WHITE PAPER

Threat Intelligence Evaluator's Guide

Introduction

Threat Intelligence is one of the most critical weapons we can use in cyber defense. Knowing which attackers are trying to target your organization, as well as how, why, and when gives you an advantage when trying to thwart these attacks. Additionally, the rise in the commercialization and re-use of malware offers an opportunity to share threat data collaboratively in order to improve everyone's defenses. In today's landscape, security researchers are a modern-day version of Sherlock Holmes. They're constantly analyzing clues to an adversary's motives and techniques, tracking down their ephemeral footprints amidst the chaos of our cyber community.

As you probably know, not every detective is as astute as Sherlock Holmes. Some make hasty conclusions, before all the facts are gathered, and others may dismiss the most important clues during investigations. Just like detectives, not all Threat Intelligence service providers are the same.

This evaluation guide is designed to help you evaluate threat intelligence service providers, so that you effectively put threat intelligence to work for you in preventing, detecting, and responding to emerging threats. We've discovered that the three most important characteristics when evaluating threat intelligence vendors include: **Completeness**, **Quality**, and **Consumption**.

DISCLAIMER: At AlienVault®, we're not shy in admitting that we deliver the highest quality threat intelligence on the planet. So, you'll also see in this white paper, that we include specific ways in which our Unified Security Management™ (USM™) platform optimizes SOC operations powered by our high quality threat intelligence subscription service - developed by AlienVault Labs and enhanced by AlienVault Open Threat Exchange® (OTX™) - to prevent, detect, and respond to the latest threats.

Threat Intelligence Completeness

How Do We Define "Completeness"?

Unfortunately, Threat Intelligence is often defined differently by vendors, organizations, and cyber security professionals. A common source of confusion is with respect to technical atomic indicators such as IP addresses, file hashes, URLs, and other artifacts (e.g. "raw" intelligence). These artifacts, without evaluation in the context they operate within, hold relatively little value, and cannot be considered "threat intelligence". Complete, fully vetted, and actionable threat intelligence includes all relevant contextual information and analysis, as well as rich metadata, so that you know who is behind an attack, as well as their tools, techniques, and procedures (TTPs).

Why Is This Important?

When included as part of an organization's security operations infrastructure, complete threat intelligence can improve an organization's ability to detect an emerging threat, as well as provide insights into how best to respond. On their own, raw indicators lack independent value, unless and until they are enriched with contextual information, as well as collaborative and validated analysis. For example, it's important to know that specific IP addresses associated with known C2 infrastructure may have interacted with systems in your environment. But that's just the start of the investigation, and only a piece of the puzzle. Knowing who owns that C2 infrastructure, what their motivations are as well as the TTPs they use, at what stage these tools fit within the overall kill chain, along with community-verified data gives a much more complete picture. This broader context provides the relevant insight you need to act upon and determine the appropriate response.

Questions to Ask Vendors:

- *What types of indicators (IOCs) do you include in the threat intelligence service?*
  What to listen for: In addition to IP addresses, file hashes, MD5 checksums, malware samples, and other artifacts, what are the contextual clues or additional insights provided? For example, contextual data such as where this attack fits within the "kill chain", network signatures, attack patterns, and detailed written adversary profiles all provide more insight into the severity of the threat and what to do about it.

- *Where do you source your threat intelligence?*
  What to listen for: Variety and type of sources beyond simple open source and public sources. The more diverse the sources, and the more analysis and vetting of these sources, the more value is added to the threat intelligence process.

- *How rich is the metadata?*
  What to listen for: Simple threat intelligence services will provide only IP address or hostname. Additional metadata information such as timestamps, geo-location, relevance, history, reputation classification, confidence level, and more fuels incident response and investigation.

