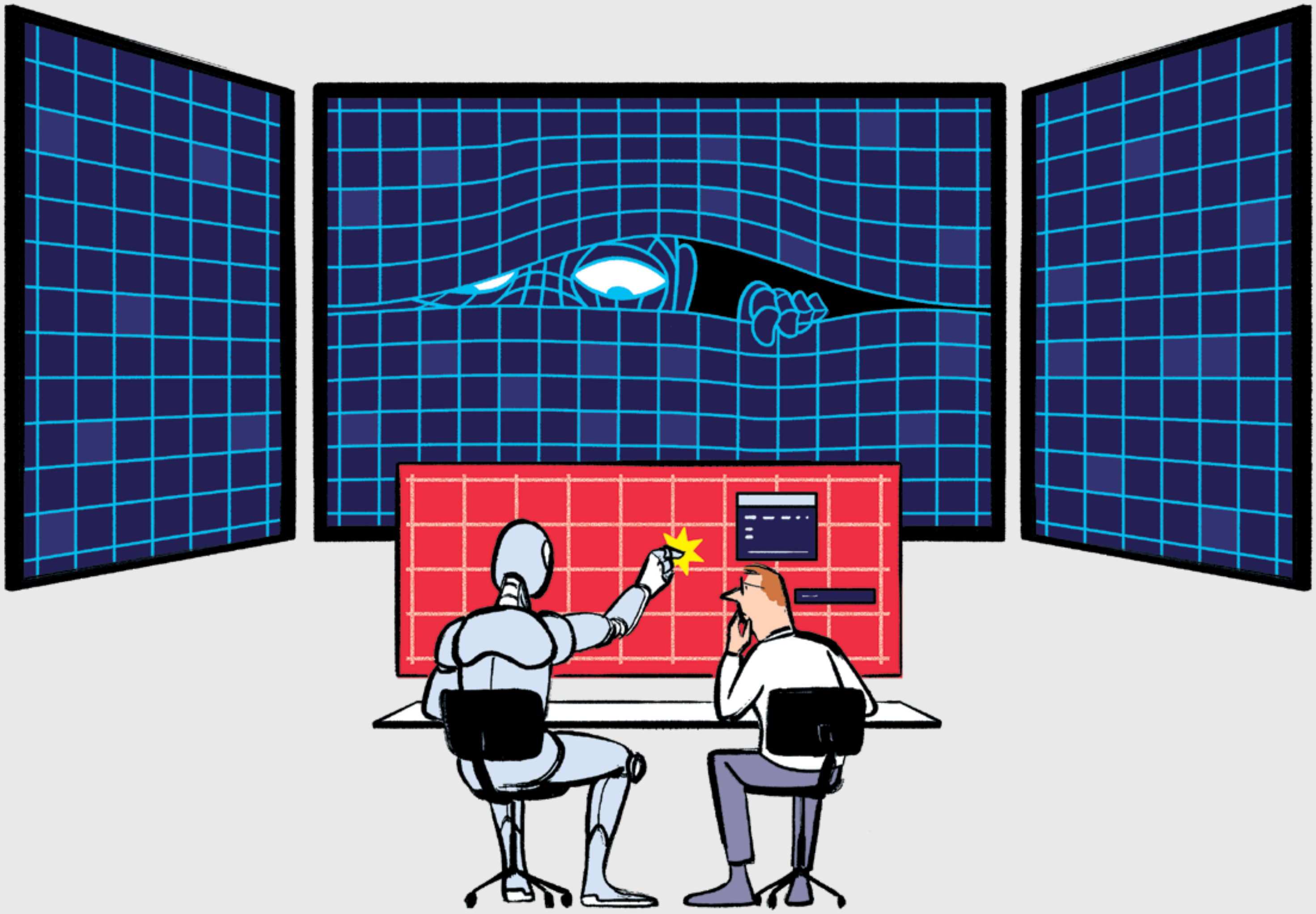
CYBER RESILIENCE

ThinkTank

Sponsored by mimecast



Transforming the SOC

Building tomorrow's security operations, today

Introduction

When you think of a security operations center (SOC), what comes to mind? Is it an organized team of security analysts and engineers who detect, analyze, and respond to incidents, always working in lockstep with business managers to execute on the security strategy? Or, is it a few analysts who spend their days reactively responding to unprioritized security issues with a variety of point tools at their fingertips?

