A Guide to Threat Intelligence Selection and Use
TABLE OF CONTENTS

Introduction ................................................................. 3

Part I: The Value of Threat Intelligence ................................. 4
  Understanding Threat Intelligence .................................. 4
  Types of Threat Intelligence | Consumers of Threat Intelligence .. 4

Part II: Ensuring High Quality Threat Intelligence .................... 5
  Understand Your Business Risk ..................................... 5
  Collect and Aggregate Data .......................................... 6
  Identify Threat Data ................................................... 7
  Prioritizing Threat Intelligence ...................................... 8
  Applications of Threat Information to Consider ................. 9

Part III: Closing the Loop & Measuring Effectiveness ................ 10

Part IV: How LookingGlass Threat Intelligence Can Help ........... 11
2020 was a challenging year in many ways, and cybersecurity was no exception. Between a rapid shift to remote work due to the COVID-19 pandemic and the Presidential Election, organizations had to face cybersecurity challenges that came in many forms, such as ransomware, phishing, supply chain attacks, and more.

Hospitals, other medical organizations, and research institutions overwhelmed by the COVID-19 health crisis, became a common target for financially motivated cyber criminals, particularly ransomware groups. These attacks can have a devastating effect. When ransomware crippled the network of a German hospital, the incident resulted in the death of a patient.¹

And a malware attack on Universal Health Services cost the organization $67 million USD.²

Financially motivated groups were not the only threat to healthcare last year. Multiple nation-state actors targeted at least seven prominent organizations working on the coronavirus vaccine and developing treatments for COVID-19.³

Unfortunately, there are many more examples of both state-sponsored and financially motivated malicious activities that can be used for financial gain or to achieve foreign policy, military, or intelligence objectives. It is very difficult for any organization to defend against attacks that it doesn’t see coming, or mitigate risks of which they are unaware.

Cyber threat intelligence—properly gathered, refined and applied—can help companies recognize business risks and implement protections that specifically address the most serious risks to the integrity and functioning of their organization.

This eBook is a guide to the selection and use of quality, actionable threat intelligence. In it, we will discuss the value of threat intelligence to any organization, identify the various types of threat intelligence services on the market today, and outline five simple steps you can take to ensure that your organization chooses and benefits from the highest quality threat intelligence.

---


---

©2021 LookingGlass Cyber Solutions, Inc. All Rights Reserved.
But what is cyber threat intelligence (commonly referred to as cyber threat intel or CTI)? How can you leverage it to protect your organization? And finally, what separates high-quality from low-quality threat intelligence?

UNDERSTANDING THREAT INTELLIGENCE

The term “threat intelligence” encompasses a broad range of information related to online or real-world threats. The National Institute of Standards and Technology (NIST) defines threat information as “any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor.”

It includes information such as security alerts; the tactics, techniques, and procedures (TTPs) of malicious actors; various indicators of threats; specific tool configurations that might help detect threats; or threat intelligence reports detailing threats and threat actors. Threat intelligence, as NIST defines it, is the aggregation and analysis of threat information in a way that adds context for decision making. While this is just one part of threat intelligence development, there are also other factors that should be taken into consideration when discussing high-quality threat intelligence delivery.

Finished intelligence product comes out of a cycle that includes collection, refinement, and enrichment by both machine and humans, as well as the process of transforming general threat information into actionable intelligence specific to an organization. Feedback and reevaluation is a necessary step of the cycle because it helps refine the program by identifying gaps and setting new requirements.

CONSUMERS OF THREAT INTELLIGENCE

Who benefits from threat intelligence? Who are the intended consumers of it within organizations? There are many possible answers to those questions because, within any organization, there are many possible audiences for threat intelligence.

Certainly, internal or external teams tasked with incident response, such as Computer Security Incident Response Teams (CSIRTs) as well as other information (“cyber”) security specialists who might work within an organization, are the front-line consumers of threat intelligence. Network and system administrators and technical support staff are also important audiences for threat intelligence, especially because they are first-line support in the event of a security incident. Beyond that, senior management and C-suite officers—including Chief Privacy Officers, Chief Information Security Officers (CISOs), Chief Information Officers (CIOs) and other executives—may be on the receiving end of cyber threat intelligence specific to their organization.
While threat intelligence may have been an obscure segment of the information security market ten years ago—dominated by small-scale and often bespoke products—that is not the case today. Today, there are scores of threat intelligence purveyors. According to Verified Market Research, in 2019 Global Threat Intelligence Market was valued at 5.54 Billion USD, and is projected to reach 20.2 Billion USD by 2027.¹

The abundance of providers and options can lead to confusion about "quality vs. quantity" and "data vs. intelligence". In both instances it comes down to the same question—is the information you are receiving relevant to your organization? While you might be impressed by a vendor’s claim of having over 200 different information sources, how useful is any of that information in regards to your organization? It’s also important to remember that data and threat information is not the same as threat intelligence. You only have threat intelligence after refinement, enrichment, and prioritization for specific business use cases.

