RelianceCyber

Sentinel Managed Extended Detection and Response (XDR) Threat Detection Service

Service Definition

G-Cloud 14

Lot 3: Cloud Support

Contact Details

Email: tenders@reliancecyber.com

Contact Number: 02038729000

Contents

XDR Overview

What is managed extended detection and response (XDR)?

XDR is eXtended Detection and Response. A platform that integrates, correlates and contextualises data and alerts from multiple security prevention, detection and response components. XDR is a cloud-delivered technology comprising multiple point solutions and advanced analytics to correlate alerts from multiple sources into incidents from weaker individual signals to create more accurate detections.

Reliance Cyber's provides this service via a cloud-hosted security support service managed by our 24x7 UK-based, CREST accredited Security Operations Centre (SOC). Underpinned with advanced security tooling integrated across your digital environment, coupled with diligent overview from our SOC analysts, our XDR service swiftly detects, prioritises and activates mitigating response actions to malicious threats attempting to compromise your infrastructure

Using Microsoft Sentinel Security Information and Event Management (SIEM), XDR will ingest log sources from either your chosen endpoints or all endpoints within your environment, monitoring and analysing them based on the risk they pose to your network. The analysing process is largely automated, allowing our SOC analysts to monitor your network in real-time, receiving almost instant alerts of any suspicious activity within your infrastructure.

Our analysts will execute remedial actions where XDR defines a threat from an endpoint, either automatically through our Security Orchestration, Automation and Response (SOAR) platform or manually, to isolate and neutralise the threat before it spreads across your network.

Where XDR defines a threat from an endpoint, our Security Orchestration, Automation and Response (SOAR) platform will execute predetermined playbooks that include alert enrichment and automated remedial actions, our analysts can also manually perform mitigation activities to isolate and neutralise the threat before it spreads across your network.

At a high level, our XDR platform will integrate with your environment as illustrated below.

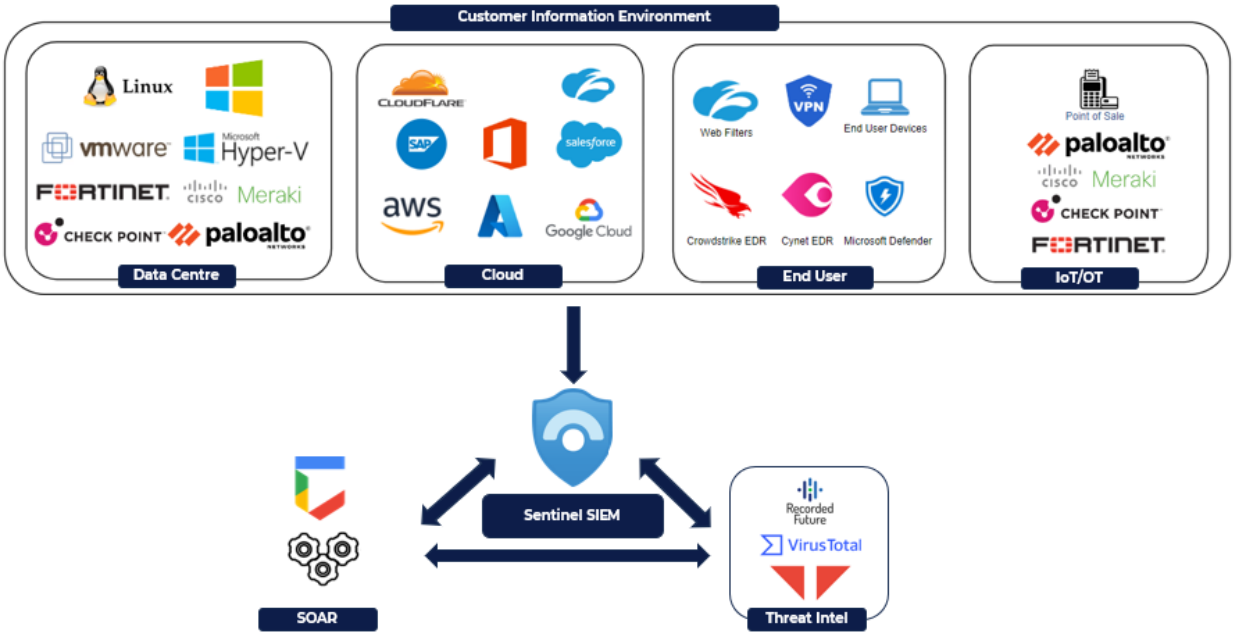

Figure 1: High-Level Technical XDR Overview

Service overview

Tailored components of the XDR service that ensures complete alignment with your organisation include:

- 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.

