LOCKHEED MARTIN

Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform

A White Paper Presented by:
Lockheed Martin Corporation

ABSTRACT

Threat Intelligence Platforms (TIP) are an emerging technology supporting organizations as they consume and then act on cyber intelligence. Lockheed Martin believes that a TIP helps an organization transition from relying solely on external intelligence sources to producing their own intelligence based on what is observed in their environment. The result is elevated cyber maturity and improved resilience against attackers.

1. INTRODUCTION

Within the past decade, computer network defense has shifted from a culture of sharing minimal information to one of intelligence overload. Previously, information regarding system breaches, malware, or attack attribution was rarely shared between organizations. Today the more common issue is how to sift through all the emails, reports, and indicators to identify actionable intelligence.

Threat intelligence is evidence-based knowledge about a threat that can be used to inform decisions regarding the response to that threat (McMillan, 2013). It includes the details of the motivations, intent, and capabilities of threat actors (Holland, 2014). In order to successfully defend against the multitude of Advanced Persistent Threats (APT) facing an organization, consuming external threat intelligence has become an increasingly important aspect of cybersecurity. However, exactly how to ingest the intelligence and successfully leverage it within an organization's environment often remains a challenge.

In addition to external intelligence, an influx of data from one's own organization can further complicate matters. Alerts from a myriad of technologies including Intrusion Detection Systems (IDS), firewalls, mail scanners, Host Intrusion Prevention Systems (HIPS), and proxies can overwhelm a defender who is trying to respond to and disposition each alert. External intelligence can quickly become an afterthought as there is no time to evaluate and implement countermeasures, making it useless. Conversely, external intelligence fed directly into these tools results only in more noise if it is not properly vetted for one's environment and mitigations are not appropriately tuned.

In order to process all of this internal and external data and have it result in actionable intelligence, a TIP can be employed. A TIP is the central management repository for all external and internal intelligence, and can provide the mechanism to act upon this intelligence.

This paper is organized as follows: section two of this paper documents related work on defining the requisite components of a TIP. Section three introduces an expansion of this definition that is based upon the Intelligence Driven Defense® approach to computer network defense. Section four outlines the seven ways an organization can apply the Cyber Kill Chain® framework in their environment using a TIP. Section five introduces the Palisade™ solution, Lockheed Martin's Threat Intelligence Platform, and section six summarizes the paper.

2. RELATED WORK

The analyst firms Gartner, Inc. and Forrester Research provide insight on the value of employing a Threat Intelligence Platform, and have each offered definitions of its components.

Gartner states that organizations looking for effective, automated methods to ingest multiple sources and formats of threat intelligence, correlate them, and act upon the information more efficiently should investigate using a TIP. They suggest that a TIP has the following six capabilities: 1) Collect intelligence from multiple sources in multiple formats and automatically enrich the intelligence; 2) Correlate intelligence and help determine which sources are the most effective; 3) Categorize intelligence to help perform analytics on threats, recognize tactics, techniques, and

procedures (TTPs), and understand relationships through modeling and visualizations; 4) Integrate the intelligence with workflow processes to further enrich existing data; 5) Provide action by supporting various integrations via Application Program Interfaces (APIs) and email notifications; and 6) Support the sharing of intelligence among trusted communities (Lawson, 2014).

Forrester states that the specific benefit of a TIP is providing Security Operation Centers with analysis platforms that can orchestrate intelligence activities. The platform should be capable of ingesting and normalizing threat intelligence, rating the value of intelligence sources, providing an analyst workspace, supporting visualization and pivoting, enriching the intelligence, and enabling the internal and external collaboration and sharing of the intelligence (Holland, 2015).

3. EXPANDING THE OBJECTIVE OF A THREAT INTELLIGENCE PLATFORM

Gartner and Forrester laid out the intention and minimal requirements for a TIP. Lockheed Martin expands on those requirements to ensure a TIP provides value in all environments. While a TIP should enable the collection of vast amounts of external intelligence, it should also provide the foundation for an organization to mature into a producer of intelligence.

An Intelligence Driven Defense® approach to computer network defense has been advocated by Lockheed Martin for over five years (Hutchins et al., 2010). The central theme is that you can learn from past intrusion attempts to generate actionable intelligence that can be put back into your defenses to make you more resilient against advanced adversaries. Connecting the dots between seemingly different data points allows a defender to recognize relationships among incidents and identify common characteristics. This allows the analyst to understand the tactics, techniques, and procedures (TTPs) of their adversary. The more complete the profile that is built on an adversary directly targeting your network, the greater the opportunity to be one step ahead of them.