How AlienVault Does It:

AlienVault takes a comprehensive approach to threat intelligence, so that what we deliver to our customers is fully vetted, validated, and structurally complete. In terms of data collection, we collect over ten million threat indicators every day, including malicious IP addresses and URLs, domain names, malware samples, and suspicious files. However, at this point, we're just getting started. AlienVault then aggregates this data in the Open Threat Exchange (OTX) platform – the world's first open threat intelligence sharing community - from a wide range of sources, including:

- External threat vendors (such as McAfee, Emerging Threats, Virus Total)
- Open and public sources (including the SANS Internet Storm Center, the Malware Domain List, as well as state agencies, industry leaders, and academia)
- High-interaction honeypots that we set up to capture the latest attacker techniques and tools. (An example of these would be our systems actively looking for websites that are redirecting to exploit kits, and then emulating a victim.)
- Community-contributed threat data in the form of OTX "Pulses" (the format for the OTX community to share information about threats)
- USM & OSSIM users voluntarily contributing anonymized data

Next, our automated systems and processes leverage machine learning capabilities to assess the validity and severity of each of these threat indicators collected in OTX.

These include:

- A Contribution System (for malware)
- A URL System (for suspicious URLs)
- An IP Reputation System (for suspicious IP addresses)

We then use threat evaluation tools established and directed by the AlienVault Labs Security Research Team to test and validate specific threat indicators. These tools also leverage machine learning capabilities and include a Malware Analyzer, a DNS Analyzer, a Web Analyzer, and a Botnet Monitor.

Here's an example involving a malware attack. Using our Web Analyzer, we verify that a domain is distributing malware. We connect to the suspicious URL, analyze and then execute the file. If the file is malicious, we mark the domain and server as malicious. We also use the latest sandboxing techniques to identify and analyze malware samples. The AlienVault Labs Security Research Team then conducts deeper qualitative and quantitative analysis on these threats. For example, we reverse-engineer a malware sample or conduct extensive research on particular adversaries and their infrastructure to detect patterns of behavior and methods.

This rigorous process enables AlienVault to go well beyond raw indicators to deliver accurate and complete threat intelligence to our customers. Detailed information on event patterns and techniques, network signatures, malware analysis, and behavioral analysis means that our customers get the complete picture on emerging threats and how to mitigate them.

Threat Intelligence Quality

How Do We Define "Quality"?

One of the most challenging aspects of evaluating threat intelligence lies in the fact that, by definition, it's veiled in the secrecy of the dark arts. Since, you are not able to peek behind the curtain to evaluate how security researchers are operating, how do you determine if the output of that research is of high quality? How confident can you be when we're talking about research conducted in stealth mode? How can you determine if the threat intelligence you rely on is accurate if it's veiled in the cloak of the deep dark web? How can you define the quality of threat intelligence when you aren't in a position to evaluate how it's generated?

Good question. We recommend using accuracy, speed, scale, and relevance as the determining factors in evaluating the quality of threat intelligence.

You can measure the quality of threat intelligence by its result, its relevance, and its impact: How accurate is it? How relevant to me? Which of my assets are impacted by this threat, now or in the past? And because things change so quickly, it needs to be in real time and scale as risks intensify.

BONUS TIP: Threat sharing and collaboration among cyber defenders also improves the quality of threat intelligence. Sharing information about threats in real time in an open forum naturally raises the bar for adversaries - in terms of their level of effort and their ability to reuse attack methods and C2 infrastructure. Even better, the entire community benefits by having advance notice and an in-depth understanding of broad-based attacks and crowd-validated threat data.

Why Is This Important?

Have you heard of the mantra, "Garbage in, garbage out?" It's almost better to have no threat intelligence at all than to have misleading threat intelligence or outdated threat intelligence informing your security strategy, process, and technology. Your team doesn't have time to sift through IP address lists, edit blacklists by hand, or read through piles of ISAC/CSIRT emails, because by the time they've finished, the data will be stale, irrelevant, and outdated.

Quality threat intelligence means you can rely on the information that is fueling your SOC so that when an alert is triggered, you're not chasing ghosts, but rather, active threats that are true priorities.

Questions to Ask Vendors:

- ***How is your threat intelligence generated?***
  What to listen for: Human analysis combined with automation, the use of machine learning algorithms, large data sets, a variety of sources (in-house, proprietary, open, public, etc.), and collaborative threat sharing). All of these characteristics increase the quality of threat intelligence. If they're just repurposing open source intelligence, without any additional analysis, walk away.

- ***Can I easily evaluate the relevance of threats to my own business?***
  What to listen for: Automated correlation between in-house vulnerabilities and those being targeted by adversaries; auto-discovery of in-house assets helps to associate emerging threats with your own environment so you can effectively prioritize defense tactics.

