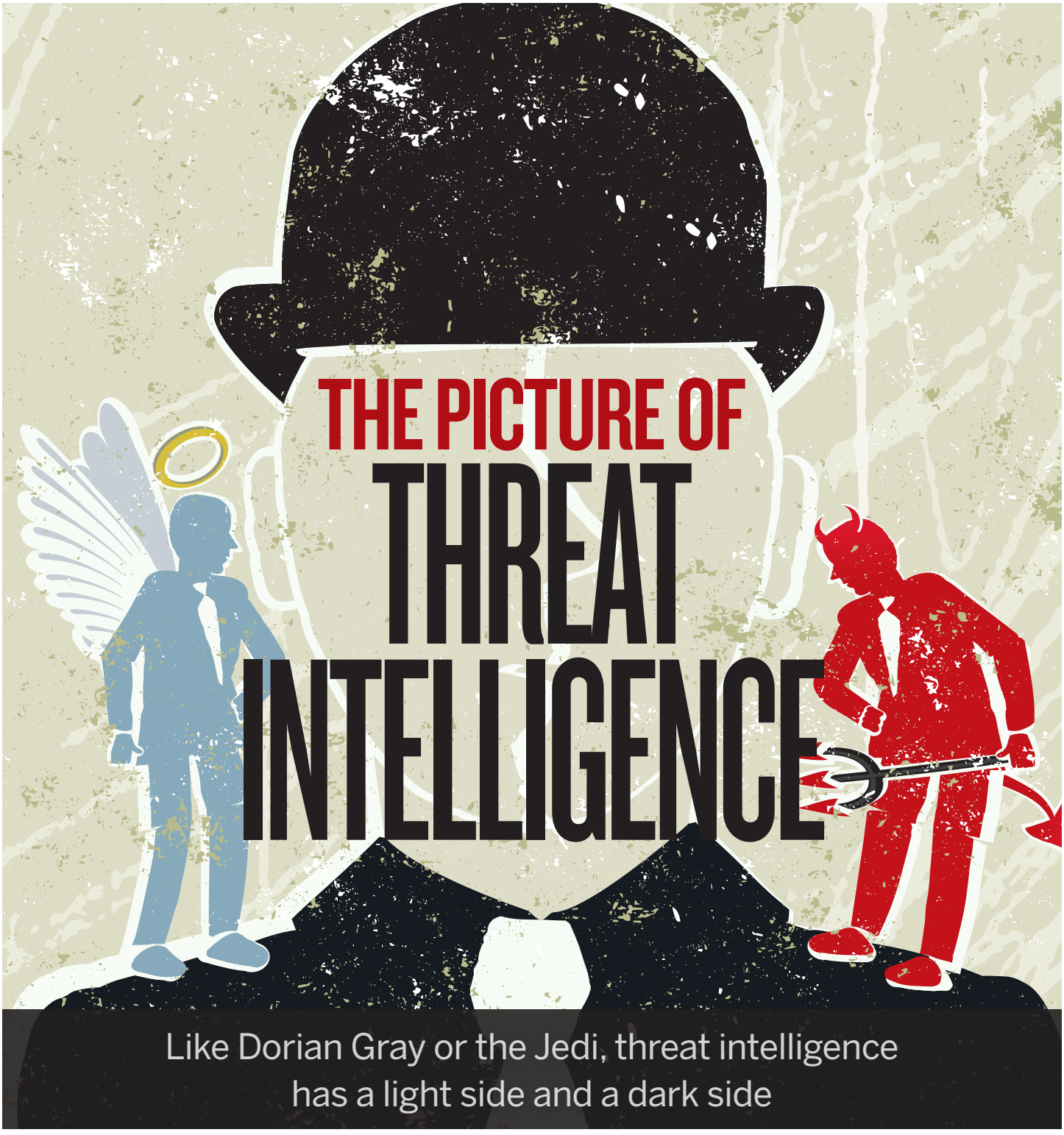

ebook

An SC Media publication

Sponsored by

ANOMALI®

ARCTIC WOLF

BLUVECTOR®

Recorded Future

Threat intelligence yin yang

Threat intelligence is a popular buzzword, but is it meeting its hype? Some swear by it; others swear at it. Evan Schuman reports.

