**Wingman Insights**
*Tech Driven. People Powered.*
*September 2026*

*3 minute read*

We wrapped up August with our first-ever SEP2 Summer Party, bringing together Team SEP2 and their families for a well-deserved day of fun to thank the people who support us behind the scenes every single day. A personal highlight was when my daughter looked around and asked, “Dad, why are there so many people here? How many people actually work for SEP2?!”. Having known SEP2 most of her life, seeing her realise how much we've grown meant the world to me.

The party was a great reminder of why we adopted the ‘4ugust’ initiative back in 2022. Operating a 24/7/365 SOC means we have to adapt how we give our team that time back - which is how ‘SOCtember’ was born. As September begins, I hope our team continues to find time to refresh and ease into the new school year.

Moving from our people to our tech, this month marks a major milestone for our SOC operations. A year ago, we announced our strategic partnership with Google Cloud to embed Google Threat Intelligence (GTI) directly into the heart of SEP2.

In our featured article this month, JC breaks down how we’ve maximised GTI over the past 12 months - from stopping dark web identity hijacking before breaches occur to speeding up threat hunting with VirusTotal and our autonomous AI agent, Casey. He also shares frontline telemetry on the sectors targeted most right now and how Mandiant intelligence is helping us neutralise state-aligned campaigns.

**Paul Starr**
Co-Founder and CEO

---

## Neutralising Identity Hijacking with GTI and Casey

Over the past 12 months, nearly every organisation evaluated on our *Wingman MDR Enhanced* service had employee credentials surfaced on dark web forums or illicit leak sites. In one recent incident, an employee used their corporate identity for an external third-party tool, exposing direct access to Microsoft Entra ID and critical financial portals.

Thanks to real-time dark web interdiction, our SOC contained the threat before attackers could execute cloud-native session hijacking.

It has been one year since SEP2 officially embedded Google Threat Intelligence (GTI) directly into our 24/7 UK-based Security Operations Centre. By combining VirusTotal’s massive malware corpus with Mandiant’s frontline intelligence, our SOC is actively blocking threats, ranging from edge exploitation in Legal and Manufacturing sectors to Russian-nexus disruption campaigns targeting UK infrastructure.

To keep pace with these evolving vectors, we also launched our Agentic SOC featuring Casey, our autonomous AI Investigation Agent. Casey instantly correlates GTI threat feeds to evaluate context, score risk, and adapt our detection libraries in real time.

Read my blog for a closer look at our latest SOC telemetry, industry breakdowns, and real-world case studies.

**Jon Cumiskey**
Head of Information Security

---

## Protecting Our Customers

Eagle Eye simplified their Google SecOps setup and accelerated their transition to cloud-native security with expert, hands-on guidance from SEP2.

*"We were early on in our journey of implementing cloud-native cyber security, and SEP2 made it easy."*

- Max Kruger, Director of Technology at Eagle Eye

See just how they did it

---

## Where You’ll Find Us

**Google Security Masterclass London**
*9th September, Google Office London*
Join us in London for an exclusive masterclass session where we share a practical blueprint for building, implementing, and managing a mature, scalable SecOps framework.
Register for the Masterclass

**SEP2 and Wiz Breakfast Briefing**
*September 10th, Duck and Waffle, London*
Join SEP2 and Wiz for an exclusive morning briefing exploring practical strategies for AI threat defence, real-world cloud security, and actionable threat intelligence. Get first-hand insights on securing scaling infrastructure via Wingman Cloud, engage in peer-to-peer discussions on high-growth sector security, and network with fellow C-level decision-makers.
Grab breakfast with us

**Securing the AI and Cloud Era**
*September 17th, The Culloden Hotel, Belfast*
As AI and cloud technologies continue to reshape the enterprise landscape, staying ahead of modern threat actors requires a collaborative approach to security. We’re teaming up with our partners at Google, CrowdStrike, and Check Point for an exclusive morning dedicated to practical strategies, live insights, and cutting-edge approaches to securing multi-cloud ecosystems.
Save your spot

**Wingman Security Connect**
*September 24th, Royal Armouries, Leeds*
It’s back! After the success of last year’s northern event (including a heated debate on whether pineapple should be on pizza) we’re gathering at Leeds Royal Armouries this year for a day of sharp insights, networking, and letting off some steam at a crossbow shooting challenge.
It’d be great to see you there!
Register your interest

---

## What's New at SEP2

**If you’re stuck in reactive firefighting mode, watch this.** Learn how real-world co-development with Spectrum enabled us to build EMEA's first Agentic SOC, cut response times, and scale threat coverage effortlessly in our interview on the Detection-First Agentic SOC.

**Struggling to disconnect?** I recently spoke with IT Channel Oxygen to discuss my approach to digital burnout, phone distraction, and the constant battle to step away from the screen.

**Great support comes from engineers who actually get what you're going through.** See how Fabian Reid is bringing years of hands-on experience and genuine customer care to our team in our interview on engineering-led Customer Success.

**What does the industry's biggest cloud security move mean for multicloud defense** and your operational strategy going forward? Read our detailed breakdown Beyond Google's Wiz Acquisition.

---

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.

---

51a St Paul's Street
Leeds
LS1 2TE

0330 043 7372
info@sep2.security