RelianceCyber

Microsoft Sentinel Managed Detection and Response (MDR) Service

Service Definition

G-Cloud 15

Lot 3: Cloud Support

Contact Details

Email: tenders@reliancecyber.com

Contact Number: +44 (0) 845 519 2946

Contents

1 MDR Overview

1.1 Service Overview

Reliance Cyber's Managed Detection and Response (MDR) is a transparent, expert-delivered security operation built to protect your business and confirm operational resilience. Combining advanced technology and human expertise to proactively detect, investigate, and respond to cyber threats in real-time, MDR functions as an indispensable extension of your team.

Supported by a 24x7x365 UK-based, CREST-accredited security operations centre (SOC) and staffed by SC-cleared, 24x7 SOC analysts, your team will always be supported by the combined efforts of real-time automation and expert human oversight. Our engineering strength, centred on the managed Microsoft Sentinel Security Information and Event Management (SIEM) and Google Security Operations (SecOps) Security Orchestration, Automation and Response (SOAR), has culminated in years of proprietary engineering and the integration of world-leading threat intelligence sources to ensure the instant containment and eradication of threats before they can cause damage.

We deliver tailored, actionable security management. The service includes continuous threat hunting, integrated threat intelligence feeds and formal reporting, all delivered with complete transparency. We integrate with and manage key client-owned solutions whilst allowing full administrative access to client security platforms.

1.2 Features

- 24x7x365 threat monitoring with proactive incident response and containment.
- SC-cleared, UK-based SOC support, using NCSC-assured incident response tactics.
- AI-enabled threat containment, with AI-powered response workflows.
- Transparent operating model tailored to internal incident response process.
- Google, Mandiant and VirusTotal threat intelligence integrated as standard.
- Expert analysis and security event correlation with Microsoft Sentinel SIEM.
- SecOps SOAR automated playbook response actively enables real-time threat response.
- MITRE ATT&CK threat modelling assessment to increase security posture.
- Proactive threat hunting by in-house experts with cross-industry expertise.
- Customisable monitoring across IT, hybrid and on-prem estate.

To get the process started, please contact one of our experienced team members by email at tenders@reliancecyber.com or by calling +44 (0) 845 519 2946.

1.3 Benefits

- Reduced security cost, increased security coverage and advanced security monitoring.
- Enhanced threat detection, extended threat visibility and increased operational support.
- Strengthened security posture with reduced Mean-Time-To-Detect (MTTD) and Mean-Time-To-Respond (MTTR).
- Automated threat response, real-time security coverage and threat containment.
- Complete threat awareness with real-world threat intelligence, improving threat response.
- Continuous evolution of service support, with in-house use cases and custom playbook integration.
- Scalable service offering with a fixed pricing model, easily scaling with your business needs.
- Seamless integration with existing security infrastructure, enhancing operational efficiency.
- Compliance with industry regulations and standards, mitigating legal risk.
- Extended threat visibility, cyber defence coverage with increased risk prioritisation.

1.4 Outcomes

- Risk reduction delivered via automated mitigation actions, stopping a cyber incident from 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.
- Real-time threat notification and containment, ensuring operational resilience backed by real-world threat intelligence.
- 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.

1.5 Technical & Customer Requirements

To integrate our MDR offering, we only require support from an IT in-house resource for at least 1.5 full-time days per week for the duration of onboarding, up to 12 weeks. We will also need to confirm that you have firewalls capable of hosting one end of a VPN tunnel to enable our engineers to securely complete their necessary work.

We will need your collaboration throughout the service onboarding to map your network and highlight the endpoints included in the MDR service. Where endpoint monitoring solutions are already in place, such as Endpoint Detection and Response (EDR) and vulnerability scanners, we will need access to integrate our technologies to provide 24x7 monitoring capability.

Ongoing service management will be conducted by our service management team, working with relevant stakeholders within your organisation to ensure a successful, growing partnership.

Where third-party licences are required, these will be purchased separately from the support service. As a Managed Security Service Provider (MSSP), we can support the purchasing of these additional licences or services as needed.

1.6 Service Constraints

As a cloud-based solution, 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 compromising performance or availability. Support is always available 24x7x365.