Without a dedicated tool to store all the information and context gleaned from an investigation, identifying those commonalities becomes impractical. In the absence of a TIP, an analyst has few options to capture the data that otherwise could provide keen insights on an attack. Spreadsheets or text files on a SharePoint site do not allow an analyst much flexibility to correlate events by leveraging historical knowledge. For example, if you identify malware that beacons out to an IP address, how can you determine whether you have previously seen that IP address in your environment? A TIP should provide the location for an analyst to input all the indicators, context, notes, intelligence, recommendations, evidence, and adversary profile information discovered during their investigation and ensure everything is easily searchable. Furthermore, a TIP should support the Cyber Kill Chain® framework for this analysis as it is central to an Intelligence Driven Defense® posture. This approach can help an analyst quickly determine the severity of an attack and then identify gaps in either the analysis or the organization's defenses.

External intelligence can be an important facet of computer network defense, and a TIP should support its consumption. However, dependence on those sources is reduced as an organization's cyber posture matures. External intelligence can provide insight into potential threats while an organization works to adopt an intelligence driven approach and develop their own analytic capabilities. As internal capabilities mature, external sources should be used to correlate what is seen in the environment and provide greater context and insight to the adversary's TTPs. The TIP should also provide a mechanism to measure those external sources, making it easy to determine which provide value. Those not beneficial to your organization should be removed – an action that will reduce noise and save money.

4. SEVEN WAYS TO APPLY THE CYBER KILL CHAIN® WITH A THREAT INTELLIGENCE PLATFORM

The Cyber Kill Chain® framework for computer network defense is not something that can be placed into an enterprise's defenses. However, there are seven ways to apply it within an organization to mitigate risk, build true resilience, better communicate, and meaningfully measure results (Hutchins, 2014). Each of these applications can be achieved or augmented with the use of a TIP that manages threat intelligence and enables an analyst to identify broader campaign activity by leveraging historical data.

4.1 PRIORITIZE SENSOR ALERTS

With so many alerts coming from so many sources, which alerts should be analyzed first? Which sensor is the most important and demands immediate attention? In order to answer these questions, an organization should list the events that are produced by each sensor and map them to the relevant stage of the Cyber Kill Chain®. The further down the attack chain to which an event maps, the higher the priority of that alert. For example, an event produced from a Network Intrusion Detection System (NIDS) maps to either the first stage, Reconnaissance, or the third stage, Delivery. However, an event from a HIPS maps to stage four or five, Installation or Exploitation, or perhaps even stage seven, Action on Objectives. Thus alerts coming from the HIPS should be evaluated first, because they correspond to the potentially more damaging event.

A proper Threat Intelligence Platform can help an organization with this by automatically ingesting alerts from a Security Information and Event Management (SIEM) or SIEM-like device that aggregates and normalizes events. The alerts should be ingested by the TIP and prioritized based on the original source of the alert. Those mapped to later stages of the Cyber Kill Chain® process should be associated with a higher priority and be displayed for an analyst to respond to first. The TIP should also provide the functionality for the analyst to respond to the alert within the tool. That way if it is an intrusion or attempted intrusion, indicators can be documented, and notes recorded to explain how the investigation was conducted. Standard courses of action can also be documented so that similar alerts are dispositioned and addressed in a repeatable and efficient manner.

4.2 PRIORITIZE ESCALATION

Another common problem for analyst teams is knowing with whom to report each attempted intrusion into the network. Investigation of an incident through the Cyber Kill Chain® framework can quickly determine the severity of the attack. Was a malicious email delivered to a recipient's inbox? Is a computer on the network communicating with a known command and control IP address? Once again, the further down the kill chain the attack progresses, the higher the incident should be reported in an organization's management chain. If an attack results in Action on Objectives – meaning the adversary was able to exfiltrate data from the network – the impact could potentially require notification to the organization's CEO or Board of Directors. On the other hand, a "shielded" attack, where malware has been installed on a host computer, but there is no command and control, may only need to be reported up to a Chief Information Security Officer, as this sort of compromise has much less impact on the organization.

A TIP can provide the platform for an analyst to record all results from the investigation of an intrusion. When an alert comes in, an analyst gathers data points and documents them in the TIP. The analyst then studies the data to understand the alert and identify how far the intrusion progressed. The TIP can map key pieces of intelligence to the stage of the Cyber Kill Chain® stage from which it was pulled to determine how far the intrusion advanced and the level of impact to the organization. This can then align directly to the level of escalation required to communicate the impact.

