www.pipelinepub.com
Volume 22, Issue 1

Closing Critical Cybersecurity Gaps: How Agentic AI is Reshaping CISOs' Strategy

By: Matt Rider

Security leaders face intensifying pressure from all angles. With attack volumes rising, AI-generated threats outpacing traditional defences, and analyst burnout on the rise, the cybersecurity landscape is demanding more than conventional responses. But AI offers a unique strategic inflection point—particularly through agentic AI, which elevates the role of security tools from reactive helpers to proactive partners.

A recent PwC survey from May 2025 showed that 79% of senior executives report AI agents are already in use in their organisations, and 66% of those report productivity gains. However, while adoption is broad, deep integration remains limited: only 35% say they've adopted agents broadly, and under half have redesigned workflows around them, the CUBE research team reports.

Meanwhile, as reported by Axios (March 2025), leading security teams are increasingly turning to agentic AI to manage alert overload and accelerate triage. Unlike chatbots that merely respond, these AI agents can take pre-approved actions autonomously.

As AI continues to evolve, Chief Information Security Officers (CISOs) face a pressing question: Can AI do more than automate tasks and summarise data? Is the key to successfully scaling security operations the deployment of agentic AI that not only provides insight into emerging threats but also empowers strategic decision-making?

Expanding Threats, Overwhelmed Teams

Across industries, the story is the same - the threat landscape keeps expanding, but resources, tools, and security teams can't keep pace.

Modern CISOs are facing more pressure than ever as threats continue to advance, and the cybersecurity skills gap remains as wide as ever. Too often, new technologies promise transformation but only add more complexity, more dashboards, and more to configure. AI is no exception in this field.

Instead of delivering what CISOs really need, many solutions simply add on a chatbot or offer rebranded tools that fail to effectively reduce analyst workloads. CISOs are left to firefight reoccurring challenges, including:

Overwhelming Datapoints. Alert volumes continue to climb. CISOs are left constantly balancing signal and noise, driving up alert fatigue. The challenge of sifting through countless daily alerts increases the risk of missing real threats, as well as increasing strain on analysts.

Increasingly Sophisticated Threats. Modern threats, especially those generated by AI, move too fast and mutate too often for traditional detection methods to keep up. Existing threat intelligence feeds and rule-based systems often fall short when faced with novel or signatureless attacks.

Burnout from Repetitive Tasks. Analysts still spend hours on repetitive manual tasks, such as reviewing logs or responding to low-level alerts. This not only leads to inefficiencies but lowers morale and drives higher staff turnover, which carries the danger of weakening an organisation's overall security posture.

Lack of Consolidation. CISOs are frequently left piecing together reports from disparate tools or manually chasing metrics from their teams. This creates lag, uncertainty, and missed opportunities to demonstrate progress or justify investments.

More than ever, CISOs need security tools that can help them overcome the most critical security operations centre (SOC) challenges, rather than add to their workloads. They need tools that go beyond just collecting insight by proactively pinpointing gaps, tuning strategies, and delivering measurable return on investment (ROI).

Security Built for CISOs

In today's fast-moving threat environment, every second counts. This is why CISOs need all the support they can get from intuitive, AI-driven security tools.

Agentic AI is changing the game by transforming what CISO outcomes look like. It can reason across datasets, adapts to new input, and stays aligned with the organisation's policies. With this, security leaders gain a much-needed tool that is not only context-aware but can act and support strategic decision-making. When implemented well,

agentic AI isn't just another automation tool—it reasons, adapts, and acts in alignment with organisational policy. It can:

Enable strategic planning. Daily posture assessments, tool rationalisation, and MITRE ATT&CK coverage analysis are translated into data-backed roadmaps to inform funding and resourcing. At the same time, agentic AI simulates adjustments or additions to security tooling and detection capabilities. This allows SOC teams to adapt tools in the instance of an actual attack, learning from the scenario and strengthening security postures. CISOs benefit from intelligent insight that enables them to evaluate how proposed actions close gaps and improve security postures.

Accelerate investigations. Agentic AI streamlines the threat investigation process by automating case summaries, threat classification, and next-step recommendations to triage faster, cut false positives, and ease analyst fatigue. This, in turn, closes the cybersecurity skills gap, adding value to SOC teams by decreasing burnout. Analysts at any level can move

quickly from detection to resolution without starting from scratch, whilst reducing mean time to detect (MTTD) and mean time to respond (MTTR).

Illuminate through visualisation. Transforming natural-language queries into insightful dashboards and trend visualisations gives clarity to raw telemetry without distracting noise. Based on this plain language prompt, the measures, dimensions, filters, and chart type are configured automatically to ease the analyst experience. Clear visualisation is about streamlining the security process to simplify dashboards to show CISOs what is impacting the network. Agentic AI provides actionable insights, direct pathways, and produces business-relevant terms for accessibility across an organisation.

Drive measurable maturity. Agentic AI enables security leaders and analyst teams to move beyond static reporting through benchmarking posture, tracking improvements, and packaging performance into board-ready business narratives. It delivers real-time, contextual insights that are aligned to business risk and outcomes. With the ability to generate executive-level summaries, surface trends, and simulate future scenarios, agentic AI helps CISOs justify security investments with clarity and confidence, while continuously strengthening their organisation's security posture.

Augment the analyst experience. As CISOs evaluate AI adoption, many will favour human-in-the-loop solutions that guide decisions but keep analysts in control. The right agentic AI solutions will empower analysts through automation, not sideline them with it. Agentic AI holds the potential to anticipate security needs and propose solutions analysts may not have considered before. These capabilities help boost overall effectiveness by delivering an extra level of input to the SOC.

Validated Opportunities & Associated Risks

Why does it matter? Agentic AI helps shift SOCs from reactive to proactive. It complements human expertise, especially as pressure mounts on teams with limited bandwidth. The trend is gaining momentum.

But… security risks are real. Reports are clear: agentic AI introduces new vulnerabilities. From prompt injection and unauthorised action to identity issues, these autonomous systems demand rigorous governance. For instance, Microsoft released a patch in July 2025 addressing a path traversal flaw in its agentic browser initiative.

Frameworks now emerging, such as Forrester's AEGIS (covering governance, identity, data, application security, threat management, and Zero Trust), offer meaningful guardrails for adopting agentic agents in responsible ways.

Driving Value with Agentic AI

Looking ahead, there's no doubt that the threat landscape will continue to evolve and drive new challenges for security teams. Agentic AI isn't a cure-all, but it offers a meaningful path forward for security leaders focused on results.

Whether the goal is to improve detection, retain talent, or justify SOC investment, AI agents have the potential to help CISOs upscale security operations. During a time when cyberthreats are more complex than ever, agentic AI holds the potential to help security leaders and their teams spend more time orchestrating strategy, not firefighting noise. The future belongs to those who can deploy agentic AI with both rigor and insight.