IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Oracle

The distinction between threat intelligence and threat data is far from academic as organizations look to address the major challenges facing security operations today.

The Threat Intelligence Renaissance: Threat Data to Threat Intelligence to Threat Detection

March 2022

Written by: Frank Dickson, Program Vice President, Security and Trust

Introduction

IDC believes there is a fundamental confusion or disconnect as it relates to the terms *threat data* and *threat intelligence*. Both can provide value, but the difference is significant, especially given the current challenges facing cloud and InfoSec professionals.

Threat data is made up of feeds or information meant to illuminate security tools and inform professionals about the current reality of the threat landscape. Representative products include data feeds or blacklists of bad malware signatures, known as bad IP addresses, bad websites, disclosed software vulnerabilities, and other associated indicators of compromise (IoCs). More qualitative forms of threat data can include the personally identifiable information of customers, raw code from paste sites, and text from news sources or social media. Threat data can be applied by InfoSec professionals to create an outcome. The onus is on the InfoSec professional to understand the value of the data, apply the threat data to a cloud environment, and subsequently take action.

Threat intelligence is fundamentally different. Threat intelligence offerings actively apply threat data to a cloud environment to either illuminate maliciousness or to remove the noise created by uninformed alerts, essentially enabling an outcome. A threat intelligence offering is, by definition, a more intimate and integrated engagement.

AT A GLANCE

WHAT'S IMPORTANT

IDC places a strong emphasis on the difference between threat data and threat intelligence. Threat data must be made actionable, so it does not introduce complexity and strain into an already overworked and limited cybersecurity workforce. IDC believes that threat intelligence is a differentiator now and will become even more of one to elevate the security posture of cloud environments and make them more resilient.

As a result, threat intelligence services can often be a gateway to a larger relationship — perhaps a managed security service. Threat intelligence is sold sometimes as a security information and event management (SIEM) supplement or in support for endpoint detection and response (EDR). The key here for threat intelligence products and services is that the onus for empowering and curating the data to enable actionable response moves from the customer to the vendor, and the creation of an outcome becomes a shared responsibility. Actionability is key so threat intelligence does not introduce complexity and strain an already overworked and limited InfoSec workforce.

A threat intelligence service shifts the responsibility for making threat data actionable from the customer to the vendor. The outcome becomes a shared responsibility.

Benefits

The distinction between threat intelligence and threat data is far from academic as organizations look to address the major challenges facing security operations today; none of the problems shows any signs of abating. First, there is an increasing chasm between the number of qualified InfoSec professionals and the open positions for those roles. The workforce shortage is acute, and it limits the creativity needed to refine processes in the security operations center (SOC). Second, tool sprawl is becoming problematic. Recent evidence suggests that companies are looking to pare down the number of vendors in their SOCs. Third, an SOC is always playing defense. The perimeter, business segmentations, and policies are established about the known premises. These processes are usually manually intensive. Cyberdefenses are in-depth and layered, and the SOC is designed to monitor and enforce its policies.

A well-curated threat intelligence offering can meet these challenges. Threat intelligence services are designed to look at an environment, accumulate data, and leverage the data to reduce the number of alerts while improving their accuracy. A mature security operations center would ostensibly provide this function as it would shape firewall rules, write integration through RESTful APIs, customize policy, continuously monitor the network for security and performance anomalies, and curate external threat feeds for an adaptive defense. We have just described an ideal security operations center, but few companies have those types of resources. Threat intelligence providers have unique or well-curated understanding of the environment or have experience in integrating multiple platforms and can apply this expertise to a client environment. A subtle but important point is that a security operations team would have to have an orchestration and automation platform (either a discrete tool, an SIEM, or a network access control solution for this function), but a threat intelligence provider has already solved the automation problem. Finally, threat intelligence has an expanded global vantage point. Different threat intelligence service offerings can anonymize different threat data from customers that interact with their services or appliances, collect known malicious DNS sites and IP addresses, and incorporate knowledge about threat actors. All of these activities would be onerous processes for individual SOC analysts.

Threat Intelligence Was Once the Tool of Choice

Not that long ago, threat intelligence was the most efficient and effective approach to security. The discovery of malware on "patient zero" (the first known victim of the malware) led to signature creation and subsequently broad distribution of that signature. Competitive differentiation between security vendors was often based on the effectiveness of skilled security researchers to identify and characterize new threats first.