Consider a third option: is it a managed services operation whose business is to successfully run an outsourced SOC with specific metrics and performance outcomes?

When it comes to the human element of team organization, cybersecurity strategy, and the tools and technology underpinning SOCs, the possibilities are endless. And what works for one company may not work for another, hence the many different combinations of how to build and operate a SOC[1]. Some organizations may not even have a SOC, yet they tackle threat detection and response day in and day out.

It's these variations, and the criticality of a SOC to detecting and responding to potential threats, that brought the Cyber Resilience Think Tank (CR Think Tank) together at RSA® Conference in February 2020, to explore the benefits and drawbacks of keeping a SOC in-house versus outsourcing it, and what a successful model might look like. As an independent group of industry influencers dedicated to understanding the cyber resilience challenges facing organizations across the globe, the CR Think Tank aims to provide guidance based on lessons learned and expertise.

[1] How Does Mimecast Help Improve the Performance of Security Operations Centers?

SOC functionality

Rather than setting the security strategy across the business, in-house SOC teams are generally responsible for executing against their companies always-on information security operations and managing the attack surface. Instead, technology and security leadership – CTOs, CSOs, and CISOs – set the tone for their cybersecurity strategy, empowering the SOC to carry it out via systems and cybersecurity tools like endpoint security, firewalls, SIEMs,[2] SOARs,[3] and more. Security operations center staff is made up of security analysts who work together to detect, analyze, respond to, report on, and prevent cybersecurity incidents.[4]

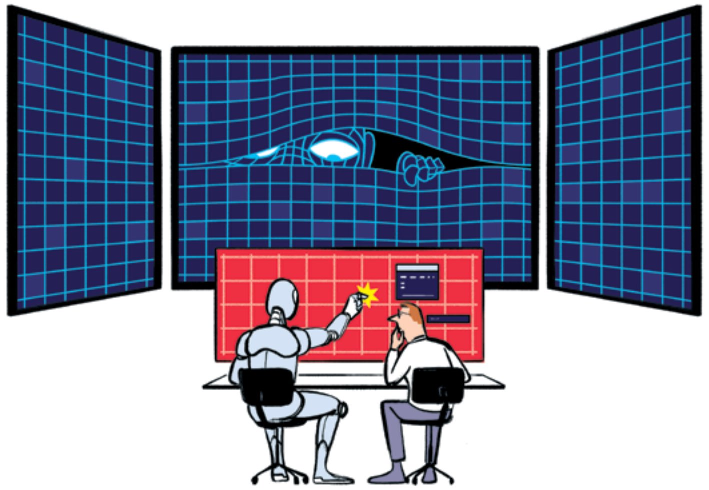
"Data is the lifeblood of the SOC," said Michael Madon, SVP & GM of security awareness and threat intelligence products at Mimecast. "These preventive systems are key data sources for the SOC to meet their success metrics, drive detections and context for integrations, and enable faster threat blocking."

With this line of thought, integration with preventive systems are critical to the efficiency and effectiveness of the SOC.

By the same token, when a company outsources its SOC to a managed services provider, the same capabilities should still apply. Outsourced SOCs should work in close communications with their in-house security counterpart to deliver event reports, share key metrics like dwell time or log status, and provide recommendations for how to improve outcomes.

Here's another important factor to consider: many organizations don't consider themselves to have a SOC, but if that organization has security event monitoring, detection, investigation and alert triage; security incident response management such as malware analysis, forensic analysis and root cause analysis; threat intelligence management; and even general reporting duties that contribute to compliance, the SOC functionality is there. And as long as organizations can collect and centralize data for their internal team or for an external managed services provider, the security function can do its job effectively.

However, regardless of whether a SOC is managed in-house or outsourced to a managed services provider, there are three primary themes that emerge when you weigh the benefits and drawbacks of each approach. Every SOC must have manpower behind it, and with the global cybersecurity skills shortage at an all-time high, the **human element** is of paramount consideration. But humans can't do it all, especially since threat actors and nation-states continue to use the most advanced technology and malware available against companies, so **technology and automation** are investments that leaders must make, no matter the structure of the SOC. Finally, what **processes and efficiencies** can be uncovered when you meld humans and automation? How do you set your team up for success?



