SATORI CONSULTING

THREAT INTELLIGENCE: A PATH TO TAMING DIGITAL THREATS

Threat management continues to be a hot topic within cybersecurity, and rightfully so. Understanding the evolving technical and behavioral threat landscape and adapting mitigation controls is the key to proactive risk management.

This document is intended to communicate how threat intelligence can be used to reduce business risk. The audience is security, compliance and IT professionals interested in proactive risk management.

May 2018

New York, 212.918.4560

Satori CONSULTING

infor@satoriconsulting.com

INTRODUCTION

Threat management continues to be a hot topic within cybersecurity, and rightfully so. Understanding the continually evolving threat landscape and adapting controls is the key to proactive risk management. Actionable threat intelligence is critical to enabling effective threat management. It provides visibility into the temperature within the threat actor community, what they are doing and how they are doing it (tactics techniques and procedures (TTPs)). The challenge is sorting through the volumes of threat data to identify what's relevant and actionable.

This document is intended to communicate how threat intelligence can be used to reduce business risk. The audience is security, compliance and IT professionals interested in proactive risk management.

THREATS

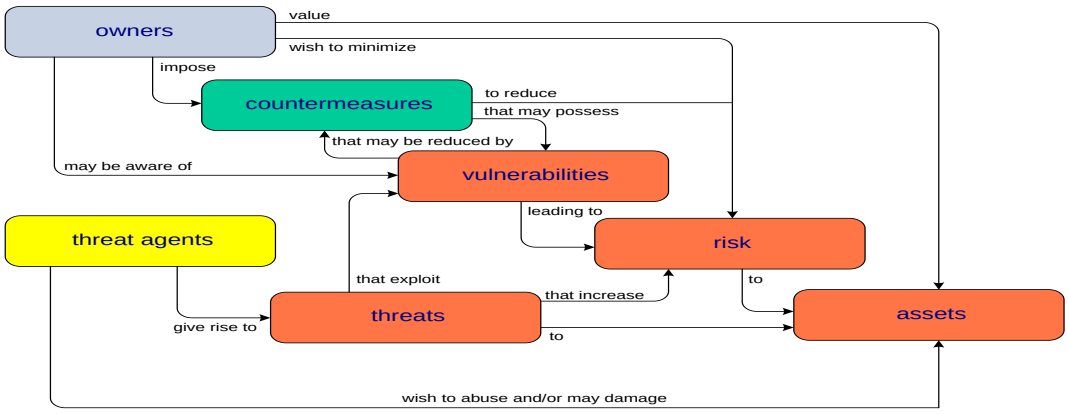
Developing effective intelligence about a threat is preceded by first understanding the nature and extent of that threat. Given the sheer diversity of threats and variety of rogue players, both state and non-state, posing them, it is crucial to understand what constitutes a threat.

Three attributes are required for a threat to exist: motive, opportunity and capability:

1. *Motive* – The drive behind threat actors desire to carry out an attack (financial gain, activism, cyber warfare, etc.)
2. *Opportunity* – Vulnerabilities present an opening for actors to use their capabilities and compromise systems. These weaknesses, internal or external, can take on the form of people, process or technology. Reducing vulnerabilities is key to minimizing threats.
3. *Capability* – The tools and skills needed to execute an attack, take advantage of vulnerabilities and compromise the environment

Threat actors that have an interest in compromising your environment (motive) and possess the tools and skills (capability) needed to take advantage of weaknesses (opportunity), represent a real threat. What's changed recently is motive. Threat actors are launching attacks that take on a life of their own and unintended targets become collateral damage. The NotPetya ransomware threat is an example of this shift. Figure 1 shows the relationship between threat actors, threats, vulnerabilities and risk.

Figure 1. Security Rationalization



The Defense Science Board (DSB) Task Force Resilient Military Systems and the Advanced Cyber Threat report defines three categories for threat actors:

- *Tier I-II* – Attackers that can exploit known vulnerabilities. This includes script-kiddies and other novices purchasing malware from the deep and dark web. Insiders typically fall within the Tier I-II category.
- *Tier II-IV* – Attackers with some level of sophistication that can find and exploit new vulnerabilities. These are lone hacktivists, or cybercriminal with good technical skills
- *Tier V-VI* - Well-funded attacker that possess the ability to create vulnerabilities within the environment. Organized crime and state sponsored hackers represent this group of attackers.

Understanding relevant threat actors that give rise to threats within the environment is critical. This helps to understand risk and the level of effort needed to manage it.

