



WHITE PAPER

# Aim Small, Miss Small: Producing a World-Class Threat Intelligence Capability

By Levi Gundert

Vice President of Intelligence and Strategy



# Table of Contents

<b>Introduction .....</b>	<b>3</b>
Business Case .....	5
Enterprise Fit.....	6
Organizational Enterprise Cybersecurity .....	8
Functional Cybersecurity .....	8
Key Team.....	8
<b>Operational vs. Strategic .....</b>	<b>9</b>
Operational.....	10
Strategic .....	12
<b>Example.....</b>	<b>16</b>
Compliance and Metrics .....	19
<b>Conclusion.....</b>	<b>21</b>

AIM SMALL, MISS SMALL: PRODUCING A WORLD-CLASS  
THREAT INTELLIGENCE CAPABILITY

# Introduction

I was standing in my firing lane sending errant shots down range to the edges of the paper target. It was the first day of a two-week firearm instructor course at the U.S. Secret Service (USSS) training facility.

One of the class instructors walked up behind me and silently observed for a few minutes before yelling, “What are you doing?”

I responded with a detailed accounting of my stance, grip, trigger pull, and breathing. He shook his head, “No, forget all of that; aim small, miss small.”

He went on as I stood there perplexed, “Flip the target so it’s parallel to your lane.” I flipped the switch on the wall and the paper target down range became a sliver of white. “Now fire,” he said.

I looked at him incredulously, raised my pistol, focused on the hair width of paper, and fired.

Assuming there was no possibility I had hit my target, I flipped the target to its original position and my jaw dropped. The target contained a linear tear through the middle. The target wasn’t completely cut in half because the bullet entered the target from a slight angle. I looked at the instructor incredulously. “That’s it. Aim small, miss small.” he said.

That experience on the firing line is a lifelong lesson that is as applicable in threat intelligence practices today as it was on that firing line a decade ago. Threat intelligence is a broad subject and the natural tendency is to produce intelligence on any topic or event regardless of its applicability to the sponsoring organization.

True success in threat intelligence, though, is largely predicated on constraining intelligence efforts to very specific business objectives, which removes the large surface area and leaves only a challenging sliver of value to pursue.

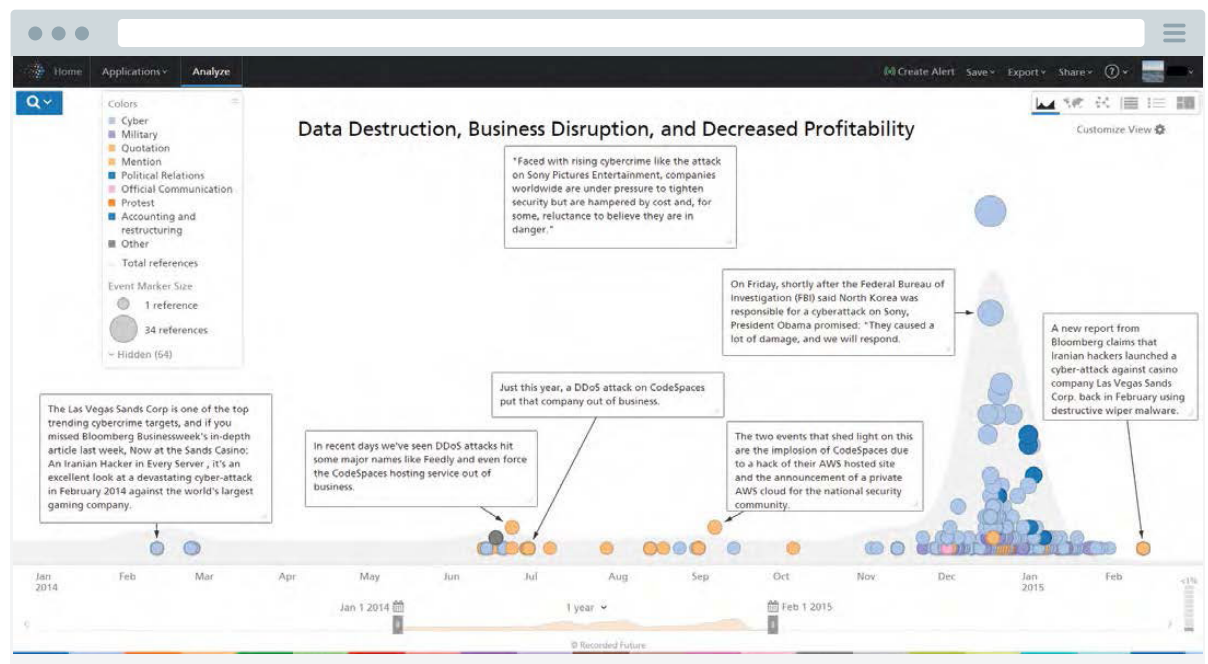
This paper focuses on critical concepts and practical details, where necessary, to produce a world-class threat intelligence capability from scratch.

## Business Case

The goal of threat intelligence is to reduce operational risk, which in turn maintains or increases business profitability. In some cases, threat intelligence contributes to an information security program that creates a competitive advantage; strong security becomes a market differentiator.

For example, I was recently sitting in the barber chair and the conversation turned to data breaches. The barber stated that she had completely changed her shopping habits to avoid a retailer that had been compromised, after the retailer's customers were made aware of the breach through large, splashy media reports. When I informed the barber that this particular retailer was seriously remediating, hiring a suite of talented professionals, and that the board of directors was directly involved in accelerating the maturity of the information security program, she seemed open to re-visiting the retailer.

