Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **September 2020**
Sponsored by **Cyren**

A Buyer's Guide to Threat Intelligence

Executive Summary

The fundamental nature of cybersecurity represents a continuous battle between bad actors, some of which are highly sophisticated and well-funded; and those who must defend networks, users, and data sources against their attacks.

The bad news is that most organizations report they are not doing well at protecting against various types of threats and attacks, such as those focused on exfiltrating sensitive data, preventing malicious sites from infecting endpoints after users click on links in phishing emails, prevent email compromise attacks, and preventing infections via mobile devices, among other problems. The well-publicized cybersecurity skills shortage is a significant contributor to these problems.

What is often missing in this fight for most organizations is the use of actionable threat intelligence that will enable security analysts and existing security defenses to better understand threats and how to prevent them from being successful. Using contextualized threat intelligence can help to enable security analysts, threat researchers and others to deal more effectively with cyber criminals by providing the information to better understand current and past attacks, and it can give them the ability to predict and thwart future attacks. Contextual threat intelligence is a force multiplier that enables security staffers to have more and better data; and to make better, faster and more accurate decisions. Plus, insightful threat intelligence can bolster current security defenses like firewalls, SOAR and SIEMs to make them more effective, and it plays an important role in proactively defending an organization. This is particularly valuable in security awareness training to ensure that users are familiar with known threats.

> ***There are various types of threat intelligence, each with specific purposes and intentions for different constituencies within an organization.***

KEY TAKEAWAYS

Here are the key takeaways presented in this paper:

- There are various types of threat intelligence, each with specific purposes and intentions for different constituencies within an organization.
- Threat intelligence is a key element of the continuous security lifecycle model because it enables security analysts, researchers, and others to analyze threats and attacks, and because it enables improvements in the security infrastructure.
- Good security awareness training is a strong complement to technology-focused solutions, since even highly effective solutions can sometimes fail to catch malicious content, particularly when there is no payload included.
- A wide variety of technology solutions must be deployed to provide an effective defense against a growing number of threats.
- Threat intelligence can be used defensively and proactively.
- A growing proportion of organizations are deploying threat intelligence and are considering it to be more important over time.
- There are many questions that should be asked of prospective vendors of threat intelligence.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Cyren; information about the company is provided at the end of the paper.

Focus on Security Best Practices

THE THREAT INTELLIGENCE SPACE

Organizations must focus on a variety of security best practices and deploy the appropriate technologies, processes, and practices to ensure that they can detect, prevent, and remediate threats to the greatest extent possible. Threat intelligence plays an important role in the overall security scheme, and can be broken down into four key subcategories:

1. **Tactical**
   This type of threat intelligence details bad actors' tactics, techniques, and procedures (TTPs); and offers security analysts, researchers, and others information about how to address specific threats. This is a mature market with many aggregators of various threat data feeds.

2. **Strategic**
   This type of threat intelligence provides non-technical information about an organization's threat landscape, which can be helpful in explaining the threat landscape to senior management, board members, and others outside of the security function. It typically consists of written reports that help decision makers to make macro-level decisions.

3. **Operational**
   This provides actionable information about specific, incoming attacks that is more time-sensitive in nature and generally highly detailed. Operational threat intelligence provides a combination of raw data and information about why this data is important. It is used by analysts to understand threats in the context of how the data can be operationalized, and it can make analysts more effective. There are relatively few vendors in this space. As the threat intelligence market matures, we are seeing a move from simple blocking or allowing, to a more context-focused use of data.

4. **Technical**
   This type of threat intelligence provides information about technical threat indicators, such as malware hashes.

The fundamental challenge for threat intelligence is that a threat needs to have appeared somewhere before. Consequently, vendors that process enormous volumes of information, as well as aggregators of threat intelligence that can gather large volumes of data, have an advantage by virtue of the fact that they are simply processing so much information. Uniqueness of information in the threat intelligence space is an important consideration since everyone in this space shares data – the portion that is unique is generally the most valuable.

