CYBER THREAT INTELLIGENCE

White Paper

Danny Pickens
Director, Cyber Threat Intelligence
Optiv

Rafal Los
Managing Director, Solutions Research
Optiv

Chris Davis
Consultant, Cyber Threat Intelligence
Optiv

Courtney Falk
Consultant, Cyber Threat Intelligence
Optiv

Matthew Shrock
Consultant, Cyber Threat Intelligence
Optiv

INTRODUCTION

Optiv research has identified a key challenge to the impact of cyber threat intelligence: the heavily diluted term "threat intelligence" attaches to a diverse array of products, services and capabilities and is not easily adopted across the various enterprise security use cases. Our experience shows that to solve this challenge, we must understand that intelligence is the connective tissue between knowing your enemy and a security strategy that enables decision advantage to significantly reduce business risk. Optiv's newly formed Cyber Threat Intelligence solution helps clients plan a holistic approach to their threat intelligence plan, then build and run successful cyber threat intelligence programs.

Tailored to each client's maturity level, unique resources and goals, this solution provides real impact to client operations and business alignment to realize a full return on their technology investments. Cyber threat intelligence is more than tools and "intelligence" feeds; it is the ability to more rapidly detect threats, perform targeted response and plan intentional security strategies. A properly defined and operationalized cyber threat intelligence solution acts as a purposeful planning tool to align the organization's threat model, security operations and business goals.

CYBER THREAT INTELLIGENCE

Cyber threat intelligence is an ecosystem that supports the decision-making process resulting from the collection, analysis, dissemination and integration of threats and vulnerabilities to an organization and its people and assets. In cyber security, intelligence information includes data concerning threats and vulnerabilities, both internal and external to an organization, that are potentially malicious in nature and may result in the compromise of systems or other assets, leading to the exfiltration of sensitive data. By receiving routine and time sensitive intelligence data from both indigenous and peripherally deployed collection elements, organizations can cross-cue among internal intelligence collectors, rapidly disseminating plans of action to satisfy all levels of requirements.

Optiv believes cyber threat intelligence is both process and product. The primary task of the intelligence process is to synchronize the information gained through collection activities to provide a consumable product to stakeholders, including senior leadership, clients, operational functions and incident response teams. The intelligence process tasks are based on established intelligence requirements set by these stakeholders or those in the organization that have been identified as the consumers of the intelligence.

Cyber threat intelligence supports the following cyber security objectives at an operational level:

- **Provide Indications and Warning (I and W)**
  Indications and warnings are used to identify and prevent vulnerabilities from being exploited within the network, as well as informing operations of potential attacks to the organization from known threat groups and their determined courses of action.

- **Perform Situation Development**
  Situation development is the provisioning of intelligence support to incident response in the event of a security incident or breach. Use this information to keep the incident response team and management aware of any new or anticipated developments throughout the incident response engagement and to provide targeted intelligence on the attacker to help remove the threat from inside the organization.

- **Support Organizational and Asset Protection**
  Supporting organizational and asset protection consists of daily intelligence operations and is used to provide insight on current and emerging threats that could negatively affect the organization. Additionally, it should include identifying the organization's high value or critical assets and their associated risks and vulnerabilities based on the organization's threat model.

- **Enable Machine Readable Threat Intelligence**
  Automated and machine ingestible intelligence information can be used to provide alerting, detection and prevention of known threats by consuming them through devices such as Threat Intelligence Platforms (TIPs), security information and event management (SIEM) systems and other security controls and devices.