However, cybermiscreants innovate as well, as lessons from nation-state actions such as Stuxnet gave birth to targeted attacks. The forefather of advanced threats, Stuxnet was an attack by U.S. and Israeli governments on Iranian nuclear enrichment facilities in 2011 and was the first accredited time a cyberattack was specifically tailored to a targeted entity. The term *targeted* additionally implies sophisticated, and the attack focused on taking advantage of four specific weaknesses in the Iranian IT systems to cripple the uranium enrichment facility. Such weaknesses were later labeled "zero-day vulnerabilities," as the weaknesses were unknown before the attack. Exploit kits became the rage, automating the exploitation of vulnerabilities on victims' machines. Targeted malware resulted in an exponential increase in the number of malicious binary variants. Ultimately, the threat intelligence signature approach succumbed to an explosion of malware variants.

Since the attacker; the tactics, techniques, and procedures (TTPs); and the weaknesses of our IT architecture are unknown, many security tools take a completely different approach to threat detection. Instead of focusing on known threats, the focus has turned to known "good" activity. We establish statistical baselines for legitimate user, application, and platform behaviors; significant deviation from the normal (anomalies) indicates potential maliciousness. Thus user behavioral analytics (UBA) was born. Threat modeling goes hand in hand with UBA. A key component to UBA is that an analytics engine develops statistical baselines about the normal behavior of each entity on the network. Such a baseline allows the analytics engine to establish context.

Although it has not been the primary differentiator in a UBA solution, threat intelligence remains an important component. First, a threat intelligence offering informs a normal baseline for each entity in the client's network. The need for agents becomes increasingly relevant as agents may not be preferable or even able to be deployed. The inability to acquire telemetry and context without agents limits correlations to the statistical analysis and indexing of logs and/or batches. Second, because threat intelligence offerings should take in multiple log and flow data, the platform is responsible for narrowing the number of alerts that its clients need to act on. Redundant alerts and false positives are the expressed responsibility of the threat intelligence service.

Threat Intelligence Changes the Threat Detection Game Again

Just as trends come and go, so do the tools we apply to secure our cloud environments. The use of threat intelligence is coming back into vogue. Please don't get me wrong. Signature-based detection as a primary source of detection is dead. We crossed that point long ago as malicious binaries can be easily customized to have a single target.

However, although cyberattacks and malware have almost infinite variability, the TTPs tend to be surprisingly consistent. Instead of focusing on malware, today's threat intelligence focuses on those TTPs. Types of malicious activities that can be monitored include remote control of an internal host, command and control activity, network and geolocation, internal reconnaissance of network systems and resources, brute-force password attempts, correlation of data collection and exfiltration, and encryption of network share drives. In fact, the most current MITRE ATT&CK Matrix describes 14 different technique categories used by an adversary to infiltrate and exploit an enterprise network. (Recently, the Reconnaissance and Resource Development categories were added left of and before Initial Access.) It is a major advantage to a software provider to show on its dashboard where an SOC analyst can mouse-click on a screen and see the information map to the ATT&CK Matrix and the catalog of techniques.

Thus threat intelligence can change the threat detection game. Anomaly-based detection is still important; however, it can be problematic as the comprehensiveness of the task can be massive. In addition, anomaly-based detection's Achilles' heel includes false positives and false negatives because detections are not deterministic but instead based on probabilities. Just because something is anomalous does not necessarily mean that it is malicious. Granted, UBA platforms get stronger the more data that you feed them. Obviously, that means there is a nascent stage in deployment where a UBA platform does require other tools while it self-tunes. Without proper controls, repeated bad behavior begins to look like non-anomalous behavior, creating a false negative concern. This is an acute concern for batch data. Finally, it may be possible for a sophisticated hacker to undermine the platform by adding so much meaningless data that as the analytics engine is analyzing data streams, the true intention of the adversary remains hidden (roughly akin to a buffering error attack).

Threat intelligence can instead inform detection. Instead of scanning an entire environment, threat intelligence can turn the focus to specific aspects of an IT architecture and specific processes, detecting maliciousness by analyzing sequences of instructions, processes, or operations. Subsequently, threat intelligence can show the potential movements of a motivated adversary and suggest accepted response techniques.

What is required to transform threat intelligence into threat detection? Threat intelligence providers will ideally focus on a few core strategies:

- **Threat intelligence has to drive actionable response**. Based on the definition, this would be intuitive, but services are differentiated based on the ease of enabling outcomes. If threat intelligence comes to the security operation center as an CSV file, it has limited usability. Threat intelligence has to be ported directly to the firewall as policy; to an orchestration engine to be used in SIEM, firewalls, intrusion detection systems/intrusion prevention systems, or endpoints (possibly) and for use in playbooks; or to IT/SecOps ticketing. Threat intelligence should provide context around the IoC use cases. It should also be specific to the organization and what it means for that particular customer.
- **Threat intelligence should be designed for the customers it serves.** There will almost certainly be times when the company will need support with configurations, greater understanding of threat reports, or to extend the platform to account for new data sources. Considering the native tongue of a threat actor helps InfoSec professionals to understand and develop a more complete picture of threats emanating in social media or on the dark web. The ability of support staff to speak Farsi, Mandarin, or other languages when appropriate makes a difference.
- **Finally, price matters.** The actionable aspect of threat intelligence requires us to consider the outcome and the investment needed to enable that outcome. It is not uncommon for a threat intelligence offering to start at $100,000 per installation and go up from there. Although threat intelligence can demonstrate real value, no organization lives in a world of limitless resources, and the reality is that threat intelligence services have to compete for static dollars with other security offerings.