THREAT INTELLIGENCE

Threat intelligence is the outcome of the collection and analysis of *relevant* data that provides insight into potential threats or ongoing attacks. This data has to be actionable and relevant to the business to qualify as threat intelligence information. There are three types of threat intelligence data: strategic, operational, and tactical.

Types of Threat Intelligence Data

- *Strategic* – Identify the cybersecurity threat trends that can have a material impact to the business. This information is used to establish cybersecurity programs needed to effectively manage risk.
- *Operational* – Understand adversary campaigns and threats in the wild. The objective is to understand TTPs used by hackers.
- *Tactical* –Leverages indicators of compromise (IOCs) such as malicious uniform resource locators (URLs), malware signatures, command and control Internet protocol (IP) addresses, and compromised device IP addresses.

Table 1 describes the use cases, target audience, and potential sources of intelligence data that provide insight into current and emerging threats. A deeper dive is needed to shed light on these sources.

Table 1. Threat Intelligence Summary

Type	Use Case	Stakeholders	Data Sources
Strategic	▪ Establish focus for business risk management ▪ Assist with the establishment of cybersecurity program ▪ Establish a guide for employee training	▪ Information Security Committee ▪ CISO ▪ Director, Security ▪ Security Architect	▪ Industry threat reports ▪ Industry breach reports
Operational	▪ Identify threats to specific technologies (e.g., IoT, control systems) or services ▪ Direct threat hunting activities ▪ Enhance employee cybersecurity awareness program ▪ Enhance the ability to respond to incidents ▪ Identify data and brand exposure (deep and dark web)	▪ Director, Security ▪ Security Manager ▪ SOC Manager ▪ Security Architect ▪ Security Engineer ▪ SOC Analyst ▪ Incident Response Team	▪ Industry and government sponsored threat alerts ▪ Social media ▪ Media ▪ Commercial threat feeds ▪ Deep and dark web

Tactical	▪ Adapt technical controls (e.g., firewalls, IDS, IPS, malware protection) to defend against known attacks ▪ Enhance vulnerability management	▪ Security Manager ▪ SOC Manager ▪ Security Engineer ▪ SOC Analyst	▪ Commercial data feeds ▪ Open source data feeds

Strategic Threat Intelligence

Strategic threat intelligence data is used to understand macro threat and breach trends that are relevant to the business. This information serves as input to assist the organization with crafting a strategic security plan and updating it periodically (at least annually).

Strategic threat intelligence should answer the following questions by industry and country/region. The data used to answer these questions should represent activity over a twelve-month period. Understanding reported successful attacks and detected attempts will provide a reasonable perspective on malicious activity.

Breaches
- What is the cost of a breach (by attack type)?
- What TTPs were adversaries using to commit breaches?
- What weaknesses were most frequently used to commit breaches?
- What attack vectors are being used to commit a breach?

Incidents
- What were the most frequent threats?
- What TTPs were most frequently used?
- What's motivating the adversaries?
- Who was being targeted?

The data sources described in Table 2 provide data points to answer the questions listed above; however, stakeholders should be aware of the provenance and completeness of the data. Most of the reports represent data collected by providers during the course of service delivery to their customers. Therefore, the data may not reflect broad threat trends. Does this limited sample disqualify the data as being credible? No. Stakeholders should be aware of this information when constructing their view of the threat landscape.

Organizations must combine the industry data contained in the data sources with insights collected from their internal threat data sources (e.g., security incident and event management (SIEM), intrusion detection services (IDS) and firewall reports). This will paint a holistic picture of their threat landscape.

Table 2. Strategic Threat Intelligence Data Sources

Intelligence Report Type	Potential Data Source
Business Risk Intelligence	▪ Flashpoint Business Risk Intelligence Report
Breaches and General Threats	▪ Verizon Data Breach Report ▪ Breach Level Index ▪ Thales Data Theft Report ▪ ENSIA Threat Landscape Report ▪ The Black Report
Software Threats	▪ Veracode State of Security
Internet Threats	▪ Akamai State of the Internet Security Report ▪ Cisco Annual/Midyear Cybersecurity Report

- Arbor Networks Global Threat Landscape Report
- Dimension Data Global Threat Intelligence Report
- Microsoft Security Intelligence Report
- Proofpoint Threat Report
- Symantec Threat Report

The CISO and Information Security Committee should review strategic intelligence data, consider evolving threats (e.g., malicious use of artificial intelligence) and business shifts, and present the top threats to the Information Security Oversight Board. This process establishes agreement across the leadership ranks and enables the CISO to update the security program and direct security investments to ensure *material* threats are managed.