The long-acknowledged core problem with threat intelligence today is the software equivalent of a Yin and Yang situation. The algorithms are smart enough to catch a massive number of log anomalies, detecting any pattern deviation that might indicate an attack attempt. That said, they are not yet smart enough to identify accurately the real threats from innocuous activity. The challenge lies, in part, between what the expectations and definitions are for the CISO and the realities of how attackers exploit corporate network vulnerabilities.

Most experts say that the viable answer is to not wait for the software to get better, lest it be forgotten that the bad guy's software is not only also getting better, but getting better faster. So the real answer is to obtain more meaningful data for the algorithms on hand.

A good example is insider context. That approach looks beyond perimeter security and attacks authenticated insiders who might not be who they claim to be. Whether credentials are stolen through social engineering, a trojan horse or other malware, the idea is that a different kind of battle must begin after a user logs in and is authenticated.

That additional data typically comes in the form of context, which considers that user's typical attributes, both the physical, what device is being used and where is it located, to the behavioral; are they logging in at an expected time, are they accessing their usual documents or does their position in the company entitle them to this data.

And yet, cyberthieves are often good at doing their homework. They might tunnel in to the user's machine, take it over and then access your network from the expected machine and the expected location. They might specifically attack personnel who would normally access the files they are seeking.

In short, this is a serious problem and the "solution" is not universally consistent.

Munish Puri principal consultant for Presearch Strategy, a security research firm, posits that threat intelligence data is getting more complex than an enterprise security system can analyze and that the CISOs are making the situation worse.

"Most organizations still divide security into different departments and create blind spots for exploitation. Adversaries, on the other hand, do not think about 'physical security' and 'cybersecurity.' They simply look for gaps. They don't ask themselves 'What's my physical security angle?' to an attack. Adversaries just find the weaknesses and exploit," Puri says. "The focus on actors, while important, is 90 degrees from how organizations need to address their vulnerabilities. Until the security organizations truly synthesize vulnerabilities from multiple domains, those blind spots will

OUR EXPERTS: Threat intelligence

Swapnil Deshmukh, senior director of emerging technologies security, Visa

Don Elledge, CEO, Edgile

Michael Figueroa, executive director, Advanced Cyber Security Center

Chad Loder, serial entrepreneur and security expert, Habitu8 and QuickSilvr Technologies

Munish Puri, principal consultant, Presearch Strategy

Mike Sanchez, CISO, United Data Technologies

Mike Spanbauer, VP of research strategy, NSS Labs

2.3B

Texting turns 25 years old this year but its peak year for texts was 2011 with 2.3 billion messages sent. 1.7 billion were sent in 2016.

– CTIA 2017

remain and surprises abound."

Puri takes this problem one further and suggests that even security language is undermining threat intelligence efforts. He maintains that "the urgency in the word 'threat'" is generating "threat fatigue," which in turn is used so often "that people are becoming inured and it's then hard to create a sense of urgency and action."

Mike Spanbauer, the vice president of research strategy for NSS Labs, a security testing company, says "One of the chief challenges with threat intelligence offerings, in practice, is their focus on providing a wide stream of threat information covering as many asset platforms as possible. This information is valuable for SOCs (security operations centers), but even with basic tailoring in place it can easily compound the 'alert fatigue' and information overload distractions already plaguing incident responders," he notes. "Threat intelligence is increasingly becoming a commodity and threat intelligence platforms are becoming as noisy as SIEMs (security information and event management systems) and quickly losing their value."

Mike Spanbauer, VP of research strategy, NSS Labs

Spanbauer believes that not only does threat intelligence today suffer from having too much information on possible bad actions, but it also has a shortage of information on good actions. And it is the information on good actions that gives us the basis for doing contextual analysis extrapolations.

"You have to have a baseline of known good behaviors," Spanbauer says. Many CISOs are "focusing too much on the perimeter. Instead of trying to keep the bad guys out, we need to better understand the baseline of who's good," he says.

Spanbauer acknowledges that the more sophisticated attackers today can do a terrific job at making security software believe they are the legitimate user they are masquerading as, but contends that more context on good behavior will address that.

"A sophisticated spear fishing attack could even emulate the user down to the node. The targeted attackers do their homework," Spanbauer says.

The accumulation of an excessive amount of threat data can be blamed on security vendors, CISOs and other security personnel, Spanbauer says. A few years ago, many threat intelligence applications delivered dozens of data fields and the software was shipped with it defaulting to almost all of those data fields selected. That was the vendors' fault, but enterprise security teams could have, but did not, simply change the default settings.