Research on the long-term effects of data breaches in public companies indicates little long-term damage to stock price.<sup>1</sup> Though there is evidence that consumers may view a company as less trustworthy or even change their shopping habits<sup>2</sup> as the result of a data breach. A successful attack targeting personally identifiable information (PII) may create a longer-term decline in sales, as anecdotally suggested by my barber, even after the stock rebounds.



*Resources spent remediating a significant incident decreases profitability.*

<sup>1</sup> <https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices>

<sup>2</sup> <http://www.forbes.com/sites/paularosenblum/2014/03/17/in-wake-of-target-data-breach-cash-becoming-king-again/>

Beyond brand reputation damage, there are numerous attack types and motivations that affect businesses, including intellectual property theft. Most recently though, data destruction has demonstrably become a powerful tool for crippling business operations and negatively affecting revenue to the point of closing the business, in some cases.

In early 2014, Las Vegas Sands Corporation was the victim of a destructive cyberattack that interrupted core gaming operations.<sup>3</sup> The attackers (allegedly Iranian government sponsored) posted a propaganda video to YouTube illustrating their full access to the Sands network, though the extent of the monetary damage is unknown.

In mid-2014, Code Spaces (an infrastructure-as-a-service [IaaS] company) went out of business following a data destruction attack<sup>4</sup> that eliminated all of the company's data (including customer data such as source code) residing in their Amazon S3 buckets.

In late 2014, Sony Pictures Entertainment (SPE) was the next high-profile data destruction target. The attack reportedly cost Sony \$157 million<sup>5</sup> before taxes and affected operational infrastructure to the point that third-quarter results were delayed<sup>6</sup> months after the attack occurred.

2014 was truly a watershed year for cyberattacks that impacted business operations and profitability.

Continuous operational risk reduction allows businesses to maintain uninterrupted profitability. Identifying risk before it negatively affects the business reduces the possibility of becoming another Code Spaces or Sony Pictures.

Regardless of worst-case scenarios, threat intelligence is a necessary capability for identifying and eliminating risk.

## Enterprise Fit

Threat intelligence is the act of formulating an analysis based on the identification, collection, and enrichment of relevant information.

Organizationally, (in the enterprise) a threat intelligence capability may be comprised of a subsection within incident response, or it may be its own team. The threat intelligence program should provide products (i.e., daily threat update) to adjacent security groups and to the business itself, where possible. These deliverables should be the product of the following six core competencies:

<sup>3</sup> <http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas>

<sup>4</sup> <http://www.csoonline.com/article/2365062/disaster-recovery/code-spaces-forced-to-close-its-doors-after-security-incident.html>

<sup>5</sup> <http://www.insurancejournal.com/news/national/2014/12/18/350502.htm>

<sup>6</sup> <http://www.reuters.com/article/2015/01/23/us-sony-results-delay-idUSKBN0KW0Q520150123>

Applying threat intelligence to an existing business requires coalition building. Program success largely depends on prerequisites, principally, understanding the core business, understanding existing operational defense workflows and requirements, understanding available telemetry, and understanding strategic assets — customers, employees, vendors, infrastructure, and applications. Most importantly, endorsements and buy-in from existing security teams are crucial.

The interaction and workflow between operational defense teams should be pre-planned, and technical details around data sharing should facilitate easy integration for the teams responsible for making security verdicts. In particular, a 24/7 security operations center (SOC) should be co-located (in the same time zone at a minimum) near the incident response and threat intelligence functions. A co-location scenario is not always feasible due to business constraints, but because of the type and urgency of information being communicated between teams, in-person communication is optimal.

In 2015, incident response functions and teams are more common than stand-alone threat intelligence groups or even internal SOC functions. When businesses decide to build a separate threat intelligence function, the political inertia is difficult to overcome, primarily because the incident response team is likely already fulfilling some threat intelligence responsibilities, like monitoring the SIEM and checking logs for anomalies.

Organizationally consolidating threat intelligence into incident response is a savvy maneuver that avoids unnecessary conflict and entrenched interests between security teams.

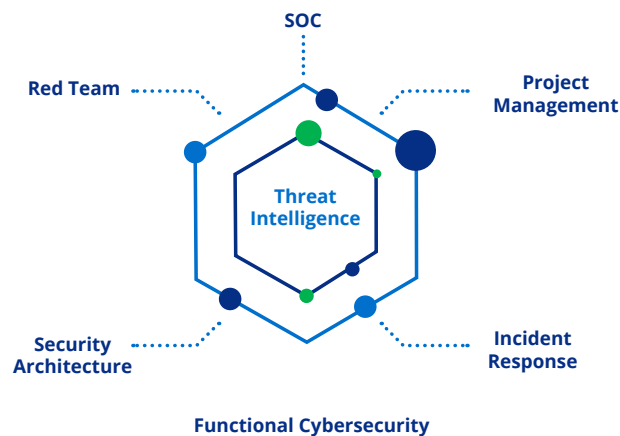
Threat intelligence should be largely focused on external threats, though a combined incident response and threat intelligence effort to proactively hunt for rogue insider activity and undetected compromises will generate stronger results. Threat intelligence should be involved in a continuous two-way feedback loop with core adjacent security teams such as the SOC, vulnerability management, incident response, security architecture (SA), project management, customer-facing fraud (where applicable), and red team.