2 Service Onboarding

2.1 Timescales

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

- **Phase 1: Rapid Integrations** - This includes tasks that are standard with all monitoring solutions, such as integrating or deploying EDR tooling, deploying the Microsoft Sentinel SIEM, integrating our Google SecOps SOAR platform and integrating Cloud environments.
- **Phase 2: Standard Integrations** - This includes integrating standard log sources we typically see across all environments. Examples of these log sources include server estates and firewalls.
- **Phase 3: Complex Integrations** - More custom or nuanced log sources that require extra scoping. This includes non-standard, legacy, or niche assets that require additional planning, such as non-standard application logs for custom, critical applications, which may necessitate custom integrations and parsing.

Note: although this typically takes 12 weeks, it can be much quicker with dedicated support from internal client security teams, cutting the overall onboarding plan by as much as 50%.

2.2 Five-Stage Onboarding Plan

Stage 1: Preparation (1 to 2 Weeks before Kick-Off) – During the final commercial stages of the contracting process, we will prepare for kick-off by assigning a Project Manager, scheduling introductory calls, a Threat Modelling workshop and data collection to identify critical and non-critical log sources.

Stage 2: Kick-Off and Design (Week 1) – We will 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 will initiate deployment of the SIEM and configuration review for existing email/communications security tooling. We will either deploy or integrate the current EDR's functionality, depending on your requirements.

Stage 3: Deployment (Weeks 2 to 5) – Focused onboarding of critical standard 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 occur during the onboarding service.

Stage 4: Tuning (Weeks 6 to 12) – Repeat the cycle, now focusing on custom or nuanced 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 the onboarding phase is complete, the project team will hand over to service management for ongoing service management throughout the remainder of the contract. Minor snagging issues may be handed over to the service management team to resolve (with your agreement) so that the onboarding project can be concluded and transitioned to our full live service.

To get the process started, please contact one of our experienced team members by email at tenders@reliancecyber.com or by calling +44 (0) 845 519 2946. We are happy to schedule a scoping workshop to ensure we provide exactly the service you're looking for.

2.3 Service Offboarding

The exit of a customer from the MDR service is not planned; it is agreed upon by the customer or Reliance Cyber, with a termination notice issued in line with the contract terms. A specific offboarding timeline will be outlined upon receipt of 30 days' notice, as it will vary depending on the customer's planned next steps and the finalisation of activities with the customer.

We will work with the customer to jointly ramp down the service(s) provided by Reliance Cyber by handing back responsibilities to the customer, or on to a replacement service provider.

All customer-specific documentation created or modified during service delivery will be provided to the customer as part of the offboarding knowledge transfer.

A joint offboarding plan will be drafted in detailed discussions with the customer during the initial stages of the offboarding process. To ensure a safe offboarding, we recommend a duration of 50% of the initial onboarding phase.

The main deliverables within the offboarding process are:

Step	Action	Requirement
Knowledge Transfer	Knowledge Transfer sessions	Customer to attend knowledge transfer sessions led by Reliance Cyber.

	Handover meeting and sign-off	Customer and Reliance Cyber agree that, upon successful execution of all closure action items, the Customer will sign the closure report. This marks the official end of the engagement.
Engagement Closure	Ticket handling	Ticket processing and confirmation by the Customer before services end.
	Deactivation	Termination of processes, meetings, final reporting and invoicing.
	Setup	Deactivation of users, infrastructure and tool environment.
Reliance Cyber Intellectual Property (RCIP)	RCIP deletion	Deletion of RCIP rules, runbooks, playbooks, SOAR actions, and all other IPs implemented to support the service's operation.

3 Service Management

3.1 Service Level Agreements

The following table illustrates our standard MDR SLAs.

Priority	*Impact*	*Time to Acknowledge*	*Time to Respond*
P1	Critical	15 minutes	30 minutes
P2	High	30 minutes	1 hour
P3	Medium	2 hours	4 hours
P4	Low	6 hours	12 hours

- **Critical (P1)** – A widespread breach impacting multiple elements of the organisation's infrastructure. This 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.

The following table illustrates our standard MDR service levels for service requests.

