



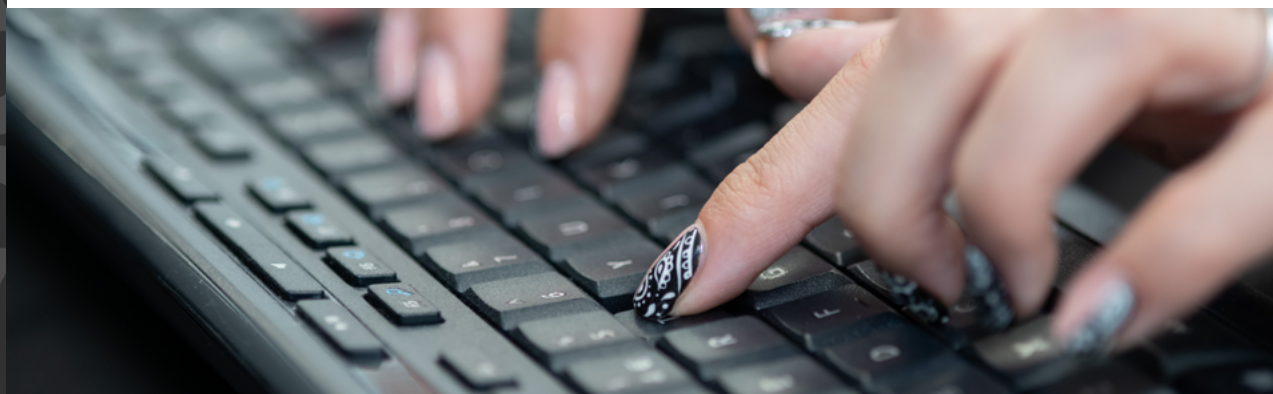
TECH DRIVEN. PEOPLE POWERED.

Solution Brief: Wingman Managed Detection and Response (MDR)

As enterprise environments grow more complex and threat actors execute attacks with unprecedented velocity, traditional, reactive detection and response are no longer enough. To survive the modern threat landscape, organisations need to look at their security posture through an intelligence-led, proactive lens.

Our Wingman MDR service is designed from the ground up as a Managed Detection and Response service that will fit your environment and deliver optimal levels of support. This is a turnkey, premium managed service that fully unifies our advanced Agentic AI framework with the global visibility of Google Threat Intelligence and the core analytics of Google SecOps (SIEM & SOAR), all delivered as a service by our UK-based 24/7/365 staffed SEP2 SOC.

SEP2 is trusted by some of the most well-known UK brands and enterprises ensuring peace of mind and robust protection against evolving cyber threats.





SEP2 provides round-the-clock, eyes-on security coverage from our dedicated SOC in Leeds, UK. Our team investigates threats, responds to alerts, and guarantees uninterrupted incident management. The SEP2 SOC is staffed entirely by SEP2 employees - no outsourcing, no subcontracting, and no offshoring.

The SOC Workflow

The SEP2 SOC combines deep analyst expertise with advanced Agentic AI agents to protect our customers' environments and accelerate threat containment.

When a case opens, our in-house AI agent Casey automatically executes initial triage. Casey performs instant SIEM searches across your wider estate, enriching data within security cases with cross-platform telemetry and threat intelligence insights, proposing upward severity reclassifications where needed.

Casey operates strictly within a human-driven loop, removing the toil and mundane tasks from our team of analysts, allowing them to focus on higher priority items. This significantly improves MTTD/MTTR rates while placing rich contextual intelligence directly at our analysts' fingertips.

By leveraging Casey, it enables our SEP2 SOC team to rapidly validate security findings, perform deep-dive analysis, and escalate

verified threats, all while ensuring each case is carefully checked by humans before any escalation or remediation action takes place.

SEP2 engages daily with customer data, leveraging security insights across their environment and investigating all suspicious behaviour, regardless of alert severity (Critical, High, Medium, or Low). There are no limitations on the time dedicated by SEP2 Analysts to the discovery and investigation process. Our solution ensures strict adherence to agreed-upon Service Level Agreements (SLAs) for response times. All insights provided by Agentic SOC agents are checked and validated by our elite team of analysts before any action is taken upon them.

