TAG Cyber
Security Annual
2022
SPECIAL REPRINT EDITION

PREVENTING ABUSE OF APIs

AN INTERVIEW WITH CAMERON GALBRAITH,
DIRECTOR OF PRODUCT MARKETING,
NONAME SECURITY

CYBERSECURITY TOOL PORTFOLIO—FRIEND OR FOE?

IS THE GOVERNMENT'S VERSION OF ALL IN THE FAMILY A REALITY SHOW?

TAG CYBER
DISTINGUISHED VENDOR
n noname

AN INTERVIEW WITH CAMERON GALBRAITH, DIRECTOR OF PRODUCT MARKETING, NONAME SECURITY

PREVENTING ABUSE OF APIs

As businesses come to depend more on their APIs as the foundation for their missions, the problem emerges of dealing with malicious fraudsters. The abuse of business logic through APIs, for example, can create security vulnerabilities which in turn can have serious consequences to the organization.

Noname Security is a leading commercial solution provider addressing these API security objectives for enterprises. We wanted to learn more about how the Noname API Security Platform reduced API security risks for modern enterprise teams.

Because APIs are used by every corner of the business, it was important for us to design a solution that supported the entire API lifecycle and delivered value to each along the way, from developers to operations to security.

TAG Cyber: What types of threats exist today for APIs?

NONAME SECURITY: APIs are the lifeblood of digital transformation. "Cloud" and "apps" are just code words that mean "lots and lots of APIs." Business critical applications and data now all run on APIs, which means it's more imperative than ever to protect APIs from any type of vulnerability—from simple misconfigurations to a full scale attack.

Unfortunately, API threats are all too common. They're on the rise, costly and time-consuming to remediate. Most enterprises lack the visibility and discoverability necessary to even detect a threat. For example, most don't know how many APIs they have, which APIs are communicating sensitive information, or even who or what the APIs are communicating with. And traditionally, once a compromise is detected, it can take months to determine the root cause of a data leak or attack to remediate. All the while, applications and environments are constantly evolving. New changes are introduced for existing APIs, and new APIs are being deployed faster than they can be secured.

TAG Cyber: How does the Noname platform work?

NONAME SECURITY: The Noname API Security Platform protects APIs in real-time and detects vulnerabilities and misconfigurations before they are exploited. The platform is an out-of-band solution that integrates with your existing infrastructure and spans across three core capabilities:

API Security Posture Management allows users to inventory every API, including legacy and shadow APIs, with automated data classification security posture details. API security analytics flags high risk misconfigurations and API security vulnerabilities in policy and specs, so that AppSec teams can prioritize remediation efforts.

API Runtime Security offers AI and ML-based models for runtime API threat detection. Then there's automated and semi-automated blocking and threat remediation.

"Shift Left" with API Security Testing features automated and dynamic API security testing for CI/CD pipelines. Users can continuously test APIs to identify security risks before they emerge.

TAG Cyber: How do you weave your solution into the modern DevOps process?

NONAME SECURITY: Because APIs are used by every corner of the business, it was important for us to design a solution that supported the entire API lifecycle and delivered value to each along the way, from developers to operations to security. The Noname API Security Platform embraces "Shift Left" and identifies performance and security issues early in the development process, identifies configuration issues and vulnerabilities within policies and specs through deployment, and provides threat detection and remediation functionality in the runtime.

TAG Cyber: Tell us more about the most typical use-cases for your product in operation.

NONAME SECURITY: The interest in our solutions evolves as the relationship grows. Most companies are aware that they have blind spots within their API estate and are interested in discovery and posture management. However, once we turn the lights on, we usually find a significant amount of issues, and an inventory of APIs much larger than the client anticipated. The runtime security and active testing capabilities then become the most typical use cases— protecting the environment from any kind of threat and ensuring the validity and integrity of all new and existing APIs.

TAG Cyber: Do you have any predictions about whether API security can play a role in future global cyberwars?

NONAME SECURITY: It's not the future of global cyberwars, *it's already upon us.* Digital transformation and cloud migration initiatives are API-first. The industry is quickly headed to an API-only world and that means the volume and severity of API threats will only increase. We see it in the news every week. It's crucial for enterprises to eliminate their API security blindspots and implement API security platforms and processes that can operate at the speed and scale of their business.

