Mighty Guides

Sponsored by

JUNIPER NETWORKS | Engineering Simplicity

7 Experts on Security Automation and Analytics

Leveraging Automation and Analytics to Upgrade Your Company's Security Posture

INTRODUCTION: SECURITY AUTOMATION

Here's the situation. Security tools keep getting better. There are more ways to implement policies and controls than ever before, and more ways to see what's going on in your environment. It's easier to identify intrusions quickly. And every day the world becomes a scarier place to store your data.

So what's the answer? If I knew that, I would have retired by now. But, I've got the next best thing—insight from seven experts on how to leverage security automation in ways that can keep you at least one step ahead of the bad guys, for now.

With the generous support of Juniper Networks, we asked seven experts the following question:

What advice, strategies, and best practices can you offer to get the most out of automation and analytics in upgrading a company's security posture?

There's lots of great advice in this eBook, as well as a sober look at the magnitude of the challenge. One thing comes through loud and clear, which is that in spite of what vendors say, security automation is not a silver bullet. But implemented correctly, it can be the best bullet you have. Our experts tell you where most people go wrong and what you can do to make it work for you.

All the best,

David Rogelberg
Publisher, Mighty Guides Inc.

Mighty Guides®

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

FOREWORD

Security operations teams are slogging through a flood of cybersecurity alerts every day. Most organizations receive more than 1,000 malware alerts every week! And that number continues to grow as cyber criminals multiply their attacks. Alarmingly, 75% of these alerts are false positives and most organizations are only staffed with enough resource to follow up on 50% of the alerts. How can you ensure you are acting on the most critical alerts and not just chasing false alarms?

Security automation and analytics have been offered as a silver bullet solution to help over-burdened security operations teams more effectively identify and remediate threats. The majority of security practitioners agree that automation and analytics can strengthen their security posture by improving the ability to separate real threats from false alarms, reducing time to remediation. However, there are also complexities involved with implementing security automation.

In this book, seven cybersecurity experts share their insight on the topic of security automation and analytics. They will share valuable takeaways to help you overcome some of the complexities associated with security automation including their best practices and which tasks to automate for the greatest impact on your security posture.

Regards,

Sherry Ryan
IT Vice President and CISO
Juniper Networks


Power in machine learning and AI.
$2.3 million average in savings.
Free up staff for other tasks.
AUTOMATED SECURITY SAVES TIME AND RESOURCES.
We've engineered a unified cybersecurity platform that streamlines your security operations and speeds time to detection while minimizing vendor sprawl. Read the industry insights
https://easylink.juniper.net/security-industry-insights
JUNIPER NETWORKS
Engineering Simplicity

TABLE OF CONTENTS

BRIAN BOBO

CISO
Sun Country Airlines

With 20 years of experience in technology, logistics, and intelligence, Brian Bobo specializes in risk mitigation, industrial controls, major software integrations, physical security, and IT security. He has proven leadership abilities, providing unique solutions that help teams run more efficiently and support business needs. He holds a BS from the United States Military Academy at West Point and an MBA from the University of Florida.

LinkedIn | Website

When he worked as a security operations center (SOC) manager for a major retailer some years ago, Brian Bobo would see one billion events per day. "Those were raw events," he says, "so 99.9 percent of them were nothing." That may seem like a lot of events, but the managed security-services provider he now uses to filter level 1 and level 2 events sees 245 billion events per day across all its customers. If 99.9 percent of those are insignificant, that means 0.1 percent, or 245 million events per day, could be substantial. Bobo uses this example to illustrate the essential role automation plays in today's security practice. There are not enough people on Earth to rationally choose the 0.1 percent of events that require a closer look, let alone analyze them.

Automation is necessary, but Bobo points out that it can be a double-edged sword if not implemented properly. For instance, when his team configured alerts to create service tickets automatically, one alert might create 50 identical tickets. "Suddenly I'm paying some really highly skilled security expert a lot of money to go in and just close tickets," Bobo says. They implemented additional automation to fix that. "Now we've automated closing multiple tickets, and we're working toward automated quarantine of activity that looks malicious."

