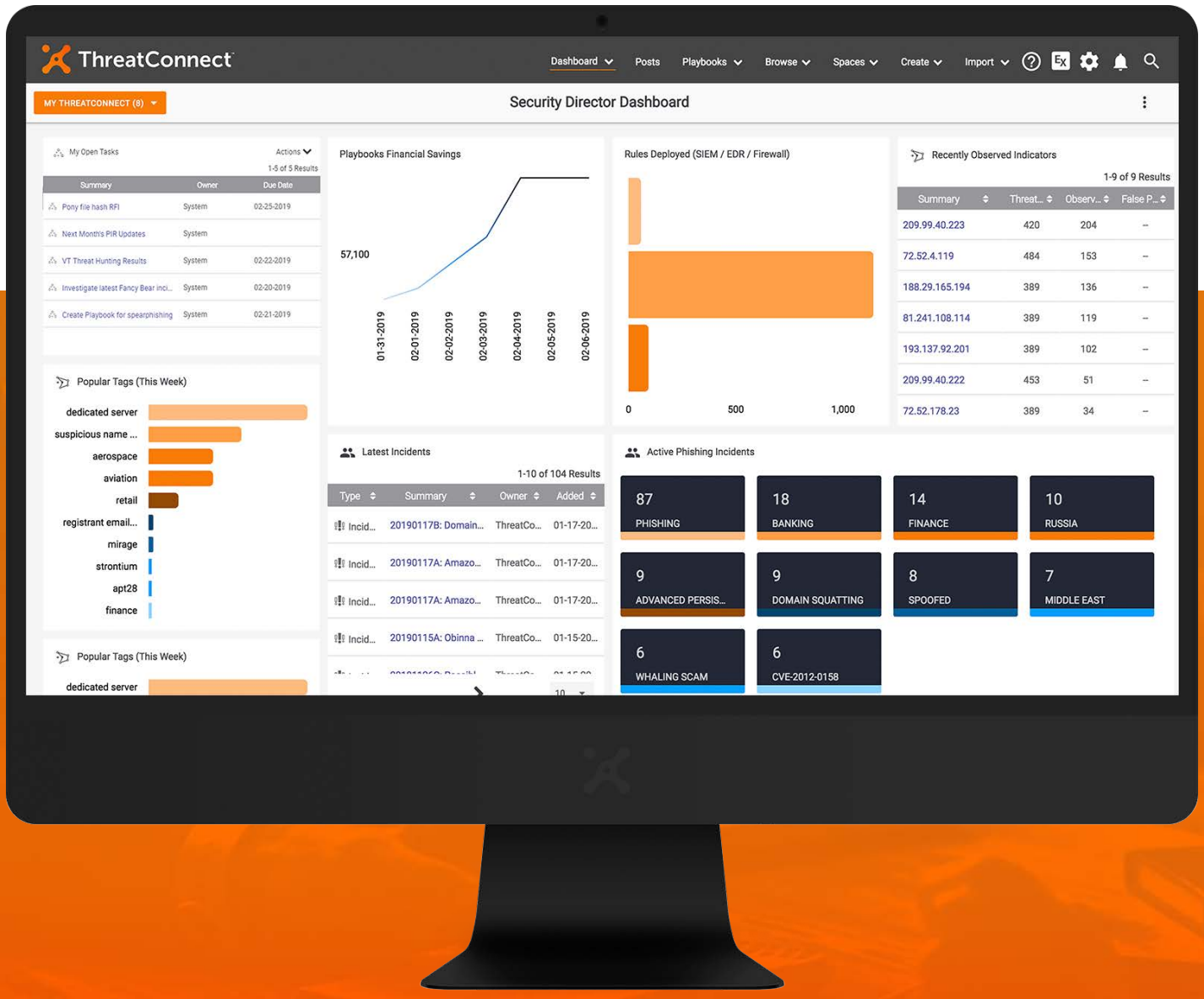
The first is seen with a cloud-based TIP, in which communities with multiple user organizations and accounts often have access to the same cloud instance. The second case is a federated model of sharing, in which threat intelligence is packaged between two instances of the TIP and data is exchanged between them. A third sharing model is that of an on-premises TIP. The on-premises instance allows sharing of threat intelligence and collaboration of data analysis between team members of one organization dispersed by geographic location, team/role, or level. Sharing threat intelligence between organizations is not as simple as just allowing the exchange of data; a TIP will need to take into account many considerations around access control, data markings or classifications, and acceptable use of the data shared. Some details to ask of your TIP are:

- Does the TIP facilitate access control to the data based on community membership or sensitivity?
- Does the TIP allow for granular security labels on the indicators, as well as specific context related to them?
- Does the TIP allow for role-based actions within a community?
- Does the TIP allow for multiple communities or trust circles?
- Does the TIP allow for communications between users in the community?

7 Does THE TIP allow you to create and share custom applications?

The TIP should give users the flexibility to build custom applications in an application runtime environment.

- Does the TIP offer a fully supported software development kit (SDK) and powerful API?
- How does the TIP let users build upon the platform?
- Can you share your custom applications with other users?
- Does the TIP approve applications for security (similar to an Apple iPhone app store or Salesforce AppExchange?)