CYBERSECURITY TOOL PORTFOLIO—FRIEND OR FOE?

JENNIFER BAYUK

For those not familiar with the remarkable story of Pegasus, the idea that a cybersecurity tool designed to bolster a nation's defenses can morph into an offensive cyberweapon may seem daft. Pegasus was first marketed as a surveillance tool designed and proven to provide intelligence with which to find fugitives from justice, thwart terrorist plots, fight organized crime and take down child pornography rings. It provided the intelligence by exploiting vulnerable phones of its targets. Its use was therefore considered in line with wiretaps and other monitoring devices available to law enforcement, at least by the U.S., until it became astonishingly clear that it was used to unjustly hunt nonviolent opponents. The most egregious example of its misuse culminated in the killing of the Washington Post columnist Jamal Khashoggi by Saudi Arabia. The company that produces Pegasus is now on the U.S. Commerce Department's list of cyberwarfare companies to which U.S. suppliers are prohibited from peddling.

As ironic as it seems, there is a thin line between even business-grade commercial cybersecurity tools and cyberweapons. Like a gun, a cybersecurity tool is not "good" or "bad" in itself, though it may be classified as such, depending on how a given operator uses it.

AN EXEMPLAR CASE STUDY

Another good example comes from the Solorigate case. SolarWinds is a widely used network monitoring tool. Though not designed as a cybersecurity tool, it can provide flow that can be used for network security analysis. Hackers designed a malware payload to exploit a vulnerability in a Microsoft security feature and packaged it within a SolarWinds software release. Using permissions granted by the SolarWinds customer ("victim") to run SolarWinds's software, the malware gained access to the victim's Microsoft authentication token signing certificate and forged access tokens that impersonated the victim's users and administrators. As is evident in the timeline in Figure 1, attackers were in

> "Like a gun, a cybersecurity tool is not 'good' or 'bad' in itself, though it may be classified as such, depending on how a given operator uses it."

the SolarWinds network, inconspicuously observing and testing malicious software for over four months before deploying it. It has also been reported that the same Microsoft attack vector in the SolarWinds package had been documented in the past, so with hindsight, it is thought to have been used prior to Solorigate. If so, this makes Solorigate a good example of the evolution of cyberweaponry. In the hands of one attacker, a difficult-to-perform exploit causes concern. In the hands of a nation-state with virtually unlimited technology resources, it is a matter of time before its full potential is unleashed.

