451 Research® | SPECIAL REPORT

Actionable Threat Intelligence

SIX DIMENSIONS CRITICAL TO SUCCESS

COMMISSIONED BY

WEBROOT® Smarter Cybersecurity™

MAY 2019

ABOUT THE AUTHOR

SCOTT CRAWFORD

RESEARCH DIRECTOR

Scott Crawford is Research Director for the Information Security Channel at 451 Research. The former CISO of the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) International Data Centre in Vienna, Austria, Scott's experience includes security management and strategy for organizations from IBM to a division of the University Corporation for Atmospheric Research in Boulder, Colorado.

Introduction

"Know yourself; know your adversary." This fundamental tenet of defense remains as true today as it was in Sun Tzu's time: you can't defend against tactics you don't know about.

Cyber defense is no exception. It is a challenge often regarded as asymmetric: the adversary has the luxury of probing any number of exposures at will. Defenders, on the other hand, must make the most of limited resources to protect the entire attack surface.

Threat intelligence can offset the adversary's advantage and give defenders a vital edge. By calling on today's more sophisticated techniques for collecting and analyzing large volumes of highly detailed data and automating how it's put to work, threat intelligence can have a real impact on optimizing the efficiency of defense, helping to focus investments on countering the tactics that adversaries actually employ.

Delivering on the Intelligence Promise

To realize this potential, however, insight must lead to action. And to be truly actionable, threat intelligence must address challenges in six vital dimensions:

1. Scale

The sheer volume of available data and data sources presents one of the greatest hurdles to actionability. Opportunistic exploits often appear in large numbers, while more targeted attacks may use finely honed methods to pursue a specific objective. All factor into the body of data that must be turned into actionable insight.

What kind of scale are we talking about? Consider that nearly four billion IPv4 addresses exist on public networks (not including more than 500 million reserved addresses set aside by the IETF and IANA). Keep in mind that multiple hosts may exist on private networks behind a single NAT IP. Some estimate the number of mobile phones worldwide to be even higher than the global population. As 'smart' technologies continue to proliferate, the numbers of systems, applications and devices online will grow to billions more.

And those are just the sources of potential data. Add to that the numbers and variants of attack tools and methodologies, as well as the attributes of attackers that can be gleaned from that information, and volume escalates far higher. According to the AV-TEST Institute:

- Over 350,000 malicious programs (malware) and potentially unwanted applications are registered every day.
- April 2019 saw 11.62 million new samples of malware in that month alone.
- MacOS malware saw a significant spike in 2018, 66 times higher than the number of samples seen in 2014.

Large-scale attacks are responsible for much of this volume – but stealthy adversaries often depend on overwhelming noise to hide more subtle tactics. Spam is a primary vector for delivering this malicious content, with billions of spam messages sent each day. This mountain of unwanted and unsolicited email is one of the most common delivery vectors for phishing and malware, and an abundant – but daunting – trove of the raw material that contributes to threat intelligence.

Clearly, getting a handle on this scale is job one for actionable threat intelligence.

2. Scope

It's not just the ability to handle large amounts of data that's important, however. Analysis that incorporates a high volume of input can still have blind spots. It's great that today's techniques can gather data from virtually all public networks – but *do* they? Resources that can handle this volume may not be as effective unless they have access to the fullest possible scope of sources.

This is not just a question of scale. Attacks that capture headlines may motivate security teams to focus on the most visible threats or exposures. Adversaries, however, are motivated to be as invisible as possible. Web crawlers are often employed to find malicious URLs used in phishing attacks – but many of these sites are built to not be accessible to crawlers.

For visibility to be truly comprehensive, a more thorough approach that uses a variety of techniques to gather input from the widest possible scope of sources is required.

3. Timeliness

One of the key advantages of modern data management and analytic systems is their agility of response. Many such architectures are highly parallel, leveraging cloud scale to deliver in seconds what in the past might have taken far longer. This is vital to arming threat intelligence, which can be highly time-sensitive. Malicious hosts or domains may only pose a threat for a limited time. Phishing sites may be live for mere hours, not days.

This can sharply limit the time window of actionability. Static output such as lists are frozen in time and can age beyond usefulness with breathtaking rapidity. The analytics that deliver this intelligence must therefore be dynamic – as close to real-time as possible – across the scope of input they must embrace.