4.3 PRIORITIZE INVESTMENT

Establishing a return on investment for security products can be an arduous task. Building a business case for future investments can be even more difficult. An organization can visually display where protections exist that detect, deny, disrupt, degrade, and/or deceive an intrusion attempt at each stage of the Cyber Kill Chain® process. A graph showing each stage of the process on one axis and the countermeasure along the other can then identify the tool in place to perform the mitigation at that stage in the box where each intersects. An empty box indicates gaps where investments can be made to further enhance the organization's protections. An example of this type of graph is shown in Figure 1.

A TIP can provide this type of graph as output by associating mitigations for every intrusion attempt to each stage of the attack. A case can then be made to invest in tools that would fill the gap areas in an organization's countermeasures. Not every box would need to be filled for every organization, but the further along the Cyber Kill Chain®, the greater the priority. For example, there may not be a need to degrade Reconnaissance activity, but there would certainly be a need to detect a command and control channel.

Additionally, TIPs could help an organization identify data gaps and source collection requirements. As analysts investigate intrusions and intrusion attempts, those stages lacking data can lead to investments in tools to close the gap.

4.4 MEASURE EFFECTIVENESS

As previously stated, attempted attacks should be investigated, analyzed, and synthesized using the Cyber Kill Chain® framework. The stage at which the attack was stopped should be documented. The goal is that over time attacks would be stopped earlier and earlier in the process.

Once again, a TIP can be the platform for an analyst to record the results of the investigation, analysis, and synthesis of each attempted intrusion. The identification of where in the Cyber Kill Chain® process the intrusion was stopped can also be recorded as a data point within the TIP. Another output of the TIP could then be a graphical representation of these stopping points over a period of time. Ideally the TIP would show a trend of analysts recognizing and preventing adversaries from reaching later stages of the kill chain, and thus becoming more effective. An example of this graph is shown in Figure 2.

	Detect	Deny	Disrupt	Degrade	Deceive
1 Reconnaissance	Web analytics	Firewall ACL			
2 Weaponization	NIDS	NIPS			
3 Delivery	Vigilant User	Proxy filter	Inline AV	Email Queuing	
4 Exploitation	HIDS	Vendor Patch	EMET, DEP		
5 Installation	HIDS		AV		
6 Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
7 Actions on Objectives	Audit log			Quality of Service throttle	Honeypot