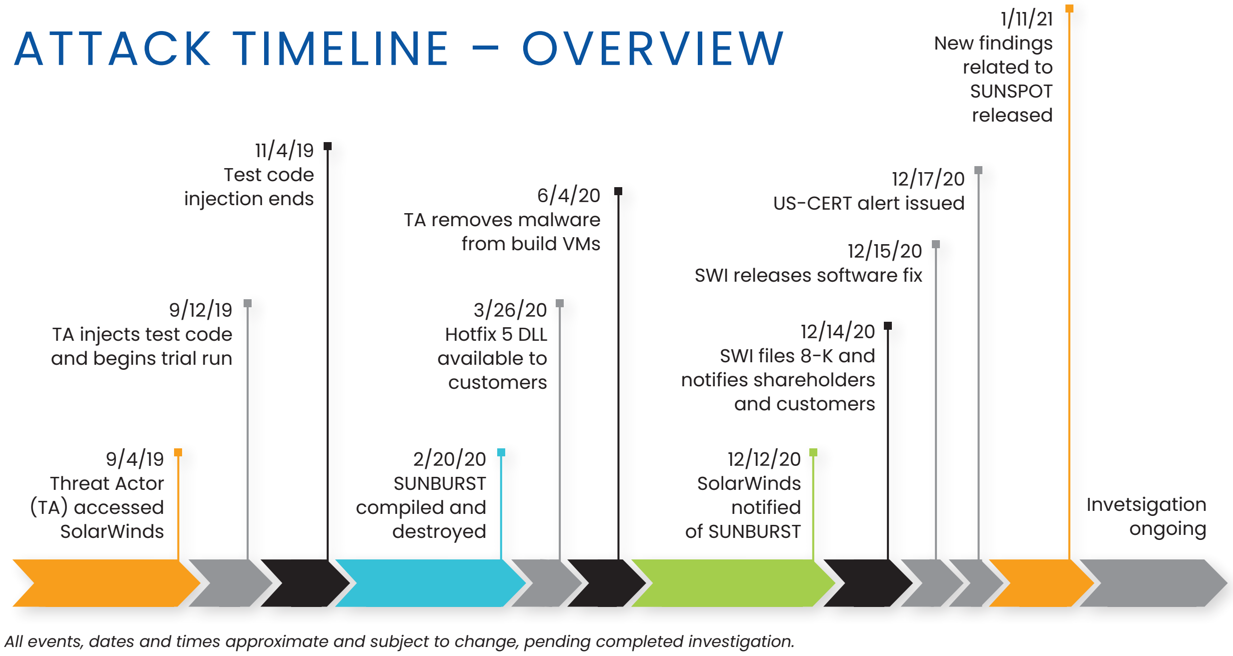

ATTACK TIMELINE – OVERVIEW
9/4/19 Threat Actor (TA) accessed SolarWinds
9/12/19 TA injects test code and begins trial run
11/4/19 Test code injection ends
2/20/20 SUNBURST compiled and destroyed
3/26/20 Hotfix 5 DLL available to customers
6/4/20 TA removes malware from build VMs
12/12/20 SolarWinds notified of SUNBURST
12/14/20 SWI files 8-K and notifies shareholders and customers
12/15/20 SWI releases software fix
12/17/20 US-CERT alert issued
1/11/21 New findings related to SUNSPOT released
Invetsigation ongoing
All events, dates and times approximate and subject to change, pending completed investigation.

Figure 1. Solorigate Hack Timeline

Although it is increasingly obvious that technology products and services can be used as both friend and foe, we have not seen a huge uptake in breach and attack simulation (BAS) on this front. It seems to be left to supplier risk management processes to sound the alarm. While many enterprises are systematically ticking off patterns using targets from the MITRE framework, not many have as systematically created BAS scenarios that assume insider access and threats to their own security tools. So we took a look at the TAG Taxonomy, with the objective of highlighting the most obvious cybersecurity tools that can be turned to foe, and review some abuse cases.

ENDPOINT SECURITY

In the early days of endpoint security tools, the focus was on security configuration change control and anomaly detection. It was assumed that the remedy for any identified threats was to change the security configuration to prevent further recurrence of the same incident, as well as to test and deploy the new configuration via a highly controlled process. Unfortunately, the ubiquity of the Microsoft desktop in combination with the promiscuous behavior of users made it impossible to control the entry of malicious software using operating system security, and more proactive tools began to emerge. The tools had the ability to quarantine software that appeared to overlap in bits and/or behavior consistent with software known to be malicious. Security professionals at the time were (and still are) peppered with requests for legitimate business software to be let out of quarantine. Now we have endpoint security that is empowered not only to quarantine suspect software but to automatically patch and reconfigure security features.

But what if the endpoint security tool is a foe? What if a nation-state has spent months analyzing the operation of the tool, including client software, automated download sites and protocols, agent communication protocols, log repositories and console features? Potentially, someone with internal access and this knowledge could identify the access control mechanisms enabling secure operation and introduce configurations and executables that could turn the software from friend to foe.

> "Now that more nation-states are engaged in cyberwar, it is more and more probable that our trust in PKI infrastructure as a friend is overly broad."

NETWORK DISCOVERY

Reconnaissance is a key element of any targeted attack. The easiest method to perform reconnaissance is with a professional asset discovery tool. Searching for the discovery tool in the TAG Taxonomy with its foe potential in mind, I started by scanning the detection categories. When I realized that of course "assets" would be a topic the Enterprise category, I still did not immediately land on it until I found it in the innocuous Enterprise subcategory of "Asset Inventory." Asset Inventory refers to a relatively benign-sounding set of tools and techniques focused on ensuring that the scope of cybersecurity technology coverage is accurate.

As in any audit of assets, technology asset inventory is compiled via inclusion and exclusion tests on an authoritative listing referred to as the "inventory." The listing sometimes contains all technology assets, including data and staff, and sometimes is limited to technology devices. Inclusion tests generally started with procurement and/or other types of onboarding records. That is, once an asset is onboard and before it is decommissioned, it is included in a listing of assets to be secured. Network discovery is the exclusion part of the test. If a device (or user or data) is automatically discovered in the enterprise technology environment that is not in the inventory (e.g., via a cybersecurity tool performing a network, credential or disk scan), the asset listing is assumed to be incorrect, and the discovered item is added to the listing. The next step is either to properly identify and document the asset, or to retire it.