Once SEP2 identifies threat actor activity that requires immediate action, we can initiate pre-approved remote response actions such as isolating hosts or disabling user accounts via semi-automated or pre-approved fully-automated SOAR playbooks.



Our Open Book Approach

Transparency is a core value at SEP2, which is why our live case-handling notes are completely visible for every alert received. These comprehensive notes provide immediate clarity regarding what is happening in a security case - via natural-language summaries generated by a security-grounded version of Google Gemini - along with our granular technical analysis from our expert SOC team, detailing key entities involved, root causes, and explicit remediation steps.

Extensible technology stack

Powered by Google SecOps, Wingman MDR provides a minimum of 365 days of hot log storage, allowing telemetry to be immediately searched, and provides seamless integrations across your entire digital estate, whether you leverage on-premises infrastructure, multi-cloud environments, third-party security logs, or custom internal applications. This extensible architecture enables real-time threat detection, rapid investigation, and coordinated response capabilities tailored to your organisation's needs.

Immediate Value, Seamless Integration

Wingman MDR is engineered for rapid deployment and immediate impact. We establish fast security coverage using a foundational telemetry baseline, instantly backed by pre-tuned playbooks, workflows, and continuously evolving detection analytics for high-quality threat handling from day one. Underpinned by Google SecOps, Wingman MDR is a fully vendor-agnostic solution which integrates seamlessly with your existing security stack, maximising your protection without displacing your current investments.

Engagement focus

This is a service designed to fit your team. We offer flexible collaboration options tailored to your preferences and working style, whether it's through your ticketing system, Slack, Teams, Google Chat, or email. Additionally, we adapt our communication frequency to a plan that best suits your team's needs and workflow.





Rapid standup

If you need expedited onboarding as part of your plan, SEP2 offers a Rapid Standup service for certified EDR products as well as your critical assets, including your Identity Provider. SEP2 aims to commence live monitoring services within 14 days of when onboarding activities commence, providing you with immediate value while we continue to integrate more deeply into your environment over time.

Service levels

At SEP2, we recognise that not every organisation has the same needs, nor are they at the same place in their cyber security journey. To help cater to all, Wingman MDR is available in different packages designed to best fit all types and sizes of organisations.

From baseline deployment support for in-house technical teams, to advanced Agentic-AI triage, hands-on SEP2 analyst response, and proactive threat hunting, Wingman MDR provides a flexible, scalable model to elevate your cyber security defences.

For organisations seeking complete visibility, our Enhanced package extends protection beyond internal log feeds with proactive Attack Surface Management (ASM) and Digital Threat Monitoring (DTM) coverage across the deep and dark web. This advanced layer combines customised threat profiling with emerging threat detections to neutralise external risks before they impact your estate, moving your business from a state of defensive reaction to absolute operational resilience.

This flexible model ensures you receive the exact level of capability you need today, with the seamless ability to scale as your environment evolves.





Review our service level table below to find the ideal package for your organisation:

*BESPOKE PACKAGE AVAILABLE. ADDITIONAL SERVICES ON REQUEST.

FEATURES*	STANDARD	ENHANCED
DEPLOYMENT AND TROUBLESHOOTING		
365 DAYS OF LOG STORAGE		
SOAR ACCESS		
CUSTOM DETECTION RULES		
VENDOR ISSUE ESCALATION		
24X7 THREAT RESPONSE		
UNLIMITED CHANGE REQUESTS		
LOG SOURCE MONITORING		
HUMAN EYES-ON THREAT CONFIRMATION		
DETAILED THREAT INVESTIGATION		
THREAT HUNTING		
SERVICE REPORTING AND SERVICE REVIEWS		
DIGITAL THREAT MONITORING (DEEP & DARK WEB MONITORING)		
ATTACK SURFACE MANAGEMENT		
CUSTOMISED RISK PROFILE (THREAT PROFILING)		
MANDIANT EMERGING THREAT DETECTIONS		

*NDR AND DFIR AS ADD ONS

SEP2 also offer EDR. Interested in our Wingman Extended Detection and Response (XDR) service? Get in touch at info@sep2.security