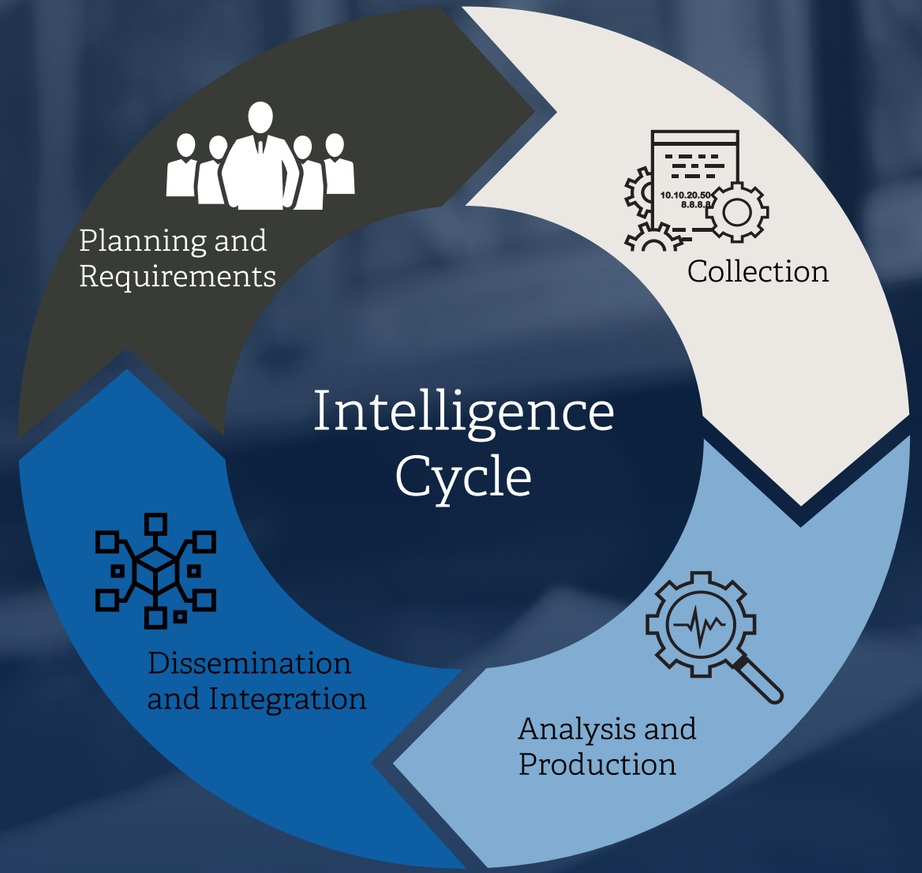
In cyber security, intelligence should be the driving force of security operations. The outputs of operational cyber threat intelligence operations help organizations identify or anticipate known or pending attacks based on an organization's security posture against threat actors' known tactics, techniques and procedures (TTPs).

THE INTELLIGENCE CYCLE
(Figure 1)

The intelligence cycle is the base methodology that directs the intelligence function to reach an actionable assessment or recommendation and provides a finished product to identified stakeholders.

The four elements of the intelligence cycle are:

- **Planning and Requirements**
- **Collection**
- **Analysis and Production**
- **Dissemination and Integration**



PLANNING AND REQUIREMENTS

The goal of an intelligence requirement is to define what data an analyst needs to collect to fill a knowledge gap. It is important to define the requirement as strictly as possible so the analyst does not waste time and resources collecting unnecessary or conflicting information. It also helps the analyst determine which collection sources are best to gain the information. Intelligence requirements mandate that you answer them as part of a strategy to analyze the threat or operating environment, often tied to the output of a threat modeling exercise. Requirements break down into three categories: intelligence requirements, collection requirements and production requirements.

Defined by the consumers, **intelligence requirements** include knowns and unknowns that revolve around questions the intelligence function needs to answer to make judgment-based, knowledge backed decisions. This provides an advantage for the client by supporting decisions with empirical data. **Collection requirements** define the data sets and sources required to collect the right information to answer the original intelligence requirement. **Production requirements** allow the intelligence function to have a defined template and cadence for the intelligence product output. *See the figure two graphic on page four.*

COLLECTION

Collection is the acquisition and triage of data needed to answer the established intelligence requirements. This data can include machine readable threat intelligence, raw data flow ingested by security devices to detect and prevent malicious activity, as well as intelligence information provided by a human analyst to enrich the production of finished intelligence reporting.

Using intelligence and collection requirements, members involved in the intelligence function are encouraged to develop a collection management plan. This plan is necessary to map all sources of intelligence collection, both internal and external, to ensure they can provide data to answer the stakeholder's requirements.

An additional necessity within the collection process is the ability to house the intelligence information from disparate sources. This involves the procurement and use of a Threat Intelligence Platform (TIP) to enable source management and the collaboration, enrichment and secondary development of intelligence throughout the analyst workflow.

ANALYSIS AND PRODUCTION

Intelligence analysis involves collaboration, data enrichment and secondary development around collected intelligence information, or what Optiv describes as the **analyst workflow**. Using this workflow allows for the production of finished intelligence, with output aligned to the consumer's production requirements. By using a TIP, the analysts can ideally collaborate based on tasking to add contextualized information pertinent to the business through enriching collected intelligence. This enrichment, known as secondary development, provides the uniqueness that aligns the analysis to the established intelligence requirements. This analyst workflow is necessary to ensure ease of use by the consumer.

DISSEMINATION AND INTEGRATION

The final piece of the process is the distribution of, and execution against, the acquired intelligence. Distribution takes place through the proper dissemination of intelligence, integration into the necessary security controls, modifications to the policies of an organization and consumption by the designated stakeholders.

Dissemination

Proper dissemination of actionable intelligence provides the most value and applicability to intelligence stakeholders. An intelligence analyst must be able to provide relevant threat information that is timely, well laid out and actionable. The analyst should be a trusted source for intelligence information so the consumers will listen to and act on the information.

Integration

Integration consists of implementing rules, signatures and policies on security devices that stem from the technical analysis included in a finished intelligence product or from the acquired machine readable threat intelligence.

The above application of the Cyber Threat Intelligence Process Model is a base for intelligence teams to mature their efforts and maintain alignment with stakeholders. Successful use of intelligence at the enterprise level requires alignment to the business and must be used as an enabler for security and business operations. Optiv's Cyber Threat Intelligence Workshop was developed to advise and assist clients with planning, building and running or maturing their intelligence functions in alignment with our frameworks. This gives organizations a competitive advantage over their attackers.

REQUIREMENTS WORKFLOW

(Figure 2)

Intelligence needed by the decision maker:

- *Will we be targeted for sponsoring the 2016 Olympics?*

Which sources collect against actors or groups?

» Identify vendor

Have we been targeted in conjunction with previous athletic sponsorship?

» Analysis of previous incidents (internal source)

Who has suffered targeted attacks due to sponsorship?

» Historical news or vertical analysis

Chief Marketing Officer:

- **Product:** Risk assessment for sponsorship
- **Cadence:** One time brief

CISO:

- **Product:** Brief on current situation IRT actor(s)/group(s) anticipated to target organization and known most likely and most dangerous courses of action based on capabilities and TPPs.
- **Cadence:** One time brief prior to the Olympics; daily/weekly update

SOC Manager / Operations / Incident Report:

- **Product:** Brief on current situation IRT actor(s)/group(s) anticipated to target organization and known most likely and most dangerous courses of action based on capabilities and TPPs.
- **Cadence:** One time brief prior to the Olympics; daily/weekly update
- **Product:** Most likely vulnerabilities that will be exploited, known exploit kits and tools to be utilized, patch management strategy and social engineering initiatives.
- **Cadence:** One time report in advance of Olympics. Continuous updates as further intelligence is collected and analyzed (ad hoc).

PROGRAM STRATEGY AND MATURITY

A cyber threat intelligence program must be a strong complement to an existing enterprise security framework. The addition of both internal and external threat monitoring, coupled with specialized tools and processes, improves an organization's ability to prevent, detect, respond and recover from incidents that negatively impact its ability to effectively operate their business. The key to successfully incorporating the concepts of cyber threat intelligence is through a program strategy approach, where purpose-driven maturity is governed and measured against organizational goals and objectives.

As with any other part of the enterprise security program, cyber threat intelligence must support a broader mission objective, otherwise it becomes a distraction and resource drain without purpose. First, take the time to understand how the addition of a cyber threat intelligence capability can support the organization's mission, then develop an implementation strategy that aligns to organizational growth and objectives and supports tactical, operational and strategic goals.

To support this effort of our clients, Optiv has developed a Cyber Threat Intelligence Program Workshop. Through this workshop, clients can:

- **Focus on their security goals**
- **Define an achievable roadmap**
- **Focus on maturing capabilities with a defined strategy**
- **Define a complete operational, actionable framework**
- **Provide a framework for measurable results and benchmarks**

THE CYBER THREAT INTELLIGENCE MARKETPLACE

The marketplace for cyber threat intelligence is currently wide and varied. It's important to understand the different products and vendors that are available so companies can choose the best fit for their organization.