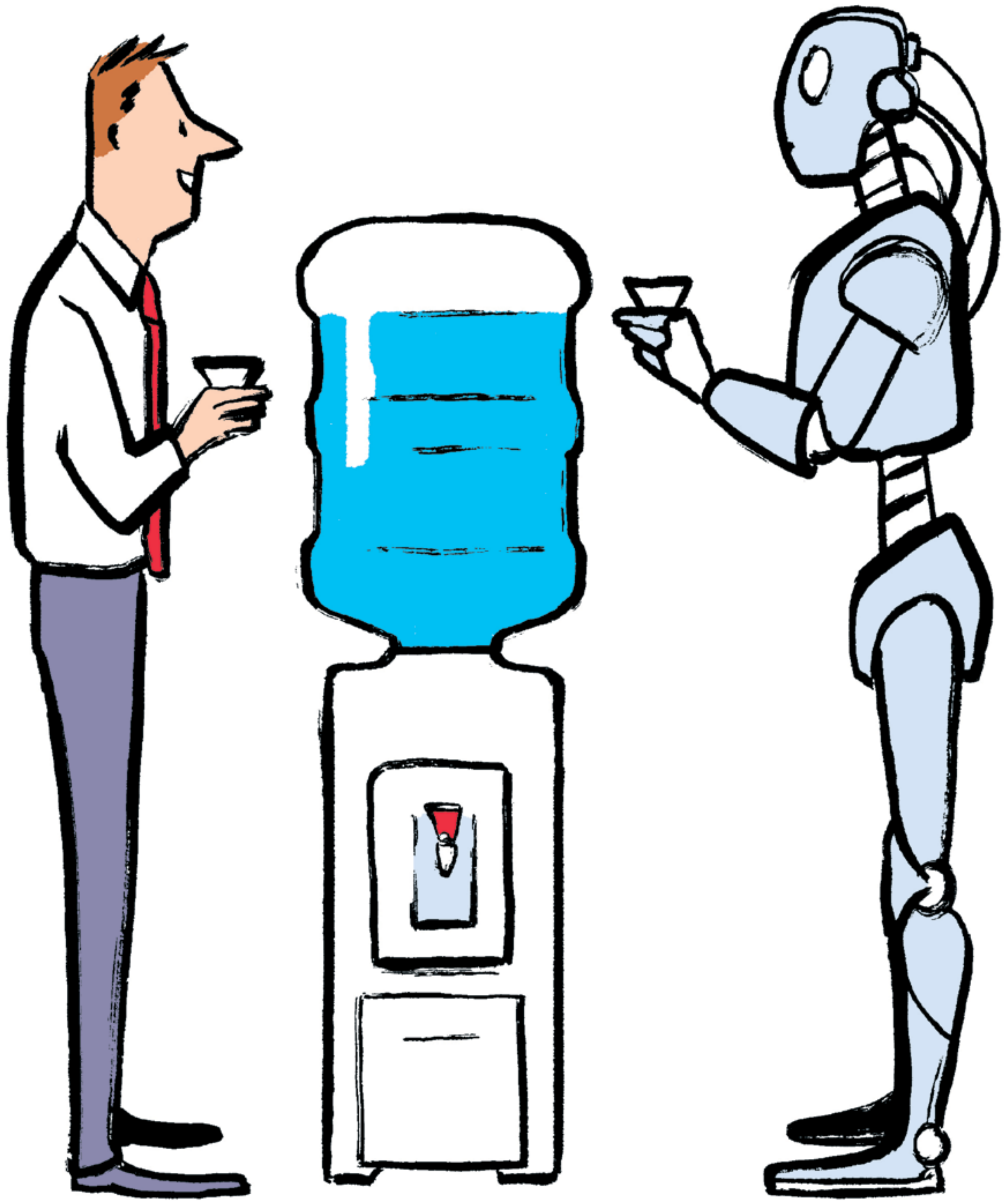
[2] Security information and event management (SIEM), TechTarget