He emphasizes the importance of selecting the right tools for your environment. He believes in minimizing the number of vendors you have by picking a strategic one that can give you a holistic view. "Nobody can give you everything, but you can select solutions that talk to each other and give you that single pane of glass," Bobo says. Many organizations make the mistake of chasing the best rated tool for each task, but

> *"You need to correlate information so you can reduce the white noise."*

that's like putting together a basketball team with all the most famous players in history. They would not play well together. "You need to have visibility across all of your security tools so you can correlate information and strip out the noise of all your devices pinging at you," he says.

Bobo notes that no matter how good his security and how great his team, they can never react as quickly as technology to malicious activity. Analytics is the critical piece that looks at trends and figures out what types of attacks you're seeing and where you might be vulnerable. "Automation and analytics are really useful," he says. "But if there's no coordination, they can actually make things worse by giving you too much information. I think of automation as something that takes really good security experts and allows them to focus on what's important, not on closing tickets or chasing false positives."

Bobo looks for two key criteria in any solution. One is its usability by the team. "If you don't have the right people to run it, you're not going to get value out of it." The other important factor is how quickly it responds to threats. "Automation needs to work quickly. I'm not so concerned about how fast it closes duplicate tickets. But automated threat-response time is critical." ■

"I think of automation as something that takes really good security experts and allows them to focus on what's important, not on closing tickets or chasing false positives."

KEY POINTS

1. **No matter how good the security is and how great the team is that manages it, they can never react as quickly as technology to malicious activity.**
2. **One important criterion for any automated solution is whether the security team has the skills and time to tune it. If they can't tune it they won't see the value.**

BRUCE PHILLIPS

SVP & CISO
Williston Financial Group

Bruce Phillips is a highly accomplished senior executive with more than 30 years of success in the financial-services, insurance, title and escrow, real-estate, healthcare, and defense industries. Leveraging extensive experience with specialized risk management, Phillips provides expert assistance to companies in recovering from a breach, regulatory compliance, strategic planning, or processes and procedures. His expertise is in data protection, risk management, cybersecurity, and technology.

LinkedIn | Twitter

One of the key driving forces behind security automation is the speed and automation of cyberattacks themselves. Security automation is the only way to respond quickly enough to stop a previously unknown threat or prevent a fast-moving attack from doing damage. "If you look at incident-response guidelines, they tell you to first identify that you might be under attack, " says Bruce Phillips, who has worked as a security architect and chief information security officer [CISO] in the financial-services industry for many years. "Then you've got to triage it and determine with key stakeholders how to respond. Then you need to close it off. But in today's environment, by the time you get to the triage stage, you're toast."

This has led to the adoption of analytics-based tools that use machine learning to define normal and abnormal network activity. But if a serious incident exposes a gap in a company's security posture, simply purchasing automation tools is often not the answer. "Automation tools do what you tell them to do," Phillips says. "But a tool without a procedure or a process is technically called shelf-ware."

That is why Phillips recommends beginning with the process, and then adopting the tool that fits the process. For example, if you have a serious incident such as a breach, your first step would be to figure out exactly what happened. You might hire an outside firm to do a detailed postmortem and make recommendations. Most likely you'll find weaknesses in your processes. "You need to understand where your gaps are, then risk-rank those gaps, and then develop a process or a program to remediate that gap. If that means getting an automation tool, you need a process first, then find the tool that will automate it," Phillips explains.

> *"Automation tools do what you tell them to do. But a tool without a procedure is technically called shelf-ware."*

This applies to incident response too, and it's usually easiest to begin with simple tasks. For example, you may have a simple process for handling suspicious emails.

Maybe users have an address where they forward suspicious emails. A security analyst scans it, looks at any attachments, does a quick check to see who owns any links in the email and when the links were registered. Based on findings, the analyst gets back to the user with a recommendation. But that process can be totally automated. Automation tools can quickly conduct the analysis and send back appropriate canned responses based on a decision tree.