## Organizational Enterprise Cybersecurity

To illustrate, security architecture is a primary beneficiary of timely threat intelligence since security architecture makes security control changes in the business based on the latest threat data. As a result, incident response should observe a drop in security incidents as SA makes iterative impactful changes to confidentiality, integrity, and availability domains such as application security, authentication, and data channels including email, web, and mobile. The red team can then help develop and test proof of concepts for internal applicability to observed external attack scenarios.

## Functional Cybersecurity

Project management acts as a communication catalyst that ensures prioritization and timely execution of architecture improvements. Incident response and threat intelligence recommendations may quickly become unmanageable without a central team responsible for coordination.



## Key Team

Businesses that create mature security teams with industry-leading resource allocation often create granular functions within threat intelligence that conform to more traditional government intelligence team structures. Source identification is concerned with maintaining a current list of human and signals intelligence (HUMINT and SIGINT) sources and continually assessing the confidence and validity of source information. The analysis group processes geopolitical and technical information from source identification, and the reporting group creates and disseminates finished reports to the relevant stakeholders.

The structure and organization of a business's threat intelligence team is secondary to appropriately addressing critical functions and capabilities. The danger in creating specific silos within threat intelligence is that team members may become frustrated and disenfranchised if they are not exercising their full skills sets across source identification, analysis, and reporting. A threat intelligence leader should be focused on exposing the team to a wide array of challenges and developing all necessary skill sets required for team success.



AIM SMALL, MISS SMALL: PRODUCING A WORLD-CLASS  
THREAT INTELLIGENCE CAPABILITY

# Operational vs. Strategic

A useful threat intelligence program automates the processing of external attack data — also known as indicators of compromise (IOCs) — from all available sources. This ensures that an organization is aware of external attacks and that internal incidents are identified based on derivative internal searching using the external attack data. Automating incident identification is phase one. Phase two is automating new defensive controls (generally “rules”) to prevent future incidents. This process is highly iterative as attack data sources update by the minute, hour, or day. This core threat intelligence function is operational because it revolves around computational resources. It is a prerequisite for a mature threat intelligence program.

Building on operational capabilities, a world-class threat intelligence program consists of strategic analysis centered around talented human resources. Analysts identify current and future information security threats to the business's strategic assets. They achieve general attribution to answer the “who, how, and why” for any given attack; they dissect attack tools, techniques, and procedures (TTPs); they evaluate attacker TTP relevance and impact in the business context; and they identify opportunities to make high-level security architecture changes that will make a large impact on adversary's ability to successfully leverage specific TTPs.

## **Operational**

### **Continuous bulk data ingestion, processing, and enrichment.**

Analysis is strategic, but it originates through operational data like external IOCs such as IP addresses, domains, and malware (malicious code) hashes. Operational data arrives in many forms across multiple mediums. For example, one data source may arrive via email and contain a CSV (comma separated) file or PDF file, and another data source may arrive via an API (application programming interface). Regardless of delivery and form type, operational data should be ingested and processed programmatically. Analysts should never spend time manually processing operational data.

### **Where the internet meets the intranet.**

To achieve a highly automated operational workflow, at least one talented and experienced data architect is required. This individual is responsible for designing data structures that are nimble and fast regardless of input source type. He or she is also engaged in creating tools for automating the extraction of specific data from unwieldy and difficult data delivery methods such as email. Practically, this individual will work with multiple external vendors and internal stakeholders to determine the most efficient implementation while also tuning the system as increasing amounts of threat data are processed in different forms (JSON, STIX, XML, etc.).

### **The data architect provides crucial experience for long-term correlation in disparate standards.**

Threat intelligence platforms (TIPs) offer to act as central repositories for threat data while also removing the pain points generally associated with ingesting, indexing, and normalizing threat information from multiple sources. A TIP alleviates pieces of a data architect's responsibilities, primarily through ever-expanding direct relationships with threat intelligence vendors, which enables custom engineering solutions.

When external threat data arrives it should be stored, processed, and correlated with internal telemetry sources. Typically a central analytics platform (i.e., HPE ArcSight, Splunk, LogRhythm, and/or Elastic Search/Logstash/Kibana [ELK]) is leveraged to index, query, and/or visualize multiple large data sets, and these platforms are naturally efficient locations to correlate external threat data in addition to hunting for undetected rogue internal activity. Telemetry should include security logs from host and network devices such as routers and firewalls, DNS logs, web proxy logs, Active Directory logs, Netflow, host and network-based intrusion detection/prevention systems (HIDS/NIDS), and when possible, full packet captures (PCAPs). Without granular operational visibility into the network, threat data becomes largely useless.

When an indicator of compromise is obtained it should be automatically compared to internal telemetry sources. When positive correlation occurs, all available information about the matching log event should be exported to an analyst ticketing system for further analysis and a verdict or recommendation. A mature threat intelligence practice will automate the creation and integration of specific defensive technology rule sets for highly trusted IOC sources. These may include firewall, HIDS/NIDS, web proxy, and email appliances.

### **Automate new defensive control rule sets.**

Before an external threat source is migrated into production, the architect should verify that the false positive rate is low and data transparency (including threat sources) is high. Further, all positive correlation security events should be automatically enriched with available external resources. High-confidence enrichment sources allow for rule-based logic to only refer threat correlation events to analysts once specific criteria is satisfied. Additionally, enrichment for positive correlation events is necessary to provide added context to the analyst in order to decrease verdict time.

