

6 minute read

I've spent a lot of time recently talking about the "catastrophe of the week." It feels like every time a new AI model drops, half the industry wants to declare the "end of security" while the other half wants to run for the hills, buy a log cabin, and live off-grid with nothing but a pen and paper.

The latest trigger is Anthropic's [Claude Mythos](#). I recently sat down with Doug Woodburn at IT Channel Oxygen to discuss [whether this really is the doomsday scenario some are making it out to be](#). There is no doubt that Mythos is a significant technical accelerator; it can find vulnerabilities in minutes that used to take human teams months to track down. But we have to remember that while the speed has changed, the nature of the threat is something we have dealt with for years. It is a tool for efficiency, not a total reimagining of how attacks work.

At SEP2, we aren't panicking. Instead, we are looking at how to use that same efficiency for the "good guys." Darren Swift, Senior Customer Engineer at Google touched on this at our Cyber Summit last week - while adversaries are using LLMs to automate 70% of the MITRE matrix, we are moving toward self-defending systems that can deploy security fixes in real-time.

If an AI model can discover a decades-old bug overnight, defensive tools like Google's *Code Mender* can help us automate the remediation just as fast. The headlines love the hyperbole, but we've survived every "game-changer" so far by staying grounded in engineering rather than buying into the hype.

Speaking of staying grounded in what works: I want to say a huge thank you to everyone who joined us for our annual SEP2 Cyber Summit last week. To our attendees, thank you for the honest conversations and for making the day so high-energy.

If you weren't able to make it, we've distilled the key strategies from the day [here](#).



Paul Starr

Co-Founder and CEO

---

## Key Takeaways from SEP2 Cyber Summit

If you couldn't make it to our SEP2 Cyber Summit this year, we've made a quick PDF for you to read. Here is a snapshot of what we discussed on the day:

### The Rise of the Agentic SOC

In my keynote, I spoke about the "22-second reality." That is the window we are seeing today where an adversary hands off a compromise to a ransomware unit. To beat that, we've moved SEP2 away from slow, tiered structures to an engineering-centric "**swarm**" model powered by **Wingman AI**. We are bringing AI into our SOC to accelerate our people, not replace them.

"We are a tech-driven, people-powered organisation. AI handles the noise so our engineers can focus on the fight."

### Context Over Endless Lists

Julia Weimer, Director of Solutions Engineering UKI at Wiz challenged the futility of traditional vulnerability management. Instead of chasing flat lists of 100,000 CVEs, Julia showed why we must shift to a **horizontal context graph** to find the actual attack paths that matter.

Over 50% of Wiz users now sit outside of security departments—putting data in the hands of developers is what actually drives remediation.

### The Self-Defending Network

Darren Swift, Senior Customer Engineer at Google explored the horizon of **machine-speed defence**. As attackers automate 70% of their work, Google is moving toward **self-healing systems** that can mathematically prove and deploy security fixes in real-time.

We have to impose a "Reconnaissance Tax" on attackers by using ephemeral cloud environments that make scanning your network too expensive to be worth it.

### Bridging the AI Trust Gap

Charlotte Wilson, Head of Enterprise Business UKI at Check Point addressed the "chaos" of rapid AI code generation. Without continuous human-in-the-loop governance, software agents can quickly "go rogue" and drift away from your corporate security policies.

"There is no single vendor that can fix all your AI problems. If they say they can, they're selling you snake oil."

[Read the full Cyber Summit Key Takeaways](#)

---

## News

### Securing the Future with Google & Wiz in Dublin

[In Person Event](#)

On 14th May, we're hosting an exclusive morning at the Google Docks in Dublin to explore the next frontier of cloud security. Join our Head of Technology, James Woodward, and Google's Ricky Francelli to discuss the "Agentic SOC" and how the industry-defining Google-Wiz acquisition is transforming multicloud defence. Spaces are limited, so register now to join us for live threat intel demos, breakfast, and networking.

[See you there](#)

### Share Your Wingman MDR Experience on Gartner Peer Insights™

If you're a Wingman MDR customer, we'd love for you to share your experience on Gartner Peer Insights™. Your honest feedback is invaluable in helping us continually improve our service and showcasing its effectiveness to the wider market. It's a quick, anonymous process that makes a real difference. Plus, you'll receive a **\$25 voucher** once your review goes live!

[Share your experience](#)

### SEP2 Wins Big at Check Point UK Partner Awards

We are thrilled to announce that SEP2 took home two major trophies at this year's Check Point UK Partner Awards: **Technical Services Partner of the Year** and **Hybrid Mesh Network Security Partner of the Year**.

As an Elite Partner, our focus has always been on technical excellence. These awards recognise the hard work of our engineering team, who now resolve **over 97% of Check Point support tickets in-house**, ensuring our customers get expert answers without the wait.

[Read more](#)

---

"Working with SEP2 means we are no longer fire-fighting; rather we can now take a step back and proactively get things sorted."

- Peter Grimley, Infrastructure Manager at Wrexham County Borough Council

[Learn more about Wingman Secure Access](#)

---

Thank you for reading this edition of Wingman Insights!

I'd really value your feedback on how you're enjoying it so far. What's working, what could be better? [Share your thoughts](#).