Figure 1: Countermeasures

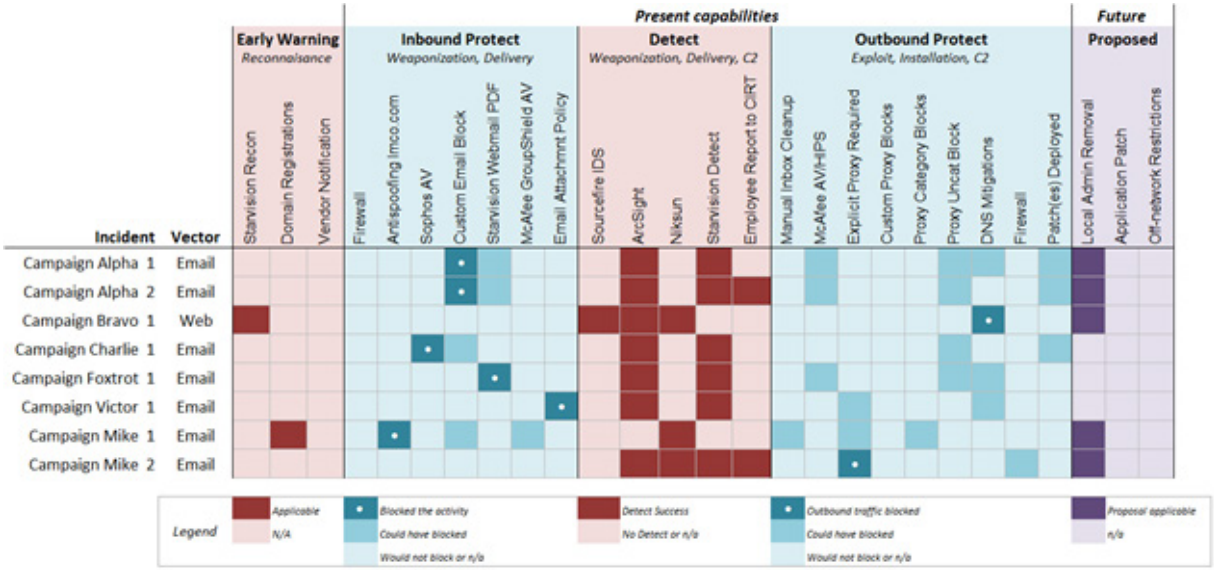

Figure 2: Measuring Effectiveness Scorecard

4.5 MEASURE RESILIENCE

If an intrusion is blocked in an early Cyber Kill Chain® stage and the organization's detections and mitigations are effective, is the organization also resilient? In other words, if it weren't identified and stopped at that point, would it have been caught lower down the kill chain? Were there layers of security in place that would protect an organization in a future attack if the adversary changed that one particular tactic, signature, or indicator? This is determined after synthesizing an attack through the entire Cyber Kill Chain® cycle – regardless of how early it is stopped. Understanding what would have happened had the adversary been successful is just as important as understanding what did happen. Understanding where defenses are in place at every stage of the kill chain – including those past the point of initial detection – is understanding how resilient the organization is. The goal is to be effective and block intrusions early in the Cyber Kill Chain®, but also to be resilient and have layers of countermeasures in place.

Once again a TIP can associate countermeasures to each stage of the Cyber Kill Chain® framework for every intrusion attempt. This includes those later stages that the attempted intrusions did not actually reach. The TIP can reveal the level of resiliency for each investigated incident and could provide the mechanism to compare the resiliency against intrusions over a period of time. As with effectiveness, the trend would hopefully show that the organization is becoming more resilient over time, with multiple countermeasures in place for each intrusion attempt.

4.6 MEASURE ANALYTIC COMPLETENESS

As has been previously discussed, an analyst's investigation does not stop with identifying and stopping an attack. One must also analyze how the attack occurred, and synthesize what would have happened had it not been stopped. This complete understanding of the potential incident can be measured against the Cyber Kill Chain® framework, which can be used as a pseudo checklist to ensure the analyst has mined all possible information. The idea of pulling data from every piece of the investigation is a critical component of the Intelligence Driven Defense® approach, as it is what provides the intelligence that informs one's defenses.

The output of good analysis is a lot of data and intelligence. Managing that data and intelligence is a function of a TIP. Furthermore, a TIP that employs the Cyber Kill Chain® framework

for an investigation can help ensure analytic completeness. It can force the analyst to think about each step to encourage a complete understanding of the intrusion attempt: Do I understand each of the stages for this attack? Have I fully investigated, analyzed, and synthesized all the information I could possibly collect? A TIP should enable an analyst to become effective at computer network defense by providing a mechanism to produce one's own threat intelligence.

4.7 IDENTIFY AND TRACK CAMPAIGNS

The final way to apply the Cyber Kill Chain® process within an organization is to group intrusions from the same adversary together into campaigns. This broader view provides insight into when a particular adversary attacks, the TTPs they commonly use, and how effective and resilient an organization is against that adversary. An organization can then prioritize and measure themselves against each adversary to further enhance their defenses. Establishing campaigns also provides a standard nomenclature to improve communications. This enables analysts to be more efficient when identifying intrusions, understanding potential next steps, and applying the proper defensive response.

An effective Threat Intelligence Platform enables analysts to determine patterns of malicious behavior learned from previous events to better address future attacks. All the data from previous investigations and the intelligence that is mined from analyzing and synthesizing intrusion attempts must be centrally stored and easy to search to enable identification of these patterns and quick recognition of relationships. Analysts connect intrusions by correlating indicators or TTPs from multiple Cyber Kill Chain® stages to determine that an attack is coming from a previously seen adversary. A powerful example of this is being able to recognize that the adversary scraping your external Web servers looking for documents is the same adversary who then sends a phishing email with a weaponized press release.
The TIP can facilitate this correlation because it holds all the intelligence and previous incident analysis.

Since the TIP is also the central location for all campaign mapping, a Campaign Heat Map or similar measurement of adversary activity should

