PROFILES IN *Confidence*

ROLAND CLOUTIER

Former Global CISO
TikTok, ADP and EMC

Current Principal
The Business Protection Group

A STRATEGIC VIEW ON CYBERSECURITY

After more than 30 years in cybersecurity leadership, including roles as Global CISO at TikTok, SVP and CSO at ADP, and VP and CSO at EMC, Roland has shifted into a strategic advisory role, supporting CISOs, CEOs, general counsels, and chief trust officers. Having led security at some of the world's largest organizations, he is now intentionally taking a step back from the day-to-day CISO seat to focus on guiding others.

While he may no longer sit in the operational role, his perspective remains rooted in the realities of running a modern security program.

That vantage point allows him to see trends across organizations, particularly as security leaders navigate increasing complexity and the growing influence of AI.

RESILIENCE AS THE FOUNDATION

Despite the innovation happening across the industry, Roland is clear that the core mission of cybersecurity has not changed.

"At the end of the day, we are operational business protection specialists for the company," he explains.

In today's environment, that responsibility starts with resilience. Rather than trying to anticipate every possible threat, the focus is on ensuring the business can continue operating through disruption.

Roland shares, "We have to start with resilience, how do we help the business maintain a minimum viable company, and how do we help ourselves maintain a minimum defensible company?"

This foundation on resilience, awareness of the threat landscape, and strong teams remains critical. But how organizations achieve it is being rapidly reshaped by AI.

AI DRIVING VISIBILITY AND BETTER DECISIONS

For Roland, one of the most immediate impacts of AI is the ability to gain deeper visibility into complex environments.

"The ability to apply generative AI and LLMs and getting information to make smarter, better decisions is going to give us such amazing transparency," he says.

This shift is not limited to one function. It extends across risk, compliance, and control validation, fundamentally improving how security teams understand their environments and prioritize action.

"It's going to be amazing, and almost every major program in stacks are going to benefit from it."

By accelerating how information is gathered and interpreted, AI is enabling faster, more informed decision making across the board.

FROM RESPONSE TO AUTO-REMEDIATION

Beyond visibility, AI is also transforming how organizations respond to threats.

"We have an opportunity today to stop malicious activity before it happens, and revert to last known good instead of having to perform incident response," Roland explains.

This would mark a shift from lengthy investigations and recovery cycles toward faster, more automated responses.

"There's going to be some new defense and auto remediation capabilities that we wouldn't have even imagined two years ago."

As these capabilities mature, they will significantly reduce both the time and effort required to manage security incidents.

SECURING AI-DRIVEN DEVELOPMENT

AI is also accelerating how software is built, creating new challenges for security teams.

"We have machine generated code that is coming at us in waves. To keep pace, organizations must rethink how they approach application security. We have to apply a new capability to consume all of that information, ensure that it's secure code, and do it at the speed that our business is building it," Roland says.

This creates an opportunity to embed security directly into development processes.

"We'll be able to implement guardrails automatically and actually be better and more secure because we can keep up with the speed of development."

EXPANDING THE ROLE OF THE CISO

As AI adoption accelerates, expectations of security leaders are expanding as well.

"CISOs have three jobs when it comes to AI," Roland explains. "One is to enable the company to run fast with AI. The second is to protect against new AI attacks. And the third is to be better business owners."

The first responsibility of enablement marks a significant shift. Security is no longer just protecting the organization, but actively supporting innovation. However, at the same time, adversaries are evolving quickly.

Roland notes that this requires organizations to continuously adapt their defenses while also improving how security teams operate as part of the broader business.

REDEFINING SECURITY TEAMS AND WORK

AI is also reshaping how security teams are structured and where human effort is applied.

"How do I reduce the number of people in my SOC by letting tier one and tier two work be done by AI?" Roland asks.

Instead of eliminating roles, organizations are shifting focus toward higher-value work.

"What I need is a human in the loop to validate the output, help prioritize, and integrate with the business. In areas like compliance and risk, this shift is already underway. I can do your compliance automatically and don't need six people collecting information. I can press a button and do it now," comments Roland.

This allows teams to focus more on strategy and decision making, rather than manual processes.

LOOKING AHEAD

As organizations continue to adopt AI at scale, Roland sees the next year as a period of rapid transformation. Security leaders will need to move faster and rethink how their teams and technologies operate.

At the same time, the fundamentals remain unchanged. Resilience and strong decision making will continue to define effective programs.

In Roland's view, the organizations that succeed will be those that embrace AI thoughtfully, using it to enhance, not replace, human judgment, while maintaining the discipline needed to protect the business in an increasingly complex environment.