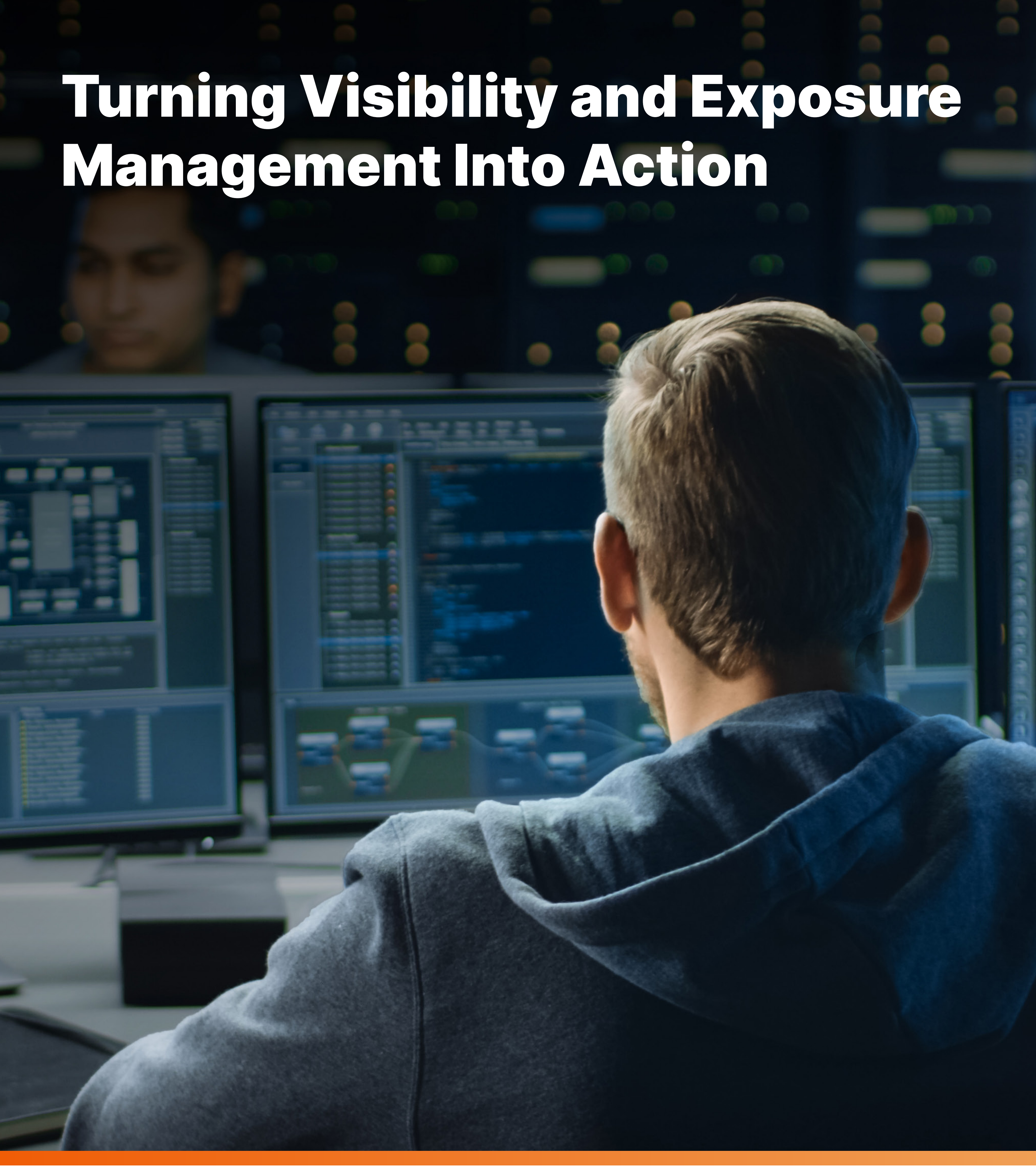
Turning Visibility and Exposure Management Into Action



iSMG
INFORMATION SECURITY
MEDIA GROUP

Axonius

Axonius CEO Dean Sysman on How ‘Actionability’ Defines Next-Gen Cybersecurity

Security teams today are overwhelmed by alerts, blind spots and fragmented infrastructure. Dean Sysman, co-founder and CEO of Axonius, said the real challenge isn’t data scarcity. It’s turning that data into prioritized, actionable intelligence for more effective defenses.

At RSAC 2025, Sysman introduced Axonius Exposures, a next-gen exposure management platform that combines insights from more than 1,200 integrations and over 40 asset types. This gives security teams the business context to understand which vulnerabilities matter and who’s responsible for fixing them. The goal is to move beyond asset management toward “actionability.”

“It’s not just about visibility,” Sysman said. “It’s about having the truth that allows you to take action in the most scalable and effective way.”

