Beginner's Guide to
THREAT INTELLIGENCE

www.alienvault.com

Threat intelligence is a popular term in the security industry, and has become a catch-all phrase for a range of technologies and approaches. This paper will help clarify what threat intelligence is, what it is not, and why threat intelligence is critical for organizations of all sizes to improve their threat detection, prioritization, and response capabilities. It will also discuss the key steps that an IT security organization needs to go through to create effective threat intelligence on their own, as well as how to evaluate threat intelligence offerings from security vendors. Finally, it will describe AlienVault's unique approach to delivering threat intelligence.

So What is Threat Intelligence?

A major recent trend in the security marketplace is to invest in some form of threat intelligence service to close the security knowledge gap and better focus scarce IT resources. But if you ask ten people what threat intelligence is, you will get ten different answers.

AlienVault defines threat intelligence as the actionable information that every IT team needs to automatically detect threats in their network and prioritize the response to those threats. It is the essential output of an organization's threat research and analysis process. Threat intelligence works by focusing the organization on the most important threats facing their networks at any given time.

Threat intelligence comes in many forms. Some of the forms that we commonly see today include IP addresses, domain names, DNS servers, URLs, file hashes, network signatures, attack patterns, and actual written profiles of attackers (like you might find in a celebrity magazine). Each of these forms is developed in a different way, some of which are automated and some of which involve painstaking manual effort. But they all can be considered threat intelligence.

Threat intelligence vendors come in many shapes and sizes. Most threat intelligence sources fall into the following three classes:

- Closed threat intelligence, like ISACs (Information Sharing and Analysis Centers), which tend to be vertically aligned and often have steep or arduous joining requirements.
- Security product vendors that deliver threat intelligence tied tightly with their products, but the data is not easily accessible outside of their products. If you have the vendor's product, this can be great, but it also means that you can only consume the forms of threat intelligence that their product can understand.
- Pure-play threat intelligence vendors that charge you a subscription to access their information. These can be a viable option, but you will still need security products and staff to analyze this information.

For the purpose of this paper, we will consider threat intelligence as actionable information about attackers, their tools, infrastructure, and the methods that every IT team needs, to detect threats in their networks, and prioritize the response to those threats.

Why is Threat Intelligence Critical for Threat Detection?

Many of the high profile breaches over the past few years have demonstrated that prevention doesn't always work, even for organizations with seemingly unlimited security budgets. New threats arise every day. It is impossible for most organizations to keep up with the constant stream of attackers, their tools, and the infrastructure they use to compromise networks. In today's threat landscape, you need to assume your organization will be breached, so your priorities need to shift towards strengthening your organization's threat detection and response capabilities. The critical weapon you can deploy on this front is threat intelligence.

Threat intelligence is the essential output of an organization's threat research and analysis process. Threat data on its own is just data, lacking the analysis component. Without the threat analysis, you won't be able generate quality threat intelligence. It is this threat analysis that is essential for converting the gigabytes and terabytes of event log data that every network generates into specific, actionable information about threats. You need to be able to curate the threat data, and combine it with supplemental information about attackers' tools, methods, and infrastructure, to produce quality threat intelligence. This enables you to instrument your security program to effectively detect and respond to threats.

The Benefits of Threat Intelligence for Your Organization

Threat intelligence has some major benefits for your organization. First and foremost, as noted above, quality threat intelligence can accelerate your threat detection, prioritization, and response capabilities. Trying to detect threats is like looking for a needle in a haystack. Unfortunately, with all of the data your organization collects, and the sophistication of the attackers, the haystacks are getting bigger. Threat intelligence enables you to focus your scarce resources on the highest priority threats facing your network.

In addition, new threats arise every day, and time is scarce. It is impossible for most organizations to keep up with the latest threats. An effective threat intelligence capability keeps you on top of these threats, improving your detection and response capability.

How Do We Generate Threat Intelligence On Our Own?

So how can a typical organization generate threat intelligence? To be sure, generating threat intelligence is complex, expensive, and time consuming.

Let's dig into what it entails.