- ***Is threat sharing and other collaborative analysis used as part of your intelligence analysis process?***
  What to listen for: Active and public sharing of IOCs such as: IP addresses, domain names, subdomains, emails, URLs/URIs, file hashes (MD5, SHA1, SHA256, PEHASH, IMPHASH, ...), CIDR rules, file paths, MUTEX names, CVE numbers and more. Threat sharing and collaboration is one of the most innovative and time-saving ways to beat cyber attackers at their own game.

How AlienVault Does It:

The AlienVault Labs Security Research Team delivers high-quality threat intelligence based on a rigorous process that starts with a variety of sources and is powered by a robust infrastructure for validation and analysis. Our automated toolset includes sandboxes for dynamic malware analysis, honeypots, and custom configurations of open source analysis tools (Cuckoo, etc.). Using automated data collection and analysis, as well as human analysis by some of the world's most respected security researchers, the AlienVault Labs Security Research Team provides organizations with reliable, accurate, and relevant threat intelligence.

To increase the quality of our threat intelligence even further, AlienVault launched the Open Threat Exchange (OTX) in 2012. One of the largest threat sharing communities in the world, OTX has attracted more than 53,000 participants in 140 countries, who contribute over ten million threat indicators daily. In addition, contributors post an average of

10 new Pulses per day (Pulses are threat analysis briefs that are contributed by our community members). There are also hundreds of thousands of contributions per day from AlienVault Unified Security Management (USM) and OSSIM product installations, which allow customers to "opt in" and share threat data anonymously.

As with many other crowd-sourced initiatives, greater collaboration leads to better quality and transparency. In addition, active threat sharing accelerates the speed by which new threat intelligence is validated and put into use by organizations. For example, companies that are in the same vertical industries are often victims of similar attacks, so quickly sharing information about these threats (and possible defense strategies) can improve security for everyone.

Threat Intelligence Consumption

How Do We Define "Consumption"?

We can define "consumption" in both machine and human terms. With respect to the "machine," threat intelligence should be easily and automatically delivered to security monitoring and assessment technologies like SIEMs and intrusion detection systems (IDS). When it comes to the "human" side of things, threat intelligence should be just as easily consumed by your IT security team. In other words, it should be written in a standard format that's easy to scan and has clear directives so that you know immediately how to respond to the threat.

Why Is This Important?

Ultimately, the goal of threat intelligence is to improve your ability to block and investigate attacks. To accomplish that, you must be able to easily integrate threat intelligence into your existing security process and technologies. If your threat intelligence service provider leaves you to figure out the integration points, or if their APIs fail to work with your gear, they've failed the "consumption" test. Additionally, if the threat intelligence provides no clear guidance on how to interpret, prioritize, or respond to the threat, it might give you a false sense of security, but in the end, leave you exposed.

Questions to Ask Vendors:

- *How will your threat intelligence service benefit our security operations?*
  What to listen for: Specifics on how you can easily consume their threat intelligence into your existing operations. Ask for examples of how customers use their content throughout their SOC workflows. Automation is key, based on how quickly threats can morph over time. It's also important to understand what guidance is provided within each piece of content.

- *How useful is the threat intelligence content? Does it actually help detect incidents?*
  What to listen for: Real world use cases… with details. Ask for a few specific examples that made a crucial difference in a customer detecting an incident - what specific correlation rules were triggered? Ask for an explanation of how this level of analysis moves beyond mere collection of raw indicators into improved detection.

- *Will subscribing to your threat intelligence service help with incident response?*
  What to listen for: Reputation classifications to help you identify known adversaries and their associated C2 infrastructure, IP addresses, tactics, etc. Contextual analysis to understand where each threat is in terms of the "cyber kill chain" stage of attack. Easily integrated into your detection, assessment, and monitoring tools for automated response.

Question for Your Team:

› *Can we consume the threat intelligence with the technologies / skills that we have?*
Why this is so important: Any additional investment into your security program should be carefully examined to determine if you'll be ready to implement it into your process, and if your existing technologies is ready to receive it. The primary technologies that can benefit from updated threat intelligence include: firewalls, network IDS/IPS, host-based IDS/IPS, vulnerability scanners, asset inventories, and behavioral monitoring tools like netflow analyzers.