Most enterprises treat such discovery tools as friends, helpful prompts to rope in shadow IT and unexpected contractors. These tools are often operated by junior analysts, and the data they collect does not typically meet business data classification as any level higher than "internal use only." In many cases, the output of the network discovery tool is automatically "integrated" into an inventory repository, such as an enterprise configuration management database (CMDB). For example, a device discovery integration often consists of python or shell scripts that insert device records into the Asset Inventory that are marked as "discovered" rather than "procured," thus creating to-do lists for technology operations to properly identify and catalog the device.

But what if the discovery tool is a foe? What if a nation-state has spent months analyzing the operation of the tool, as was done in Solorigate, including the tool's scheduling, discovery protocols, data gathering and integration scripts? Potentially, someone with internal access and this knowledge could target the code in the integration scripts with injection techniques similar to those used against web applications calling SQL.

PUBLIC KEY INFRASTRUCTURE

The weaknesses of PKI have been obvious since 2011, when the trusted certificate authority (CA) DigiNotar was discovered to have signed fake public keys for over 500 websites. The impact of this discovery cascaded from successful man-in-the-middle attacks on these sites to revocation of DigiNotar as a CA by multiple browser publishers, causing unintentional denial-of-service attacks on legitimate sites, as browsers would no longer recognize their legitimacy. The issue was not resolved until DigiNotar was taken over by the Dutch government.

Yet PKI technology has not changed to reduce the risk that a fully trusted CA can knowingly operate for the dark side. In fact, with the increase in adoption of DomainKeys Identified Mail (DKIM), in which email headers are validated using a public cryptographic key in an organization's Domain Name System (DNS) records, reliance on PKI for site communication is even more prevalent. Ironically, secure DNS (DNSSEC) uses cryptographic digital signatures signed with a trusted public key certificate to prevent DNS spoofing and DNS cache poisoning. The history of those DNS attacks dates back to the DigiNotar time frame, and both attack types were attributed to nation-states even in 2011. Now that more nation-states are engaged in cyberwar, it is more and more probable that our trust in PKI infrastructure as a friend is overly broad, and PKI should be scrutinized for foe capabilities that negatively impact business.

CONCLUSION

By design, cybersecurity tools tend to have overly broad access to data and operating system security configuration. Rather than being left off the list for application security testing, they should automatically be bounced to the top of the queue. Their treatment from a cybersecurity assessment perspective should receive the same rigor applied to critical business application cybersecurity risk review.

IS THE GOVERNMENT'S VERSION OF ALL IN THE FAMILY A REALITY SHOW?

DAVID HECHLER

The **Aspen Cyber Summit** focused on the federal government's need to work collaboratively with the private sector in order to protect the nation's critical infrastructure. It was called "Exploring Collective Defense in a Digital World," and the emphasis throughout the two days was most decidedly on "collective." It could have been called "We're All In This Together."

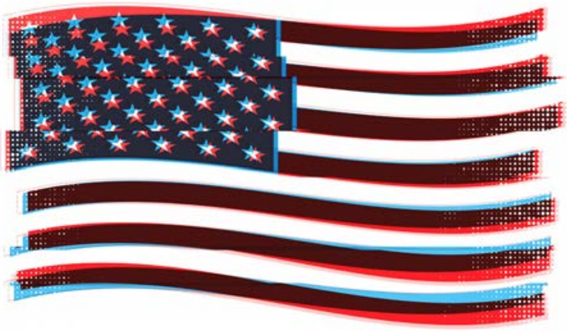
But just a few weeks earlier, Josephine Wolff, an assistant professor of cybersecurity policy at Tuft University's Fletcher School of Law and Diplomacy, wrote an article that suggested government agencies had serious problems working with each other. Specifically, she noted serious tensions between the offensive and defensive sides of the government's house. As I prepared for the conference, I wondered whether any of this would come up.