You need access

to the latest external threat data, and you need to collect, parse, and normalize your own extensive security event data. You then need to correlate events from across your network to identify attacks. Identifying those few events that signal malicious activity requires in-depth knowledge of attacker techniques.

You need to create response guidance for your security team to respond to threats. And you need to push out updates to a wide range of security controls to instrument them with the latest information to detect malicious activity.

All the while, you need to stay abreast of changes to the threat landscape to ensure your security controls can detect the latest threats. This includes researching malicious activity detected in your network to understand the attacker's intent.

And these steps need to be repeated frequently to ensure up-to-date detection.

Let’s examine these steps in a little more detail.

Collecting security and network event data is relatively easy, with almost every operating system, device, and application generating a log file that log management systems can collect and manage. Data correlation and analysis, on the other hand, is an extremely complex process. Correlation is the process of identifying and linking seemingly unrelated events across a wide range of data sources. It requires the use of sophisticated correlation directives to be able to find relevant events buried within gigabytes or terabytes of log files.

Most IT teams lack the technology and resources to automate the correlation and analysis process. They often rely on simple collection of log files for their threat analysis. Compounding this challenge is the fact that, for all IT teams, security is often just one of many essential responsibilities to the organization. The IT team likely does not have the time or technologies to manage and sort through the mountains of log data collected by all of their critical systems. They also lack the time required to perform the necessary research to understand the latest techniques and infrastructure used by attackers to detect today’s emerging threats.

As a result, it is no surprise that generating threat intelligence is out of reach for most IT teams.

What are some Options from External Threat Intelligence Vendors?

Given the challenge in generating threat intelligence on your own, one option to consider is to subscribe to an external threat intelligence service. This effectively outsources your threat intelligence gathering process, which can save your team a lot of time and resources. However, there are some downsides to this approach.

You will still need resources on hand to make this threat intelligence meaningful for your organization. You will have to answer a range of questions about the data you're receiving, including:

- How does this threat data apply to my network and systems?
- Am I vulnerable to this threat?
- Can my systems detect this threat?
- Am I being targeted?

Essentially, your staff will need to do the tuning of your security controls on their own.

What are some Options from External Threat Intelligence Vendors?

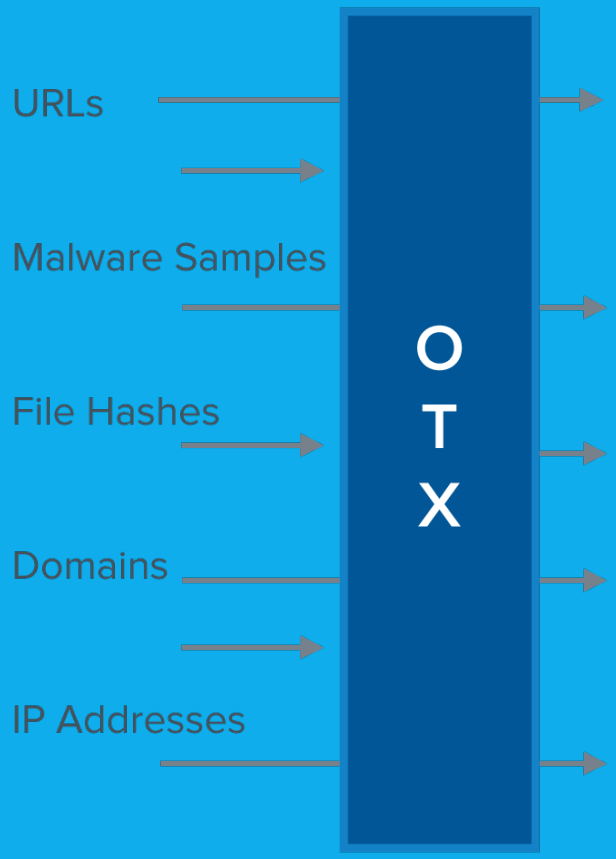
You will need to integrate the threat intelligence information into your Security Information and Event Management (SIEM) or security platform. This is not an easy process. Instrumenting your security platform to ingest the threat intelligence information will take time and resources.

Finally, these threat intelligence services are costly, starting in the tens of thousands and going into the millions. Most organizations simply do not have the budget to take on this recurring expense.