[3] SOAR (Security Orchestration, Automation and Response), TechTarget

[4] What is a Security Operations Center (SOC)? – Digital Guardian

The human element

The skills gap in cybersecurity is well documented; a 2019 study by (ISC)2 showed the cybersecurity workforce gap in the U.S. is approximately 500,000, and by estimating workforce gaps in 11 major economies around the world, it is believed that we have a cybersecurity talent shortage of just over 4 million.[5]



At the rate companies are going, the corresponding growth rate would need to reach 145% to close the gap. Some leaders are taking the opportunity to upskill their workforce to maintain security operations and boost morale. Because of this skills gap, a driving challenge for SOCs, unsurprisingly, is staffing: analysts at every level are already scarce, and analysts in place can be overwhelmed or overworked, resulting in low morale and high attrition.[6]

“The primary driver for us are skills,” said Claus Tepper, head of cybersecurity operations Absa Group. “And I think South Africa is, as everywhere else, fundamentally challenged to getting the right people on board.” To solve for that, Absa jumpstarted an academy to develop and train talent, which has proven to be necessary and successful thus far. However, like many hard-earned skills, Absa Group has found there are many years of time needed before students become truly SOC-efficient.

The skills gap in cybersecurity

500,000

Cybersecurity talent shortage

4mm+

[5] Strategies for Building & Growing Strong Cybersecurity Teams, (ISC)^2 Cybersecurity Workforce Study

[6] Artificial Intelligence (AI) and Security: A Match Made in the SOC, IBM Security

At Cybereason, Chief Security Officer Sam Curry started an apprenticeship and internship program, believing that security leaders must open the doors to more diverse candidates with different thinking. In the program, at any point in time, there are five people who aspire to be analysts, none of whom have a technical background. The struggle, he noted, is that as an industry we designed our tools for level three analysts, who tend to think like threat actors and have a 'trust but verify' approach to systems and data output. Against this backdrop, security organizations need a mix of automation, diverse thinking, and more employees to supplement expertise.

Still, according to Malcolm Harkins, Chief Security and Trust Officer at Cymatic, we can develop the talent we have with a bit of time and effort:

> I believe structure drives behavior
>
> **Malcolm Harkins,** Chief Security and Trust Officer at Cymatic

"I believe structure drives behavior," Harkins said. "We've had creative ways of getting people out of their day jobs, such as job rotations between teams, and factory tours for security and management at just the cost of time and travel, because when people understand the criticality and unique needs of a function, they're usually impressed.

You can do that for two people, Harkins said, and "they'll spread the message far and wide." He cautioned, however, that for engineering and security teams who are able to execute well in the company's SOC, you must be disciplined enough to use employees' skills for burst capacity, and ensure they get back to their day jobs quickly. Without that discipline, "everyone always gets sucked into the SOC."

But when it comes to an outsourced SOC, managed services providers face the same skills shortage that traditional companies do.

Dr. Sam Small, Chief Security Officer at ZeroFOX, made the case for a partial approach to external vs. internal SOCs.

"An outsourced SOC can easily manage individual incidents on your behalf," Small said, "but if you outsource all of your pain receptors, so to speak, you may lose the ability to spot broader patterns or internalize and address new trends.

"Even when you're paying someone to look at your problems, they're not necessarily looking at the big picture the way an in-house staff might," he said.

The idea of mapping cybersecurity threat trends is certainly not new, but it can be difficult to achieve when the number of incidents is too high for humans to manage. According to Shawn Valle, Chief Security Officer at Rapid7, the amount of times he's heard that an external SOC is three or four hours late to report an incident is unacceptable.

"We all know that if it's ransomware or some other malicious code," Valle said. "It'd take milliseconds to spread across your entire network. Usually I hear that lack of manpower is the culprit, but it's akin to having a home alarm system that goes off after the police file their report and leave your house."

The argument for zero, partial, or a fully outsourced SOC staff may never be resolved, but experts agree that when SOC analysts and engineers are tuned into your organization's cybersecurity strategy, business processes and overall business, the relationship is no longer transactional. Instead, the relationship and the outcomes of the SOC are directly tied to the security needs of the business.