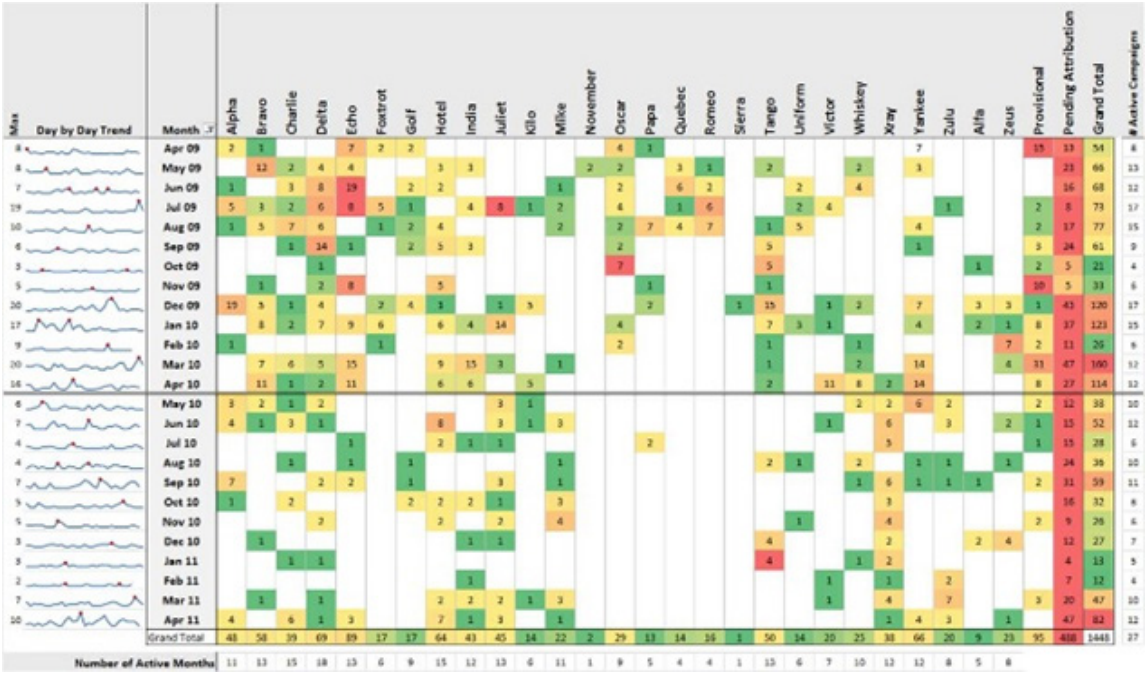

Figure 3. Campaign Heat Map

be an output of a TIP. This heat map can help organizations build a profile of past and current adversary activity, helping them better understand when, where, and how they will attack again in the future. A sample Campaign Heat Map is shown in Figure 3.

5 . THE PALISADE™ PLATFORM

Lockheed Martin developed the Palisade™ solution to enable analysts to correlate malicious activity. It is not just an intelligence ingest engine or broker; it is a tool for analysts that supports the adoption of the Intelligence Driven Defense® methodology. Palisade™ is a centralized platform that integrates with an organization's SIEM to provide enterprise-wide alerting capability and manage all threat intelligence – internal and external. It also enables the tracking of countermeasures to ensure the organization is properly acting upon the intelligence that has been mined.

The Palisade™ solution empowers analysts to focus their efforts and adopt an Intelligent Driven Defense® approach by providing a platform for incident investigation and response that is aligned to the Cyber Kill Chain® framework. It allows for the identification of broader campaign activity through the connection of disparate events by leveraging historical intelligence from previous incidents. The Palisade™ platform is an enabler for a more effective approach to computer network defense – an approach that is fueled by analyst tradecraft and intelligence.

6 . CONCLUSION

Threat Intelligence Platforms are an emerging technology that help an organization to consume and then act on cyber intelligence. Rather than relying solely on external intelligence, a TIP can also enable an organization to transition to producing their own actionable intelligence. This is a more reliable, sustainable, and cost-effective model for the long-term defenses of an organization. Properly employing a TIP can enhance an organization's cyber maturity and improve resiliency against advanced adversaries through the adoption of an Intelligence Driven Defense® approach to computer network defense. This can mean the difference between a reactive and vulnerable security state and a proactive, or even predictive, computer network defense posture that is capable of identifying and stopping current attacks, and preventing future attacks.

References

Rick Holland. Threat Intelligence Buyer's Guide, 10 February 2014. URL https://digital-forensics.sans.org/summit-archives/cti_summit2014/Threat_Intelligence_Buyers_Guide_Rick_Holland.pdf

Rick Holland. Threat Intelligence is Like Three Day Potty Training, April 2015. URL https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf

Eric Hutchins. Understanding the Cyber Kill Chain™: Applying Intelligence to Computer Network Defense, Rick Holland. Threat Intelligence is Like Three Day Potty Training, April 2015. URL https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf

Eric Hutchins, Michael Cloppert, Rohan Amin. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2010. URL https://isgs-gen.external.lmco.com/sites/ECS/Marketing/White%20Papers%20and%20External%20Publications/Cyber%20Kill%20Chain%20Whitepaper.pdf,

Craig Lawson. Technology Overview for Threat Intelligence Platforms, 10 December 2014. URL https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms

Rob McMillan. Definition: Threat Intelligence, 16 May 2013. URL https://www.gartner.com/doc/2487216/definition-threat-intelligence

For more information on cybersecurity solutions
Email: cyber.security@lmco.com
Phone: 855-LMCYBER (856) 562-9237
www.lockheedmartin.com/cyber

PIRA# CMK201507003