"Once you have a playbook, you can automate it to an appropriate level," says Phillips. "That usually depends on how much you trust your process and your tools." If you are comfortable automating a response that could shut down switches or operations, that is where you should be. If you are not comfortable doing that, you might set the tools to raise red flags and call everyone's phone so someone can make a fast decision. "You determine the level of response automation," says Phillips, "and you can ratchet it up over time. It all comes back to understanding your capabilities, building your playbooks, and finding a tool that can help you automate. That's the path you have to go take, because without automation, you're an easy target." ■

"It all comes back to understanding your capabilities, building your playbooks, and finding a tool that can help you automate."

KEY POINTS

1. **Begin with a detection and response process, and then adopt the right tool that will help you automate the process.**
2. **You can determine an appropriate level of security automation, but success comes down to understanding your capabilities, building your playbooks, and finding automation tools that fit your process.**

DON WELCH

Chief Information Security Officer
Penn State University

Don Welch is the CISO for Penn State, and was previously CISO for the University of Michigan and Michigan Medicine. He was cited as a White House Champion of Change in 2009. Welch served 25 years in the US Army, retiring as a colonel. He earned a BS from West Point, and a PhD in Computer Science from the University of Maryland.

Website | LinkedIn

Don Welch, chief information security officer (CISO) at Penn State University, oversees security in a complex IT environment. "We have 24 campuses and 16 colleges with a total of 84 different IT organizations. We have hotels, residence halls, dining, retail, and healthcare. We even have an airport and a nuclear reactor. We deal with just about every compliance framework," he notes. Welch maintains that securing all of this would not be possible without automation tools.

One aspect of the security practice that makes automation a practical necessity is the difficulty in hiring and retaining qualified security analysts due to a global shortage of this talent. Training someone often sets them up to move on to a higher-paying position. An alternative approach is finding people who don't have a security background but do have the right talent and aptitude, and training them to do security work. Instruction begins by assigning trainees some of the simpler tasks. But Welch points out that these are often functions you can perform with an algorithm.

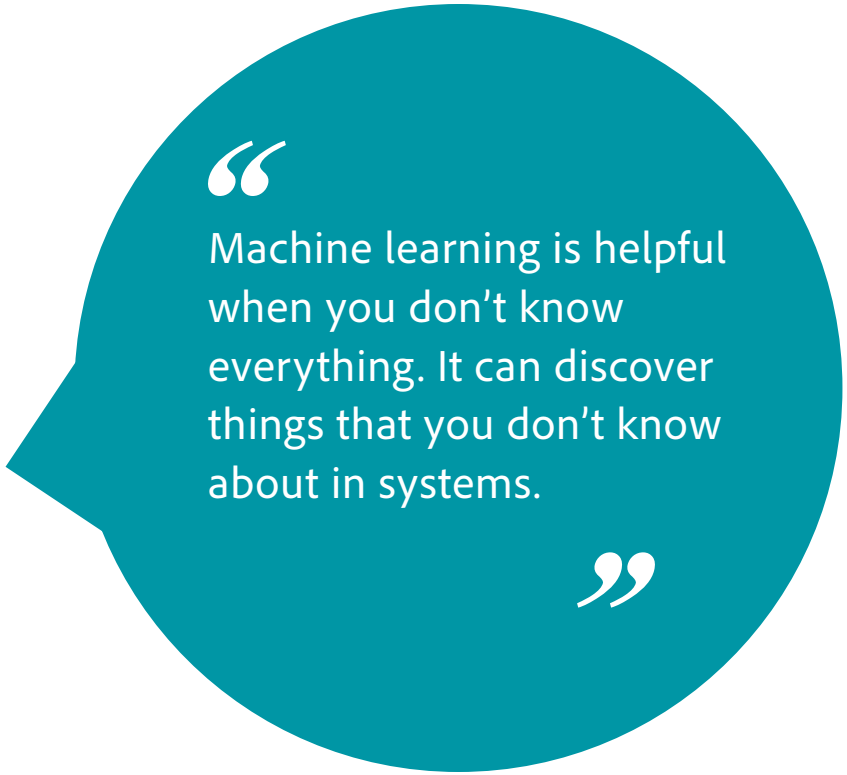
There is also the need to respond quickly, more so than is possible if people are driving the response process. "You've got to stop attacks before damage is done," says Welch. "If you can write an algorithm to respond to an incident, then it needs to be automated. If you're not automating it, then you're wasting resources, because people are slower and more expensive. You need to have security people who are focusing on the more difficult things."