> Even when you're paying someone to look at your problems, they're not necessarily looking at the big picture the way an in-house staff might
>
> **Dr. Sam Small,** Chief Security Officer at ZeroFOX

Technology & automation

Of course, in 2020, it's impossible to discuss empowering IT security professionals to do their jobs better, faster, and more efficiently without the words "augmented", "assisted", or the phrase "AI". There's a reason for that – automation has the potential to transform the life of a SOC analyst by reducing alert fatigue, improving productivity, and even lowering mean time to resolution (MTTR).

However, the CR Think Tank, and other experts in the cybersecurity community, caution against freewheeling automation. Curry believes that awareness about automation is key: the more tasks you automate, the more you can telegraph your actions to threat actors.

"Automation itself is a form of vulnerability," Curry said. "You have to check your blind spot at pseudo-random intervals to see who's hiding there because the machine will become predictable and therefore exploitable. So, the mission is not to automate for the sake of it, but to make the humans more effective, improving the value of their output without weakening the whole."

This concept of improving humans' value through automation was echoed by Maurice Stebila, CISO, Digital Cyber Security, Compliance and Privacy Officer, Strategic Advisory at HARMAN by Samsung.

"I think we're at a crossroads where we're going to start seeing an AI Cyber Analyst," Stebila said. "In fact, I'm seeing it happen already. Organizations are applying machine learning to the decisions that level 1 and level 2 analysts make for every single incident in the last five years, which frees up the analysts for other tasks. Instead of a person spending five or ten minutes every hour on certain tasks, the AI Cyber Analyst can take a nanosecond."

Stebila noted that in many cases, these organizations with AI Cyber Analysts believe they can get to a point where data analysts can actually do prevention and put a block in instantly.

This may seem advanced, and it is – any organization without a solid pipeline of tier 1 and tier 2 analysts, or that has spotty incident management in the last several years, should focus on those critical foundational elements before any kind of AI implementation. A SIEM can help do this job, gathering data and creating a holistic view of a security environment – in-house or managed – over time.

For newer companies or those that have transitioned away from a security posture with incomplete security data, Valle described how he believes companies should approach automation; while it's typically an ongoing conversation, in general security leaders should begin with automating first.

"Software developers build based on APIs, and then build UI on top of APIs, which is worthy of exploration in SecOps teams," he said. "That strategy of building automation from the beginning, we believe, makes analysts stronger and better versus using fewer people."

Valle added that in many other organizations, automation and tools come too late in the game, and there are distractions or some event or incident that takes the focus away. Instead, when it's part of the culture early on, it's naturally a component of every process.

Small of ZeroFOX believes in deploying a culture of automation acceptance. Small believes cybersecurity automation should be democratized, and to do that, the logic behind it should be widely available to line managers and business unit leaders. In other words, organizations, large and small, tend to keep SOC secrets close to the vest.

But when CISOs can explain why and how decisions are made based on technology, it widens the lens of understanding, brings other decisionmakers into the process, and helps treat automation as a kind of prototyping mechanism instead of magic. And when it's time to alter point tools or incident response functions to mitigate cybersecurity vulnerabilities and check blind spots, line of business managers should already be in the know.