An analyst may decide to investigate a threat correlation event further, they may confirm the correlation as an incident which is referred to the incident response team for remediation, or they may decide to acknowledge the correlation but mark it as a false positive.

Consider malvertising. An employee visits a mainstream news website and is redirected to another website that attempts to deliver an exploit and subsequent malware payload via the employee's web browser or associated application (Java, Flash, Silverlight, etc.). The website redirection occurs because of an advertisement that appears on the news site. The redirection code only appears in one out of every thousand impressions.

### Malvertising

An external threat source includes the news website domain in an hourly update. Internal telemetry reveals positive correlation with the employee in question. If the event is enriched and forwarded to an analyst for further analysis, the analyst will observe the web session in the web proxy logs, but it will be nearly impossible to replicate the activity that caused the addition of the news domain in the threat feed because it was caused by an elusive advertising delivery network. The analyst will conclude that the news site is not hosting malicious code and close the ticket, but it costs the analyst the most precious of resources — time.

An automated and refined operational threat intelligence program ensures that high-fidelity external threat data will always be processed without manual intervention, leaving threat analysts to the important work of strategic analysis.

### Strategic

#### Assessing a threat's likely impact.

Imagine watching a Skee-Ball<sup>7</sup> game where different size balls are rolled up the ramp at varying speeds toward a target comprised of multiple rings.

The balls represent threats and the rings indicate business relevance. The outermost ring includes general threats that may affect all industries. A good example is a commodity phishing campaign. The next inner ring represents industry-specific threats. In the retail industry, this ring would include point-of-sale (POS) malware. The center ring is the business's strategic assets including employees, customers, infrastructure, applications, and vendors.

Prioritizing the identification and dissection of threat events and sources that are landing in the center ring provides maximum value to the business. Information gathering for an unknown purpose other than vague future applicability is a waste of resources. The process of originating and enriching strategic intelligence should always be focused on the objects that are most likely destined for the center ring.

Since IOCs are automatically processed in the operational workflow, analysts are able to focus on building external relationships, proprietary information sources, adversary attribution, trend identification, employee and customer education, internal hunting, attacker TTPs, and corresponding defensive architecture recommendations.

<sup>7</sup> [https://en.wikipedia.org/wiki/Skee\\_ball](https://en.wikipedia.org/wiki/Skee_ball)

## Relationship Building

The lifeblood of threat intelligence.

Threat intelligence is a severely stunted capability when performed in a vacuum. External relationships are the lifeblood of successful threat intelligence teams. Sharing and receiving relevant and timely attack data allows a business to proactively protect itself before it becomes a victim.

Participating in formal and informal trust communities (such as ISACs) is crucial for decreasing risk not just in the immediate enterprise, but also in the same industry and the community at large. Participation requires time and resources; from transacting across email to attending security conferences, these activities need the support of the business. Relationship building must be a priority for threat intelligence to be successful.

## Proprietary Information Sources

Building powerful resources.

Threat vendors also provide strategic intelligence, but developing in-house proprietary capabilities to obtain consistent information about a particular topic or event source is a valuable endeavor to enhance long-term value.

For example, building an internal web crawler that analyzes the web page code of the business's top 5,000 daily web destinations may provide insight into drive-by attacks. That insight is appreciated when collaborating with the security architecture team on defensive solutions because threat intelligence is providing tangible data points, not anecdotal conjecture or, blindly and without context, regurgitating a vendor's statistics.

## Adversary Attribution

Attribution is worthwhile, because motivation informs methodology.

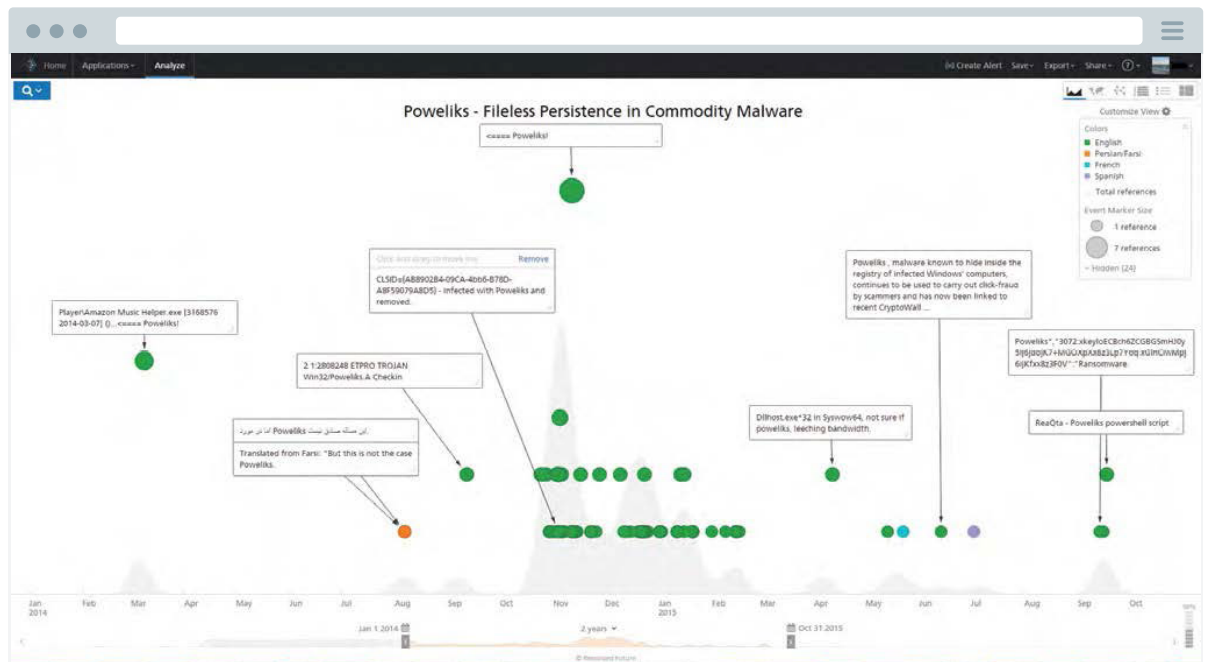
When a sustained and disruptive distributed denial-of-service (DDoS) attack is underway,<sup>8</sup> it's useful for senior leadership to understand attribution, derivative motivation, and methodology for the attack. Without attribution, it's difficult to inform the decision makers that need to address the potential for future attacks. Attribution is difficult and time-consuming work, but a successful effort is especially valuable when a business's strategic assets are involved. Always assume that following a targeted attack the C Suite and board of directors will be interested in the general "who and why," probably more so than the specific "how."

