TECH DRIVEN. PEOPLE POWERED.

Solution Brief: Wingman Managed Detection and Response (MDR)

As enterprise environments grow more complex, reliable threat detection and response becomes non-negotiable. Having the ability to consistently respond to threats across technology silos and in a timely manner is crucial for organisations. Our Wingman MDR service, powered by Google SecOps, is designed from the ground up as a Managed Detection and Response service that will fit your environment and deliver optimal levels of support. Built on the core technology of SIEM, SOAR and Google Threat Intelligence, and delivered as a service by our UK-based 24/7/365 staffed SOC, Wingman MDR brings detection and response capabilities to organisations of all sizes and types.

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 staffed, eyes-on 24/7/365 services from our dedicated SOC in Leeds, UK. The SOC investigates threats, responds to alerts and guarantees uninterrupted handling of our customers' security incidents around the clock. The SEP2 SOC is fully staffed by SEP2 employees: no outsourcing, no subcontracting & no offshoring.

The SOC Workflow

The SEP2 SOC team possesses extensive expertise in protecting our customers' environments against threats, creating detection rules, and leveraging threat intelligence in their workflows.

We engage 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 volumes of time dedicated by SEP2 Analysts to the discovery and investigation process; however, our solution ensures strict adherence to agreed-upon Service Level Agreements (SLAs) for response times.

Once SEP2 identifies threat actor activity that requires immediate action, we are able to initiate pre-approved remote response actions such as quarantining hosts or disabling user accounts.

Open book analysis approach

Our case handling notes are visible to our customers for every alert received. This commitment to openness sets a new standard for transparency and accountability, showcasing our dedication to service excellence as a market-leading provider.

Extensible technology stack

Wingman MDR provides up to 365 days of searchable data and a wide variety of integrations, ensuring that the system suitably reflects your environment - whether it be through on-premise infrastructure, multi-cloud, off-the-shelf security logs or custom tooling and internal applications. Our service is powered by Google SecOps, which facilitates real-time threat detection, investigation and comprehensive functionality for undertaking response actions.

Immediate Value, Seamless Integration

Wingman MDR is a turnkey solution designed for rapid, effective deployment. We start with a minimum viable set of telemetry to quickly establish security coverage, which is immediately supported by our predefined and pretuned processes. This includes a standard playbook of workflows, procedures, and analytics, ensuring consistent and high-quality threat handling from day one. Our detection content is also regularly evolving to keep pace with the latest threat actor techniques. Furthermore, while underpinned by Google SecOps, our service is technology agnostic and provides integration with third-party detection and response technologies beyond our core platform, ensuring full value from your existing security 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 alongside critical assets. SEP2 aims to commence live monitoring services within 14 days of receiving your order, giving you 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 basic deployment and support services for organisations with skilled technology teams of their own, to automated threat confirmation and investigation, and even fully managed threat hunting, Wingman MDR offers a spectrum of solutions to enhance and improve your cyber security.

*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