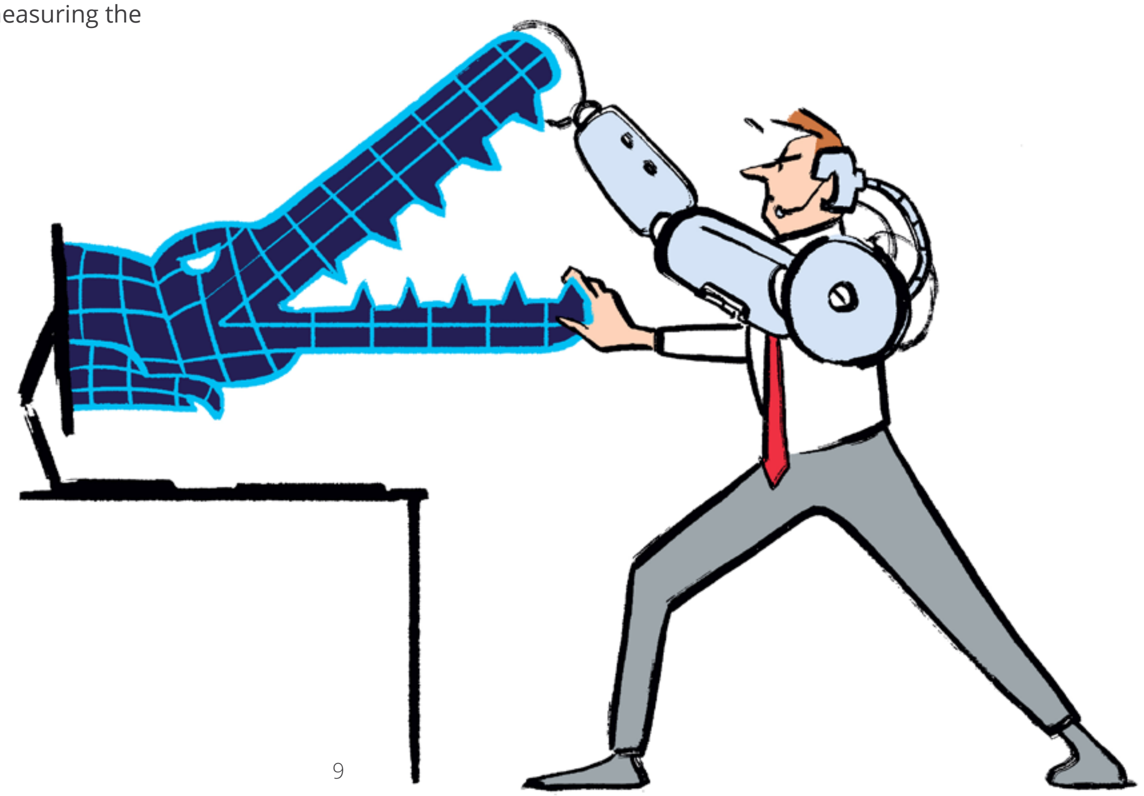
Members also discussed how in some cases using data visualizations tools can make a difference, creating dashboards measuring the SOC in a variety of ways. In further phases, these data visualization tools can be leveraged for narratives about the business' overall security posture when speaking to a technical audience like analysts, as well as up-leveling the narrative for a business audience made up of directors, VP-level and above.

This kind of process and efficiency allows communication to flow both ways about what tools might be triggering an environment change, the events coming in, and of course, how those changes affected the product and business.

Still, automation acceptance, or any culture change, is a tall order for many organizations, particularly those with deep silos or a lack of cross-functionality. Sue Lapierre, Vice President, Information Security at Prologis believes in a message of urgency.

"You have to make sure that your message to the business is that security is always chasing," she said. "And we are: the bad guys are always changing their tactics and we have to keep up. If there's a new product or service being launched in the business, for example, how are we going to protect it?"

Business and security should be in lockstep to be proactive whenever possible, to avoid the security chase.



Processes and efficiency

Today, there's broad agreement that a blend of analysts at varying levels plus automation and orchestration tools create the most efficiency in a SOC, whether that SOC is managed externally or internally.

However, there's more to the story. Many companies subscribe to the idea of putting teams physically next to each other to create agility and/or foster communication. At smaller or newer organizations, for instance, it can behoove security leaders to place managed detection and response SOC teams next to the product team, which can be extremely effective in informing how Scrum teams iterate and build new tools.

This approach can also assist in streamlining ticketing between product and SOC. CR Think Tank security leaders sanction this approach due to the belief that ticketing should be streamlined; for example, if the security team identified an issue that turned out to be an operational performance issue, it can be caught by security personnel due to its anomalous behavior, recognized and managed due to the proximity to others. James Lugabihl, Senior Director of Execution Assurance at ADP, noted the importance of a governance, risk and compliance (GRC) platform that gives the SOC a single source of truth that allows for integration of cyber incidents, fraud incidents, compliance, and more.

On the flip side, some of the aforementioned larger organizations with deep silos and missing cross-functionality prefer to put SOC and network operations centers (NOC) together. According to Curry, logically these two functions go together. However, CR Think Tank members agree that there are stipulations before anyone can claim success when the SOC and NOC work in tandem.

"There can be some cross-pollination between the network team and the security team, because there's so much communication between the two that needs to take place," said Stebila. "If we get both of these folks in the same room, we can help the business because it doesn't matter whether it's a security-related incident via some type of virus, or whether it's a fan that shut down, it just means the server is down. Those teams should be together to figure it out."