<sup>8</sup> [https://en.wikipedia.org/wiki/Operation\\_Ababil](https://en.wikipedia.org/wiki/Operation_Ababil)

## Trend Identification

Proactively identify new TTPs and their relevance to the business.

Trend identification may include macro projects such as determining next year's top cyber threats to the enterprise. Macro trends are generally viewed through quarterly or annual lenses. As previously mentioned, 2014 was a banner year for high-profile data destruction attacks, and 2015 has been notable for prominent data breaches across multiple industries including the Office of Personnel Management (OPM),<sup>9</sup> Ashley Madison, and Anthem. In addition to addressing defensive control improvements, analysts should be using collective data points to prognosticate on perceived future threats.



*Poweliks — advanced commodity malware — will it successfully operate in your environment?*

Micro trends include identifying the release of new tools likely to be leveraged by adversaries. Micro trends tend to be daily or weekly. A good example is the recent advances in post-exploitation toolkits that misuse legitimate tools, and realistic chaining scenarios that may include PowerShell,<sup>10</sup> Mimikatz,<sup>11</sup> and Windows Management Instrumentation<sup>12</sup> (WMI). Pushing beyond the increasing use of the postexploitation tools trend, a world-class threat intelligence team will dissect each tool and work with the red team to fully understand the potential success of each tool in the network environment. Will Mimikatz successfully produce user credentials? Is PowerSploit effective on a workstation lacking administrator access? Are there additional mitigating defenses that render PowerSploit impotent? Answering these types of questions is a strategic exercise.

### Security Awareness

Provide value to employees in their daily lives.

Employee security education equals reduced risk<sup>13</sup> and the threat intelligence team is uniquely qualified to iteratively build and deliver security training because of its comprehensive threat knowledge. This is a time-intensive but strategic function that adds immediate value when applied systematically. Educational curriculum should be developed and delivered with a focus on easy digestion and applicability in employee's personal and professional lives.

### Internal Hunting

Monitoring for rogue insider activity and/or undetected external attacks is another strategic function that threat intelligence should be regularly performing in tandem with incident response. Knowledge of the network topology and available telemetry sources is a prerequisite, but great hunters are creative and able to produce new hunting methodologies based on pattern and anomaly recognition in single and combined data sets. Examples include analyzing employee time zones and baseline activity times, or scrutinizing HTTPS traffic destinations utilizing unique user agent (UA) strings, or searching the "long tail" of unique registry keys or memory processes across all of the enterprise's workstations.

### Attacker Tools and Architecture Recommendations

Identify the adversary's choke point and execute defensive controls.

Lastly, identifying higher-level adversary "choke points" that correspond to TTPs is a primary strategic activity. For example, analyzing malicious code (malware) campaigns reveals that most attackers leverage dynamic DNS (DDNS) for their command and control (C2) infrastructure. Identifying DDNS<sup>14</sup> as a strategic choke point allows threat intelligence to engage with incident response and security architecture to implement an effective solution, such as DNS response policy zones (RPZ).

<sup>10</sup> <https://github.com/mattifestation/PowerSploit>

<sup>11</sup> <https://github.com/gentilkiwi/mimikatz>

<sup>12</sup> <https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/local/wmi.rb>

<sup>13</sup> <https://books.google.com/books?hl=en&lr=&id=XnBOhKHJKMQC&oi=fnd&pg=PA1&dq=employee+security+education+reduce+risk&ots=NMsrv7w5Yq&sig=PqghPPBkICDFvXDfDtBjyBjxnIA#v=onepage&q&f=false>

<sup>14</sup> <http://blogs.cisco.com/security/dynamic-detection-of-malicious-ddns>

AIM SMALL, MISS SMALL: PRODUCING A WORLD-CLASS  
THREAT INTELLIGENCE CAPABILITY

# Example




Thus far, discussing the differences between operational and strategic activities has been high level. The following is a specific example that illustrates the differences in more detail.