WHAT STEPS ARE NEEDED TO ENSURE HIGH QUALITY SECURITY INTELLIGENCE?

UNDERSTAND YOUR BUSINESS RISK

It goes without saying that organizations need to have a firm understanding of the risks they face before investing in or even considering a threat intelligence operation. Risk assessments are the best way to identify and prioritize these risks. Properly conducted, they require a thorough consideration of your organization’s mission and various functions, its IT and organizational assets, as well as its reputation, such as its links to other groups, individuals, nations, and so on.²

Risk assessments will help you identify direct and indirect threats that are relevant to your organization, the vulnerabilities within your organization, and the risk they pose. They also help you determine the kinds of risk, and likelihood of harm to your organization as a result of threat actors exploiting known vulnerabilities.

Returning to the attacks targeting the healthcare industry, many healthcare organizations appeared to be unprepared to face cyber threats even before the pandemic: a report published in 2017 states that only 18% of surveyed organizations allocated more than 7% of their IT budget to security, with 41% of respondents dedicating less than 3% to security.³ However, a properly conducted risk assessment can identify that threat actors

² https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication...
may have an interest in targeting an organization. That risk assessment could highlight the need for stronger security of critical assets, flag potential insufficient internal controls, and identify other ways an organization can be vulnerable to an attack.

**COLLECT AND AGGREGATE DATA**

When gathering threat intelligence, whether through an in-house team or through a third-party threat intelligence vendor, we recommend casting the net broadly based on the results of previous risk assessments. Aggregating many data sources will ensure the breadth of collection adequately covers your organization and also provides much-needed context about any threats that are likely to impact it. Aggregation also provides a valuable assessment of whether multiple sources are corroborating a threat, thereby giving the information more reliability and confidence on its accuracy.

Among the sources of threat information, you should consider:

**Network, Infrastructure, and Connectivity Data**

This is likely the largest bucket of information in your threat intelligence program, and the hardest to define clearly. In most cases, this category will include log and event data from a wide range of network infrastructure including routers and firewalls, wireless access points, remote access services (like VPN), network-based intrusion prevention systems, Dynamic Host Configuration Protocol (DHCP) servers, and so on. The kinds of data captured and analyzed from logs will include the source and destination IP addresses associated with particular events, event time stamps, the Media Access Control (MAC) address, port numbers accessed (TCP/UDP), the host names used, actions performed, and status or error message codes.

**Application Data**

Application Data is another useful source of threat information. This includes data from operating systems, web browsers, email servers as well as security monitoring tools like antivirus and host intrusion prevention products. The data collected might include file attributes, system events like sudden shutdowns or failures, commands entered, registry settings, and configuration files.

**Actors, Users, and Owners**

Information on the specific end users or asset owners is critical and might include user identity (user name), source IP address(es), applications used, web sites visited, and so on.

**Active Threats**

Active threats are described by threat indicators of an active or pending attack such as Internet Protocol (IP) addresses for hostile nodes or command and control servers, malicious or suspicious Domain Name System (DNS) domain names, file hashes, or URLs for known, malicious executables. They are also described by the previously
referenced TTPs that are associated with a specific threat. TTPs include the tendency to use a certain type of malicious software, attack tool, or software exploit to gain presence and persistence on a victim’s network. Certain combinations of tactics (say: spear phishing or watering hole attacks followed by introduction of a specific exploit) can also help describe the behavior of a specific cyber actor.

Known Vulnerabilities

Information about known vulnerabilities in software or hardware elements is critical to developing actionable threat intelligence. While the media and trade press might harp on the use of a “zero day” (or previously unknown and undiscovered flaws), most successful cyber attacks leverage security holes that are well-known and described. Often, vendor patches for these holes are available, but have not been widely deployed. Information on vulnerabilities may include details about affected software versions, vulnerable components, and links to patches or workarounds from national CERTs, ISACs, product security incident response teams (PSIRTs) as well as resources like national vulnerability databases (NVDs).

Analyst Insights and Reports

Reports from analysts working inside a firm or on behalf of third-party contractors are another valuable source of threat information. These individuals, often working as part of incident response teams, can deliver updates about a wide range of topics including the shape of specific malicious campaigns, TTPs used in those campaigns, exploit code and tools encountered, motives and likely targets, as well as ways to mitigate or recover from attacks.

IDENTIFY THREAT DATA

Once you have collected threat information, how do you know which of it is relevant to your organization? If threat information aggregation is about “casting a wide net,” information identification is about looking in that net and asking “which fish have I caught?”