> ***The fundamental challenge for threat intelligence is that a threat needs to have appeared somewhere before.***

One of the issues that consumers of threat intelligence, as well as the providers of it, must address is the growing volume of data. There is a substantial volume of data generated each day and, as a result, the "noise" level continues to increase. The volume of sophisticated, highly targeted attacks has not increased dramatically, but the level of noise has. The problem is that as noise increases, bad actors find it easier to slip a threat into a data stream that can do significant damage.

THE CONTINUOUS SECURITY LIFECYCLE

The "continuous security lifecycle" model defines the process of identifying, assessing, protecting, and monitoring the status of an entire security infrastructure, including all the elements contained within it. Security can properly be represented as a lifecycle because it must continually be managed and improved owing to the dynamic nature of the threat landscape.

Threat intelligence is an integral part of the continuous security lifecycle model because it helps security analysts, researchers, and others to analyze threats and attacks, and because it enables improvements in the security infrastructure. Good threat intelligence uses data from the past and present, and it enables addressing future threats:

- **Past**
  Analysts and researchers can review log data from a wide variety of sources across the infrastructure to determine whether the extended threat infrastructure was active on the network at some point in the past.

- **Present**
  Analysis of current threats can identify what is happening right now and discover the connected infrastructure across threat vectors and across the network.

- **Future**
  Data gleaned from analysis of past and present threat activity can be used to monitor malicious domain registrants and lock down new threats before they have an opportunity to operate within the environment.

USING MULTIPLE VENDORS

It can be useful to employ multiple vendors' threat intelligence feeds, since each has its own strengths and weaknesses. For example, one vendor may focus primarily on email threat data, but have relatively little data about threats that could impact Slack or Microsoft Teams users. The use of multiple vendors of threat intelligence in combination can exploit their respective strengths and will improve the efficiency and efficacy of threat intelligence within an organization.

DEPLOY ROBUST SOURCES OF THREAT INTELLIGENCE

Threat intelligence aggregates data points on cybersecurity threats and incidents across a broad variety of data sources, using analytics to identify trends and assess various risk factors. Cybersecurity professionals who have visibility only into security trends within their own organization are at a disadvantage relative to those who use threat intelligence that encompasses data from a much broader arrays of sources – in some cases analyzing billions of emails each day, for example. This enables the development of deep insights on how to detect and prevent emerging attacks and strengthen defenses in light of forecasted trends. Threat intelligence provides expert views on actual threat levels, such as whether a ransomware denial-of-service threat is real (because the cyber criminals behind the threat have the actual capability to carry out the threat) or only a scare tactic to fool victims into paying the ransom.

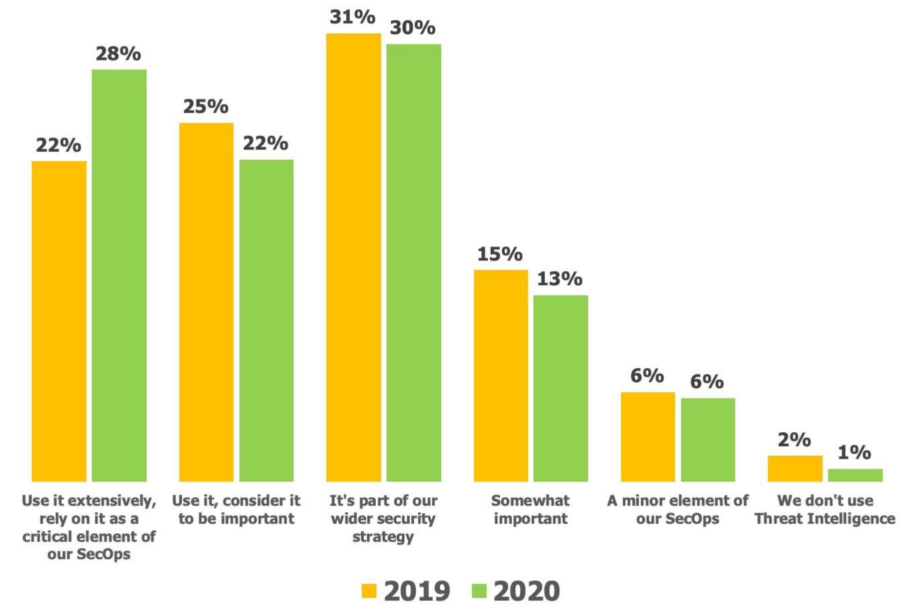
Threat intelligence gets better with larger volumes of data.