MalCrawler is a company that makes software designed to detect nation-state-generated malicious code. Occasionally MalCrawler tweets information about specific samples, often with a geopolitical nexus. The information is open source and valuable. Five examples from a two-month period include the following:

 **MalCrawler** @MalCrawler · Jul 10  
#SaudiArabia targeted in a cyber espionage campaign using #APT #Malware  
d46b5b75d78789b2af00f1ecf37ca744

 **MalCrawler** @MalCrawler · Aug 17  
#India targeted in cyber espionage campaign by #APT #Malware most likely from old foe #Pakistan b34d78b9e30eb0e96d4304c89ca991cb

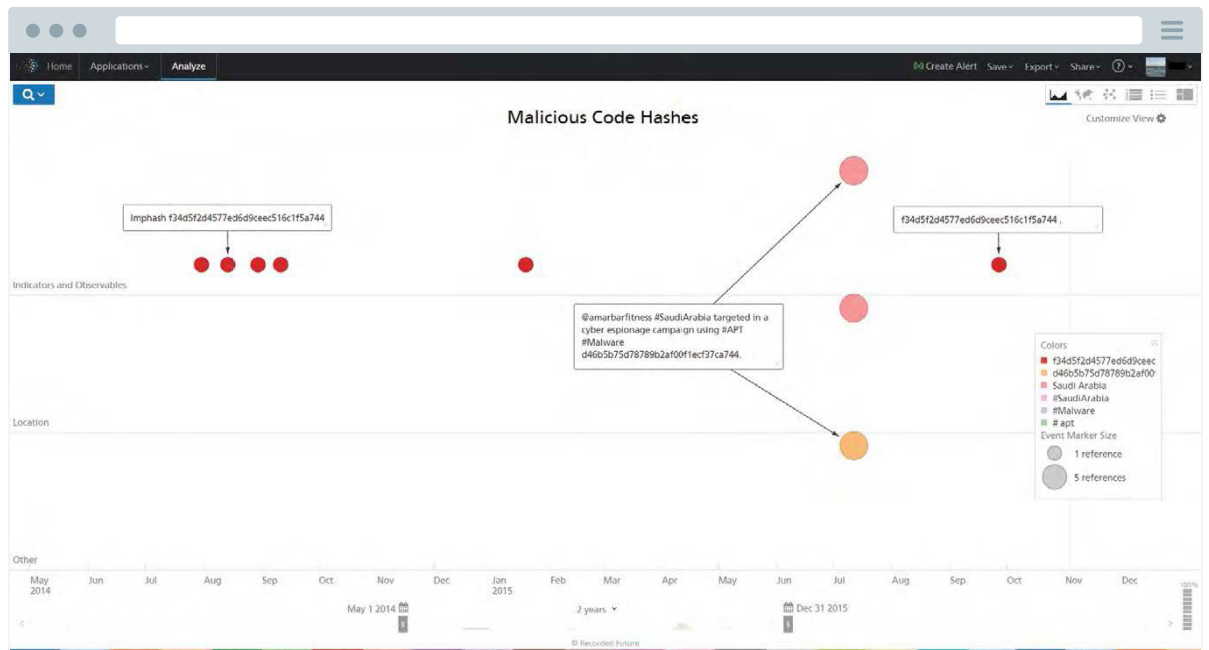
 **MalCrawler** @MalCrawler · Aug 27  
#Jordan targeted by #APT #Malware as #Syrian conflict discussion are taking place in #Russia w/ Abdullah  
178c87ab954214cbdd989b458eace411

 **MalCrawler** @MalCrawler · Sep 9  
Cyber espionage campaign against #Iraq via. #APT #Malware issues from #ISIS #Iran #Maliki investigation  
ba89582d8ec8f003cd0bc82c25687af0

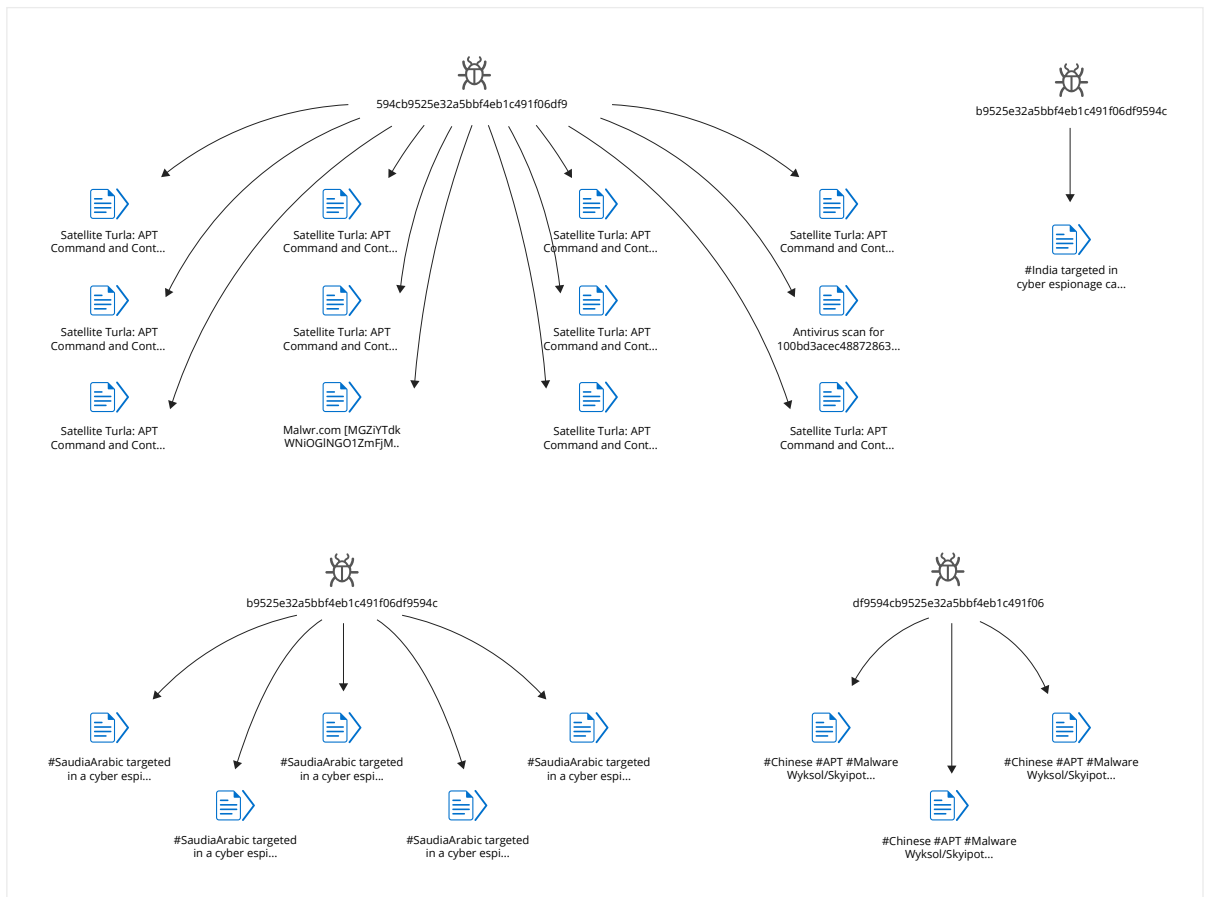
MalCrawler is a Twitter source that all companies should be consuming because nation-state-originated malware affects all industries at one point or another. Business applicability begins in the middle “industry ring,” going back to our Skee-Ball reference, and if internal correlation is identified, then the information becomes “center-ring” applicable. The final disposition is primarily relevant for correct metrics tracking.