In this kind of environment, tools that have machine-learning capabilities and are able to initiate incident responses automatically are essential. They allow you to take the burden of routine alerts and response off people, and provide more information when an analyst becomes aware of an alert.

> *If you can write an algorithm to respond to an incident, then it needs to be automated.*

They also work as discovery tools in a changing environment. "Machine learning is helpful when you don't know everything. It can discover things that you don't know about in systems. It helps you define what's appropriate behavior and what's not."

Successfully using automation tools in a security practice requires the team to develop new skills. As tools become smarter, it is not as important that security analysts know the nuances of coding, for example. "We want people to master the interfaces of these tools so they can leverage them and use their brains to do the things that they do best," asserts Welch. This sometimes requires helping people develop a different attitude toward the technology. He has seen very skilled analysts saying they can still do it better than the tools, and there are some things they will always be able to do better than the tools. In the end though, people have to learn how to use the tools to make themselves more effective. "The most important thing is the attitude of the people," Welch says. "You can do a lot as a leader to help people handle this change." ■



KEY POINTS

1. **Analysts who have invested a lot of time in developing their skills sometimes resist tools that can do certain things better and faster. They need to recognize they can use these tools to become even more effective as analysts.**

2. **Failing to automate security processes that can be automated is a waste of resources. People are slower and more expensive. They should focus on things they do well.**

DR. REBECCA WYNN

Head of Information Security &
Data Protection Officer
Matrix Medical Network

Dr. Rebecca Wynn has a proven track record of taking companies to the next level of excellence in many sectors, including government, financial services, fintech, healthcare, information technology, legal, semiconductors, and retail. Named 2017 Cybersecurity Professional of the Year at the Cybersecurity Excellence Awards, she is a "big-picture" thinker with nearly 20 years of experience in information security, assurance, and technology.

Linkedin | Twitter | Website | Blog

In today's threat environment, uniform security-management tools that consolidate logs, monitored data, and correlation analysis into a threat-management dashboard have become essential to an effective cybersecurity practice. "That's what we do," says Rebecca Wynn, senior director of information security at Matrix Medical Network. "It's no longer a matter of whether you're going to be breached. It's happening. The question is how quickly you identify and overcome it with as little damage as possible. That's a whole different mindset."

Security automation speeds incident detection and response, and it leverages precious security personnel. However, implementing effective security automation is not as easy as simply buying and installing the right tools. Many factors, ranging from how they are deployed to how they are used, make all the difference between tools that add insight to a security practice and ones that are installed and then forgotten, or worse, provide a false sense of security. Wynn offers this advice that can help companies successfully build automation into their security practices:

- **Before you buy a tool, know what tools and functionality you already have.** "A lot of companies have security tools that are underutilized," Wynn notes. "They are spending security budget on shelf-ware." There are a number of reasons why companies end up in this situation. Sometimes they buy a tool for a specific purpose and fail to take advantage of its other capabilities. Other times poor implementation results in poor tool performance or too many false positives. They never trust the tool, and end up ignoring it. "Before you buy anything, you need to know what you are already paying for," she adds.
- **Understand the difference between infrastructure deployment and security deployment.** Infrastructure deployment is installing the tool and making it functional. Security deployment is training the tool to perform its security functions accurately and reliably. "Security deployment includes determining the traffic you need to analyze, and teaching the tool what noise looks like," Wynn says.