It's important to consider that threat intelligence gets better with larger volumes of data. Consequently, a threat intelligence platform that is informed from the analysis of billions of emails each day will almost always be better than one based on hundreds of millions of daily emails. The larger the volume of emails that are analyzed, the greater the likelihood that threats will be discovered, giving an additional edge to SOC teams that are charged with analyzing threats.

Threat intelligence can be used both defensively to protect against access to malicious domains or to identify those that have a poor reputation or that are likely to be used for attacks; and proactively, to investigate and prevent future attacks. Good threat intelligence provides a much broader view into threats than would ever be possible using only intra-network data sources.

A growing proportion of organizations are deploying threat intelligence and are considering it to be more important over time, as shown in Figure 1.

Figure 1
Use of Threat Intelligence
2019 and 2020



Source: Osterman Research, Inc.

Questions to Ask of a Prospective Threat Intelligence Provider

There are many providers of threat intelligence and their offerings are quite varied. Here are some questions that decision makers and evaluators should ask of prospective vendors that are under consideration:

- **What is threat intelligence expected to provide?**
  Is the threat intelligence intended for consumption by security analysts, researchers and others who will be analyzing threats and trends; or will the data be consumed by SIEMs, firewalls, and other hardware or cloud-based systems. Or both?

- **What is the target market for the threat intelligence feeds?**
  Related to the above, who within the organization will be using the content from the threat intelligence feeds? Security or SOC analysts? CISOs? Non-technical staff members who need the "50,000-foot" view of security threats?

- **What kind of threat intelligence is offered?**
  What types of threat intelligence are available? Tactical information for blocking suspicious domains? Strategic intelligence for producing written reports intended for senior management or the board? Operational intelligence that will be used by analysts to better understand threats so that they can be more effective in their work?

- **How much expertise and infrastructure is required to use threat intelligence feeds?**
  Will proprietary hardware or software be required in order to use the vendor's threat intelligence feeds? Will special training be required for security analysts, SOC analysts, researchers and others?

There are many providers of threat intelligence and their offerings are quite varied.

- **What sources will be supported?**
  Will the threat intelligence platform support a variety of sources, including commercial sources of threat intelligence, internal data sources, open source data feeds, etc.?

- **In what format is the data provided?**
  What data format(s) are supported? JSON, XML, CSV?

- **From what sources is the threat intelligence drawn?**
  There are a number of questions that should be asked about the sources of threat intelligence from a particular provider:

  - From what sources does the vendor draw its threat intelligence? Email? Collaboration tools like Microsoft Teams or Slack? Application files? IP/domain URLs? DNS? Network data? Other sources?

  - Does the provider use their customers' data as part of their threat intelligence source content? If so, how is the data anonymized or otherwise protected from a privacy perspective?

  - Is the content extracted from across a wide range of industries, or is it more narrowly focused on specific industries?

- **How large is the base of threat intelligence?**
  How many millions or billions of email and other pieces of content are processed each day that inform the threat intelligence feeds? How has this changed over time and how is it expected to change in the future?

- **How frequently is the threat intelligence data refreshed?**
  What percentage of the threat intelligence data feed is new in the last week? In the last 30 days?

