



THREAT INTELLIGENCE

Solution Primer

Rafal Los
Director, Solutions Research
Office of the CISO, Optiv

James Robinson
Director, Information Security, Optiv

Jason Clark
Chief Strategy and Security Officer, Optiv

Rob Brooks
Threat Intelligence Manager, Optiv

Woodrow Brown
Director, Research, Optiv

Introduction

To improve detection, response and resolution of relevant threats to their business, security leaders and their teams are turning to the promise of intelligence-driven security. An intelligence-driven approach to security is different than other methods because it seeks to provide defenders with key data and capabilities exactly when they are needed, to maximize resource effectiveness and minimize damage incurred.

One of the key challenges with this new approach is that the term “threat intelligence” has become heavily diluted and attached to a very diverse array of products, services and capabilities which aren’t easily adopted across the various enterprise security use cases. This paper will help enterprise security leaders understand exactly what threat intelligence is, and how their enterprises can leverage key capabilities to more effectively defend their organizations.

Meeting Business Needs

Security organizations need to rapidly modernize information, approaches and platforms. Those security organizations still relying on legacy technologies and approaches will increasingly find that they do not have the tools in place to defend against current threats.

Modern security organizations require more complete and timely information about direct threats to their business – both potential and existing. High fidelity information including known bad binaries, IP addresses and other key pieces of data assist automated tools and human analysts in making rapid security decisions with greater accuracy. A comprehensive approach increases efficiency of detection and response, while minimizing negative business impact.

Threat Intelligence Defined

While threat intelligence has been defined in many different ways, Optiv defines threat intelligence for the enterprise as:

Threat•Intelligence n. - 1. An ecosystem of contextually relevant and evidence-based knowledge – integrated into platforms and tools – to quickly and accurately address dangers to individuals, organizations or assets in a standardized, consumable format.

A comprehensive approach increases efficiency of detection and response, while minimizing negative business impact.

Components of the Threat Intelligence Marketplace

The threat intelligence solution market is categorized into three key sub-groups:

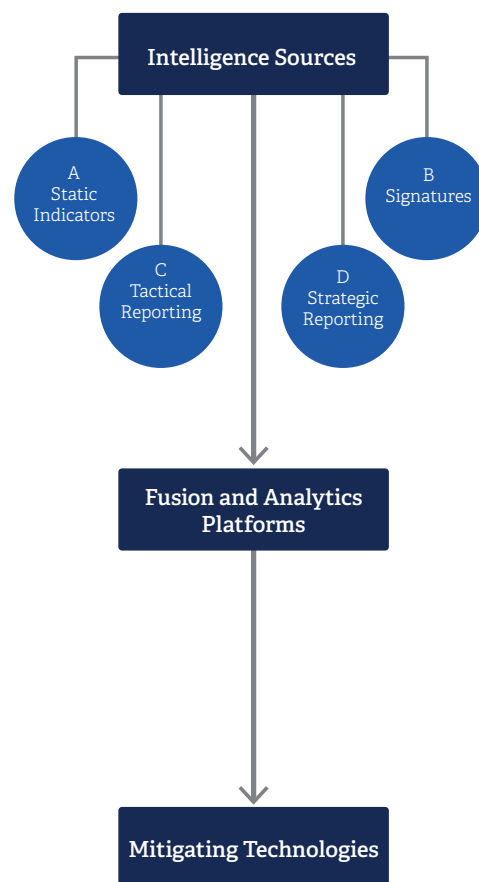
Intelligence Sources: organizations, products or persons that produce raw data points (indicators), refined or finished intelligence, or some combination thereof can be classified as threat intelligence sources. These organizations have operational capability in one or more of the following areas: identify, classify, validate, refine and distribute threat data. This group further breaks down into the following specialized sub-groups:

- A. Static indicators** – reputation-based atomic indicators such as IP addresses, domain names, URLs and object or file-level hashes focusing on fidelity, severity and timeliness primarily for the rapid ingestion and utilization by automated systems.
- B. Signatures** – composite artifacts made up of associated static indicators used to describe a threat and focusing on comprehensive analysis to aid in detection, purposeful remediation and intelligence sharing.
- C. Tactical reporting** – directly actionable intelligence highlighting a specific threat actor, ongoing campaign or imminent threat with associated supporting details for detection, response and recovery operations.
- D. Strategic reporting** – high-level strategic intelligence focusing on threat actors, ongoing campaigns or long-term threats for the purpose of strategic decision-making.