THE NEW KID ON THE BLOCK

In **"CISA Can't Succeed in the Pentagon's Shadow,"** Wolff argued that the U.S. Department of Homeland Security has never been given enough power to properly defend the nation's critical infrastructure, which is what its Cybersecurity and Infrastructure Security Agency (CISA) was created to do. CISA actually has several important roles, including working with regional officials to help secure elections. But the main focus for this conference was its role in helping to protect U.S. critical infrastructure by working with the companies involved, about 85 percent of which are in civilian hands.

Since its inception in 2018, CISA has been overshadowed by the Department of Defense, Wolff wrote. The National Security Agency and U.S. Cyber Command are the real powers in charge, she said. The Biden administration has expressed a desire to "marshal a whole-of-nation fight to confront digital threats," Wolff noted. But to do so, she continued, "it needs to embolden CISA so that it can begin to compel businesses and critical infrastructure

At a recent conference, government officials seemed intent on showing that they could work effectively not just with the private sector, but also with each other.



operators to take the necessary steps that will actually protect the country's most vital systems and networks."

She suggested that one recent development might be a hopeful sign. In July, Jen Easterly was confirmed as CISA's director. Easterly is a former NSA official herself. She helped launch Cyber Command. So "it's possible to interpret her new position as a sign of just how far the two departments have come in finally being able to work together and how well established and respected the DHS cybersecurity operations finally are," Wolff wrote. It's also possible to view Easterly's selection as a sign that the military has achieved hegemony, she added, pointing out that the top cyber officials in the White House, Chris Inglis and Anne Neuberger, are also former NSA officials.

Easterly was the conference's first speaker. She spent much of her time reviewing her 10 weeks on the job. She had plenty to say about collaborating. The most eye-catching piece was the new group CISA established in August: the **Joint Cyber Defense Collective** (JCDC). The partners include all of the government's heavy hitters: DoD, NSA, Cyber Command, DOJ, FBI, and more. From industry they've lined up Amazon Web Services, AT&T, CrowdStrike, Google Cloud, Microsoft, et. al. No signs of any friction there.

Interestingly, her bookend as the day's last speaker was Rob Joyce. Joyce is the government's fourth leader in the cyber realm, and he has not only spent much of his career as an NSA official, he's the only one of the four who is there now. He heads its **Cybersecurity Directorate**. Earlier in his career there he led the offense. His new job mostly involves intelligence.

Between Easterly's **presentation** and Joyce's, lots of examples of partnerships were discussed. (I wrote about some of them here.) But there was also talk about the need for an offensive response to the onslaught of attacks. "We can't only play defense," said Kevin Mandia, CEO of FireEye. He wasn't alone in urging more from the government. One example that drew praise from many quarters was the clawing back of at least some of the ransom that Colonial Pipeline paid to regain control of its data. In this instance, the FBI rather than Cyber Command was credited for the accomplishment.

THE NSA TAKES THE STAGE

When Joyce finally took the stage (yes, most of the panelists were really there), he was joined by journalist and author Garrett Graff, who directs cyber initiatives for Aspen Digital. Graff's first question was about a warning the NSA had just released concerning VPN vulnerabilities. "This was a **document**," Joyce responded, "that talked about what you should have in consideration for securing your VPN. And it was done jointly with CISA. They are our deep partner these days. There's almost nothing we put out that we don't do jointly with CISA—often CISA, NSA, and FBI together."

There was more along these lines. For instance, Joyce said that NSA has stood up its own **Cybersecurity Collaboration Center** to build relationships with private industry. It lacks the scope of CISA's JCDC, but it is a notable development for an agency with a go-it-alone ethos. But Joyce was not there to discuss his agency's conversion to collaboration. The topic of the session was "The Next Generation of Threats," and Graff skillfully probed for answers.

During the first year of the Trump administration, Joyce served as cybersecurity coordinator on the National Security Council for about a year before the position was eliminated. Graff asked him what's changed four years later. "The idea that cyber crime has become a national security issue," Joyce replied. "That to me is a dramatic change. And you see the government utilizing all elements of our power to include the foreign intelligence team, the offensive cyber team in the efforts to work against ransomware."

So what are the country's top threats? Joyce listed ransomware as No. 1. No. 2 is disinformation, he said, which is both "a cybersecurity problem and a malign influence problem." After that comes the nation-state threat. "Russia, China, Iran, North Korea: they roll off so easy," he said, "because those are the big ones we always see doing very obnoxious things in cyberspace." And the last is critical infrastructure. It's an area that "we've always known and worried about," but in the last five years it's grown urgent to lock down "for our national security."