Timeliness of analysis is only one part of the equation, however. This data must also be put to work as swiftly as it's delivered. Continuous and ongoing consumption of this data – by technologies that monitor, block and defend against attacks, as well as by those that provide insight to analysts – is necessary to keep intelligence-driven defense current and effective.

4. Adaptability

We've equipped our threat intelligence efforts with scale, scope and speed. How can we further separate signal out of all the potential noise?

It's easy to say that modern analytics can improve threat intelligence by optimizing efficiencies. Distinguishing behavior that poses a threat, for example, may be far more efficient than cataloguing virtually endless variants of attack tools such as malware.

But there is another dimension to threat data that in many ways makes its analysis unique: threat actors are intelligent adversaries whose tactics change in response to new opportunities for exploit as well as changes in defense. This means that threat analytics must respond to these dynamics and adapt accordingly.

This has been one of the great opportunities for technologies that can learn. Machine learning systems can develop their own models of malicious behavior – and they can further automate the dynamic adaptation of these models or develop entirely new ones when presented with new evidence.

This, in turn, improves the actionability of threat intelligence in two key ways. Defensive technologies that can consume this content are provided with more accurate data that improves their performance. Learning algorithms that filter out noise for human analysts also free highly valuable personnel to do what they do best: apply human discernment to reveal intentions and correlate activity to actors, motivations and appropriate response.

5. Applicability

All these advances have brought vast improvements in the signal-to-noise ratio of threat intelligence – but they still leave organizations with one important question: *How does this apply to **me**?*

It's not a trivial question. Even high-fidelity data can leave organizations with too much to handle, unless a few practical lenses are applied to help sharpen its focus. Finely tuned threat intelligence can answer questions such as:

- Does the evidence correspond to targets in my environment? If it doesn't line up with an organization's actual exposures, it may not be as valuable.
- How great an impact is this activity really having? Communicating how it affects other organizations with similar exposures can be a valuable enhancement to threat intelligence and increase vigilance where needed.

6. Context

Often, the applicability of threat intelligence is not fully revealed by individual data points in isolation. Knowledge that a certain tactic is used to gain an initial foothold is not as useful as knowing the sequence of actions that lead to a specific outcome.

This is where threat intelligence must deliver depth as well as breadth. With all the emphasis on data gathering and analysis at scale, it can easily be overlooked that attackers may not use a single exploit in isolation. Nor are they necessarily confined to a single, linear path toward an objective. An individual adversary may pursue a number of ways to access multiple objectives. The mitigation of a single one of them may not be sufficient to mitigate the threat.

Threat intelligence that connects these relationships can tell a highly valuable story. It uncovers methods that, in isolation, may not raise concerns – but when they reveal patterns and sequences of activity, they may also reveal the seriousness of a threat. This capability can also be predictive when it indicates where an adversary may move next – which helps make defense more proactive and better prepared for attacks before they have serious impact.

A Multidimensional Advantage

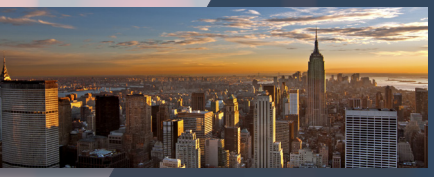
All of these capabilities make threat intelligence a key enabler of security effectiveness on multiple levels:

- In tactical defense, intelligence-consuming security technologies are better able to respond to the real-world tactics organizations face today. Not yesterday – and maybe not even a few hours ago. When they can act on predictors of activity, they can help guard against malicious actions before they have an impact.
- In security operations, actionable threat intelligence helps make analysts more productive and better able to deal with a wider range of threats. It helps improve the efficiency and effectiveness of response, and gives analysts the insight needed to inform security management.
- In security strategy, actionable insight into threat activity guides decisions that make the most of the security investment. When insight is predictive, it can also indicate where investments may be needed to adapt to new or increased threats.

The delivery of this potential requires providers that can equip their efforts with the necessary scale and scope – in as close to real-time as possible – with high-quality data derived from analysis that learns from a changing threat landscape. These are providers that can deliver insight that's actionable for each business they serve, from data-driven security technologies tuned for a specific environment to insight that is vital to tailoring an effective security program to an organization's unique needs.

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.



NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
505 Montgomery,
Suite 1052
San Francisco, CA 94111
+1 212 505 3030

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®