For example, if distributed denial of service (DDoS) is considered a top threat the budget should include the necessary tools, services (e.g., Prolexic) and training to defend against it. Additionally, initiatives should be included in the portfolio to enhance and continually validate the effectiveness of response processes.

The Director of Security and Security Architects play a key role in the process of implementing strategic intelligence. Continuing with the DDoS example, the Director of Security ensures validated operational processes are in place to detect and respond to DDoS attacks.

Security Architects use strategic threat intelligence to alter the security architecture and collaborate with the architect community (e.g., application, data, infrastructure, and cloud architect) to consider relevant threats during the design and implementation of technology solutions – build security in. For example, if application DDoS is a top threat to the organization the security architect may recommend mitigating controls such as a web application firewalls (WAF) and assist with implementing leading software development practices to handle attacks. The objective is to address both network and application level DDoS attacks.

Operational Threat Intelligence

Operational threat intelligence is used to understand the constantly changing threat landscape. How are attacks being carried out? Who is being targeted? It details active or impending attacks and enables the organization to quickly respond and defend against them.

Actionable operational threat intelligence addresses the following points:

- How are the adversaries conducting attacks?
- What exploits are being used?
- What attacks are active?
- What attacks are impending?
- Who is being targeted?

The sources of operational threat intelligence data are described in Table 3. These sources fall into one of three categories: open source intelligence (OSINT), Information Sharing and Analysis Centers (ISAC), and commercial services. OSINT consists of information publicly available on the Internet. There are many blogs and forums sponsored by media, industry associations, service organizations, and independent experts. At a minimum, organizations should subscribe to CERT alerts and other trusted source to maintain a reasonable understanding of threats. There is no shortage of OSINT data and much of it is redundant. The issue is finding what matters and acting upon it before you become a victim.

ISACs are closed forums focused on providing intelligence to specific industries (e.g., healthcare, government and finance). They combine OSINT with their research, and data submitted by organizations participating in the community to produce threat intelligence insights. These insights provide a targeted industry view of industry relevant threats. Most ISACs are fee based but some, such as MS-ISAC, offer their services for free to promote effective risk management.

There are many organizations that offer fee-based commercial intelligence services (see Table 4). The intent of commercial services is to provide capabilities to filter out the noise and quickly identify relevant and actionable threat data and cover a broad scope of threat intelligence. These services come with policy-based filtering, event enrichment, alerting and other value-added capabilities. For example, threats referencing active DDoS attacks using memcached reflection are routed to Security Operations Center (SOC) Analyst for investigation. The SOC Analyst collaborates with the appropriate personnel to assess the risk and apply the appropriate countermeasures. Additionally, the architect community is also contacted to raise awareness and ensure system architectures and builds are modified, as appropriate.

Table 3. Operational Threat Intelligence Data Sources

Operational Intelligence Categories	Threat Intelligence Sources
Open Source Intelligence (OSINT)	Security Blogs ▪ Security Boulevard – security bloggers network ▪ Security Affairs Research Forums ▪ CERT Alerts and Advisories ▪ BeSpacific ▪ thecipherbrief ▪ threatbrief ▪ thehackernews ▪ threatpost
Information Sharing and Analysis Centers (ISAC)	▪ Automotive ISAC ▪ Communications ISAC ▪ Education ISAC (REN-ISAC) ▪ Financial Services ISAC (FS-ISAC) ▪ Gaming and Hospitality (G-ISAO) ▪ Healthcare (NH-ISAC) ▪ Information Technology ISAC (IT-ISAC) ▪ Legal Services Information Sharing and Analysis Organization (LS-ISAO) ▪ Multi-State ISAC (MS-ISAC) ▪ Retail Cyber Intelligence Sharing Center (R-CISC) ▪ Transportation ISAC

Some commercial services provide additional services such as insight into activity on the deep and dark web. This service highlights activities such as credentials of employees or company data being sold, ransomware variants available in the marketplace or shifts in adversary behavior. Deep and dark web services include risk monitoring and alerts the organization that it has been breached (credentials or data available in the marketplace) or new relevant threats are emerging that must be further investigated. Organizations that are high-value assets - collect and/or process vast amounts of personal and/or sensitive data, offer services that can directly impact the health of an individual (e.g., healthcare, biomedical), or manage critical infrastructure (e.g., telecom, water utility) - should consider leveraging deep and dark web services.