- **How timely is the threat intelligence data?**
  Is it published immediately from actively identified threats, or is it sourced from third parties based on events that may have occurred days or weeks ago?

- **Can the vendor tailor threat intelligence feeds to specific customer requirements, the industry in which they participate, etc.?**
  Can analysts, researchers and others tailor feeds to their organization's requirements for special investigate projects and other purposes?

- **To what extent are false positives generated in the threat intelligence feeds?**
  Given that false positives can waste analysts' and researchers' time, are metrics provided for the number of false positives that will be generated in the feed? How variable is this false positive rate? How has it changed over time? What is the cause of these false positives? What is being done to reduce their number?

- **To what extent is the threat intelligence unique and different relative to other providers?**
  If the data across different threat intelligence feeds is substantially different from one provider to another, we might expect that each provider can offer more value because they are presenting unique information that does not overlap. On the other hand, if data is unique only to that provider, does this indicate that one or another provider is not providing adequate coverage across the entire threat landscape?

- **How does the vendor deal with the increasing volume of noise in threat intelligence feeds?**
  There is a significant difference between including every bit of threat intelligence data available versus providing less content, but more context. The latter can

> ***How many millions or billions of email and other pieces of content are processed each day that inform the threat intelligence feeds?***

make analysts and researchers more efficient by reducing the number of incidents and other data points so that the analysis can be more efficient.

- **To what extent does the threat intelligence data integrate with the security infrastructure?**
  Threat intelligence is useful as a source of content for SIEMs, firewalls, SOAR solutions, and other elements of the security infrastructure. How well does the threat intelligence provider enable ingestion of their data into these solutions and how much work is required on the part of security staff?

- **What tools are provided for SOC and other analysts?**
  What are the tools that are available to analysts, researchers and others that will enable more efficient use of threat intelligence feeds? For example, does the vendor offer a disassembler (to reverse engineer malware), a log analysis tool, and the like?

- **To what extent is the threat intelligence contextualized?**
  What analysts, researchers and others charged with managing security need is not just data, but context around that data. For example, decision-making about a particular phishing URL is more effective if other data is available, such as the brand being phished, whether it involves a web or cloud application, whether or not it pretends to be from a government source, any malicious IP address with which it might be associated, and so on.

  Is suspicious content in the threat intelligence data simply given a malicious/non-malicious rating, or is the content rated in some way (critical, important, non-critical, etc.) or is it given a specific score? Is other context about the data available, such as metadata? To what extent can analysts or researchers walk through bad actors' TTPs?

- **To what extent can data from various threat intelligence feeds be correlated with one another?**
  One of the advantages of using multiple threat intelligence feeds is the ability to correlate data contained within them to help identity more serious threats – namely, those that multiple threat intelligence providers are seeing. Analysts and researchers can use correlated data across different feeds to gain additional insight into specific threats or threat trends.

- **To what extent can data from threat intelligence feeds be correlated to data that a customer already has about its own security infrastructure?**
  As a corollary to the point above, can the threat intelligence feed not only be correlated with other purchased or open source feeds, but also with information that customers already know about their own infrastructure? This can help with gaining insight into threats and scoring them appropriately.

- **To what extent are use cases provided for customers?**
  Use cases are helpful for customers to help them understand how applicable specific threat intelligence feeds can be used. Gartner recommends taking a "use-case-centric" approach to selecting threat intelligence vendors, since this data can be used in a variety of ways and should be selected based on how it will be used. Different use cases for threat intelligence data include things like prioritizing vulnerabilities that exists within the network; monitoring for violations of the corporate brand; or providing a source of intelligence for firewalls, SIEMs, and other elements of the security infrastructure. Vendors of threat intelligence data should be selected based on how well their data will satisfy these use cases.

  Viewed another way, use cases for threat intelligence could range from a malware analyst who submits anywhere from five to 30 files per day for analysis to a system, such as a firewall, that automatically sends hundreds or thousands of files each day.