Operationally, threat intelligence analysts should not be concerned with manually adding the Malcrawler hashes to a database or initiating a search in internal telemetry. Rather, the analysts should be confident that all open source hashes are automatically ingested and compared regardless of specific source.

The periodic delivery of hashes leads to a derivative automatic analysis that involves querying third-party (and hopefully proprietary) malware runtime (detonation) resources and using the retrieved metadata to search for internal instances in network traffic or on endpoints. If this process is already automated then a threat intelligence analyst may determine that the above five hashes are strategically significant to the business. If so, then the threat intelligence analyst will initiate an analysis — to determine associated samples, attribution, and assess the likelihood of future victimization — that will conclude in a report.



A timeline view of applicable hash references on the web.



Maltego transforms provide quick high-level context.

In this example, the analyst may query all five of MalCrawler's MD5 hashes<sup>15</sup> in VirusTotal and use the resulting imphash to identify additional related samples in Malwr.com. In the case of the sample alleged to be targeting Saudi Arabia (above), the MD5 hash d46b5b75d78789b2af00f1ecf37ca744 leads to an imphash of f34d5f2d4577ed6d9ceec516c1f5a744.

The MalCrawler hash provided in relation to targeting in Jordan — 178c87ab954214cbdd989b458eace411 — also produces the same imphash. Malwr.com returns over 100 related samples for this imphash, the most recent sample includes network traffic to the domain bungneedle.no-ip.org. One of the samples contains a unique Mutex — lJSIDMUTpHdAGEAi — that may lead to association with further samples that become pieces of the larger analysis. When third-party resources produce minimal metadata for a particular sample, then the proprietary malware lab and static analysis capabilities become important.

This is particularly true with advanced malicious code that is capable of detecting runtime and virtual environments. A good example of advanced code (compared to criminal commodity malware) is Turla.<sup>18</sup> Allegedly, Turla is the work of the Russian government and traditional attempts to obtain runtime metadata from Turla samples is less effective than mainstream malware.



The above hash produces sparse runtime details in common malware resources. In order to fully harvest all relevant information from this sample, the sample itself is needed for manual static analysis. When a scarce sample is needed, the power of the trust networks becomes crucial to identify an industry peer who has access to the sample and is willing to share it.

## Compliance and Metrics

Regulatory compliance requirements continue to increase within information security. Due diligence may involve one or more frameworks such as ISO 270001, NIST CSF, PCI DSS, and HIPAA. Threat intelligence is evolving as a standard, and it will be years before audit frameworks fully incorporate the threat intelligence function. For example, in Appendix A of the Cyber Security Framework<sup>19</sup> some threat intelligence functions are covered within the Identify and Protect functions such as Risk Assessment and Awareness and Training, but the framework does not include some of the core operational and strategic functions previously mentioned in this report.

<sup>15</sup> <https://en.wikipedia.org/wiki/MD5>

<sup>16</sup> <http://blog.virustotal.com/2014/02/virustotal-imphash.html>

<sup>17</sup> [https://en.wikipedia.org/wiki/Mutual\\_exclusion](https://en.wikipedia.org/wiki/Mutual_exclusion)

<sup>18</sup> [https://en.wikipedia.org/wiki/Turla\\_\(malware\)](https://en.wikipedia.org/wiki/Turla_(malware))

<sup>19</sup> <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

The NIST roadmap<sup>20</sup> identifies areas for future development, specifically, section 4.2 highlights “Automated Indicator Sharing,” which is a core threat intelligence competency. Section 4.5 refers to Data Analytics, which is also important for the internal hunting function referred to in the roadmap as “discernment of attack patterns.”