Table 4. Commercial Threat Intelligence Data Sources

Provider	Public Threat Sharing	Open Source Intelligence	Closed Source	Deep & Dark Web Monitoring
AlienVault (4IQ)	✓	✓	✓	✓
Anomali	✓	✓	✓	
Digital Shadows		✓	✓	✓
FlashPoint		✓	✓	✓
Intel 471		✓	✓	✓
LookingGlass	✓	✓	✓	✓
MassiveAlliance		✓	✓	✓
RecordedFuture	✓	✓	✓	
Surfwatch		✓	✓	✓

Planning and operations personnel use operational threat data to identify and defend against relevant threats to the environment. As previously described, this information is typically received by the SOC and prioritized based on the potential business impact. These alerts must be analyzed, investigated, and resolved. The challenge is sorting through the mass of data and focusing on what's important. Maintaining situational awareness and establishing relevance is critical to effective use of threat intelligence.

Tactical Threat Intelligence

All organizations leverage some form of tactical threat intelligence. Technologies such as firewalls, proxies, and malware protection software receive data regarding malware signatures, hashes, malicious IPs, and command and control resource information from external feeds to defend against changing threats. Additionally, tactical threat intelligence feeds are integrated with SIEM systems and other SOC tools to identify potential threats that should be further investigated.

Tactical threat intelligence must be highly automated to defend against the many exploits on the Internet and the complexity of today's IT environment. Security Engineers must work across the organization to ensure the integrity of these feeds.

THREAT INTELLIGENCE IMPLEMENTATION

Implementing threat intelligence and achieving the desired outcome requires a focused effort within the organization. The outcome of any threat intelligence effort is actionable information to manage threats. The steps required to achieve this outcome include:

Threat Intelligence Implementation Steps

1. *Establish and maintain situational awareness* – This is critical sorting through the noise and identifying what's relevant (see Situational Awareness section below)
2. *Define the outcome* – Determine the goals that must be achieved. For example, understand threats in the health care industries along with the TTPs used by actors. Another example could be identifying IoT threats. A good definition of the outcome enables identification of the appropriate data sources.
3. *Collect threat data* – Research data sources that provide relevant threat intelligence to achieve the intended outcome. This ranges from web content to commercial data feeds (e.g., Recorded Future). Establish a process to ingest data from the various sources and stage it for analysis

4. *Analyze threat data* – Process the data using contextual information (situational awareness) to identify what's relevant and provide initial priority recommendation
5. *Produce threat data* – Deliver clear, actionable data and make it available to stakeholders in a fashion they can easily consume

These steps should be applied to strategic and operational threat intelligence to proactively identify, understand and manage risk. Tactical threat intelligence is handled differently due to the well-defined integration with security technologies.

Context

The key to effective threat intelligence implementation is situational awareness. Understanding context is critical to enabling prioritization of threat intelligence information. Organizations must make contextual reference information available to assist in this process. The information must contain up to date information that describes the current state of the environment (see examples below). For example, the critical systems list must contain products and technologies deployed. This includes open source software, application frameworks, protocols and other technologies used to deliver services.

Contextual Information

- Asset inventory (includes registered domain names, certificate authorities, etc.)
- Critical systems list (includes product information)
- Architecture diagrams
- Network topology (includes external IP address blocks)
- Security architecture definition
- Vulnerability management report
- Key suppliers (includes cloud service providers and subscribed services)

SUMMARY

Threat intelligence has become a decisive feature of cybersecurity because its quality and effectiveness will directly impact risk within the enterprise. In many ways, threat intelligence will overarch many aspects of cybersecurity because of the extent of live-connected networks and their susceptibility to external and internal threats.

Threat intelligence provides visibility into adversary activities and enables organizations to adapt controls and protect assets. Most organizations are good at leveraging tactical threat intelligence, but today's dynamic threat environment requires additional focus. Effective use of operational threat intelligence has become critical keeping adversaries at bay. Additionally, thoughtful use of strategic threat intelligence gives the organization a better chance at building in the right security controls and efficiently managing cyber risk.

The return on effort in establishing a great threat intelligence program can be significant. The absence of effective threat intelligence may lead to preventable security breaches.

48 Wall Street
Suite 1100
New York, NY 10005
Phone 212.918.4560

info@satoriconsulting.com