AlienVault's Approach to Threat Intelligence

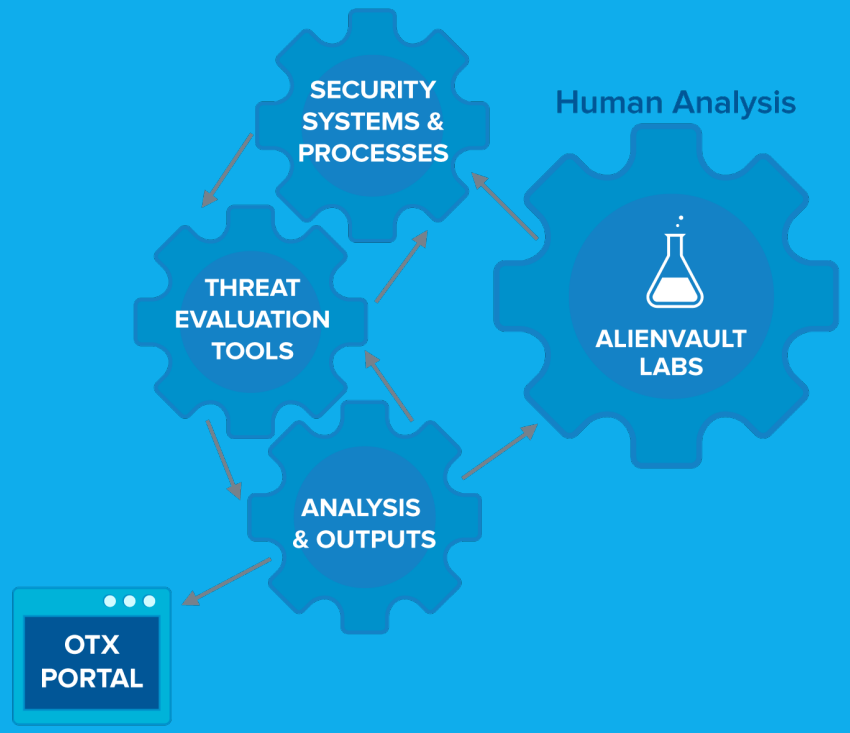
AlienVault® takes a comprehensive approach to our threat intelligence. First, we collect millions of threat indicators every day, including malicious IP addresses and URLs, domain names, malware samples, and suspicious files. AlienVault aggregates this data in the Open Threat Exchange (OTX) platform, from a wide range of sources, including:

- External threat vendors (such as McAfee, Emerging Threats, Virus Total)
- Open sources (including the SANS Internet Storm Center, the Malware Domain List, as well as from collaboration with state agencies 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)
- AlienVault Unified Security Management® (USM) & AlienVault OSSIM™ users voluntarily contributing anonymized data



Next, we have set up automated systems and processes which leverage machine learning capabilities to assess the validity and severity of each of these threat indicators collected in the Open Threat Exchange® (OTX™). These include:

