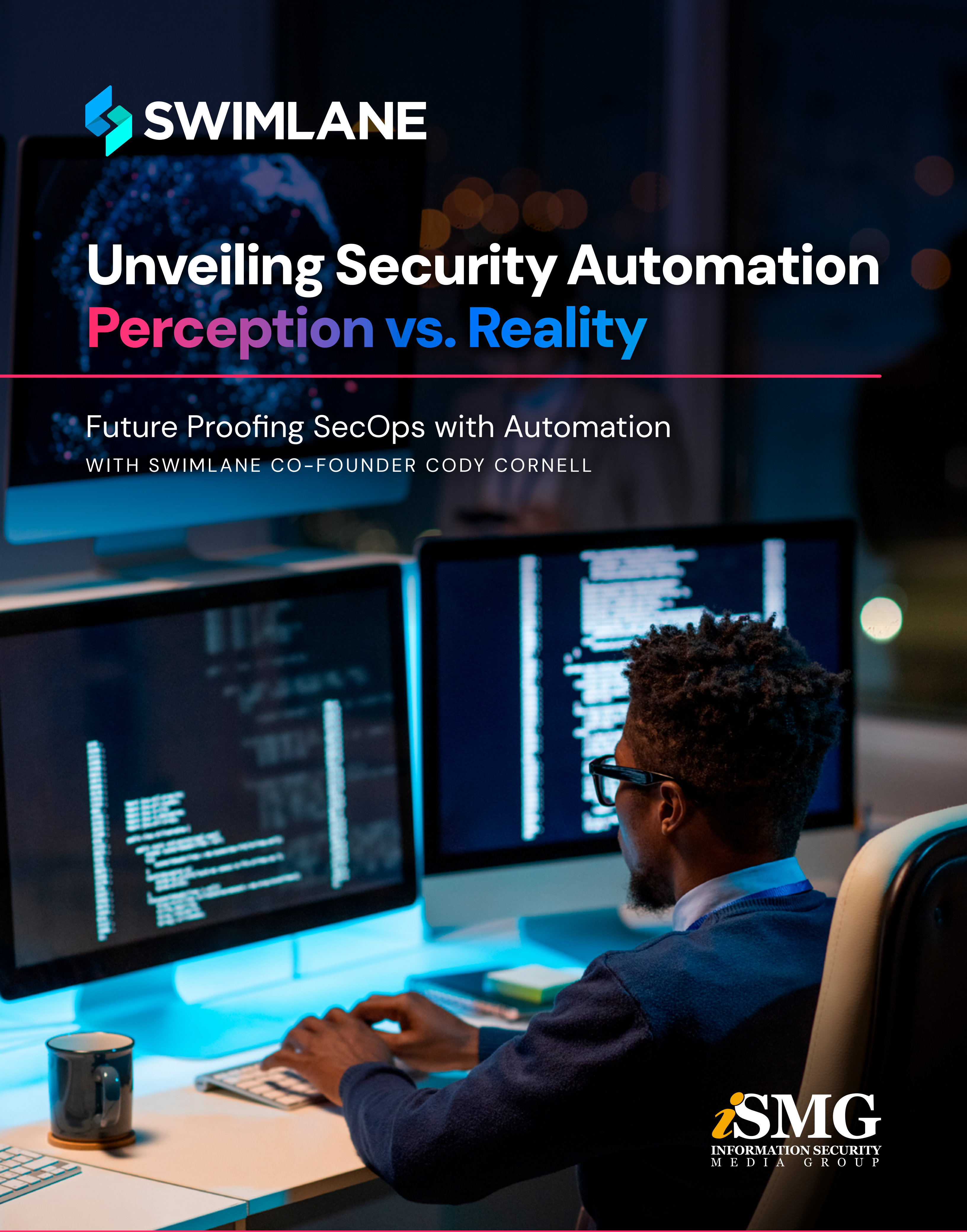
SWIMLANE

Unveiling Security Automation Perception vs. Reality

Future Proofing SecOps with Automation

WITH SWIMLANE CO-FOUNDER CODY CORNELL



iSMG
INFORMATION SECURITY
MEDIA GROUP

CODY CORNELL

Cornell is responsible for the strategic direction and development of Swimlane's low-code security automation platform. His focus on the open exchange of expertise allows him to work closely with industry-leading technology vendors and partners to identify opportunities, streamline and automate security operations activities that speed cyber response and enable security automation initiatives.

The C-suite and boards are more involved in cybersecurity decisions than ever before, but executive leaders still have a huge disconnect between perceptions and operational realities. This gap leads to miscommunication and missed expectations that could pose great risks to the enterprise, said **Cody Cornell**, co-founder and chief strategy officer with Swimlane.

Swimlane's 2023 Cyber Threat Readiness Report found that 70% of executives think all security alerts are being managed – starkly contrasting the 36% of front-line employees who say alerts are being addressed.

"The hard thing about working in security ops is you have to be right all the time – unlike an attacker who has to be right once at a moment in time," Cornell said. "As an offensive team, you have to be right all the time. If you have this known gap of things being left unchecked, unresolved, unmitigated, then you have risk exposure."

While enterprises have embraced automation, it's often not embedded as a core competency. Automation is a journey, and it involves a maturation process. Organizations should evolve their automation capabilities through systematic adoption of frameworks, he said.

