Managed Detection and Response Services

G-Cloud Service Description

April 2023

Contents.

1. MAINTEL CYBERSECURITY. 2

2. SERVICE OVERVIEW. 3

2.1: Benefits 3

2.2: Outcomes 4

2.3: Timescales 4

2.4: Five-Stage Onboarding Plan 5

2.5: Service Offboarding 5

3. SERVICE MANAGEMENT. 6

3.1: Customer Success Team 6

3.2: Service Level Agreements 6

3.3: Key Performance Indicators 7

3.4: Ongoing Training 7

4. OPTIONAL EXTRAS. 8

4.1 : Phishing 8

4.2: Endpoint Detection and Response Management 8

5. SERVICE CONSTRAINTS. 9

1. Maintel Cybersecurity.

MDR provides round-the-clock monitoring, detection, and response to potential threats.

The service includes:

- Continuous monitoring of the network for suspicious activity
- Advanced threat detection using artificial intelligence and machine learning.
- Rapid response to potential threats to mitigate damage.
- Expert team available 24/7 for support and consultation
- Regular reporting and analysis to track security performance.

Maintel MDR enhances your cyber security defences, taking full advantage of existing security tooling.

This service aims to work in alignment with your future strategic roadmap, continuously refining your defensive posture and maximising the ROI from your existing security capability and the MDR Service.

This is a 24/7/365 MDR service delivers a wide range of benefits which may help to protect your core business capability and enable you to focus on your future business goals.

Highly trained and capable Security Consultants quickly identify, mitigate, and defend against threats and threat actors, allowing you to focus internal capability on other key priorities.

2. Service Overview.

Tailored components of the service ensure complete alignment with your organisation.

- Workshops and in-depth discussions to fully understand the digital environment, threat landscape and risk appetite.
- Alignment of communication flows between operating teams and stakeholders.
- Integration of in-house and custom rules built specific to your environment.
- An agreed approach of how and when automated mitigation responses are actioned.

2.1: Benefits

- High speed deployment.
- Operated and supported from UK-based Security Cleared (SC) analysts.
- Reduced cyber risk and enhanced security posture for a fraction of the cost of building an internal team with the necessary capabilities.
- The service supports compliance and regulatory obligations, tailored around your organisation to support all necessary reporting responsibilities. Data ownership, segregation, residency, security, and compliance is strictly enforced according to your needs.
- Industry leading mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR). Our advanced automation swiftly identifies and mitigates typical cyber threats, ensuring proactive response to critical threats.
- Rapidly reduced threat mean-time-to-contain (MTTC) through wire-speed analysis and automated mitigating actions.
- Fixed price model, based on the size and scope of your environment, providing reassurance of consistent payments, and allowing you to forecast without the worry of yearly increases.
- We will continually integrate the service with the latest detection rules and hand select new tooling through meticulous market research. We are not tied down to any single tooling or vendor, meaning our recommendations are focussed on what will work best for your organisation.
- Continuous operation, with no need for maintenance downtime. New rules, changes or additional tooling are delivered live after detailed testing requirements have been achieved in test environments by our expert analysts.
- 24x7x365 threat detection, response, isolation, mitigation, and remediation.

2.2 : Outcomes

- Risk reduction delivered via automated mitigation actions, stopping a cyber incident becoming a business impacting breach.
- Complete visibility with no compromise on endpoints being monitored.
- Operational alignment achieved by response communication integration, removing any friction and gaps between cyber teams.
- Accountability and partnership through a robust Service Management framework, providing contextual and timely information between both parties and all relevant stakeholders.
- Our SOAR platform automatically enriches alerts using multiple Threat Intelligence sources, providing you with comprehensive incident details for confident decision-making.
- Continual improvement throughout the service lifetime, from as small as regularly updated rules that block new threats to additional integrated tooling that further enhances your security. This is all at no additional cost.

A robust onboarding process ensures rapid security deployment, contingent upon your collaboration for necessary approvals and access. This guarantees swift and effective security, whilst granting our engineers sufficient time to fine-tune automation rules and playbooks, preparing seamlessly for integration into our live SOC environment.

