Mighty Guides®

Sponsored by

Trustwave®

7 Experts on Advanced Threat Detection

Expert advice on how to detect and respond to threats faster and more effectively

As the focus of cybersecurity shifts toward early threat detection and response, many organizations wrestle with how best to improve their capabilities in the face of increasingly complex

IT environments, growing attack surfaces and a daunting threat landscape.

Security strategists have many decisions to make. They must decide how to prioritize the assets they protect, and how to allocate their limited detection and response resources. At a time when machine learning and automation are playing an increasingly important role in detection and response, how do companies decide what should be automated and what is best left in the hands of humans?

To answer some of these questions, and with generous support from Trustwave, we asked seven security experts the following question:

What advice can you give that would help a business detect and respond to threats faster and more effectively?

As you might expect, answers varied based on the types and sizes of organizations represented by our experts. One interesting theme that comes out in these essays is that it's not just about the tools. For instance, triggering a rapid response does you little good if you don't have a detailed response plan in place.

I trust you will find that these essays provide useful and interesting insights from the trenches of a fast-moving, every-changing cybersecurity battle.

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.

© 2018 Mighty Guides, Inc. I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622 I www.mightyguides.com

FOREWORD: ADVANCED THREAT DETECTION AND RESPONSE

The security professionals I speak with regularly know they need to move from basic threat prevention to being able to detect and respond to advanced threats, what I like to call being adaptive in your security approach. Cybercrime is a remarkably lucrative business. Hackers are continuing to evolve, adapt, and innovate. While threat prevention is still critical, we need to recognize the likelihood of being breached and prepare our response.

The pressure on security professionals when a breach is discovered is intense. It might start in the middle of the night with a phone call about your company's data being for sale on the dark web or finding out from the media that you have been breached when you check your twitter feed in the morning. What follows can be chaotic – lack of visibility, misinformation, miscommunication. Preparing for a chaotic situation though can take the chaos out of the situation. It'll still be stressful but following a playbook you've practiced dozens of times is way easier than figuring things out on the fly.

We believe it is possible to detect and respond to threats faster and more effectively. We created this Mighty Guide so that industry leaders can share examples of how their organizations are combining the right people, advanced process and the best technologies to build security programs ready to deal with today's advanced threats.

Regards,
Chris Schueler
Senior Vice President of
Managed Security Services
Trustwave

Trustwave®

Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data, and reduce security risk. Offering a comprehensive portfolio of managed security services, security testing, consulting, technology solutions and cybersecurity education, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers
in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.

TABLE OF CONTENTS

FIRST YOU MUST UNDERSTAND YOUR THREAT LANDSCAPE

DANIEL SCHATZ

CISO
Perform Group

Daniel Schatz is CISO at Perform Group's London office. Prior to this he led the global Threat and Vulnerability Management program for Thomson Reuters. He is a chartered security professional (CSyP) and a member of the International Systems Security Association (ISSA-UK), and he holds several qualifications including CISSP, CISM, CCSK, CVSE, MCITP-EA, ISO 27001 LA/LI, and MS Information Security and Computer Forensics.

Twitter I LinkedIn

Daniel Schatz, chief information security officer (CISO) at Perform Group, advises that improving threat detection and response begins with a thorough understanding of your threat landscape. Only then will you be able to make the right decisions about technologies and resources needed to strengthen detection and response capabilities in ways that best serve the business.

"Knowing your business profile is crucial to understanding threats that are actually of relevance to your business," Schatz explains. "As a sports media company, we may not worry so much about nation states compromising our networks and stealing our sports data. But that changes if you are a defense contractor or critical national-infrastructure provider. Assuming that nation states are not necessarily your main concern, you no longer have to look at the top level of the threat capabilities out there. So we may be more worried about opportunistic attacks by cybercriminals, ransomware, cryptocurrency miners, maybe hacktivists and disgruntled customers. Business profile dictates how you need to shape your threat management and advanced threat detection."