Clearly, the most important “fish” are those that are relevant to your organization. You’re looking for information and risks that readily apply to your operating environment and organizational assets, and address threats that those assets may face.

If you only cast a wide net, you will likely end up with a lot of unusable fish: irrelevant data that may interfere with incident response by slowing down analysts and introducing noise into the threat monitoring function that makes it harder to categorize and prioritize new information.

To ensure that threat information is relevant, you need to verify that it comes from trusted sources offering insight into your operations. Be mindful that the more sophisticated the adversary, the higher the likelihood they are able to inject false information or misleading indicators that can cause analysis and investigation to be led astray. Data obtained from sector-specific ISACs are likely to address platforms and threats that are highly relevant to organizations operating within those sectors.
Threat intelligence that includes specific TTPs can be put to immediate use in blocking attacks, identifying compromises, or informing analysts on patterns to watch that may indicate zero-day attacks. Likewise, information culled directly from groups within your organization or from business partners, suppliers, or even competitors can be correlated with your own internal threat information to provide a fuller picture of a particular threat actor or campaign.

In contrast, low quality “data dumps” compiled from underground forums or voluminous but undifferentiated information about new and emergent malware, hacking groups, or software exploits may have the opposite effect: overwhelming an organization that hasn’t developed the expertise, processes, and systems to digest the information. In some cases, those data dumps may not contain legitimate information, and is the result of actors deliberately posting information for fraudulent gain or to mislead recipients to obfuscate their true intentions.

For example, retailers might benefit greatly from threat intelligence related to new “point-of-sale” (POS) malware variants identified attacking competitors. However, manufacturers, which don’t have or manage POS terminals, would receive little benefit from that intelligence unless the TTPs associated with such malware share a common set of behaviors that are applicable to both environments.

Threat intelligence providers can aid in this by categorizing and ranking the information they deliver, specifying relevance to specific targets and sectors.

Threat intelligence providers can aid in this by categorizing and ranking the information they deliver, specifying relevance to specific targets and sectors. It is relevant to you to know that a particular TTP is a confirmed threat because it has attacked your organization or peer organizations.

PRIORITIZING THREAT INTELLIGENCE

The final step in ensuring access to high-quality threat intelligence is to prioritize the data you have gathered and identified as useful to your organization. To continue the fishing analogy: Having identified the useful fish and thrown back the rest, you now need to pick out those fish that are the most nutritious—those which will aid in your survival the most.

There are different approaches you can use to prioritize data, many rooted in your risk assessment and risk management framework. Ask yourself, for example, “Which of these pieces of information is the most relevant?” In determining relevance, you may focus on data that helps you prioritize your activities to address known business risks.

PRIORITIZE THE INFORMATION WHICH ENABLES YOU TO TAKE SPECIFIC STEPS TO MITIGATE THREATS.

When assessing what information matters, for instance, consider “actionable” data—threat information that enables your organization to take specific steps to mitigate a threat, block a future attack, or otherwise address a known risk.

Returning to recent cyber attacks on healthcare, threat intelligence culled from prior similar attacks might have provided TTPs and indicators that could help map an adversary’s infrastructure. Organizations may have found those TTPs actionable, paving the way for firewall rules to block and alert on such traffic. Examples of prior phishing campaigns might have alerted administrators to similar campaigns targeting their employees and, thus, to the presence of malicious actors on the organization’s internal network.
APPLICATIONS OF THREAT INFORMATION TO CONSIDER

Vulnerability Management

Vulnerability management plays a critical role within any IT department. But staying on top of software vulnerabilities and patches is also a time-consuming and often expensive task. This is especially true when patches and updates necessitate disruptions in the availability of key IT assets. On the flip side, examples of companies that ignored warnings about serious and exploitable vulnerabilities and then paid the price are too many to count. Quality threat intelligence can be a powerful tool to help organizations prioritize vulnerability management programs to address immediate risks.

For example, when the hacking group Shadowcrew dumped a string of powerful Windows-based exploits on the black market, Microsoft and other vendors released patches soon after. But organizations that lacked threat intelligence indicating that underground actors and nation state groups were leveraging the Shadowcrew exploits may have put off applying the patches, leaving them vulnerable to subsequent attacks. Such vulnerability to attacks include WannaCry and NotPetya, which spread through one or more of those exploits.

Brand Protection

Properly vetted and qualified threat intelligence can be an invaluable tool for protecting your brand, particularly in cases of network compromise, data and intellectual property theft, or brand impersonation.