> ***One of the advantages of using multiple threat intelligence feeds is the ability to correlate data contained within them to help identity more serious threats.***

- **How well-versed in threat intelligence does a customer need to be in order to be able to use the threat intelligence feeds efficiently and effectively?**
  Do security analysts and other security staffers need to be experts in threat intelligence in order to use a vendor's data properly? How much training or expertise will be required?

- **Can customers of the threat intelligence feeds submit files for analysis?**
  Some threat intelligence vendors enable their customers to submit files for analysis, a capability that can help security teams to gain more understanding about suspicious content and also alleviate in-house staff from needing to analyze it. If the threat intelligence vendor offers this service, is there a limit on the number of files that can be submitted per day? How long does it take for the analysis to be performed? Is there an extra charge for this service?

- **How are customer-submitted files analyzed?**
  If the threat intelligence vendor enables customers to submit files for analysis, how are they analyzed? Static analysis, in which source code is automatically examined? Code analysis, that simulates the execution of the suspect code? Behavior analysis, that evaluates the intended actions of a suspicious file? Sandboxing, that will safely execute a file in a safe environment? Is a combination of these allowed? If sandboxing is used, are the sandboxes physical (which is highly resource intensive) or virtual?

- **What kind of threat intelligence reports are provided?**
  To what extent is reporting available in the threat intelligence offering? Are different reports available for different constituencies across the company, such as the board of directors, security analysts, the CISO, senior managers, etc.? Are real-time alerts available for the most serious threats?

- **To what extent can the ROI of the threat intelligence feeds be demonstrated?**
  One of the best measures for any investment is its return-on-investment (ROI). Can the threat intelligence vendor(s) under consideration demonstrate any sort of ROI to demonstrate the value of their offerings? If so, how do they do this?

- **How does the vendor address privacy issues in the context of threat intelligence?**
  Privacy is becoming a more serious issues as a result of newer privacy statutes, such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and a growing number of other, similar statutes. Since there is not always an exception in privacy regulations for malicious data, how does the threat intelligence provider do what they do while at the same time protecting the privacy of the data? For example, can sender reputation data be used for threat intelligence while maintaining compliance with privacy regulations? Sender reputation is extremely powerful as a source of threat intelligence, but carries with it significant privacy implications.

- **How does the vendor charge for its threat intelligence offering(s)?**
  Does the threat intelligence provider offer tiered pricing? Are reports charged an extra fee based on the type of report or their volume? Is there an extra charge for customer submission of suspicious content?

- **What type of support is provided?**
  Does the provider offer telephone, email or chat support? What is the turnaround time on support calls or emails? Are higher fees charged for escalated support? Can any customer analyst or researcher request support, or can only designated contacts do so?

- **What is the quality of the data?**
  Data quality in threat intelligence feeds is essential and almost always trumps

If the threat intelligence vendor enables customers to submit files for analysis, how are they analyzed?

quantity. For example, ten indicators of compromise (IOCs) that are important to understand will always be more useful than 200,000 IOCs that are not useful. How does the vendor of the threat intelligence data ensure that they are providing high-quality data.

Summary

Threat intelligence is an essential element of any security infrastructure because it can enable analysts and researchers with the information they need to analyze threats and attacks. Moreover, threat intelligence provides information needed by the security infrastructure – firewalls, SIEMs, SOAR and the like – so that these solutions can operate more effectively and identify and block a greater proportion of threats and attacks.

About Cyren

More than 1.3 billion users around the world rely on Cyren's 100 percent cloud security solutions to protect them against cyber-attacks and data loss every day. Powered by the world's largest security cloud, Cyren (NASDAQ: CYRN) delivers fast time-to-protection with award-winning email security, cloud sandboxing and DNS filtering services for business, and threat intelligence solutions for service providers and security vendors.

CYREN

www.cyren.com

@CyrenInc

+1 703 760 3320

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.