Even with an understanding of your threat landscape, you still need to make decisions about allocating money and resources. Not all assets require equal protection, and nobody has unlimited security resources. "Prioritizing security practices is dictated by the business goals as well as the business environment," says Schatz. "As a security expert, my job is to ensure that we do the right thing in terms of information security. I know how to provide good security hygiene across the board, »

> *Knowing your business profile is crucial to understanding threats that are actually of relevance to your business.*

but the company has critical assets that require more protection. Those critical assets are not identified by me. They are identified by the business." Schatz emphasizes that it's up to the business partners and senior leadership to decide what is most important for the company in terms of the value that they produce for their customers, for their partners, and also as it relates to the regulatory framework that governs IT operations.

Those priorities are typically based on business risk. "The business leaders understand market and financial risks. We help them understand our cyber risk," says Schatz. And that becomes the basis for directing threat detection and response efforts. In Schatz's case, this approach has led to decisions about applying some machine-learning-based tools as part of their security information and event management (SIEM) solution particularly around log inspection, and some endpoint tools with advanced capabilities. But it's a work in progress. "We certainly look at advanced technologies and we're deploying some things on a proof-of-concept basis," notes Schatz. ■

> "Prioritizing security practices is dictated by the business goals as well as the business environment."

KEY POINTS

1 Understanding your threat landscape enables you to make the right decisions about technologies and resources needed to strengthen detection and response capabilities in ways that best serve the business.

2 The CISO's job is to deliver good security hygiene across the business. Most businesses have critical assets that require more protection. Those critical assets are not identified by the security team. They are identified by the business.

YOU NEED TO BUILD A RESPONSE COMPETENCY BEYOND TECHNOLOGY

DAVE RUEDGER

Chief Information
Security Officer
RMS

Dave Ruedger is an established director of cybersecurity and IT operations with demonstrated success building, deploying, and managing secure IT operations across heterogeneous computing environments. He is a self-directed individual with a proven track record of managing IT infrastructure, operations, business applications, product development, and support, and a leader who motivates individuals to succeed while promoting a collaborative team environment.

LinkedIn

For many organizations, responding quickly and comprehensively to a serious incident is difficult. Often companies are not prepared for the kind of zero-day event that catches them by surprise and makes headlines. Dave Ruedger, chief information security officer (CISO) at RMS, believes that effective detection and response capabilities come not only from having essential technology, but also through building special teams and response playbooks. Clearly, monitoring for threats anywhere in our network is an essential piece of the security puzzle, but you also have to have a team approach that looks beyond the security tools. “Incident response is tricky, because you’re covering a lot of different areas,” Ruedger notes. “In addition to your standard security-monitoring metrics, you’ve got application security and internal threats. You can’t depend on tools alone. You have to build a team environment.”

Ruedger recommends building a red-blue team environment that continuously looks at the technologies you have, like your security information and event management (SIEM), and focuses on behavior patterns. They develop behavioral baselines for different kinds of activities, and then playbooks of how to respond when they detect variances in the normal patterns. “For example, we might go into a service account and start doing activity that you wouldn’t normally see users do and then see if we can detect that,” he explains. “If we do detect it, then we baseline exactly how well we respond, to see if we are managing to our playbooks, who are we notifying, how quickly, and how we respond to that overall threat.” Ruedger emphasizes the importance of taking the right actions when an alert is triggered. “I think that’s where many organizations fall down,” he says. »

> *Incident response is tricky, because you’re covering a lot of different areas. You can’t really depend on technology alone. You have to build a team environment.*

He recognizes the role of next-generation tools in improving detection and response. "I think a lot of the next-gen technology is making it easier," he says. "Having artificial intelligence for example to baseline behavior to detect anomalies is really good." But he also points out that it takes a long time to tune those technologies to your environment. In many cases you may spend as much time tuning the tool as you would creating custom rules that define anomalous behavior.

