ARBITIUM

ARBITIUM INSIGHTS

The SOC Is Dead. Long Live the Agentic SOC.

John Remo, Co-Founder & CEO | March 18, 2026

Last month, Gartner released its top cybersecurity trends for 2026. Buried in the usual parade of acronyms and quadrants was a phrase that should stop every security leader mid-scroll: **"AI-driven SOC solutions destabilize operational norms."**

Destabilize. Not enhance. Not augment. Destabilize.

If you have spent the last decade building a SOC, staffing a SOC, or funding a SOC, that word should land differently. Because Gartner is not describing a future state. They are describing what is already happening.

We Solved Detection. We Never Solved Execution.

Here is what most cybersecurity vendors will not tell you: we solved detection years ago. Between EDR, NDR, SIEM, and the alphabet soup of monitoring tools, the average enterprise generates somewhere between 10,000 and 100,000 alerts per day. The data is there. The signals are there.

What is not there is anyone to act on them.

ISC2's latest data puts the global cybersecurity workforce gap at 4.8 million professionals, growing at 19% year over year. That is not a gap you hire your way out of. That is a structural failure in how the industry operates.

And the numbers tell the story. In a recent study of AI-automated incident response, 74,826 out of 75,000 alerts were filtered and resolved autonomously. Only 174 required human review. Of those, just 38 were true positives. The technology to execute at machine speed exists. The question is whether organizations are willing to let it.

The Three-Tier SOC Was Built for a Different Era

The traditional SOC, with Tier 1 analysts triaging alerts, Tier 2 investigating, and Tier 3 doing threat hunting, was designed when a major enterprise might process a few hundred incidents per week. That model assumed human attention was the bottleneck, but it was a manageable bottleneck.

In 2026, that assumption is laughable. Attackers are leveraging AI to personalize attacks at scale, generating novel malware variants for each target. IBM X-Force observed a 44% year over year

increase in the exploitation of public-facing applications. North America became the most attacked region for the first time in six years, accounting for 29% of all incident response cases.

The three-tier model was not built for this volume, this velocity, or this sophistication. And adding more humans to the conveyor belt is not a strategy; it is a coping mechanism.

What Agentic AI Actually Means for Security Operations

Let me be precise about what "agentic" means here, because the term is already being diluted by marketing departments across the industry.

An AI copilot suggests actions. A human decides. A human executes.

An AI agent reasons, acts, observes the result, and adjusts autonomously. It does not wait for a human to click "approve." It operates within defined guardrails, but within those guardrails, it moves at the speed of the threat, not the speed of a shift change.

Gartner forecasts that 40% of enterprise applications will feature task-specific AI agents by the end of this year. Yet only 6% of organizations have an advanced AI security strategy in place. That is a 34-point gap between adoption and governance, and it is where the real risk lives.

The agentic SOC is not about removing humans. It is about redefining what humans do. In a well-designed agentic model, Tier 1 and Tier 2 work is automated entirely. Human operators become strategic: they set policy, define response parameters, handle edge cases, and focus on adversary behavior that requires judgment, not pattern matching.

The Uncomfortable Truth About Human in the Loop

Every vendor in cybersecurity right now is saying "human in the loop." It is the safety blanket phrase that makes boards comfortable and keeps procurement moving.

But here is the uncomfortable truth: if your human is in the loop for every decision, you do not have automation. You have a suggestion engine with extra steps.

The organizations that will define the next era of cybersecurity are the ones willing to put humans *on* the loop, overseeing, governing, and course-correcting, rather than *in* the loop approving every action. That

is the difference between a SOC that responds in seconds and one that responds in hours.

Forrester's research supports this directly: AI-led detection and response can reduce incident response times by up to 70%. But that reduction only materializes when the AI is empowered to execute, not just recommend.

What Security Leaders Should Do This Quarter

First, audit your alert to action ratio. How many alerts does your SOC generate per day? How many result in an actual response action within 60 minutes? If that ratio is below 5%, you have a detection system masquerading as a security program.

Second, map your response workflows honestly. Identify every step that requires a human to click, approve, or copy-paste between tools. Each of those steps is latency, and latency is the attacker's advantage.

Third, have a candid conversation about what "human in the loop" means for your organization. Is it a governance framework, or is it a bottleneck you have given a comforting name? The answer to that question will determine whether your SOC is ready for what 2026 is bringing.

The SOC is not dead because it failed. It is dead because it succeeded, at a problem the industry has already moved past. Detection is solved. Execution is the new frontier.

The organizations that thrive in this new landscape will not be the ones with the most analysts. They will be the ones that figured out how to let machines execute at machine speed while humans govern at human wisdom.

The agentic SOC is not coming. It is here. The only question is whether your organization is ready to stop watching and start acting.

To discuss how your organization can prepare for the agentic SOC era, visit arbitium.com/contact.

John Remo is the Co-Founder and CEO of Arbitium, an autonomous AI execution platform for cybersecurity. He previously led engineering and security operations for global enterprises.

Sources referenced: Gartner Top Cybersecurity Trends 2026; ISC2 Global Cybersecurity Workforce Study 2025; IBM X-Force Threat Intelligence Index 2026; Forrester Security Predictions 2026; World Economic Forum Global Cybersecurity Outlook 2026.