Threat Intelligence Platforms

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

TABLE OF CONTENTS

CHAPTER 1:

Know Your Enemy, Know Yourself

More than one-third of the world's population has access to the internet. And some of those people are not very nice. With high-profile breaches hitting companies as well-invested in security as Target, NASDAQ, Ebay, and Adobe, IT decision-makers know that it's only a matter of time until they face breaches of their own.

Today's threat environment is complex and dynamic. The internet was built for connectivity, not security, and 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. Organizations today face Advanced Persistent Threats (APTs) and organized, criminally motivated attacks launched by adversaries with the tools, training, and resources to 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, organizations need to react to threats. But if you are only reacting, you are playing a never-ending game of catch-up and clean-up. A big-picture view of the threat landscape and a proactive stance are necessary to protect organizations from the multitude of threats that are being launched toward them every day.

To develop this big-picture view and plan a proactive stance, organizations need to constantly harvest and process knowledge about their adversaries. 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 larger, more complex, and more efficient as time passes. Organizations have to constantly examine their defensive positions and adjust their operations and strategies to defend themselves against the evolving technologies and adversaries that endanger their assets. In the same way that an individual pays for a gym and attends it regularly to keep fit, organizations must make a continual investment and commitment to protecting their assets.

Any delay is a moment of risk. While your security professionals are meeting with vendors, some adversary is searching for a way to get into your network. 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.

Action Beats Reaction: Capture and Deploy Intelligence to Build a Strong Defense

Companies need to gather intelligence about the threats that endanger their systems. Intelligence provides companies with a means to fend off threats in progress and, in many cases, to prevent adversaries from ever infiltrating the network at all. The use of threat intelligence leads to a more holistic and 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, organizations 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 can 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 an organization to prioritize its defenses around highly-targeted assets, focusing on remedying 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), an organization can develop strong, practicable 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 SIEM, this is an ideal place to start, as several raw sources of internal network event data are already present here, such as event logs, DNS logs, firewall logs, etc. 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 the organization's security team or someone with specific knowledge of the 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 will typically be 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, an organization first needs to understand the types of threats targeting its assets. This requires the mapping of business processes to specific geographic, political, and industry-focused threat classes. Once the classes are identified, then the organization 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 will understand which intelligence is most relevant to it.

Variety. Incident detection and prevention should not typically rely on one medium, technique, or capability, and the threat intelligence used to enhance that incident detection and prevention should not do so either. Thus, for operational intelligence, a combination of host- and network-based indicators and signatures should be used. Likewise, a combination of indicators or other detection techniques that will 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.).

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.

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, then 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.

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 an organization's risk posture, security planning will drive architecture decisions and refine 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 will open 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 will yield wider access to data through deeper trust relationships with partners and access to more communities. As 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 leads to further opportunities to join additional private groups and benefit from the information shared within them.

CHAPTER 3:

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 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 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 will typically be 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 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.

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 the 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 times to live before they are dropped from the blocklist.

The TIP enables action on the intelligence by providing APIs and connectors for out-of--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 easy capacity to use threat intelligence in 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 they will generate when they fire), signatures that are contextually linked to a threat, 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 ability of a TIP to put signatures into context can speed response, minimize "alert confusion", and make 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.

Another powerful capability of a TIP is to enable the addition of 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.

A TIP can maintain historic data on assets and personnel targeted or compromised to trend adversary intent and objective. This will assist ongoing and future incident response engagements.

TIPs can aid incident response enhancement and metrics. During incident response engagements, a TIP that is integrated with end point 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 ability to share threat intelligence is facilitated by the TIP, which assists in its creation and enables the sanitization of any sensitive or controlled data, thus making the threat intelligence safe to 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 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, 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). 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 are many languages and standards emerging today, with MITRE's STIX language becoming a potential leader among the financial, tech, and US 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, 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 activity. A TIP uses these capabilities to provide 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 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.

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.

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.

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 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 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 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 organizations 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 their organizations' 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.

CHAPTER 4:

The Future of Threat Intelligence

Some aspects of threat intelligence are easily predicted. The number, type, and efficiency of threats and adversaries will continue to increase. Every advance in security technology entices hackers to test it. Organizations will have to invest greater resources in protecting their assets and will have to explore other ways to secure their networks, such as sharing and using community-driven initiatives to identify threats and mitigate risk.