In this video interview with Information Security Media Group at Black Hat USA 2023, Cornell also discussed:

- Key highlights from the 2023 Cyber Threat Readiness Report;
- The challenges of perception alignment in managing security alerts;
- How Swimlane's ARMOR Assessment helps security leaders identify security gaps.

Report Findings and Surprises

TOM FIELD: What are some of the key findings of Swimlane's 2023 Cyber Threat Readiness Report?

CODY CORNELL: What really stood out to us was that there seems to be a pretty big disparity between the perception that executives have versus what the people that actually are doing the work, the people that are sitting at the desks with their hands on the keyboard, have. We saw in the survey that the great majority of executives, somewhere around 70%, think that all of their security alerts are being managed. If you ask the people actually doing the work, the number is half of that. It's around 35%. It's interesting to see the perception mismatch of what's being done and, more concerningly, what's not being done.

FIELD: What surprised you?

CORNELL: The thing that surprised me was twofold. One: There's an expectation among leadership and people that are doing the work that they're never going to be able to fill all their roles, so there are always going to be vacancies, which for some organizations is a struggle.

Two: Across a lot of different topics, be it the number of alerts that are being managed or what type of tools they should be using, there seems to be a pretty big gap between what people that are doing the work and people that are running those teams think is the current status of things. When you have those expectations and perception mismatches, that creates communication issues and it can create missed expectations.

The Biggest Gap

FIELD: What is the biggest misalignment you found?

CORNELL: The biggest misalignment we found was around the perception of how much people were actually getting done versus how much was being left on the table.

FIELD: What's at risk because of that?

CORNELL: The hard thing about working in security ops is you have to be right all the time – unlike an attacker who has to be right once at a moment in time. As an offensive team, you have to be right all the time, and keeping up with

> "There's an expectation among leadership and people that are doing the work that they're never going to be able to fill all their roles, so there are always going to be vacancies, which for some organizations is a struggle."

that is really concerning. If you have this known gap of things being left unchecked, unresolved, unmitigated, then you have risk exposure. If you look at the changes that are happening with the U.S. Securitities and Exchange Commission (SEC) and how people have to report on security breaches and what the government's trying to do with breach notification, that's a lot of risk – not just for the organization and brand but also for leadership. They're becoming much more responsible personally and as an organization for what might happen.

The Automation Journey

FIELD: Let's talk about the state of automation. Everyone desires to have more automation in their organization. But where do you see enterprises displaying their immaturity when it comes to automation?

CORNELL: A whole group of organizations haven't really embraced automation as a core competency. We talk a lot about endpoint security and log management, and that's how the leading organizations that are really addressing all their alerts are using automation. It's how they're achieving that. Historically, we've thought about doing that within security operations inside of the SOC, but where we see people excelling is outside of the SOC. They're supporting automation across the security landscape inside of their organization.

FIELD: How do you recommend that organizations mature their automation capabilities and, at the same time, be able to future-proof or help future-proof their SecOps?

CORNELL: Automation is a journey, and there's a maturation process. Organizations that have adopted automation and started to see value from it should think about how they adopt frameworks that will allow them to mature it systematically, because it's not one of those things that just makes an instant leapfrog. You've got to work at it. That's why we put together our ARMOR Framework. It helps organizations put together the metrics and the KPIs they should be looking at to know if they're making improvements.

> “If you’re maturing, you’ll start to get a lot of time back and get much more consistent and effective results. You’ll see it in the happiness of your team and the results of the program, and you’ll be better at leveraging your tools.”

The ARMOR Assessment

FIELD: What is the ARMOR Assessment, and how does it help organizations, particularly security leaders, identify the gaps that need to be addressed?

CORNELL: Our ARMOR Framework comes in two parts. There’s a readiness assessment and a basic level operations maturity. Are you ready for operations? That means: Do you have executive alignment? Do you have the right people on your team? Do you have the tools in place? Can you go off and do this successfully? Then, once you’ve started down that journey, we have a tangible and tactical set of measures that you can use to determine if you’re doing this right and getting better. We call it the ARMOR Matrix. A lot of things, such as MITRE ATT&CK and OODA loops and kill chains, help threat detection, but there’s not as much out there for automation maturity. We want to help people close that last mile on automation and remediation.

FIELD: Assessment’s one thing, but how do you then put the results to work?

CORNELL: The results show you’re maturing if the number of alerts that you’re managing manually goes down, if the enrichment is happening automatically and if you’re closing things from a mitigation perspective without having to do that by hand. If you’re maturing, you’ll start to get a lot of time back and get much more consistent and effective results. You’ll see it in the happiness of your team and the results of the program, and you’ll be better at leveraging your tools. You’ve made lots of investments in those tools, and you’ll get a lot more out of them.

Assess Your Readiness

FIELD: Where can our audience learn more about this?

CORNELL: They can take a readiness assessment on our website. There’s both a readiness assessment and an ROI calculator around automation.

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps reduce process and data fatigue, overcome chronic staffing shortages, and quantify business value.

The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit swimlane.com.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · Just for Credit Unions CU INFO SECURITY® · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk® TODAY · CAREERS INFO SECURITY® · Data Breach® Prevention. Response. Notification. TODAY · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io