Ruedger highlights the need to build team cohesion around security within the company. "We've created a gamification culture within the company," he says. "On a regular basis we offer an internal, capture-the-flag-type hackathon. We pit individual groups against each other that are working on a release for a product. By forcing them to get outside their core competency and view things from the hacker perspective, it helps to raise security awareness of things they should be thinking about as they develop." But it's more than just a fun way to find vulnerabilities. "That healthy competition creates better security," Ruedger says, "but it also gets people together to collaborate. It kills two birds with one stone." ■

> "We baseline exactly how well we respond, to see if we are managing to our play books, who are we notifying, and how quickly."

KEY POINTS

1 Build a red-blue team environment that continuously looks at the technology you have, such as your SIEM, and focuses on behavior patterns.

2 Building team cohesion around security within the company is an effective way of improving detection and response. One way to do that is with an internal hackathon competition between technology teams.

DAVID BILLETER

Chief Information Security Officer
CA Technologies

David Billeter is chief information security officer for CA Technologies, where he is responsible for leading CA's global and diverse information security and IT risk strategy. Previously he led information security for Staples and the InterContinental Hotels Group. Outside of the office, David is an active member in the cyber security industry in the Boston area.

Website I Blog I LinkedIn

Automation is an essential part of more effective detection and response, but David Billeter, chief information security officer (CISO) of CA Technologies, maintains that when strengthening detection and response, the best place to start is not with technology. "One thing that we see security teams finding they can only go so far with their automation," he explains. "Often they focus on automating the front end. While that's all well and good, you really need to look at the end-to-end processes. If you're just focused on the front-end processes, often what you're doing is creating tickets really fast. But tickets don't fix the system."

Billeter believes that it's important to begin at the end of the process, the aftermath of an incident. How are you going to deal with state attorney-general offices? How are you going to deal with law enforcement? How are you going to deal with press requests? What kind of information are you going to put up on websites for customers? Who are you going to have at the table when you're responding to these things? What processes are in place so that you can actually respond to the attacks and stop them or limit their effect? Can you wipe and rebuild a system? Are you ready to do that, and who's going to make that call? "You have to be very clear ahead of time, because the time to be figuring these things out is not in the middle of a crisis," he says. "It's not just a tabletop exercise. You really have to think through all the possibilities."

Once you refine your response and recovery processes, then you start focusing on improving capabilities earlier in the detection and prevention process, because it's these functions that trigger proper responses. To successfully automate the detection and response process, begin with parts »

> *One thing that we see a lot of with automation is security teams finding they can only go so far with their automation.*

of the process. The individual pieces working successfully become building blocks for end-to-end automation. "I like to automate different kinds of functions and then use those as building blocks toward automating front-end activities," says Billeter. "As long as you have the back-end activities ready to go, they become the tools that you use to build the automation that goes end-to-end."

He believes in managing detection and response holistically, and not getting distracted by technology decisions before back-end processes are worked out. Technology decisions should come later. He also emphasizes the importance of considering business culture as you work out these process details. For example, some companies have a low risk tolerance - a breach would be very bad for their business. Other companies have a higher risk tolerance. It's not that anyone wants to be breached, but not every company has the same approach to risk or where they want to focus their resources. "You'd be surprised," Billeter says. "Some companies care a lot about breaches, while others don't care as much, and there may be very good reasons for that. Too often we see security teams creating one-size-fits-all playbooks that include things that are not really relevant." ■

> "I like to automate different kinds of functions and then use those as building blocks."

KEY POINTS

1 Begin at the end of the process, the aftermath of an incident. Once you refine your response and recovery processes, then you start moving your capabilities forward into detection and prevention, because it's these functions that trigger proper responses.

2 It's important to manage detection and response holistically, and not get distracted by technology decisions before back-end processes are worked out. Technology decisions should come later.

YOU NEED TO CONSIDER SECURITY PROCESSES AND TECHNICAL CONTROLS

DEEPAK PALAKUNNATH KUNNENKERI

Information Security & Audit Manager (RISO)
Fuji Xerox Asia PAcific Pte Ltd.