> *The question is how quickly you identify and overcome a breach with as little damage as possible.*

TAKE THE TIME TO TRAIN YOUR TOOLS

"It takes time to do this right. People often fail to budget for that when they buy a security-automation tool."

- **Know who's responsible for security controls and building rule sets.** It's important to know who is implementing rule sets that govern the tool's operation. "I find a lot of times the security tools are installed by infrastructure teams who also put in the rule sets," Wynn explains. She notes that infrastructure teams have different priorities than security teams. Their goal is to get the tool installed as quickly as possible. They will most likely install rules templates based on vendor recommendations and leave it at that. This fails to optimize the tool for the company's unique IT environment.
- **Set and forget doesn't work.** Wynn stresses the importance of doing the extra work of building your own rule sets. It is a necessary step for the tool to deliver the kind of information that security analysts need so they can focus on deeper issues. She also points out that the bad guys are already practicing on default templates. "Anyone can download a free trial. The bad guys are practicing to see how to get around that rule set."
- **Use tools to strengthen, not replace, staff.** Wynn emphasizes the importance of training staff to use the tools. In some cases, by studying a tool's automated capture analysis, analysts can use the tools to sharpen their own analytical skills. "You need to always be training staff up to do this," says Wynn. "My best analysts are not the ones with degrees. They're the ones with that natural inquisitiveness." ■

> "Security deployment includes determining the traffic you need to analyze, and teaching the tool what noise looks like."

KEY POINTS

1 **Security automation speeds incident detection and response, and it leverages precious security personnel. However, implementing effective security automation is not as easy as simply buying and installing the right tools.**

2 **Doing the extra work of building your own rule sets is a necessary step for the tool to deliver the kind of information that security analysts need so they can focus on deeper issues.**

SIJMEN RUWHOF

Freelance IT Security Consultant / Ethical Hacker
Secundity

Sijmen Ruwhof has been an aficionado of anything related to internet security and developing secure software for 20 years. He specializes in hacking, IT security research, and performing advanced penetration testing. In the past 13 years he has executed approximately 650 security assessments. Ruwhof works as a freelance IT security consultant and ethical hacker for major banks, governmental organizations, and high-profile companies in The Netherlands.

Linkedin | Twitter | Website | Blog

From Sijmen Ruwhof's perspective, the complexity of today's IT environments has made an ethical hacker's job easier than ever. "I break into systems for my customers, with permission of course," he says. "I report on all the security vulnerabilities I find and advise customers in how they can protect themselves against hackers."

In his view, there are two essential parts of a cybersecurity strategy. One is monitoring, detection, and remediation. The other is vulnerability testing. This is true whether you are trying to repair a breach that has already occurred or prevent one from occurring in the future. "You need to see what's going on, analyze traffic, and look for discrepancies with normal traffic," Ruwhof explains. "You also need to search for vulnerabilities. Vulnerability testing finds and closes holes. Monitoring detects exploits of holes that have not been found."

He emphasizes that these two go hand in hand. Some tools even allow you to feed security testing results directly into your security-monitoring solution so that you can correlate vulnerabilities to actual monitored traffic and network activity. For instance, if a security alert indicates a file server may be under attack, and this correlates with a vulnerability identified by the testing tool, chaining these two together enables much faster insight and response, and fewer false alarms.

Automation plays an essential role when processing data from multiple tools and sources. It enables systems to identify important data while eliminating redundant information much more quickly than humans. Using a security information and event management (SIEM) product to consolidate and correlate data from various testing and monitoring tools requires analytics, machine learning, and automation, but it takes a lot of effort to properly configure security automation tools properly.

> *Make a road map of what you want to automate. Then see what security products... reduce time to process these.*

AUTOMATION TOOLS NEED TO BE TUNED TO RISK SCENARIOS

"You have to tune them," Ruwhof says. "Otherwise you'll get unusable results. If a tool generates an alert, the security operator should trust that the alert is really important. If the tool always generates alarms, then nobody will listen to it anymore."