BONUS TIP: Consider whether you have the right skillset on your team to be able to review, understand, and act on emerging threat intelligence. If your team lacks this skillset, working with an MSSP partner may be your best bet. Or, you might consider using a multi-functional platform that combines all of the core SOC technologies plus continuous emerging threat intelligence updates. (Hint: That's how we do it.)

How AlienVault Does It:

The AlienVault Labs Security Research team delivers updated analysis about emerging threats and underlying attack infrastructure to the USM platform via our USM Threat Intelligence Subscription. The team regularly updates eight coordinated rule sets, including correlation directives, IDS signatures, and incident response templates, which eliminates the need for organizations to tune their systems on their own. The analyzed threat data is also fed back into the AlienVault Labs analytical systems and tools, enabling us to make future correlations of threat indicators. This comprehensive approach eliminates the need for organizations to generate threat intelligence and tune their security controls on their own.

The Open Threat Exchange (OTX) also enhances the AlienVault Labs threat intelligence in the generation of new IDS signatures, correlation rules, and vulnerability signatures so that USM continuously detects the latest threats and triggers the relevant alarms. These updates occur on an ongoing basis, meaning that USM is capable of detecting even the newest malware.

Available as an aspect of the USM portfolio, OTX is also available for open integration with other security technologies, from open source to commercial security products. Currently, we offer direct connections for Bro and Suricata IDS, as well as the STIX and TAXII specification. OTX also provides open SDKs in Java, Python, and Go. OTX Pulses posted by community members and AlienVault researchers also provide specific guidance on interpreting the threat, so that you know what to do and how to protect your organization.

THREAT INTELLIGENCE EVALUATION CHECKLIST

THREAT INTEL TYPE	EXAMPLES / DESCRIPTION	PROS	CONS	COMPLETENESS	QUALITY	CONSUMPTION
Closed threat intelligence	ISACs (e.g. IT-ISAC, FS-ISAC)	• Relevant/targeted to industry • Community-based (emails, portal)	• Arduous joining requirements • Manual vs. automated (difficult to consume)	★★	★★★	★
Proprietary threat intelligence	NGFW, IPS/IDS, Endpoint Security and other product vendors	• Automated, operationalized • Product community-based (auto "opt-in")	• Difficult to access outside of their products • Non-trivial to Integrate/ consolidate with other	★★	★★★	★★★

THREAT INTELLIGENCE EVALUATION CHECKLIST CONT.						
THREAT INTEL TYPE	**EXAMPLES / DESCRIPTION**	**PROS**	**CONS**	**COMPLETENESS**	**QUALITY**	**CONSUMPTION**
Pure play threat intelligence service providers	Various SaaS vendors	Specialized focus on threat intelligence	• Non-operationalized (requires staff / skills to act on it) • Lacks integration into workflow and technologies	★★	★★★★	★★
Threat Intelligence Platforms (TIPs)	Various SaaS vendors - consolidate TI content (from above sources)	• Consolidated content increases data quality • Helps manage TI workflow	• Non-operationalized (requires staff / skills to act on it) • Lacks collaborative capability	★★★	★★★★	★★
AlienVault Labs Threat Intelligence, AlienVault OTX and AlienVault USM	Unified platform that combines essential security controls with collaborative and operationalized threat intelligence	• High quality, collaborative threat intelligence automatically updates SOC monitoring tools • Collaborative threat sharing platform improves security for all	• Not applicable	★★★★★	★★★★★	★★★★★

Summary

While most would agree that threat intelligence is a critical success factor in finding and fighting the latest threats to your business, it's not always clear how to pick the right vendor or how to put that vendor to work for you. We hope this guide provides a roadmap to use for making the most of threat intelligence in your security program.

As one of the first providers to establish an open threat collaboration platform (AlienVault OTX), AlienVault is uniquely positioned to provide a complete full lifecycle solution for security defense. By using AlienVault USM as a foundational element for your SOC, you can immediately put the power of AlienVault Labs threat intelligence into action, as well as collaborate with other security defenders within AlienVault OTX.

Learn more about AlienVault's unified approach to threat detection:

- AlienVault Unified Security Management overview
- AlienVault's approach to threat intelligence
- Learn more about the AlienVault Labs threat research team
- Join the Open Threat Exchange