Predictive analytics become ever more important as threats grow in number and sophistication. Predictive analytics use contextual data to predict trends and patterns. In order to aggregate information to the best extent, sharing between organizations – even rival organizations – will become the norm.

Federal and state government regulations dealing with cyber security have exploded in recent years and are expected to expand even further in the future. Recently, the SEC has issued cyber security guidelines for financial institutions and New York State has begun auditing financial firms cyber security defenses (Camh, 2014). Laws that require commercial organizations to share information are likely on the horizon. Already, the Justice Department has made it possible for businesses to share security data without breaching anti-trust laws (Fung, 2014).

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.

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.

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.

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.

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.

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.

Automate. Many of these steps, particularly those relating to operational threat intelligence, can be automated using the right platform. The right platform should save organizations' 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.

APPENDICES

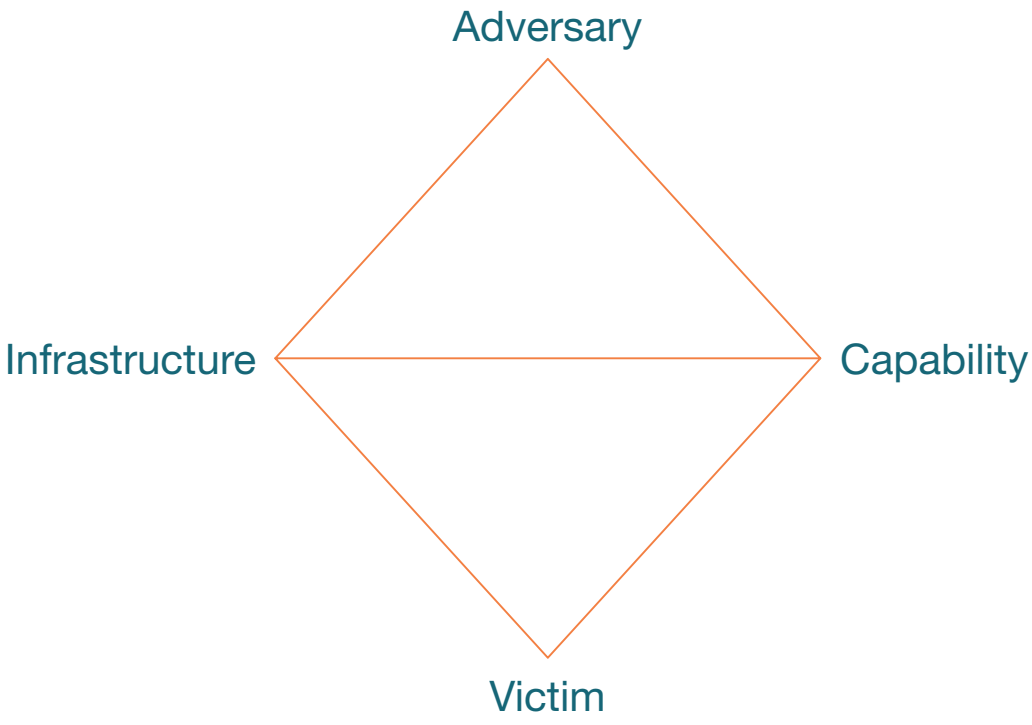
The Diamond Model for Intrusion Analysis

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 cyber activity. 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 are 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 approaches.

- **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, End Point 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?

#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?

WORKS CITED

Build Vs. Buy. (n.d.). Retrieved July 10, 2014, from ThreatConnect: http://www.threatconnect.com/why_threat_connect/build_vs_buy

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.com: http://www.threatconnect.com/files/uploaded_files/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 InformationWeek 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 Washington Post: http://www.washingtonpost.com/blogs/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

About Cyber Squared Inc.

Cyber Squared Inc., is a leading provider of advanced threat intelligence products and services including ThreatConnect®, the most comprehensive Threat Intelligence Platform (TIP) on the market. With a superior understanding of the relevant cyber threats to its clients' business operations, Cyber Squared determines risk and develops individualized, effective security strategies and processes for risk avoidance. ThreatConnect delivers a single platform in the cloud and on-premises to effectively aggregate, analyze, and act to counter sophisticated cyber attacks. The ThreatConnect TIP can be accessed by visiting www.threatconnect.com. Learn more about Cyber Squared Inc. and our other services at www.cybersquared.com.