Rob Joyce heads the NSA's Cybersecurity Directorate.

"You are the author of what is probably the most famous line about nation-state cyber threats," Graff said. "Russia is a hurricane; China is climate change."

It's still true, Joyce said. Russia is a disruptive force, often seeking to tear down adversaries by disseminating misinformation and malign information. And they actively gather intelligence on both governments and critical infrastructure. All make them dangerous, he added.

"Scope and scale, China is off the charts," said Rob Joyce. Its number of cyber actors "dwarfs the rest of the globe combined."

China still looks like climate change to him. "Scope and scale," he said, "China is off the charts." Its number of cyber actors "dwarfs the rest of the globe combined," he observed. "You talked about the difference four or five years ago to today," he said to Graff. "The difference I see is we respected them less. It was always broad, loud and noisy." But what they're finding, he went on, is that based on those numbers, the elite members of that group "really are elite." That makes them a sophisticated adversary.

The required response? Understand, disrupt and find ways to push back, Joyce said. "Defense is really important," he acknowledged. "But you also have to work to disrupt." The strategy is "continuous engagement," he said. "We've got to put sand and friction in their operations so they don't just get free shots on goal."

When people hear terms like "continuous engagement," he went on, "they think offensive cyber. It is," he said, "but I would say that the releases we've done jointly with CISA and FBI about the N-day vulnerabilities that those [adversary] teams like to use, that knocks them back just as much, and is just as important." As is working with the international community to establish "the expectation that these things won't be tolerated," he added.

What about Bitcoin, Graff asked. Is ransomware a cryptocurrency problem as much as a criminal problem? "Certainly without profit there is no ransomware problem," Joyce agreed. And crypto is the mechanism. But he called it both "a benefit and a liability." The transactions can be watched. "They're all very public," he said. "The question is, can you de-anonymize and connect them?" That's the challenge.

The other big challenge is quantum-resistant cryptography. When quantum computing arrives, unless they're prepared with cryptography that can withstand it, security will quickly dissolve. Confidentiality algorithms, encryption algorithms, and authentication protocols will all be vulnerable, Joyce said. Now is the time to plan, he explained. That's their Y2K problem, but "orders of magnitude bigger." Asked how it's coming along, Joyce said "I'm feeling really good." For the classified networks, "we already have the protocols and the encryption technology," he said. And they're working with NIST to select commercial standards. "After you have all those things," he said, "it's the retrofit—it's the get it into everything and build it backwards."

THE BOTTOM LINE

So what are we to make of Wolff's concerns that CISA has been minimized? And if she had a point, were the conference presentations reassuring? To some extent, I think they were.

Even if the conference primed the pump for partnership, it does say something that so many individuals, including speakers from the private sector, spoke about the need for collaboration. Likewise, the decision by CISA and the NSA to create organizations designed to facilitate more effective cooperation between the public and private sectors—and in CISA's case, between government agencies as well—doesn't guarantee these will yield results. But it proves it wasn't just talk.

As for the way the government balances the two sides of its house, it's no secret that the offense in cyberspace has long outstripped the defense. And that's not going to change just because people talk a good game. It's also true that the offense is always going to get more credit (when its activities are made public). But if there was ever going to be a time to recognize that the country needs both sides functioning effectively, this is it.