Works Cited

WORKS CITED

Caltagirone, S. (n.d.). Diamond Model of Intrusion Analysis – A Summary. Retrieved from ActiveResponse.org: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond_summary.pdf

Caltagirone, S., Pendergast, A., & Betz, C. (n.d.). The Diamond Model of Intrusion Analysis. Retrieved May 1, 2014, from ThreatConnect: http://www.threatconnect.com/wp-content/uploads/ThreatConnect-The-Diamond-Model-of-Intrusion-Analysis.pdf

Camh, J. (2014, July 9). State Governments & the Future of Cyber Security Regulation. Retrieved July 10, 2014, from Information Week Bank Systems and Technology: http://www.banktech.com/compliance/state-governments-and-the-future-of-cyber-security-regulation/d/d-id/1279216

FBI – Intelligence Cycle. (n.d.). Retrieved July 1, 2014, from Federal Bureau of Investigation: http://www.fbi.gov/about-us/intelligence/intelligence-cycle

Fung, B. (2014, April 10). Washington is making it easier for businesses to swap notes on hackers. Retrieved July 9, 2014, from The Washington Post: https://www.washingtonpost.com/news/the-switch/wp/2014/04/10/washington-is-making-it-easier-for-businesses-to-swap-notes-on-hackers/

Holland, R. (2014, February 11). Actionable Intelligence, Meet Terry Tate, Office Linebacker. Retrieved August 13, 2014, from Forrester Research: http://blogs.forrester.com/rick_holland/14-02-11-actionable_intelligence_meet_terry_tate_office_linebacker

Hutchins, E. M., Clopperty, M. J., & Amin, R. M. (n.d.). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved from Lockheed Martin Corporation: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Lewis, J. A. (2014, March). Cyber Threat and Response – Combating Advanced Attacks and Cyber Espionage. Retrieved July 22, 2014, from Center for Strategic and International Studies: http://csis.org/files/publication/140313_FireEye_WhitePaper_Final.pdf

Mukaram, A. (2014, June 10). Cyber Threat Landscape: Forecast. Retrieved July 9, 2014, from Recorded Future: https://www.recordedfuture.com/cyber-threat-landscape-forecast/

Norse. (2013). Ponemon 2013 Live Threat Intelligence Impact Report. Norse Corporation.

NSA. (n.d.). Defense in Depth. Retrieved from National Security Agency: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

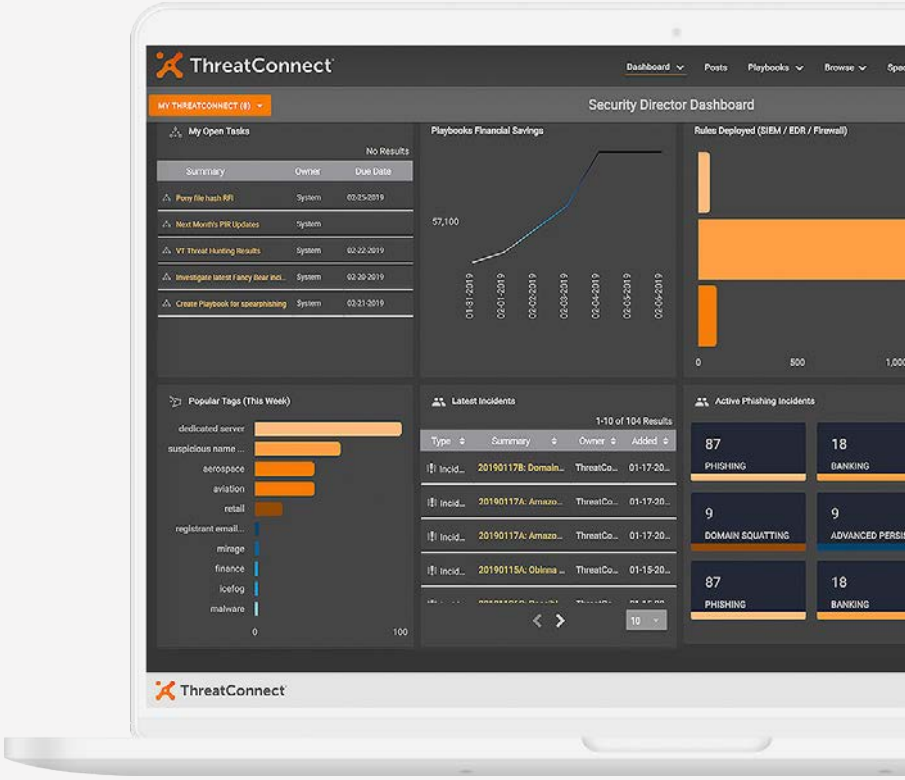
Quotes. (n.d.). Retrieved July 9, 2014, from The Official Website of General George S. Patton, Jr.: http://www.generalpatton.com/

Scenarios and Attack Graphs. (n.d.). Retrieved May 3, 2014, from Carnegie Mellon School of Computer Science: http://www.cs.cmu.edu/~scenariograph/

Structured Threat Information eXpression — STIX™. (n.d.). Retrieved May 1, 2014, from Making Security Measurable: http://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf

Interested in learning more about how ThreatConnect can help unite your security team and protect your enterprise?

THREATCONNECT.COM



Request A Demo

Call **1.800.965.2708** or visit **threatconnect.com/request-a-demo**

ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708