In this video interview with Information Security Media Group at RSAC Conference 2025, Sysman also discussed:

- Why attackers exploit visibility gaps rather than zero-days;
- The shift from vulnerability management to exposure management;
- Axonius’ emergence as a strategic cybersecurity platform.

Sysman co-founded Axonius, a cybersecurity platform provider now valued at $2.6 billion. He previously co-founded Cymmetria and prior to that served as a captain in an elite Israeli Intelligence Corps unit.

DEAN SYSMAN
Co-Founder and CEO, Axonius

> **“Every organization we go into, we realize they have a lot of gaps, they have unprotected assets, they have open entry points that they didn’t even know about. They have a lot of vulnerabilities that they never even saw, let alone fix.”**

Blind Spots in Infrastructure

TOM FIELD: Where do you see enterprises most challenged to gain visibility across all of their digital assets?

DEAN SYSMAN: It's a difficult challenge because when we started our company Axonius, about eight years ago, we saw that organizations had a very fragmented infrastructure. You have many different products, many different controls. They all know very deep information about something. Your identity product might know a lot about your identities, your endpoint protection might know a lot about your endpoints. Your cloud platform knows a lot about your cloud, but they don't talk to each other and they don't understand each other.

And to understand everything in your environment became a very difficult challenge. And when we started, I was working for one of the largest cybersecurity teams in the world, and we found that they'd been breached by a Chinese state actor, but we couldn't do anything about it because they had no idea why that device that was infected was even there. They had no idea who owned it, they had no idea why it was there, what was managing it. We couldn't figure that out. For us, to solve the problem of understanding everything that an organization has is one of the most foundational things for cybersecurity and IT teams. And everything else depends on being able to solve that challenge.

Unseen Assets, Open Doors

FIELD: How do you see adversaries taking advantage of the visibility gaps?

SYSMAN: When you look at most breaches that happen today, they don't happen because of a very flashy zero-day. For every organization, the most likely threat scenarios involve either the exploitation of well-known vulnerabilities, the use of misconfigured and exposed devices accessible via the internet, or the compromise of unsecured identities. It's all those things that they're just taking advantage of the open opportunities to get into the environment. From the beginning, we experienced rapid growth, because every time we got into an organization and we would connect all their controls, all their data silos into our platform, that was our uniqueness, that's how we created what is now called the CAASM category - the Cyber Asset Attack Surface Management category. Today, we provide visibility into everything an organization has by aggregating data from over 1,200 different sources.

And every organization we go into, we realized they have a lot of gaps, they have unprotected assets, they have open entry points that they didn't even know about. They have a lot of vulnerabilities that they never even saw, let alone fix. And that visibility is the starting point to what we now call something a lot more important and a lot deeper than just having visibility, which is actionability. How do you turn all that data into truth that allows you to take action? Because organizations and security teams have a lot of data, but what they need in order to be able to take action is the truth that allows them to understand what the right action is.

The Axonius Approach

FIELD: Can you share why Axonius Exposures is a breakthrough in vulnerability management?

SYSMAN: When organizations work with us, vulnerability management becomes part of a broader approach we refer to as exposure management - a more comprehensive strategy that encompasses vulnerability management. Our product, Exposures, is designed to address this expanded scope. What they want to do is be able to understand all those exposures and exposures are vulnerabilities, but there are also misconfigurations, there are also things exposed to the internet that shouldn't be, or understanding what are the things that are exposed to the internet. Historically, what a lot of vulnerability management platforms did was try to give the technical risk behind a vulnerability - finding the CVE, finding the severity score of how bad that vulnerability is. But what we know is important to organizations, first of all, is that they can't solve all their vulnerabilities. That's impossible. We have customers, some of the largest Fortune 500 companies have dozens of millions of vulnerabilities that will never all get fixed, because you don't know what the fix will impact.

You don't know what the fix will do from a business standpoint. So they have to prioritize. They have to understand what they can fix and what they can't. And the second thing is forget about what is the technical risk, what is the business risk. If that is some developer's test instance that they spun up and it's in its own network, even if it has the most severe vulnerability, do you care about that? You probably don't, because that's just a test machine that nobody's going to have access to. But even a low severity issue on your most important server doing your payments that's exposed to the internet, that's probably a high priority thing. So what we're realizing is that in order to do exposure management, understand the risk, prioritize what organizations need is not just a technical risk, it's also the business context of what those assets are.

What role do they play in the organization? Who are their owners? And that's why a lot of our customers told us, "We want you to be the platform that does exposure management for us, because you are the only place that has the business context of those assets because that's what you've done. You've created the most deep and wide understanding of what our assets are." And that's the major thing that we're talking about now with this launch of exposure management, how do you tie in all the data feeds, all the technical risk, but also all the business context in order to be able to understand what action to take from that truth?

Early Feedback: High Impact

FIELD: What's the initial feedback from your beta customers and the analyst community?