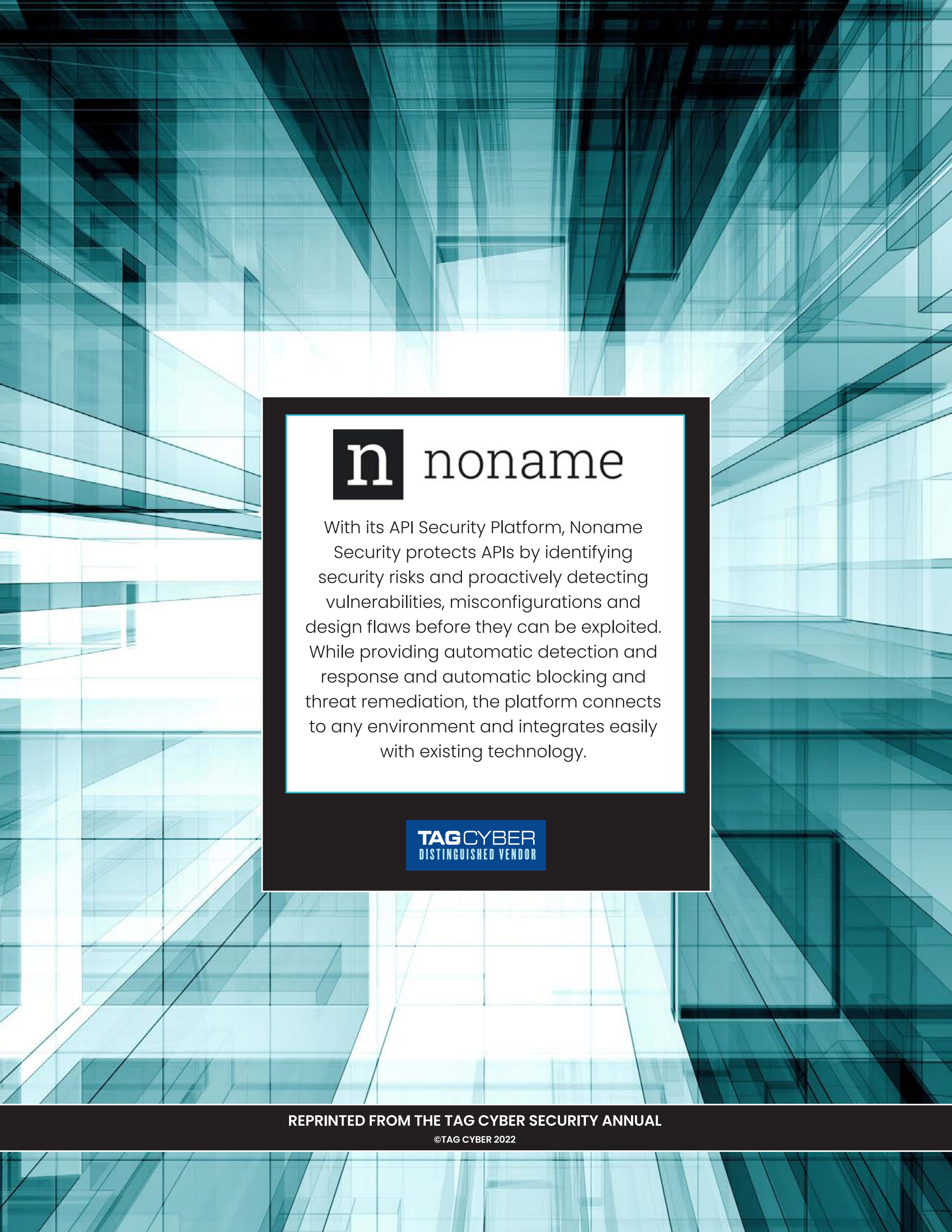
I think it does make a difference that Easterly made a name for herself at the NSA. And she has decades of high-level, relevant government experience. But what may be even more important is that defense suddenly seems top of mind. The country may never have appeared more visibly vulnerable.

The public heard about SolarWinds, and it sounded bad. But it was hard for a lay audience to understand what had happened. And then it only seemed to be about spying. Colonial Pipeline was very different. It was the infrastructure. And there were tangible results. Long lines at gas stations were on the evening news. All of those scattered ransomware attacks suddenly hit home in a big way. And they have not abated.

Where was the government?

At the conference, Rob Joyce talked about getting "left of theft." We need to be able to prevent these attacks, he said. "We really don't want the government, or any institution, to be really good at incident response. We've got to get ahead of that."

It's been a humbling time. The president of the United States had a talk with the president of Russia and told him the attacks had to stop. But they haven't. The talk about cooperation at the Aspen Cyber Summit didn't feel staged to me. It seemed to come from a bit of humility and a sense of necessity.



n noname

With its API Security Platform, Noname Security protects APIs by identifying security risks and proactively detecting vulnerabilities, misconfigurations and design flaws before they can be exploited. While providing automatic detection and response and automatic blocking and threat remediation, the platform connects to any environment and integrates easily with existing technology.

TAG CYBER
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL