TECH DRIVEN. PEOPLE POWERED.

Solution Brief: Wingman Threat Intelligence

In a rapidly evolving threat landscape - now accelerated by the rise of AI-driven attacks - access to verified, actionable threat intelligence is no longer a luxury: it is a necessity. However, for many organisations, the prohibitive costs of top-tier vendors and the intensive engineering resources required to manage these advanced platforms remain significant barriers to entry.

Wingman Threat Intelligence has been designed to eliminate these barriers. We provide a fully managed, results-oriented service that transforms vast streams of threat intelligence data into precise, actionable guidance tailored to your specific environment.

By leveraging our strategic OEM Threat Intelligence partnership with Google, we harness the immense global visibility of Google's native telemetry, combined with Mandiant frontline insights and VirusTotal Indicators of Compromise (IOCs) to fuel our operations. This top-tier intelligence is delivered as actionable outcomes by our 24/7/365 UK-based SOC, ensuring your organisation stays ahead of tomorrow's threats, without the burden of hefty vendor costs or management overhead.

Key service outcomes

The Wingman Threat Intelligence service provides several critical outcomes to strengthen your security posture:

Customised Risk Profiles	Stay ahead of threats with a real-time intelligence profile tailored to your unique organisation. We provide curated IOCs and TTPs specific to your industry, vertical, and size. Gain visibility into how similar organisations are being targeted and receive actionable SEP2 recommendations to harden your estate.
Deep & Dark Web Visibility	Discover threat actors referencing your data in Underground chat forums, create monitors for leaked usernames and passwords and be notified of attackers attempting to impersonate your organisation via domain protection alerts.
On-Demand Intel Requests	Obtain detailed reports regarding which specific threat actors are targeting your organisation, as well as their known Tactics, Techniques, and Procedures (TTPs) or gain information on IOCs which your organisation is concerned about.
Attack Surface Management (ASM)	Increase the visibility of your external attack surface by mapping risks across networks, code repositories, and supply chains to alert upon unseen vulnerabilities which attackers could leverage, as well as SEP2 expert recommendations on resolution steps.

Our OEM Partnership

Driven by our commitment to be “Tech Driven, People Powered,” SEP2 has made a significant investment to become a strategic OEM partner for Google Threat Intelligence.

This elite status enables us to deliver a service focused on premium, intelligence-led outcomes for customers, who may have previously found this cost-prohibitive. From identifying dark web threat actors to delivering granular remediation advice, we empower organisations of all sizes to transition from reactive cycles to proactive resilience.

Digital Threat Monitoring (DTM)

DTM workflows extend your security perimeter into the deep and dark web to identify threats before they manifest as active breaches. Our service provides proactive visibility into leaked credentials, brand impersonation, and ransomware preparation, allowing you to understand exactly how your organisation is being targeted externally.

Key DTM capabilities of our Wingman Threat Intelligence service include:

- **Compromised Credentials & Data Leak Detection:** We continuously monitor the deep and dark web for leaked usernames, passwords, and sensitive corporate information.
- **Brand & Domain Protection:** Our team can highlight malicious domains that mimic or impersonate your organisation and monitor for mentions of your hosts and netblocks in underground machine-access listings.
- **Infrastructure & Supply Chain Vigilance:** Detect mentions of your network vulnerabilities by Initial Access Brokers on the dark web and provide critical visibility into potential ransomware attacks or threats facing your supply chain partners.

Attack Surface Management (ASM)

ASM provides the continuous visibility required to proactively manage your external footprint. By gaining an “attacker’s view” of your organisation from the outside in, we can identify unknown assets, vulnerabilities, misconfigurations, and other issues within your organisation, before they are exploited.

Key ASM capabilities of our Wingman Threat Intelligence service include:

- **Continuous Asset Mapping:** We identify all internet-facing assets - from known and unknown domains to IPs, cloud storage buckets and even code repositories.
- **Vulnerability & Exposure Assessment:** Our team can identify misconfigurations, application-layer issues, and expired certificates across your critical infrastructure and web applications.
- **Authenticated Cloud Discovery & Assessment:** Scan for vulnerabilities across your cloud infrastructure

The SEP2 Difference

- **24/7/365 UK-Based SOC:** Our Leeds-based, ISO27001-certified SOC triages every ASM and DTM alert, transforming complex threat signals into actionable guidance so your team can focus on remediation, not investigation.
- **Flexible Integrations:** We can deliver alerts through your preferred channels using your native toolsets such as Slack, Teams, Jira, or ServiceNow - ensuring escalations via familiar workflows.
- **Continuous Service Refinement:** Through regular service reviews, we continuously tune your DTM and ASM monitors, as well as maintain your customised threat profile, ensuring the threat intelligence insights provided remain relevant as your organisation grows.
- **Strategic Reporting:** We can provide both C-suite and technical-level reporting, giving your leadership a clear understanding of your external security posture, the threats facing your organisation and the Return On Investment (ROI) of the service.

A Service Tailored to Your Needs

At SEP2, we recognise that not every organisation has the same needs, nor are they at the same place in their cybersecurity journey. Whether you are a growing SME or a large enterprise, Wingman Threat Intelligence is available in tiered packages designed to provide the right level of protection and insight for your specific environment.

If you would like to discuss how Wingman Threat Intelligence help protect your organisation, please get in touch: info@sep2.security