The onboarding of the service is operated as a project, with an aligned Project Manager and team of engineers responsible for the process.

Critical milestones are communicated and agreed with your key stakeholders.
A process of Threat Modelling ensures the solution coverage is appropriate to protect against threats specific to your organisation and common threats in the UK public sector.

Onboarding of the service will be scheduled to take place during normal UK business hours of 09:00 - 17:30.

2.3 : Timescales

Typically lasting 12 weeks, the key milestones aligned with our onboarding process consist of:

Week 1	Deployment of SIEM and integration with threat intelligence feeds.
Weeks 2 to 5	Onboarding and tuning of critical log sources into the SIEM, with 24/7/365 monitoring and management by our expert analysts.
Weeks 6 to 12	Onboarding of non-critical log sources, completing the onboarding phase and transitioning to service.

2.4 : Five-Stage Onboarding Plan

Stage 1	**Preparation (1 to 2 Weeks before Kick-Off)** During final commercial stages of the contracting process, we prepare for kick-off by assigning a Project Manager, scheduling introductory calls, Threat Modelling workshop and data collection to identify critical and non-critical log sources.
Stage 2	**Kick-Off and Design (Week 1)** We engage in collaborative design through a kick-off workshop, requirements analysis, environmental assessment, connectivity definition, asset scoping, roadmap building and Solution Design document production. We initiate deployment of the SIEM and configuration review for existing email/communications security tooling.
Stage 3	**Deployment (Weeks 2 to 5)** Focused onboarding of critical log sources and SIEM rules in the SIEM. Ongoing workshops and calls with technical and leadership teams ensure effective monitoring and managed detection and response to threats that occurring during the onboarding service.
Stage 4	**Tuning (Weeks 6 to 12)** Repeat the cycle, now focusing on non-critical log sources. Ongoing support to ensure "business as usual" activities are uninterrupted. Continuous testing and tuning of SIEM output for optimal performance.
Stage 5	**Transition to Service** Following sign-off that onboarding phase is complete, the project team will handover to Customer Success for ongoing service management throughout the remainder of the contract. Minor snagging issues may be handed over to Customer Success team to resolve (with your agreement) so that the onboarding project can be concluded and transitioned to our full live service.

2.5 : Service Offboarding

Whilst we aim to retain our partnership with you for as long as possible, we also want to make sure that any transition of capabilities happens smoothly, and therefore part of our service is to ensure that the exit of a customer from the service is conducted professionally and reliably. We will jointly ramp down the service(s) provided by handing back responsibilities. A joint offboarding plan will be created.

3. Service Management.

3.1: Customer Success Team

The Customer Success team ensures you derive maximum value from your investment by providing comprehensive ongoing support and communication. During onboarding, you will be assigned a Customer Success Manager (CSM), whose primary responsibility is to foster a positive and collaborative experience throughout the service period. The CSM will support evolving needs through intimate knowledge of your service and effective communications. The CSM ensures the continued success of the overarching service, as well as adherence to the contracted SLAs.

3.2: Service Level Agreements

Specific service level agreements will be defined throughout onboarding, based on different threat types, impact to operational technology and overall service impact. We can, and do, visit clients' sites as part of the relationship management aspects of the service.

The following table illustrates our standard service levels.

Priority	Impact	Notification	Update within
P1	Critical	30 minutes	1 hour
P2	High	60 minutes	2 hours
P3	Medium	4 hours	4 hours
P4	Low	12 hours	12 hours

Critical (P1)	Widespread breach impacting multiple elements of organisation's infrastructure. Includes IP theft, damage to multiple production systems or serious e-crime. Public services, the corporate network and/or systems would be directly affected, and automatic mitigations may not be in place.
High (P2)	Unauthorised access to a mission-critical system. The core network has been targeted and a threat is present. P2 Incidents require hands on investigation from an analyst.
Medium (P3)	Generic malware or suspicious activity is detected on the network. The threat is present, but processes are in place to mitigate the risk and protect the network. Detections inside a DMZ may be classified as Medium.
Low (P4)	Low priority security alert that poses no serious threat to the organisation. This may include a reported SPAM email or an unknown connection to Guest Wi-Fi.