This caused quite a few "duplicate and overlapping data points" and it has only been recently, Spanbauer recalls, that he has seen security teams reducing the number of accepted fields "to six or 10 at most, down from dozens."

He also blames many of those vendors for overpromising on how well their software could deal with that much data, with marketers proclaiming "that their feeds provided everything a CISO or SOC would need."

Spanbauer also faults the threat intelligence security vendor community for allowing extensive incompatibilities to exist between almost all threat intelligence products. "Every vendor has its own (proprietary) data scheme and it's an incredibly painful process to stitch one feed to the next," he says, adding, "It's like three blind men looking at three different pictures: Nobody knows what they are looking at."

This is not a trivial problem. Security teams need multiple systems tracking threats because they all have their strengths

73M

Number of estimated jobs to be displaced in the US by 2030. China and India, the top two job losers, are expected to lose 236 million and 120 million, respectively.

– McKinsey

and weaknesses. "Security teams must understand which data fields they already possess. You have to be able to correlate all of this threat data to make any information actionable."

Chad Loder, a serial entrepreneur who founded Habitu8 and QuickSilvr Technologies, agrees that the feeds are part of the problem, pointing to more than 150 different threat feeds that are available, including many open source offerings.

The problem Loder identifies is that there now exists a gulf between how humans and the tools function. He pointed out that there is a great deal of always changing information along with a certain level of uncertainty which the tools can't handle well.

Other than the National Security Agency, the entity that likely tracks more potential threat activity than anyone is payment card giant Visa. Swapnil Deshmukh is senior director of emerging technologies and security at Visa and he sees enterprise threat intelligence today as being in an undesirable position.

Chad Loder, serial entrepreneur and security expert, Habitu8 and QuickSilvr Technologies

"Threat intelligence technologies are unable to keep up with the ever-evolving threat landscape. They generally are regular expression or policy-based tools that inspect network traffic. And it turns out it's a Catch 22," Deshmukh says. "Sophisticated attacks tend to obfuscate the attack payload, making it difficult to be detected via known threat intel tools. A few companies are working on the challenge by building cognitive learning techniques that provide context to the payload, but the true test of the tool will be efficiency in gathering and parsing threat intel feeds."

The context approach, which Deshmukh advocates, suffers from the after-the-fact predicament in that it cannot start its analysis until after the attacker gets into the system. From there, it is a race to see if the system can detect anomalies and act on them — or, even slower, alert a human to determine what to do — before the bad guy can successfully steal the targeted data. Software is fast, but well-practiced bad guys are too, especially given that they are also using software to help steal the data.

"If (the bad guys) are trying to mimic routine traffic noise, a lot of attackers will be able to exfiltrate data from your network" before threat intelligence software and its human overlords can act, Deshmukh says. That assumes the software and mammals can even figure out it's an attack.

Deshmukh argues for some manual authentication methods that are slower but more effective, such as "calling up a colleague to make sure" that he/she is indeed the one currently in the system. Even better, Deshmukh says, a system could seek additional biometric authentication prior to granting access, such as the system "calls you and asks you to authenticate yourself by turning on your video."

Another security aficionado who is worried about the current state of threat intelligence is Don Elledge, the CEO of the security regulatory compliance firm Edgile. The essence of the problem from Elledge's perspective is that many of today's threat intelligence packages were envisioned and created during another era and are now ill-suited to battle the security problems facing CISOs in 2018, let alone the near future.

"The problem with threat intelligence is that our traditional security model has become too complex to effectively identify threats. The tools have improved, but they can't deal with the exponentially increasing complexity of the modern enterprise operating around a

94%

Only 6% of all comments to the FCC regarding Net Neutrality were unique with 94% duplicate comments or fake identities; 21.7 million "comments" were submitted.

– Pew Research Center

traditional security model," Elledge says. "The traditional model was built on the concept of a private network and this model still exists as the primary mindset in the security community. The private network model was never designed to operate in the digital age and we have seen a continued manipulation of the private network to try and support the digital transformation."

The problem is that today's networks are ill-defined. Entry can come from corporate campuses just as easily as from a mobile device located overseas, from a consumer laptop that appears to be in an employee's home or from an IoT device connected to the corporate network that is sending out data to a command and control server thousands of miles away. Sensitive corporate data exists in the enterprise as well as on various cloud platforms from third-parties with their own security headaches.