To be successful, Ruwhof advises first investigating risky scenarios specific to the company, and then building detection rules around those scenarios. "Make a road map of what you want to automate," he says. "What are the risks, what are the labor-intensive tasks? Then see what security products that the organization uses can reduce time to process these."

Tuning the tools is not a set-and-forget proposition. For the outputs to be most valuable, they must be maintained. "It's really important that you keep tuning the tools because things in the company change, networks change, and attackers change their methodology," Ruwholf says. "You have to maintain it." He adds that automation will never eliminate the need for human analysts. "There are always things that need manual verification," he notes. "These tools are only as strong as the logic put into them." ■

KEY POINTS

1 **Automation plays an essential role when processing data from multiple tools and sources. It enables systems to identify important data while eliminating redundant information much more quickly than humans.**

2 **To be successful with security-automation tools, you must first investigate risky scenarios specific to the company, and then build detection rules around those scenarios.**

CORRELATING SECURITY DATA FROM MULTIPLE SOURCES REQUIRES DEEP LEARNING TOOLS

SLIM TRABELSI

Senior Security Architect
SAP

As security architect at SAP, Slim Trabelsi designs and develops innovative cybersecurity solutions for the company and its customers, focusing on threat intelligence and big data analysis. He is also a security expert within the European Commission. Trabelsi drew on his strong background in privacy and data protection to design privacy solutions for the SAP Cloud Platform.

Linkedin | Twitter

One of the main challenges facing security teams is processing large amounts of data to identify serious threats and take timely action. Slim Trabelsi, senior security architect at SAP, explains that to detect and prevent an attack before it happens, most cybersecurity teams use threat intelligence platforms to collect and display data from multiple sources. "We try to monitor everything," he says. "We acquire data from many, many sources, both internal and external."

Internal data sources include the corporate network, firewalls, the authentication and identity management system, and the entire infrastructure. "We monitor it and receive alerts about unusual behavior," says Trabelsi. External data sources include data feeds from big security companies, tools that constantly monitor social media and the dark web for certain kinds of information, and shared threat attack data from other large companies with whom they have collaboration agreements. "Every single external feed is non-structured data, and much of it is redundant," Trabelsi explains. "For example, one source might give me an IP address that is blacklisted, but I don't know why. Then I learn from another source this is used for spamming. I might learn from another source that this IP address is a customer IP address."

Monitoring and analyzing all this data from both internal and external sources is the only way to get a complete picture of potential threats. For instance, sophisticated attacks are often automated and involve multiple coordinated attack vectors such as social engineering, malware, and denial of service. "To detect complex attacks like this, you need to correlate all the threat intelligence to get a complete picture," says Trabelsi. "If we have only a few sources and we look at them one by one, we won't get the big picture and then we will miss the attack."

The real challenge is how to make sense of huge amounts of data when much of it is redundant. That data must be processed in real time, classified, filtered, structured, and prepared so that it can be properly

> *We try to monitor everything. We acquire data from many, many sources, both internal and external.*

consumed by the threat intelligence platform. "In the end, the threat intelligence platform needs clean data to give the alert on time and with all the information related to the alert. The only way to do this is to apply deep machine learning to that data," says Trabelsi.

Even with a very large team of security analysts, it's impossible to process all this data, yet many companies are reluctant to adopt the levels of machine learning and automation they really need. One reason is they simply don't trust the tools. As an example, Trabelsi cites one company that was bogged down looking at all its security incident tickets. They complained they were spending too much time looking at every ticket, and there were too many tickets containing false positives. "I told them we could use machine learning and teach the machine to identify false positives. We could use relative information and message structures to prioritize tickets. But they didn't want to do that because they were afraid they would miss something." Trabelsi pointed out that by looking at all the tickets and not giving enough attention to high-priority items, they already were missing things.

Another barrier to adoption is the fear that machine learning and security automation will replace staff. But Trabelsi believes this is a mistake. "Machine learning is not replacing the human," he says. "It allows them to stop looking at redundant information and spend more time on the important things." ■

> "To detect complex attacks, you need to correlate all the threat intelligence to get a complete picture."