Fusion and analytics platforms: data enrichment and triage tools that aggregate, normalize, correlate and facilitate response. Additionally, enrichment platforms provide internal context to externally sourced data and/or comprehensive context from external sources for the purposes of enrichment.

- › **Fusion platforms** – provide for the capability to ingest raw intelligence data, perform triage functionality such as aggregation, validation, prioritization and contextual analysis, and execute appropriate actions. Actions may include automated push of triaged threat intelligence into an automated system for action, feeding into a data warehouse such as a security information event management (SIEM) system for further analysis, or execution of incident response work streams and case management.
- › **Analytics platforms** – enable enrichment of atomic indicators through cross-correlation, relationship modeling and data analysis across a wide variety of platforms, data stores and sources for a more complete picture.

Mitigating technologies: technologies in this category are comprised of commercial and open-source tools and automation that aid in various operational tasks of ingestion, development, triage, enrichment, collaboration, distribution, execution



and feedback. Often a single platform or tool performs multiple functions to varying degrees. These are categorized into functional categories:

- › **Prevention** – technologies using early-warning threat data and shared indicators to prevent attackers from achieving initial objectives and penetrating an organization's defenses.
- › **Detection** – technologies focused on leveraging available threat data and intelligence feeds as early as possible in the attack chain to detect adversaries and prevent them from reaching their objectives.
- › **Response** – technologies focused on reacting and responding to active threats to provide operational support with the goal of identifying compromised nodes, disrupting the adversary and preventing completion of objectives.
- › **Recovery** – technologies focused on post-breach recovery and restoration of services, processes and systems.
 - Investigations and forensics – tools used to perform evidence and artifact collection during and post-breach to build a case or share information internally or externally.
 - Remediation – tools for the express purpose of removing and recovering from a breach or infection of malware and bringing the system back to a steady operational state.

Operationalizing Threat Intelligence

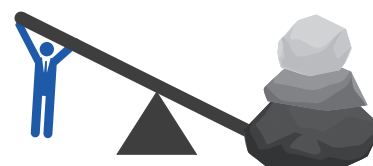
Fundamentals

Any organization can take advantage of threat intelligence capabilities. The results depend on varying degrees of planning, prerequisites and operational maturity.

The less mature a security organization is the more heavy the reliance on vendor-supplied tools and decision-making based on threat data. For example, a security organization may simply leverage an IP reputation feed into a next-generation firewall (NGFW) which would provide automated blocking based on IP address reputation to decrease the amount of triggered alerts. The net effect is one of decreasing the amount of noise analysts must review, and potentially increasing the efficiency of the response process.

More mature organizations that adopt an intelligence-oriented security program rely less on pre-canned response and increase their level of direct involvement. These organizations develop business-sensitive methodologies, capabilities and threat data drawing on internal context fused with external

More mature organizations that adopt an intelligence-oriented security program rely less on pre-canned response and increase their level of direct involvement. These organizations develop business-sensitive methodologies, capabilities and threat data drawing on internal context fused with external content to determine appropriate response.



Leveraging Threat Intelligence

- 1. Threat and Vulnerability Management
- 2. Change, Configuration, Asset Management
- 3. Cross-Silo Workstreams and Response

content to determine appropriate response. It is not uncommon for security organizations of advanced maturity to begin contributing indicators of compromise (IoCs) and threat indicators to their sharing communities such as the various Information Sharing and Analysis Centers (ISACs).

Leveraging Threat Intelligence

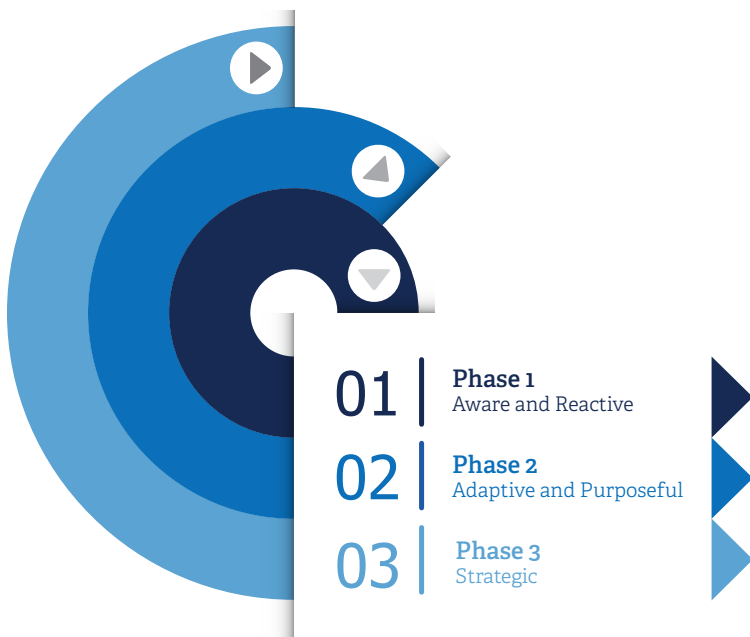
To meaningfully consume and act on threat intelligence beyond the basics of automation, the enterprise security organization should possess at least these three key capabilities:

1. **Threat and Vulnerability Management Program** – One of the foundations of an enterprise security strategy is a threat and vulnerability management (TVM) program. A TVM program is critical in part due to the identification and classification of critical assets, which helps the security team focus defense on assets critical and important to the organization. Threat intelligence, as a maturing capability, is a logical extension of a mature TVM program that is built upon the knowledge of internal threats, vulnerabilities and risk classifications. Without a strong internal TVM program, risks identified by the threat intelligence program are unlikely to receive the proper prioritization to be addressed.
2. **Change, Configuration, Asset Management** – In order to effectively utilize threat intelligence data, the enterprise security organization must be able to tell what any particular asset is, what changes have been allowed or made to it, and its proper configuration. Without this base capability, the enterprise security organization will spend more time tracking down asset owners and investigating objects rather than actively fighting threats. As a result, an attempt to leverage threat intelligence will simply become a drain on time and resources.
3. **Cross-Silo Workstreams and Response** – To successfully utilize threat intelligence, organizations must have visibility and be able to respond effectively across functional IT units within an enterprise. Threat intelligence often requires that the security organization collects, analyzes and communicates threat information outside of the security realm in order to receive cooperative support from functions such as risk and network operations. These functions generally do not fall within the enterprise security team's domain of responsibility. Thus, if a security organization does not have solid cross-silo workstream and response framework, it will likely encounter an uphill battle to leverage the newly acquired threat intelligence data into actionable tactics.

A strategic approach is required to effectively integrate threat intelligence into an existing security program.

Developing a Program Strategy Approach

A strategic approach is required to effectively integrate threat intelligence into an existing security program. There are three basic phases to develop an initial threat intelligence consumption capability.



Phase 1 – Aware and Reactive

Drivers

Initially, enterprise security organizations consume threat intelligence to raise threat awareness and gain increased visibility into existing threats. This additional visibility further helps to focus critical expenditures, potentially providing cost-savings. Additionally these organizations leverage automated response platforms dormant within their infrastructure to raise security without dramatically increasing costs. The organization should use threat intelligence as a built-in operational capability, leveraging response systems via product suites enabled with threat intelligence data from vendors with already deployed tools in the environment.

This data comes in the form of lists of known bad URLs, IP addresses, bulk malware signatures, and DNS domains and is used by existing automated technologies to identify high risk, high fidelity activity and mitigate through automated means.



Components

- Threat intelligence data and response capabilities within existing tools like anti-malware suites, firewalls, IPS, security information and event management (SIEM) and web and email gateways.

Capabilities

- Increase awareness and drive visibility of security issues – provide hard data to help in security-related decisions.

Operational Advice

- Emphasis on leveraging existing tools and infrastructure – minimally invasive, while providing noticeable security value;
- Utilize automation to get faster, more accurate response to potential issues; and,
- Focus on reducing background noise in your security tools, while fine-tuning the ability to detect real threats.

Phase 2 – Adaptive and Purposeful

Drivers

Once security organizations become more adaptive to real threats, they begin to use more advanced tools and techniques to detect and respond to live threats. Using a mix of raw data and automation, and relying more increasingly on human-based processes they become more strategic in their defense.

With a more clear understanding of the nature of threats to their organization, security teams can focus on protecting business-critical assets such as personally identifiable information (PII), electronic protected health information (ePHI) and intellectual property. This path leads to a more structured approach to incident response and program maturation through strategy development. Organizations will start to consume raw and refined data from intelligence sources, and push into leveraging more advanced response systems integrated with fusion and analytics platforms to identify, investigate and respond efficiently to threats.

Components

- Raw intelligence from diverse intelligence sources in structured, consumable format;



- Operationalized fusion and analytics platform for research, triage and analysis of raw data;
- Specialized analysts and response personnel; and,
- Well-defined strategy and operational processes to facilitate targeted response.

Capabilities

- Significant reduction in the noise (non-actionable alerts) security devices produce through fine-tuning, process maturity and intelligence;
- Decrease in the likelihood of long-term undiscovered compromise through internal and external intelligence factors;
- Efficient orchestration of people across different operational silos, repeatable processes and effective tooling; and,
- Capability to define and measure key performance indicators (KPIs) against business goals, and identify leading and trailing indicators.

Operational Advice

- Focus on creating a scalable operation;
- Develop highly repeatable processes and workflows, implemented across the organization;
- Set up a formal team of analysts and responders, and develop specialized skills;
- Focus on repeatability and efficiency of processes through continuous improvement, leveraging tools where applicable to improve efficiency of detection, response and resolution; and,
- Develop and share internally-derived threat indicators and threat observables in standardized formats (STIX, etc.).

Phase 3 – Strategic

Drivers

Organizations with the need for highly developed and optimized threat intelligence capabilities consume and produce a significant amount of intelligence. In addition, these organizations develop processes and tools, and share intelligence in structured ways with various parts of their community



and the broader intelligence community as well. While few organizations require this level of operational excellence, the shift from broad spectrum intelligence to an adversary-focused view provides razor sharp clarity to optimize strategy and tactics in even extremely adverse threat environments.

Components

- Highly structured program strategy and operationalized tactical response, driven by targeted, externally derived, adversary-focused intelligence;
- Formal, highly specialized threat intelligence organization focused on collecting, analyzing and producing targeted, direction actionable threat intelligence; and,
- Specialized tools for advanced detection and response including binary analysis tools, sandboxes and forensics analysis tools.

Capabilities

- Analysis of large quantities of targeted intelligence focused on adversaries, actions and TTPs to rapidly produce actionable results;
- Contribution to the broader intelligence community of knowledge data in the form of TTPs, IoCs and observables in various standardized formats; and,
- Identification of trends which pose a danger to the organization and create tactical guidance for the mitigation.

Operational Advice

- Focus on optimizing resources and leveraging automation wherever possible to minimize human lag-time in response capability;
- Optimize detection through information sharing, near real-time analysis of deviations from established baselines – even producing externally shareable threat intelligence; and,
- Tightly integrate tools and processes across operational IT boundaries to maximize effectiveness and minimize business disruption.

The incorporation of threat intelligence into a security strategy and tactical operation plan requires forethought, guidance and a goal aligned with business need.

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.

The incorporation of threat intelligence into a security strategy and tactical operation plan requires forethought, guidance and a goal aligned with business need.

Special thank you to:

Jason White
Security Director, Beth Israel Deaconess Medical Center

Michael Santarcangelo
Writer, CSO Magazine

Robb Reck
CISO, Pulte Financial Services

References

1. CybOX – <http://cybox.mitre.org/>
2. STIX – <http://stix.mitre.org/>
3. TAXII – <http://taxii.mitre.org/>
4. MAEC – <http://maec.mitre.org/>
5. OpenIOC – <http://wzwww.openioc.org>
6. CIF – <https://code.google.com/p/collective-intelligence-framework/>

For more information, including details about the Optiv threat intelligence solutions blueprint, contact SolutionsResearch@Optiv.com.



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.

© 2015 Optiv Security Inc. All Rights Reserved.

12.15 | F1