SYSMAN: A lot of excitement and a lot of amazing potential. And we were already seeing with some of our initial customers how it transformed their ability to pinpoint what is the capacity to solve the most urgent needs and problems that they have. And in our launch announcement, we even had one of the vulnerability management leaders for one of the top Ivy League universities in the world explaining how first they used us from an asset management perspective, but very quickly they realized we were the platform that held the data that allowed them to get to the truth that takes them to the action of how to prioritize their vulnerabilities, how to understand the true risk, not just from a technical standpoint, but from a business context standpoint.

From CAASM to Actionability

FIELD: Where does exposures fit within the Axonius Asset Cloud?

SYSMAN: Besides exposure management or exposures as a product, what we launched a few weeks ago is a new way to perceive us not as a product startup company anymore, but as a major platform vendor. And the reason is that what we built in order to create that CAASM category was over 1,200 different adapters that know how to get the data from everywhere it resides in the organization. We also now understand not only devices where we started from, identities, vulnerabilities, installed software, SaaS, applications, permissions, licenses. We have over 40 different asset types that we understand about

> "Organizations and security teams have a lot of data, but what they need in order to be able to take action is the truth that allows them to understand what the right action is."

the infrastructure. And there's not a single platform offering in the world that understands these many different types of assets to such a wide variety. And we also understood that those adapter connections not only allow us to read data, but also enable us to perform action. And today, we have over 450 different actions in our enforcement center. So that combination of getting the data from everywhere, understanding every type of asset, correlating that data together, de-duplicating it, normalizing it, and then being able to take action, that's a very powerful platform.

And customers have always asked us to do a lot more than just visibility, than just asset management. And that's why we declared the category we created in 2018, CAASM. We declared that it's dead, and we believe in a new way of thinking about it that we call actionability. It's not just about visibility - it's about having actionable truth that enables organizations to respond effectively. By leveraging comprehensive data, our platform empowers users to manage and prioritize exposures and risk, and to take action in the most scalable and efficient way. We also announced our Identities product, which is going to compete in the IGA category, in the ITDR category, and allow organizations to see their entire identity inventory being able to prioritize identity life cycle and permission management. So we're just starting out to understand the potential of how our platform can help organizations.

Risk Prioritization With Context

FIELD: Does actionability distinguish you from other vulnerability management platforms?

SYSMAN: Absolutely, because I think everybody has more vulnerabilities than they can ever solve. Everybody has more data that they could ever want. And what you need is the truth. So for example, if I want to solve a vulnerability, the obvious way to do that is to patch or to upgrade that software version. But many times I have no idea what's going to be the impact of that. In order to understand the impact, I have to understand what does that asset do? What is its role? Which business application or business service this might interrupt? But also who's the owner? If I have a vulnerability in my operating system, the owner of fixing that might be someone in my IT department.

But if it's a vulnerability in one of our applications that we developed, it's going to be somebody in the engineering department. And depending on all those details is what we suggest is the right action to take when you want to solve it. And sometimes the action is not even to patch, it's to use a mitigating control to, for example, block that device from the internet. And reachability is also a huge part of it. Can that vulnerability even be reachable by an attacker? And how do we use that in order to mitigate the problem sometimes?

Tailored Solutions, Unified Platform

FIELD: You built five discrete products on top of the Axonius Asset Cloud. How do they meet different customer needs?

SYSMAN: We try and cater to specific categories or budget line items that organizations have. We have exposures, identities, we have SaaS apps, which is our ability to show all the different SaaS apps an organization has and then check their security configuration. And that category is called SSPM. We have other soon-to-come news about our platform. We're constantly innovating and adding more and more things because our customers are telling us, "We want you to take this platform. And the uniqueness of the understanding you have of the environment, your ability to take truth to action and be able to do that for a lot of the problems that we have." And we're becoming one of the strategic platforms for many of our customers that they invest in.

Value-Driven Product Evolution

FIELD: What's next?

SYSMAN: We're constantly thinking every single day about how do we deliver value to our customers? This is something I tell our customers all the time, is that there are so many existing categories, existing trends that companies competing over that have very specific criteria for who's going to be the most successful. And in endpoint protection, it's your detection rate. In firewall, it's your throughput. For our problem, the only way that it's valuable is based on what our customers and our users say is the value that they're getting. So we're obsessed about measuring and using those measurements as our north star of how do we continue to increase the value that we bring to customers. And we have one of the highest NPS scores - a Net Promoter Score - of customers. It's usually in the high 70s or low 80s. I don't know of any other cybersecurity product that's ever had that, and we're very proud of that because it shows how much our customers promote our solution to others.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 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, OT security, AI 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® CU iNFO SECURITY® Just for Credit Unions GOV iNFO SECURITY® HEALTHCARE iNFO SECURITY®

iInfoRisk® TODAY CAREERS iNFO SECURITY® ~~Data Breach~~. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

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