Don Elledge, CEO, Edgile

Indeed, it is common that a seemingly authorized user logs into the network solely to jump into a cloud courtesy of a sales or manufacturing third-party-controlled application. Beyond having to trust a third-party, these cloud operations limit how much contextual information the corporate network can collect. In other words, once a user logs into Salesforce or Workday, for example, the enterprise security system will often have no visibility into what the user is trying to do, preventing it from alerting when unusual behavior happens.

Elledge adds that cloud and IoT communications are undermining network security.

"A lot of that information is encrypted and protected. More and more things are being requested outside of the network," he says. "The monitoring of the network layer is providing less and less information and context. The modern enterprise doesn't have an inside and an outside anymore. It's much more virtual. The current model is kind of falling apart in front of our eyes, with a huge amount of unstructured data."

"To identify and protect against threats, you need to have a manageable and known environment," Elledge continues. Private networks today extend around the world, have an increasing number of connections, hundreds of thousands of nodes, [and] people and systems increasingly moving [data] easily across the perimeter. Most companies do not really know where their network begins or ends, he notes.

"Business realities are driving a digital transformation and we need a security transformation to support these trends. Companies have to think differently about security. The model that places our primary defenses at the network perimeter no longer works as systems, people and data move and exist across the perimeter," he continues. "We need to start embracing the digital transformation from a security perspective."

For example, if users have controlled views into data across public networks, companies can reduce or remove the need to download data into the unstructured spaces where companies lose control of the information. By embracing the public network securely, Elledge notes, companies can make services available and reduce the complexity and increase the manageability of our private networks.

"Moving from the one-to-many security model of applications operating over public networks, instead of the many-to-many security model of private networks, we can decrease the level of complexity by 100 times or more," he says.

Another complicating factor is context,

24%

Percentage of businesses treat preventing, preparing for and responding to risk as a strategic business priority.

– Travelers 2017 Travelers Risk Index

but not in the sense of understanding a user's network behavior. This other context problem involves an enterprise's own network elements.

"What's more subversive, though, is that the system supply chain prevents organizations from completely understanding what threats can possibly apply to them," says Michael Figueroa, executive director, Advanced Cyber Security Center, an umbrella organization for various security concerns. "An organization may implement a new device in its infrastructure that solves a critical business need without having any visibility into the various software packages, utilities and libraries used by the manufacturer to build the device. Without that exposure, security teams have no ability to adequately defend [based on] the findings of their threat intelligence efforts."

Michael Figueroa, executive director, Advanced Cyber Security Center

That lack of visibility can fuel a wide range of other problems. "Threat intelligence systems and techniques lack the context to quickly act on the indicators. Threats are seen from a technical perspective, one that may indicate a new rule to apply or system property to examine, rather than from an attack perspective," Figueroa says. "As such, the most sophisticated security operations are given limited understanding of how important one individual event may be against a steady stream of threats. That undermines their ability to prioritize and makes most threat intelligence activities useless."

Figueroa makes the case that context-based defenses can be undermined by "the anomaly perspective, presuming that the attacker is not going to act like the user," whereas attackers often do a commendable job impersonating the identities that they steal. Sometimes, "attackers are actually [using] a VPN (virtual private network) to that [victim's] computer so that they can look like the user when they hijack [the user's] machine," he says.

The typical security center manager response, Figueroa says, is "if we just had a little more data." Figueroa says that a slide he often uses in security presentations reads "'I now have enough data,' said never by a data scientist."

"We're always seeking more data, but our ability to collect data far exceeds our ability to process it in any reasonable way," Figeuroa says.

One CISO, Mike Sanchez of United Data Technologies, says many of the perspectives of his fellow CISOs are decidedly not helping the threat intelligence cause. "CIOS typically think in the terms of that red team stuff; that is the usual thinking. They are not having business-centered conversations.

"We are having these problems because CISOs are looking at tech solutions, but they are not taking the time to check what the business requirements are," Sanchez says. "They don't spend enough time and energy identifying their true risk exposure in a quantifiable method and that affects all decisions downstream," he continues. "That is the problem, and if it wasn't the problem, we wouldn't have had all of these issues we are seeing today with Equifax and other data breaches which happened because sound business practices were not in place or ignored." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

29%

Percentage of sites that had at least one mobile device running a cryptojacking script in November 2017

– Wandera survey