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



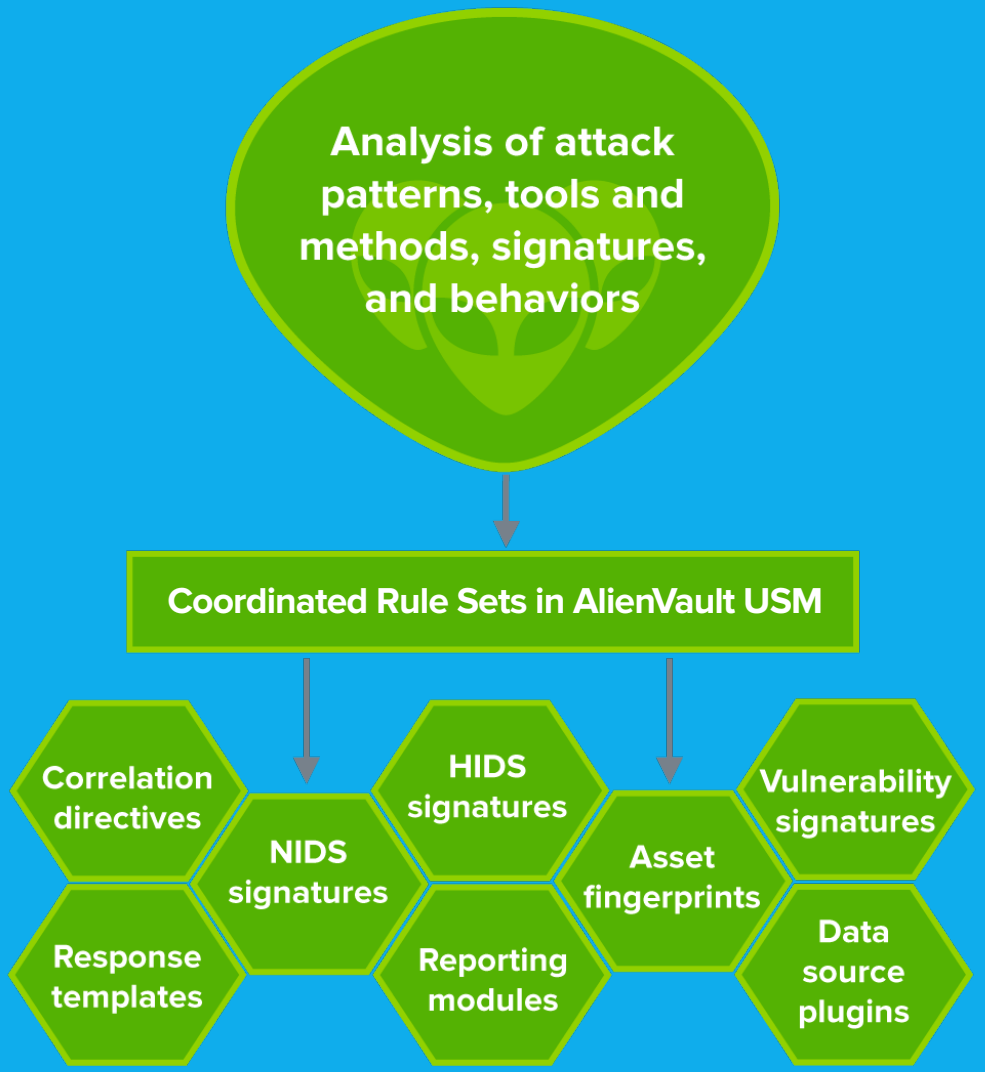
We then use threat evaluation tools established and directed by the AlienVault Labs team to test and validate specific threat indicators. These evaluation tools also leverage machine learning capabilities and include a Malware Analyzer, a DNS Analyzer, a Web Analyzer, and a Botnet Monitor. To take one example, we verify that a domain is distributing malware using our Web Analyzer. We connect to the suspicious URL, analyze, and then execute the file, and if the file is malicious, we mark the server as malicious.

The AlienVault Labs research team then conducts deeper qualitative and quantitative analysis on the threats. For example, they will reverse-engineer a malware sample, or conduct extensive research on particular attackers and their infrastructure to detect patterns of behavior and methods.

The AlienVault Labs team delivers all information about the threats and the attack infrastructure to the USM platform through the AlienVault USM Threat Intelligence Subscription. The team regularly updates eight coordinated rule sets, including correlation directives, IDS signatures, and 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 them 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.



Conclusion

Threat intelligence is essential for effective and timely threat detection and response. You have to assume the attackers will get through your defenses. Threat intelligence is what will enable you to quickly detect threats and prioritize your response.

However, threat intelligence is very difficult and time consuming to generate for most organizations. AlienVault takes a unique approach to delivering threat intelligence, building it directly into the USM platform. We undertake an exhaustive analytics process to generate threat intelligence, and we make it very accessible to resource-constrained organizations. If you do consider an integrated approach for your threat intelligence, consider AlienVault USM with the included Threat Intelligence subscription.

Next Steps: Play, share, enjoy!

- Learn more about AlienVault USM Threat Intelligence
- Get hands on with AlienVault USM
- Join the Open Threat Exchange (OTX)

ALIEN VAULT

www.alienvault.com