Yet, security leaders should be wary of operational issues potentially overtaking security issues.

According to Harkins, operational issues, especially in a large firm, are always swamping security issues, potentially overworking analysts, and drawing them away from detection and response. His recommendation is to sit the teams adjacent to each other, while ensuring structural and operational separation. And whenever possible, build team rotations in to build depth of knowledge, expertise, and appreciation across teams.

Efficiency and metrics underpin the separation of operations and security; companies of nearly all maturities and sizes focus on spending its budget for tools and its budget for staff as effectively as possible, and derive measures for success based on those factors. An example of a success metric is dwell time, which can range from under an hour to two or three hours in a very efficient organization.

Dwell time – as in how quickly an incident is discovered and remediated - is an incredibly important measure of a SOC's success, but experts caution against focusing solely on lowering timing.

"You have to understand the time needed to resolve every problem and communicate those individually," said Curry. "If you set a single goal time, you get people to chase detection instead of dwell time, which of course brings the overall time down. We just need to be careful not to put bias in one part of the cycle."

According to Tepper, when security leaders encourage analysts to upskill in other areas and provide tangible ways to improve those skills, such as an academy or a certification, all metrics tend to improve.

From a government perspective, Ari Schwartz, Managing Director of Cybersecurity Services at Venable, believes efficiencies come from an outsourced SOC.

> "
> You have to understand the time needed to resolve every problem and communicate those individually
>
> **Sam Curry,** Chief Security Officer at Cybereason

"One recommendation I can see for government cybersecurity is to ensure automation is part of the official guidelines," said Schwartz. "Beyond that, outsourcing to an MSP is considered contracting, which works really well for a lot of government agencies. And, you can find a number of efficiencies in a colocation model."

In-house vs. outsourced

Depending on your business needs, outsourcing your SOC to a provider may have too many drawbacks to be useful; there can also be a lack of trust due to inconsistencies in the vendor's reporting or missing the vendor's full potential, such as if the outsourced SOC is sending across too many false positives or underreporting potential threats.

However, if the outsourcing vendor isn't receiving all the data that's necessary to succeed – i.e. only receiving some of the logs – it can erode trust in overall cybersecurity posture. In addition, managed services providers have to contend with the same skills-related trends facing in-house SOCS: the talent pipeline is extremely thin, no matter where in the world they are.

When an external SOC is in line with business processes and your business, it can be tremendously valuable. For example, when IT and IT security professionals receive information about the events taking place in their environment, how to fix them, while considering how these events would impact the overall business long-term, that's when the relationship becomes a partnership.

Some businesses, potentially the ones struggling to keep tier 1 analysts in-house, might consider outsourcing their tier 1 analysts only. Keeping tier 2 in-house, this frees up the majority of the security operations team to focus on engineering tasks, such as building or acquiring and implementing IT security products, as well as other solutions needed across the company to protect employees and customers.

No matter your SOC format, "Since most companies' security functions are seen as hobbyist or not in the core business, you have to triage based on what the business cares about, and then show value backwards," said Curry. "I think the most important thing that security can do is get really tight with the business."

8 Tips for SOC Transformation

No Matter the Organization's Size

1. **Know the Business Goals.** Tune your SOC analysts and engineers tightly to your organization's cybersecurity strategy and overall business.
2. **Think Cross functional.** Bring cross-functional decisionmakers into the process when making decisions on technology to get buy-in from key stakeholders.
3. **Avoid the Chase.** Business and security should be in lockstep at regular intervals, to avoid the security chase and keep SOC practices fresh.
4. **Separate Operational from Security.** To keep efficiency (and morale) high, avoid allowing operational issues to swamp security issues.
5. **Define Success Metrics.** Find the right success metrics for your SOC to work towards, and continually measure success.
6. **Continuous Skill Building.** Encourage security analysts to consistently upskill and reap the rewards with better overall metrics.
7. **Get the Right Data.** Set your managed SOC up for success by ensuring they have all the right data they need to succeed.
8. **Build a True Partnership.** If you outsource, make the relationship a true partnership by ensuring the external SOC is aligned to your business processes and your business.