Deepak Palakunnath Kunnenkeri is an information-security evangelist with more than 15 years of expertise in cybersecurity, IT audits, regulatory compliance, and cloud and robotic security. He believes staying conversant and combating cyber threats is the key to surviving the digital world. Drawing on his business acumen, he empowers the organization to turn information risk into a corporate advantage and achieve robust digital hygiene.

Twitter I LinkedIn

Being able to respond quickly and effectively to threats depends on several factors. Deepak Palakunnath Kunnenkeri, information security and audit manager for Xerox Asia Pacific, points to three specific areas that contribute to advanced threat detection and response capabilities:

- **Administrative controls.** These include having procedural controls, processes, and response plans in place; having access to the right threat intelligence; and maintaining security awareness among the security team and employees. "You must have an effective threat detection and incident response plan in place," says Palakunnath Kunnenkeri. "This plan should be regularly reviewed and tested. It's also important to focus on employee and security-team awareness." In addition to having a specific response plan and maintaining a culture of security, it's also important for the security team to have access to the latest threat intelligence. Palakunnath Kunnenkeri says, "You need to subscribe to a good source of threat information, like computer emergency response team [CERT] information. In Singapore we have Singapore CERT. In the US there is US CERT. You can also receive the latest threat information from security service providers. It's important to register so you can be sure that as a security organization, you are well up to date on the threats." »

> *You must have an effective threat detection and incident response plan in place that is regularly reviewed and tested.*

YOU NEED TO CONSIDER SECURITY PROCESSES AND TECHNICAL CONTROLS

- **Technical controls.** Technical controls include controls that manage access, authentication, data validation, and other technical security functions. Palakunnath Kunnenkeri recommends making these more proactive functions. The best way to implement proactive controls is to integrate security policies and controls into the DevOps application development process.
- **Detection and response.** Of course, a key element of advanced detection and response is having technologies and automated processes capable of identifying serious threats that trigger alarms. Palakunnath Kunnenkeri notes the necessity of focusing on the most critical kinds of activities. "You need to have a huge focus on privileged activities like administrative activities in critical systems," he says. "You need a well-configured SOC [security operations center] that can monitor critical systems. By focusing on those kinds of activities and threats rather than all data in the environment, you will have a much faster response time." ■

> "You need to have a huge focus on privileged activities like administrative activities in critical systems."

KEY POINTS

1 Effective threat detection and response requires having both administrative controls (such as procedural controls, processes, and response plans) and technical controls (including access control, authentication, data validation, and other technical security functions) in place.

2 A key element of advanced detection and response is having technologies capable of identifying serious threats that trigger alarms. Automation plays an essential role in advanced threat detection and response.

IMPROVING DETECTION AND RESPONSE DEPENDS ON MULTIPLE FACTORS

DILIP PANJWANI

Chief Information Security Officer & IT Controller
Larsen & Toubro Infotech Ltd (LTI)

Dilip Panjwani is a hardcore professional with 18-plus years of experience in IT and IS. He is a seasoned, hands-on manager with a proven record of developing and implementing information technology systems and information security controls based on global best practices. Panjwani is the head CISO, chief data privacy officer, and IT Controller for Larsen & Toubro Infotech Ltd. Previously, he was the director of information security at FIS Global.

Twitter | Website | LinkedIn

To improve threat detection and response in a security practice, Dilip Panjwani, chief information security officer (CISO) and IT controller at Toubro Infotech, emphasizes the importance of considering a number of factors in the overall threat landscape. "The first thing any organization or CISO needs to do is to really understand the stakeholders and attack surfaces that are applicable to the line of businesses. This varies from one organization to another as well as from the industrial vertical perspective," says Panjwani. Doing this involves considering a number of factors, including:

Customers and location. Panjwani says it's important to understand who are the business's customers and where they are located. "For example, are the company's operations in a risky location that is already having a lot of hack attacks or infiltration attacks? You have to factor in threats and risks associated with that region."

- **Risk modeling.** Security teams need to document and score risks, and this needs to include risks associated with partner and vendor channels. "When you have an infrastructure to maintain, you have to understand what kinds of services you engage in the organization," Panjwani explains. "This includes the specific vendors you rely on, and the kinds of services you receive from both material vendors and non-material vendors." Most importantly, you need to know how to engage with these vendors if they are compromised so that you can isolate yourselves from their risk and prevent it from escalating into your organization. »

> *When you have an infrastructure to maintain, you have to understand what kind of services you engage in the organization.*

IMPROVING DETECTION AND RESPONSE DEPENDS ON MULTIPLE FACTORS

- **Recognize the changing nature of threats.** Panjwani notes that threat profiles are not the same now as they were five years ago. Attacks are more automated now with ransomware servers and bots that are constantly attacking. "The detection and response mechanism also has to be automated," he says. "It cannot be that the SOC level one analyst is reviewing each and every event coming down to him. You cannot rely on that one person to be able to detect and start a mitigation and response plan at the same speed that the attacks are coming in. Machine learning is definitely something that we have to leverage in the world today."
- **Apply the right threat intelligence.** The threat-intelligence team is an important part of effective detection and response, but you must be selective in the threat intelligence you use. "You have to rely on intelligence feeds in a thoughtful manner," says Panjwani. "You cannot just rely on open feeds alone. You will need to customize intelligence feeds in a way that is specific to your organization, in areas where you operate, and also in your industry vertical, along with the assets and vendors that you are dealing with."

These are key factors that need to be considered as you build out your advanced threat detection and response strategy. ■

> "You will need to customize intelligence feeds in a way that is specific to your organization."

KEY POINTS

1 You need to consider risks associated with partners and vendors, including how to engage with them if they are compromised so that you can isolate yourselves from their risk and prevent it from escalating into your organization.

2 You cannot rely on one person to detect and start a mitigation and response plan at the same speed as the attacks coming in. Machine-learning tools are essential in today's threat environment.

USE TECHNOLOGIES AND STRATEGIES THAT WORK WITHIN YOUR RESOURCE CONSTRAINTS

JONATHAN LEVINE

Chief Technology Officer,
Chief Information Officer,
Chief Information
Security Officer
Intermedia

As CTO, CIO, and CISO at Intermedia, Jonathan Levine manages and directs 200 matrixed staff members. He has more than 20 years of experience guiding technology operations through financial, operational, and key decision-making by identifying, quantifying, and managing risks and opportunities for organizations and clients. He leads all aspects of solutions delivery for significant global initiatives, from initial conception through delivery.

Threat detection and response has become an arms race between the good guys and the bad guys, where the good guys have to win every time, while the bad guys only have to win once. Jonathan Levine serves as chief technology officer, chief information officer, and chief information security officer (CTO/CIO/CISO) for a mid-sized technology company, and like many in his position, he does not have unlimited resources to fight the never-ending security battle.

On the detection front, he uses two key strategies to look for intrusions:

- **Search for unusual activity patterns:** "We pull in data from all of our production systems, and we look for unusual patterns of behavior," says Levine. One example is administrators logging in on their days off. Another relates to the way they configure servers such that system-administrative activities are supposed to occur on administrative servers. If they see someone jumping from production machine to production machine without using the administrative servers, that's an indicator of compromise. Levine emphasizes the importance of comparing activity across the environment. "I think cross-system event correlation across your infrastructure is one of the best things you can do."
- **Attractive decoys:** We set up honeypot servers," Levine explains. "These honeypots look like file servers, they look like mail servers, they look like database servers, but they're not. And we

> *Cross-system event correlation across your infrastructure is one of the best things you can do.*

> don't expect anybody to connect to them. If somebody does connect to them, it means that it's somebody who is not familiar with our infrastructure." Activity on those servers raises a big red flag, and they have intercepted several attacks using this method.

On the alert and response side of the equation, when they see indicators that they are under attack, they alert level-one system operators who do more investigation. Technologies will only take the detection and investigation so far. People are still needed to determine if an indicator is a real threat or a false positive. "We alert level one system operators, and they're the ones who filter out the issues," says Levine.