Considering Oracle

Oracle has been on a tear as of late, introducing new security offerings at a feverish pace in its efforts to differentiate itself as the most secure and trusted cloud provider. Its latest offering is its new Threat Intelligence Service. The offering is straightforward. Oracle curates threat data from four primary sources:

- Oracle telemetry and investigations
- Open source feeds (Tor, abuse.ch, etc.)
- Honeypot network
- CrowdStrike partner intelligence

Oracle subsequently takes the curated data and applies it to its Oracle Cloud Infrastructure (OCI). InfoSec professionals can then quickly and easily get the benefit from threat intelligence–based detections in their environment. As Oracle leverages its own InfoSec professionals and threat researchers to architect and deliver the offering, customers reap the benefits of Oracle's expertise in defending its own cloud environments, including observed telemetry and threat research teams spanning its software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) offerings. The result is higher coverage across feeds and fewer false positives. The insights are curated to be prescriptive, with overall confidence assessments based on source, frequency, quality of sightings, and recency to help analysts prioritize alerts.

Customers are able to actualize the benefits of Oracle's expertise in defending its own cloud environments, including observed telemetry and threat research teams spanning its SaaS, PaaS, and IaaS offerings.

Although the integration and automation of Oracle's security expertise is compelling, the time to value is the clearest and most differentiating benefit. The offering has out-of-the-box integrations with Cloud Guard to reduce complexity, with plans to expand integration into other OCI services. In addition, as Threat Intelligence Service is an organic component of Oracle Cloud Infrastructure, the need to manage your own data is eliminated, along with the resulting complexity. Finally, the threat intelligence service is provided at no additional cost — as in *free*. Oracle's approach is to raise the security conversation to one of resiliency, making the cloud environment more secure by design. Enabling curated and readily actionable threat intelligence is one way to make OCI safer from the ground up.

Looking to extend threat intelligence into action, Oracle recently launched Cloud Guard Threat Detector, a detection and response service informed by real-world attack tactics, techniques, and procedures. Cloud Guard Threat Detector runs targeted threat models aligned with the MITRE ATT&CK framework, looking for malicious TTPs and assigning risk scores based on attack progression.

Cloud Guard Threat Detector is informed by data from the Threat Intelligence Service, delivered with out-of-the-box integration across OCI and other Oracle properties. The service is native to OCI, with curated and managed behavioral models anchored in the MITRE ATT&CK framework, and it delivers unified progression-based scoring for effective alerting with low noise. Finally, as Oracle is highly motivated to distinguish OCI as the most secure cloud environment, it is offering the Cloud Guard Threat Detector free of charge for paid tenancies to motivate adoption.

Challenges

The key challenge to the Oracle offerings is that they are new. New often makes security and cloud professionals nervous, even coming from an organization the size of Oracle. Although the native integrations and threat intelligence will provide quick time to value, the platform may have hiccups as it matures. In addition, if a customer is wedded to some of its current threat feeds, integrating them may take time. Also, the Cloud Guard Threat Detector is limited in the number of use cases that it currently addresses, although it will clearly be strengthened as Oracle introduces additional use case models over time. Finally, the Oracle offerings only add value to OCI. As multicloud is the rule rather than the exception, additional tools may be required to provide standardized multicloud SOC analysis capabilities.

Conclusion

Delivering and maintaining secure cloud environments can be challenging. Often, it is not the hard costs but soft costs that can be the most vexing. This is the reason IDC places such a strong emphasis on the difference between threat data and threat intelligence. Threat data must be made actionable, so it does not introduce complexity and strain an already overworked and limited InfoSec workforce. IDC believes that threat intelligence is a differentiator now and will become even more of one to elevate the security posture of cloud environments and make them more resilient. Oracle is addressing the challenges described in this paper and positioning InfoSec professionals to secure OCI environments.

About the Analyst

Frank Dickson, *Program Vice President, Security and Trust*

Frank Dickson is a program vice president within IDC's Security and Trust research practice. In this role, he provides thought leadership and guidance for clients on a wide range of security products, including data security, cloud security, ransomware, and emerging products designed to protect transforming architectures and business models.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com