KEY POINTS

1. **The real challenge is how to make sense of huge amounts of threat intelligence data when much of it is redundant. The only way to do this is to apply deep machine learning to that data.**
2. **Even with many security analysts, it's impossible to process all the data, yet many companies are reluctant to adopt the levels of machine learning and automation they really need. One reason is they don't trust the tools.**

STEVE STONEBRAKER

Principal Security Architect
Guaranteed Rate

With 10 years of information-security experience, Steve Stonebraker believes basic IT hygiene, next-generation technology, and a mature cyber program are needed to protect organizations effectively. He specializes in securing networks, applications, and systems in public and private clouds. Previously, he managed DevOps, systems-engineering, and performance-engineering teams. He holds an MS in Computer Information Network Security from DePaul University and is a Red Hat Certified System Administrator.

Linkedin | Twitter | Website | Blog

Maintaining security depends on three things: being able to see and collect activity data, being able to interpret the significance of that data, and being able to act on the data. Because of the complexity of today's IT environments and the need to respond quickly to threats, automation plays an essential role in each of these areas. "You should be automating everywhere you can," says Steve Stonebraker, principal security architect at a financial-services company. "But you can't just start automating out of the gate."

Stonebraker believes automation begins with knowing everything in your environment. "You have to establish a configuration management database (CMDB) that stores information about every device you own, whether it's a server, firewall, or switch," he says.

The CMDB contains configuration information and dependencies of all assets in an IT environment at any point in time. Building a CMDB manually would be an arduous task, especially in a complex environment. Fortunately there are many tools that continuously discover, track, and map dependencies of IT assets. The CMDB becomes an important tool in monitoring configuration changes in relation to incident management. As environments become more cloud-based and businesses use infrastructure-as-code to build out their IT environments, traditional CMDB information becomes part of an infrastructure template used to deploy assets quickly. Whether it's a CMDB or a template, the key point for security is knowing what you have, and being able to monitor and log all activity related to those IT assets.

Once you have the visibility and activity logging, you need to be able to interpret it. "All that log data needs to go to a security information and event management system [SIEM] where it can be analyzed and interpreted to generate alerts," says Stonebraker.

> *"You should be automating everywhere you can, but you can't just start automating out of the gate."*

SECURITY AUTOMATION BEGINS WITH VISIBILITY

"That's your first layer. It provides situational awareness of what's going on in the environment, and it can trigger alarms, but it doesn't tell you exactly what's happening." That requires further analysis of incidents that look potentially malicious, such as unusual logins and net flow analytics that show anomalous data transfers. More advanced tools can identify and track unusual activity and provide information about exactly what was happening in the network at the time the activity began. This helps analysts more quickly decide how to respond.

Taking action is the ultimate goal, and this, too, is becoming automated. "It really depends on what you want to do," says Stonebraker. "You can set up things like automatically locking accounts or forcing CAPTCHA if there are too many failed logins. You can also use automation and analytics to make decisions as to whether or not to start quarantining and blocking traffic."