At one end of the spectrum are Threat Intelligence Platform (TIP) providers, such as Threat Connect or Anomali, and endpoint vendors, such as CrowdStrike or Carbon Black, who have threat intelligence automated into their client agents. These vendors specialize in collecting and aggregating threat indicators, malicious actor tactics, techniques and procedures (TTPs) and providing a space for either human analysis or the automated output for detection and prevention.

At the more strategic end of the threat intelligence spectrum are vendors like the Ponemon Institute, Gartner and IDC. These firms produce in-depth, analytic reports that describe the state of threat intelligence as a whole.

No one tool or vendor is a perfect fit for every client. Because every organization and budget is different, each solution and implementation must be customized for the client. As organizations better understand cyber threat intelligence and how to best integrate it into their own workflows, their desired solutions will change as capabilities mature.

Breaking Down the Marketplace

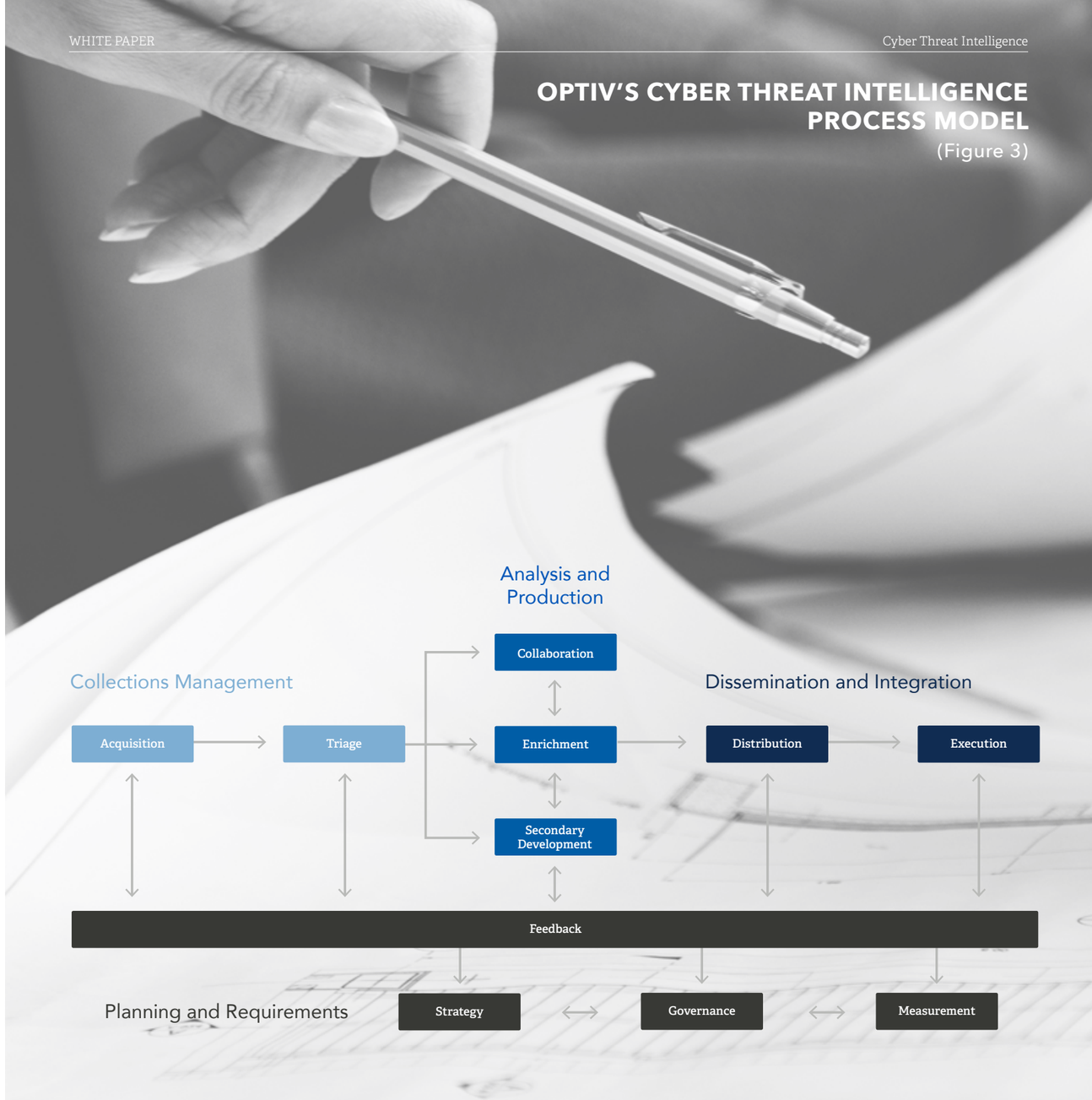
On average, organizations spend $112 million on all IT operations, including licensing and maintenance fees, labor costs and investments in supporting technologies and overhead. Of that budget, an average of 7.4 percent is allocated to IT security, with 9.3 percent going to threat intelligence operations (both internal and external).[1]

From our research, approximately one-third of enterprises studied have bought into the threat intelligence solution space because they believe there is value in the capabilities they can deliver to the business. Yet very few have been able to articulate that value in a meaningful and business-relevant manner. Furthermore, market confusion and micro-segmentation have contributed to an untenable situation for many security leaders as they struggle to operationalize competing technologies, vendor priorities and to integrate all of these into workflows in their security operations. The solution space is highly fractured with niche products, boutique services and little cross-industry cooperation and integration capabilities. This forces enterprises to develop their own program models and operational strategies, and to integrate disparate solutions into their program frameworks.

As technology and research matures, the possibility of finally ending dependence on signatures for identifying "bad things" is becoming more real. The security industry, since inception, has largely tried to find and develop patterns of attacks such as malware and exploits. Signatures today typically reference YARA or SNORT, which seek to describe attributes and identify families of malware, rather than describe a specific variation of a virus. Organizations are moving past just the identification of Indicators of Compromise (IOCs) traditionally sought to define known behavioral and technical indicators of a particular type of attack or adversary. Many have recently turned to a new concept defined as Indicators of Attack (IOAs), which creates a set of known behaviors that indicate malice earlier in the attack chain before the compromise is achieved. Organizations must understand that their adversaries are humans and not the software they develop.

OPTIV'S CYBER THREAT INTELLIGENCE PROCESS MODEL

(Figure 3)



MOVING FORWARD WITH OPTIV

Cyber threat intelligence is quickly moving from an over-used industry buzzword, to being recognized as a necessity for organizations to understand and stay ahead of quickly evolving threats. Security organizations are also investing in better ways to prevent, detect and respond to attacks. Optiv looks to bridge this gap with the introduction of our Cyber Threat Intelligence solutions to help remove confusion surrounding the implementation of intelligence. We can then provide a blueprint for logical progression in planning, building and running cyber threat intelligence programs.

The incorporation of cyber threat intelligence into a security strategy and tactical operations plan requires forethought, guidance and goals aligned with business needs. Partner with Optiv to learn more about our Cyber Threat Intelligence solutions:

- **Cyber Threat Intelligence Program Workshop**
- **Cyber Threat Intelligence Consulting Services**
- **Cyber Threat Intelligence as a Service (proactive attack indications and warning)**

OPTIV'S PROGRAM MATURITY MODEL
(Figure 4)

Call to Action

Security organizations are investing in better ways to prevent, detect and respond to attacks. Tools and approaches that yield greater certainty and reduce time to respond help minimize negative impact to the business.

A logical progression in developing a mature security posture is to find and implement various aspects of threat intelligence, including next-generation technologies and business processes, into the enterprise security program. This allows teams to consume, use and eventually create the intelligence necessary to guide action.

References

1. "The Importance of Cyber Threat Intelligence to a Strong Security Posture," Ponemon Institute, March, 2015 - https://www.webroot.com/shared/pdf/CyberThreatIntelligenceReport2015.pdf

For more information, including details about Optiv's cyber threat intelligence solutions, contact info@optiv.com.

Want to learn more?

Insight on Cyber Threat Intelligence is an ongoing series of thought leadership at Optiv. Click the links below to download other corresponding materials on the subject.

Cyber Threat Intelligence Consulting Services - At-a-Glance Brief

Cyber Threat Intelligence Program Workshop - At-a-Glance Brief

---

Executive Sponsors

Danny Pickens

Director, Cyber Threat Intelligence
Optiv

Rafal Los

Managing Director, Solutions Research
Optiv

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.