Request Category	*Description*	*Resolution Time*	*Target*
Service Request	Standard Service Requests	< = 2 Business Days	> = 80%

3.2 Key Performance Indicators (KPIs) & Service Credits

Service Area	KPI / Priority / Impact	KPI / SLA Performance (Targets Measured Monthly)	Service Credit for Each Monthly Service Period
INCIDENT: Assign and Respond – This is the time from when the SOC analyses the alert until the incident is raised with you and initial findings are provided.	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 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) by Reliance Cyber 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 for the reporting month for non-adherence.
	P3 - Medium	98% < 4 hours	N/A
	P4 - Low	98% < 12 hours	N/A
Service Health: Reporting of interruptions – Time taken for reporting of Critical health issues causing service-affecting outages of Reliance Cyber's core platforms.	Critical	98% < 4 hours	5% service credit of the monthly charge for the service line in the reporting month.

3.3 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 cover the service as a whole and individual parts where necessary. Where different parts of the organisation have other requirements, we will tailor the sessions around you. This is included in the flat-rate onboarding and ongoing service costs.

Some examples of training and support include:

- **Microsoft Sentinel SIEM and Google SecOps SOAR 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 on reviewing incidents, investigating specific events, and making the best use of your dashboards.
- **EDR Tooling Workshops.** Led by our engineering team, we will review your EDR tooling's configurations and advise on remediation activities to bring them in line with best-practice coverage and configuration. We advise that these workshops be 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 for completion internally.

4 Reliance Cyber Overview

Reliance Cyber is a Managed Security Services Partner (MSSP), dedicated to fortifying our clients through cyber security. With a rich legacy spanning 20 years, Reliance Cyber has emerged as a trusted and innovative MSSP, continually reinvesting to ensure our clients receive the best security support on the market. This has enabled us to recruit the best SC specialists and develop market-leading capabilities focused solely on cyber security.

Operating 24x7x365, we prioritise collaboration, transparency and long-term trust-based relationships with clients to navigate the ever-evolving landscape of cyber threats.

4.1 Core Capabilities

Reliance Cyber's core services are structured around three strategic pillars, reflecting our holistic approach to cyber threat management across managed, proactive and reactive services.

- **Managed Services** – We deliver enhanced security operations through continuous monitoring, proactive threat detection, and rapid remediation. Operating 24x7 on our clients' behalf, our managed services include Managed Detection and Response (MDR), Managed Endpoint Detection and Response (EDR), Managed Secure Access Service Edge (SASE), Phishing Monitoring and Vulnerability Management.
- **Proactive Consulting Services** – We support clients in identifying and addressing vulnerabilities before threat actors can exploit them. Our proactive security offerings include Cyber Threat Intelligence, Crisis Simulations, Compromise Assessments and a range of bespoke solutions tailored to meet each client's unique risk landscape.
- **Reactive Consulting Services** – When incidents occur, we provide expert incident response and recovery support. Our services are delivered using methodologies certified by CREST and aligned with guidance from the National Cyber Security Centre (NCSC). Leveraging deep digital forensics expertise, we help clients contain, investigate, and recover from cyber incidents swiftly and effectively, minimising impact and enabling lessons learned to strengthen future defences.

RelianceCyber

Additional Services That Compliment MDR

Where MDR serves as your organisation's frontline defence against potential threats, our supplementary services extend this security shield. Whether integrated as bolt-on features or standalone services, they prioritise pre-emptive measures to safeguard your network. All are also available through G Cloud: Lot 3.

NCSC-Assured CREST Digital Forensics Incident Response (DFIR) Retainer

When MDR alone isn't enough, our DFIR Retainer service offers immediate support to swiftly contain and minimise damage to your network. With a global incident response team at your side, we provide digital forensics, stakeholder liaising, regulatory engagement and assistance in service restoration.

Cato Managed Secure Access Service Edge (SASE)

When traditional VPNs and fragmented tools fail to secure your remote workforce, our Managed SASE service provides a unified, cloud-native architecture. We combine SD-WAN with comprehensive security-as-a-service to deliver seamless connectivity and consistent policy enforcement. With our experts managing your edge, we provide secure web gateways, zero-trust access and real-time threat protection for every user, regardless of location.