Early notice about stolen customer or employee data, for example, allows a breached organization to notify law enforcement and begin the process of responding to the incident and closing off network access to the criminals, all before the thieves are aware of their discovery. Similarly, companies selling software and services can use threat intelligence to spot pirated or rogue software, websites, or mobile applications that are (ab)using their brand. Threat intelligence that monitors suspicious domains may tip off an organization to the early stages of spear phishing and targeted attacks on employees, customers, or business partners.

Physical Security

While much threat intelligence is focused on online threats, the line between online and physical risks is blurry—and getting blurrier by the day. Nation-backed hacking groups and multi-national cyber criminal organizations may present both online and physical threats. So too hacktivists, terrorists, and other ideologically-motivated actors.

Accordingly, threat intelligence can pinpoint online chatter indicating physical harm to your physical assets, such as company offices, employees, board members, or business partners. Dark markets offer clues ranging from stolen identities to requests for fake uniforms and badges that may signal heightened interest by bad actors in your organization. Photos posted to online bulletin boards may reveal casing or stalking activity that warrants increased physical security at particular locations or in connection to specific employees.

Recent events such as the cyber attack targeting a water treatment plant in Florida in February 2021, or Chinese threat actors targeting India’s power grid during the same month, suggest that online and real-world threats are converging. Threat intelligence helps organizations get a head start in protecting themselves against threats that may have cyber/physical manifestations.
Like any other technology or service, threat intelligence is not a "set it and forget it" offering. As with most security investments, you should continually monitor the performance and effectiveness of your threat intelligence investments and assess their value, measured against the goals of your risk management framework.

At a high level, you should tailor results from your threat intelligence program to support risk-based decisions. The outcomes associated with your threat intelligence program should adjust as your organization changes and matures: from mergers and acquisitions and changes in the IT or operational environment, to the emergence of new vulnerabilities and security threats.

Existing documents, such as “NIST Special Publication 800-137 on Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”, provide a solid framework for maintaining ongoing awareness of information security, vulnerabilities, and threats in modern, dynamic IT environments.

Prior to deploying a threat intelligence program, your organization should implement a comprehensive ISCM strategy that encompasses the use of threat intelligence along with more traditional information security technology, processes, procedures, and people.

Properly done, ISCM programs will help your executives and senior IT and risk staff set priorities and manage risk consistently throughout your organization. They will also measure effectiveness, including metrics that establish a meaningful measure of security status, the effectiveness of discrete security controls, compliance, and an awareness of new threats and material changes within your environment.

As with other information security investments, you should subject threat intelligence services to the same, continuous monitoring and scrutiny. The goal throughout is to support risk management decisions and ensure that those decisions are both informed and justifiable, based on reliable security metrics and a solid understanding of your organization’s risks.

1 [https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf)
LookingGlass integrates our high-quality threat intelligence into every aspect of our comprehensive portfolio of products, so organizations can confidently anticipate, understand, detect, and prevent cyber threats.

**scoutPRIME®**

*See what your adversary sees.*

scoutPRIME provides an “outside-in” view of the internet infrastructure you care about—your own and your supply chain—combined with threat and risk indicators to deliver a more accurate external threat landscape and continuous situational awareness so you can prioritize resources and jump-start your response to reduce risk and exposure.

**scoutTHREAT™**

*Model your adversary’s capabilities.*

scoutTHREAT provides an adversary-oriented focus to understanding your cyber risk, improving the efficiency and productivity of your analysts with defined workflows.

Analysts can more quickly and easily uncover adversarial capabilities, track motivations, highlight adversaries attacking your sector, and compare these tailored threat actor profiles to your organization’s security controls and mitigations to identify where to invest additional protection.

**CloudShield Eclipse™**

*Attain transparent trusted network visibility and control.*

Our current CloudShield solutions, built upon a proven history of patented deep packet inspection and manipulation, provide trusted network visibility, telemetry, threat detection, and response by stopping or preventing malicious traffic versus merely logging or alerting.

Implement a full range of advanced network security responses at machine speed to not only stop the threat as it occurs but shape your adversary’s experience to delay and deter future attacks through deceptive mitigations.
LookingGlass develops cybersecurity solutions that empower organizations to meet their missions with tailored, actionable threat intelligence and threat mitigation capabilities that move at machine speed. By linking the risks and vulnerabilities from an organization’s external attack surface to customized threat actor models, LookingGlass provides a more complete view of cyber risk and enables systematic definition and deployment of mitigations to defend against the threats that matter. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect financial systems, ensure telecommunications are cyber-resilient, and safeguard national security interests.

NOT DONE GATHERING INTEL? CONTACT US!
https://www.lookingglasscyber.com/about-us/contact-us/

KNOW MORE. RISK LESS.

@LookingGlassCyber
@LG_Cyber
/company/LookingGlass
/LookingGlassCyber