3.3: Key Performance Indicators

Service Area	KPI/Priority/Impact	KPI/SLA Performance (Targets Measured Monthly)	Service Credit Per Monthly Service Period
INCIDENT: Assign and respond. This is the time taken from the alert being analysed by the SOC and the incident being raised to you with initial findings	**P1- Critical**	98% < 30 minutes	10% service credit of the monthly charge for the service line in the reporting month for non-adherence.
	P2 - High	98% < 60 minutes	5% service credit of the monthly charge for the service line in for the reporting month for non-adherence.
	P3 -Medium	98% <4 hours	N/A
	P4 - Low	98% < 12 hours	N/A
INCIDENT: Through-life management – Incident Response. This is the time taken from the completion of any response action(s) and the notification of their completion (resolution) to you (including any further recommendations where relevant).	**P1- Critical**	98% < 30 minutes	5% service credit of the monthly charge for the service line in the reporting month for non-adherence.
	P2 - High	98% < 60 minutes	3% service credit of the monthly charge for the service line in for the reporting month for non-adherence.
	P3 -Medium	98% < 4 hours	N/A
	P4 - Low	98% < 12 hours	N/A

3.4: Ongoing Training

To ensure everyone has a complete understanding of the solution and how it functions, we will set up training sessions and ongoing workshops to go over the service as a whole, as well as individual parts where necessary.

Where different parts of the organisation have different requirements, we will tailor the sessions around you. This is included as part of the flat rate onboarding and ongoing service costs.

Some examples of training and support include:

SIEM Workshops	As the main data monitoring tools for the service, these are crucial to the everyday delivery of our security monitoring service. Custom workshops will advise how to review incidents, how to investigate specific events and how to make best use of your dashboards.
EDR Tooling Workshops	Led by our engineering team, we will review your EDR tooling's configurations and advise remediation activities to bring in line with best practice coverage and configuration. We advise these workshops are best done at least annually.
Threat Modelling Workshops	Conducted during onboarding, and then annually thereafter, these sessions test our understanding of your environment and critical business processes. From these sessions we will validate our understanding of your environment, making updates to our solution where necessary or providing remediation activities to be completed internally.

4. Optional Extras.

This section outlines optional extras that will incur a charge.

4.1 : Phishing

A Security Review of emails submitted to the MDR team by your security team from your users (this is not a direct to user service). Where a malicious email has been identified you will be notified (not the user) if there are any actions to be taken.

- MDR team will automate the initial triage and analysis of a suspected email to ensure a consistent approach Is taken for every artifact which is followed up with a manual review.
- Entities such as URL's & attachments will be scrutinised to identify potentially malicious artifacts which pose a risk to your organisation.
- For identified malicious emails, we will identify and notify you of the same email sent to any other users. Note this is conditional upon the email event logs being configured to Microsoft Sentinel.
- For emails identified as malicious we Investigate where users have clicked on suspicious links.
- In the event an email is identified as malicious and requires an action to be taken we will notify you with details of the incident through a ticketing system.
- All submissions will receive a verdict of the email from the MDR SOC.
- MDR team will support 20 submissions a day. Where an increased total Is required per day, further calculations of the effort required on the MDR team should be discussed with your Account Manager and a cost for such work provided to you.
- MDR team will respond to all submissions within 24 hours.

4.2 : Endpoint Detection and Response Management

Supported Technologies: Defender for Endpoint, CrowdStrike

- The team works with IT teams or third-party IT providers to migrate you from existing Endpoint Security solution (if applicable) to Microsoft Defender for Endpoint or Cynet.
- The team will plan the deployment, based on your existing licensing (if applicable), making use of all available functionality.
- The team will advise on additional licensing which may be required to improve coverage of the most likely threats you should expect to face.
- MDR team project manage deployment of solution and integration with service.

5. Service Constraints.

Maintel MDR functions 24x7x365, with no downtime due to updates or changes. Updates are thoroughly tested in a test environment before being applied live to the service.

This allows us to continually update the service throughout its lifetime, without having to falter on performance or availability. Support is always available 24x7x365.