Levine has another strategy to minimize his detection and response load. "We try to offload things that aren't core to our business," he says. "If I'm not hosting my own accounting system, for example, then the security of the accounting system is somebody else's problem. Focusing our efforts on things that are core to the business, the money-making things, helps us limit our attack surface." ■

> "Focusing our efforts on things that are core to the business, the money-making activities and infrastructure, helps us limit our attack surface."

KEY POINTS

1 Monitoring for unusual patterns of behavior is essential in being able to detect and analyze threats.

2 Technologies will only take the detection and investigation so far. People are still needed to determine if an indicator is a real threat or a false positive.

AUTOMATION IS KEY TO IMPROVING DETECTION AND RESPONSE

LESTER GODSEY

Chief Information Security Officer
City of Mesa, Arizona

Lester Godsey is the CISO for the City of Mesa, Arizona. With over 24 years of public-sector IT experience, Godsey has presented at the local, state, and national levels on topics ranging from telecommunications to project management to cybersecurity. He has taught technology and project management at the collegiate level. A published author, he holds a BA in Music and an MS in Technology from Arizona State University.

LinkedIn

The key to today's advanced threat detection and response is automation. "You need to automate early detection and response as much as possible, because you're dealing with so much information," says Lester Godsey, chief information security officer (CISO) of the City of Mesa. "Once you've got a sense of the threat, if something rises to a high enough threat level, then you assign it to staff or call up other tools to further determine if it is an actual security incident."

Godsey notes that automated detection and response has played a role in shifting the focus of security strategies in recent years. "The initial focus of endpoint-protection tools was prevention, keeping bad things out. But now the major vendors have shifted toward endpoint detection and response [EDR]." This is happening because the reality in today's world of complex network environments is that things are going to get in. "You have to be able to respond when things actually get into the system," Godsey says.

Automating both detection and response is key. On the detection side, Godsey looks for suspicious behavior patterns. For example, he has automated alerts set to trigger if activity monitoring detects impossible logins. "This has actually happened to us, where somebody in our engineering department logged in and then literally two minutes later they log in from South Africa." Based on that alert, an analyst can check what is behind the abnormal activity. »

> *You need to automate early detection and response as much as possible, because you're dealing with so much information.*

Automating responses beyond just alerting also helps strengthen defenses. "We're planning for automating the process to reset a user's password and force them to change a password," says Godsey. However he advises a cautious approach to response automation. "You need to have a high degree of confidence in the steps you would take before you consider automating. Having that process confidence is the dividing line between what you automate and what you don't automate."

Godsey notes that process confidence is not the only criteria for deciding what responses to automate. Another important factor is the risk associated with taking or not taking the action. For instance, if an automated response disrupts a critical operation, this can pose a different kind of risk. On the other hand, the greater risk may result from a lack of action. Godsey says, "In the instance of resetting users' passwords, there's a high degree of risk in not automating and users failing to take that action. On the other hand, any risk that comes from forcing everyone to change their passwords because of a false positive is pretty minimal."

Godsey also recommends keeping an eye on technology developments, because new capabilities are always becoming available. "The solutions get better to match the increasing threats, with greater focus on machine learning and artificial intelligence," he says. ■

> "You need to have a high degree of confidence in the steps you would take before you consider automating."

KEY POINTS

1 Automating both detection and response is key to strengthening a defensive strategy.

2 When automating threat response, you need to have confidence in the response process you are automating, and you need to weigh the risk of taking immediate action against the risk of not acting

XAVIER MERTENS

SANS ISC, Senior Handler
Xavier Mertens Consulting,
Freelance Security
Consultant & Owner

Twitter | Blog | Website

“

Focus on those things that are the most critical threats to the company. Ask what you need to detect immediately or what would be disastrous to your regular business operations. Create a short list of three to five key threats, and investigate how to detect those threats and how to respond to them in an efficient way.

”

Trustwave Threat Detection & Response Services

24x7 around-the-globe delivery.
Powered by Trustwave SpiderLabs.
Customized for you.

Learn More

Trustwave®