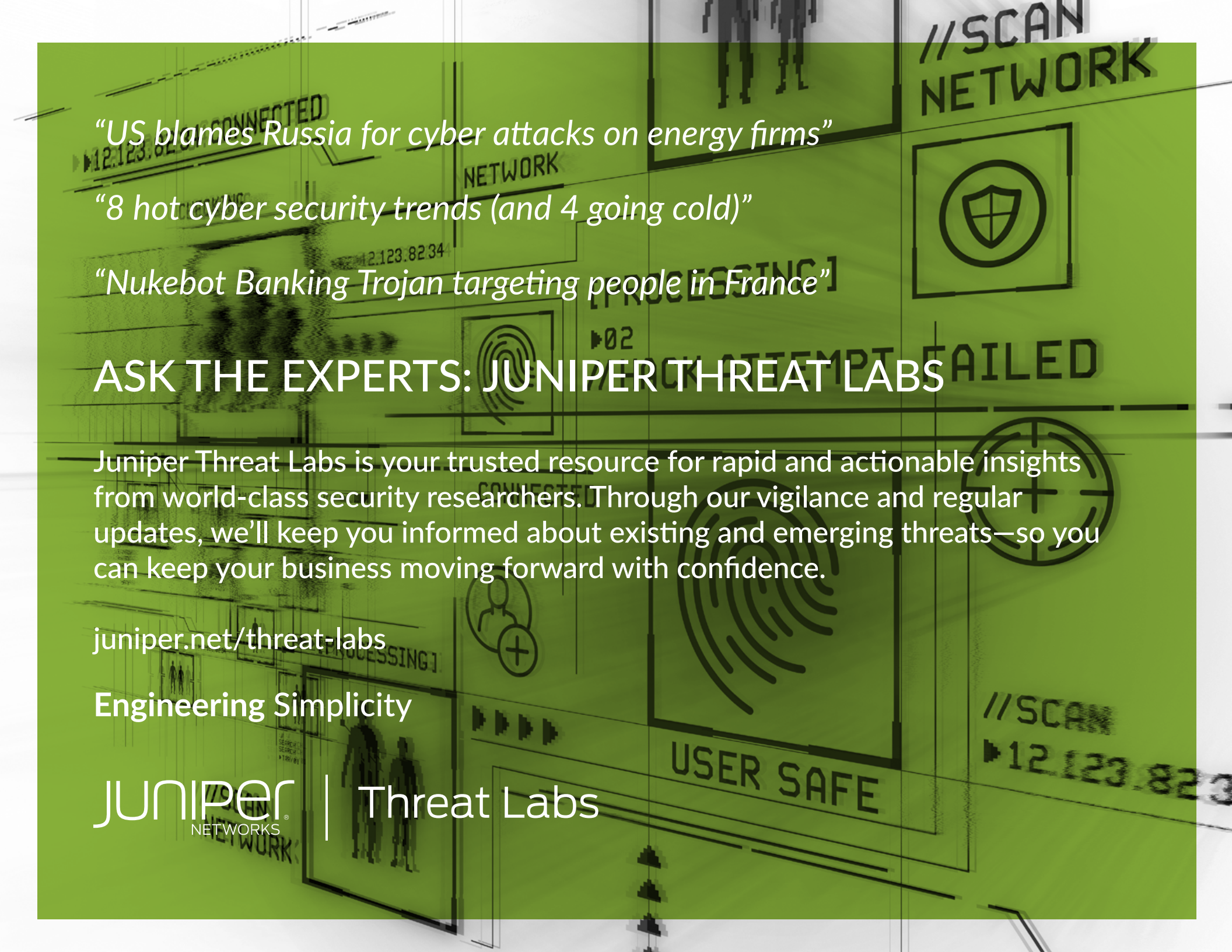
Stonebraker believes that to automate security successfully, you must know what assets are in the environment and have the tools to track those assets. You also have to be prepared to invest in the tools and skill sets needed to run them. Finally, he says, doing it right takes time. ■

"You can use automation and analytics to make decisions as to whether or not to start quarantining and blocking traffic."

KEY POINTS

1 **The key point for security is knowing what you have, and being able to monitor and log all activity related to those IT assets.**

2 **More advanced tools can identify and track unusual activity and provide information about exactly what was happening in the network at the time the activity began. Taking action is the ultimate goal, and this, too, is becoming automated.**



“US blames Russia for cyber attacks on energy firms”

“8 hot cyber security trends (and 4 going cold)”

“Nukebot Banking Trojan targeting people in France”

ASK THE EXPERTS: JUNIPER THREAT LABS

Juniper Threat Labs is your trusted resource for rapid and actionable insights from world-class security researchers. Through our vigilance and regular updates, we’ll keep you informed about existing and emerging threats—so you can keep your business moving forward with confidence.

juniper.net/threat-labs

Engineering Simplicity

JUNIPER NETWORKS | Threat Labs