The Bottom Line

Assuming a company has the right funding and C-suite support to start a next-generation SOC, Think Tank experts recommend allowing the current SOC – whether it's in-house or managed – to live out its useful life, while keeping an eye on what changes the company wants to make and build them incrementally:

1 **Continually support current analysts as much as possible.**
Be aware of their workload, potential alert fatigue, and overall morale.

2 **Build the talent pipeline.**
This is a smart strategy no matter what, and given the gaping maw that is the cybersecurity skills gap, it's a critical SOC success element.

3 **Streamline talent and provide communication channels that foster a more seamless handling of ticketing, incident response, and more.**
Whether the SOC/NOC approach is right for the organization, or if the SOC/product team is the right choice, or even if your organization should choose to keep teams separate but build in regular job rotations – build the talent strategy and maintain it.

4 **Leverage technology**
such as a SIEM or SOAR that can gather events from end user' devices, servers, and network equipment, as well as security equipment such as firewalls, AV scanners or IPS and help to manage the investigation and response processes.

5 **Use this gathered data for smart analysis over time and share it with other business leaders in your organization.**
Use this gathered data for smart analysis over time and share it with other business leaders in the organization.

Once the organization gains a holistic view of its information security environment and can communicate it cross-functionally, augment its SIEM with a SOAR. Or, determine whether its SIEM provider can offer a SOAR capability, which would help cut down on additional tools and vendors in what's likely an already cluttered environment.[7]

Security leaders should always consider the factors that make an outsourced strategy, or a partially outsourced strategy, right for their business. If it's as simple as 'make vs. buy', and there's a preference for keeping tier 1 analysts outsourced for their outside perspective, that may be the answer, especially if the cost of hiring a managed services provider is more attractive than building it in-house.

Still, the variety of factors put forth here may create a compelling reason to look again at the value of hiring and developing talent internally. No matter the conclusion, no SOC can function without skilled analysts and engineers using advanced cybersecurity tools and automation, while being supported by an efficient organization with clear business processes and cross-functional collaboration.

[7] Decluttering Your Security Environment, CR Think Tank

About Cyber Resilience Think Tank

The Cyber Resilience Think Tank is an independent group of industry influencers dedicated to understanding the cyber resilience challenges facing organizations across the globe, and together, providing guidance on possible solutions.

They define cyber resilience as: "an organization's capacity to adapt and respond to adverse cyber events—whether the events are internal or external, malicious or unintentional in ways that maintain the confidentiality, integrity and availability of whatever data and service are important to the organization."

Malcolm Harkins
Chief Security &
Trust Officer
Cymatic

Juan Harmse
Head of Resilience Strategy &
Engagement
ABSA GROUP

Taylor Lehmann
CISO
AthenaHealth

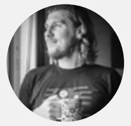
Gary Hayslip
CISO
SoftBank Investment Advisors

Sue Lapierre
VP, Information Security
Officer
Prologis

Peter Tran
Vice President, Head of
Global Cyber Defense &
Security Strategy
Worldpay

Dr. Sam Small
CSO
ZeroFOX

Maurice Stebila
CISO, Digital Cyber Security,
Compliance & Privacy Officer
HARMAN by Samsung



Jakub (Kuba) Sendor
Software Engineer
Yelp

James Lugabihl
Senior Director, Global
Security
ADP

Ari Schwartz
Managing Director of
Cybersecurity Services
Venable

Stephen Ward
CISO
Home Depot

Dawie Wemtzel
Head of Forensic
Investigations
ABSA GROUP

Chris Wysopal
Chief Technology Officer
Veracode

Sam Curry
CSO
CYBEREASON

Greig Arnold
CISO
Vista Consulting Group

Bill Brown
CSO
ClickSoftware

Marc French
CISO, Managing Director
Product Security Group

Josh Douglas
VP Product Management
Threat Intelligence
MIMECAST

Scott Eigenhuis
Associate Director,
Information Security
ILLUMINA

Shawn Valle
CSO
RAPID7

Michael Madon
SVP & GM Security Awareness
and Threat Intelligence
Mimecast

Claus Tepper
Head of Cyber Security
Operations, Absa Group

For more insights from the
Cyber Resilience Think Tank, visit
mimecast.com/ThinkTank

Printed on Recycled Paper