Metrics are important in threat intelligence like in any other discipline. The absence of measurement in threat intelligence is particularly troublesome because demonstrating business value is already difficult within the context of an evolving audit framework that fails to include core threat intelligence competencies.

### **Function over form.**

Operational metrics are measured around IOCs. Examples include tracking the number of threat information sources, number of respective IOCs produced (leads), number of IOCs that produced verified positive correlation with internal telemetry (alerts), number of defensive technology rules generated, and number of redundant IOCs among threat information sources are all useful data points. The creation and availability of granular operational metrics will assist in refining high-fidelity threat sources and eliminating low-relevance sources.

Strategic metrics are less tangible but they capture the higher-level work being accomplished. The strategic metrics should include number of relevant TTPs identified, number of employees and/or customers trained, number of internal hunting “finds,” number of external community engagements, and number of threat reports produced (scored by business relevance).

Supporting adjacent security functions is important and capturing those indirect metrics will assist executive decision makers, but primary threat intelligence key performance indicators (KPIs) must be developed to communicate standalone value. For example, threat intelligence contributes to incident response KPIs like Mean Time to Detect (MTTD) or Mean Time to Remediate (MTTR), and threat intelligence additions to those KPIs are important to capture, yet they remain KPIs for another function (in this case incident response). The creation of useful threat intelligence KPIs requires thoughtful reflection on the business’s goals and credibly measuring the daily contributions and impact to the larger cybersecurity program.

<sup>20</sup> <http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf>

AIM SMALL, MISS SMALL: PRODUCING A WORLD-CLASS  
THREAT INTELLIGENCE CAPABILITY

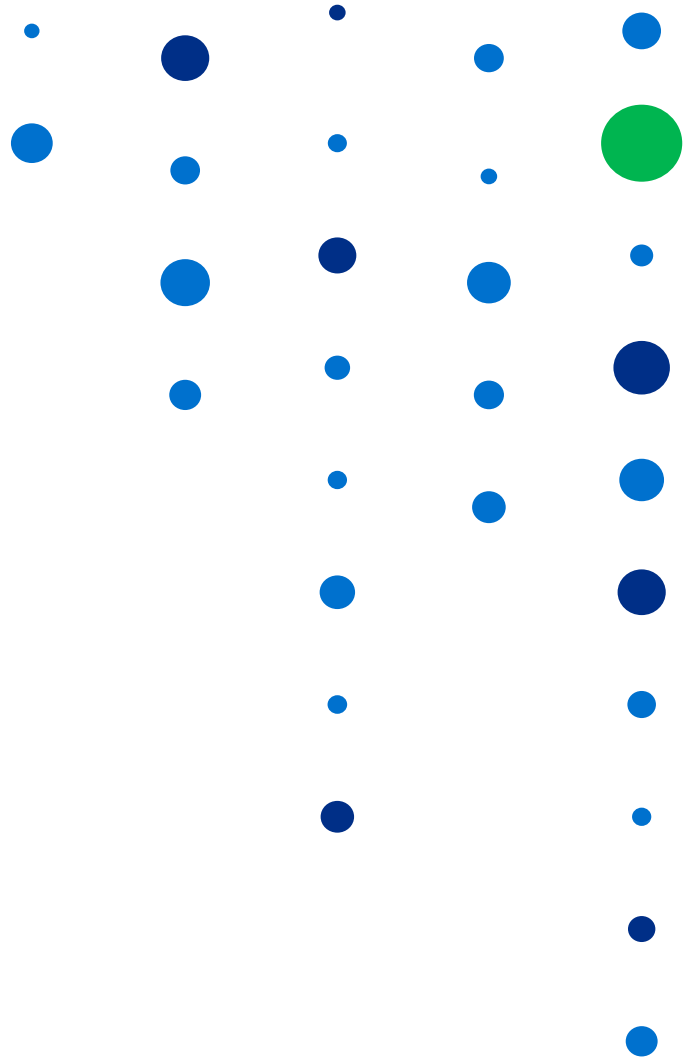
# Conclusion

Threat intelligence as a practice is, at present, still an elusive concept for many companies. Successful threat intelligence programs identify and measure tangible business goals, including reducing operational risk and solidifying a competitive advantage through market differentiation. When building a threat intelligence program it is critical to understand the core business, operational defense workflows and requirements, available telemetry, and strategic assets.

Producing intelligence on any topic or event regardless of its applicability to the organization won't protect the organization and reduce risk in any demonstrable way. The success of a threat intelligence program is dependent on the understanding of business objectives, but also building in the processes that allow for the objectives to be met. A continuous two-way feedback loop with supporting teams (the SOC, incident response, security architecture, red team, project management, etc.) will help improve the usability of both operational and strategic intelligence.

Lacking standardized frameworks, threat intelligence must be vigilant about creating metrics that help demonstrate business value. This is a challenge — as with any area of information security — because reporting on the absence of an event is intangible and won't help strengthen the relationships (internal and external) that allow a threat program to thrive.

Creating a world-class threat intelligence program requires an understanding of the business and its strategic assets. It requires the identification of relevant adversaries and their TTPs while working in partnership with the larger security organization to build relevant defensive security controls that increase visibility and allow the organization to reduce risk and increase profitability.



[www.recordedfuture.com](http://www.recordedfuture.com)



@RecordedFuture

#### About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.