Although tailored to your needs, the core functionality of the service consists of the following tools, systems and capabilities:

- Microsoft Sentinel Security Information and Event Management (SIEM).
- Google Security Operations Security Orchestration, Automation and Response (SOAR).
- Built-in, tailored private and public integrated Threat Intelligence, backed by our in-house threat intelligence team. The threat intelligence team work across our customer base to highlight the latest threats and trends. This knowledge allows them to implement security measures both specifically to certain customers and across all industries.

- Endpoint Detection and Response (EDR) tooling, either as part of the overall service or integrated with your existing EDR tooling.
- 24/7/365 monitoring, detection and response from our CREST certified UK-based SOC analysts.
- Integration of in-house and custom rules built specific to your environment. All custom rules will be created throughout onboarding.
- Weekly threat hunting and Threat Intelligence reporting on new and emerging threats.
- Dedicated Threat Hunting team reviewing new and emerging threats and proactively searching for signs of yet to be discovered malicious activities within your environment.
- Continuous rule integration throughout the lifetime of the contract, ensuring ongoing support against new and emerging threats.
- A blended approach of automated responses and human analysis.
- Continuous improvement throughout the lifetime of the contract.

Benefits

- High speed deployment providing baseline protection within 48 hours (EDR deployment and monitoring).
- Operated and supported from our 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. As a technology-agnostic vendor, 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.

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**.

Technical & Customer requirements

To integrate our XDR offering, we will 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 for our engineers to work from during the integration of the service.

We work in partnership with our customers. To do this we will need your collaboration throughout the onboarding of the service to map out your network, highlighting the endpoints that you want to be a part of the XDR service. Where endpoint monitoring solutions are already in place, such as 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 Customer Success Team, who will work with the relevant stakeholders within your organisation to ensure a successful, growing

partnership. Fortnightly service reviews calls will be scheduled that require the attendance of your support staff.

Where third-party licenses are required, these will be purchased separately from the support service. As an MSSP, we can support the purchasing of these additional licenses or services as required.

Service Constraints

As a cloud-based solution, XDR functions 24x7x365, with no downtown 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.

What is included in our XDR service

XDR is a scalable support service tailored to your environment and its unique requirements. We will scope your environment to build a solution using technology and tooling that seamlessly integrates and compliments your existing infrastructure. An EDR solution will be deployed where required, and integrated into our XDR support service for 24/7 monitoring by the Reliance Cyber UK-based SOC.

Most importantly, our Sentinel SIEM and Google Security Operations SOAR solution will be deployed and integrated alongside your existing environment to constantly monitor your log sources and security event generating infrastructure. The SIEM will ingest your log sources, before being contextualised through the selected Threat Intelligence platforms. This will feed through to the SOAR platform with actionable intelligence based on the capture and analysis of security event information, allowing automated mitigation or manual containment activities by our experienced SOC analysts to respond to threats based on pre-agreed response actions and the threat impact aligned with the incident.

The XDR service will include:

- **A tailored onboarding process**, crafting a customised XDR solution built to integrate smoothly with your existing environment. This will consist of the deployment of the selected tooling and integration of your log sources into the platform. Log sources will be integrated either through pre-configured connectors or, usually where legacy hardware is involved, custom made connectors, created by our in-house security operations team.
- A **Threat Modelling workshop** conducted during onboarding, and annually thereafter. Leveraging insights from this workshop, we craft bespoke rules that are then deployed to ensure comprehensive coverage of your log sources. Annual workshops allow us to validate the security support we are providing, whilst highlighting any changes that can be made to continually improve your security posture.
- **Deployment of Sentinel SIEM and Google Security Operations SOAR platforms** to constantly monitor, detect and deploy mitigating actions to threats before they cause an incident to your environment.
- **Deployment/integration of EDR tooling**. The Endpoint Detection and Response (EDR) tool will be integrated within Reliance Cyber's SOAR, with pre-configured, automated responses to threats agreed during onboarding and enabled throughout the service. These will be continually reviewed and updated throughout the service lifetime.
- The execution of **pre-agreed response playbooks**, enabling the remediation and containment of incidents with pre-agreed approval dependent on the threat level and situation.

- Application of **Reliance Cyber's foundational SIEM rules**, consisting of over 700 default security measures to protect against common threats. These will be tuned to reduce false positives to an acceptable threshold during onboarding.
- **Threat Intelligence feeds** ingested into the SIEM, with the Reliance Cyber SOAR automatically investigating your IP addresses, file hashes, URLs and domain names for threats.
- **24/7/365 monitoring of your entire IT estate**, allowing our technical analysts to swiftly detect and contain incidents before they can cause harm to your network.
- **Weekly threat hunts**, driven by the latest intelligence from Reliance Cyber's primary Threat Intelligence platforms.
- **Annual maturity reviews** to ensure your security is in line with best practice.
- **Ongoing engineering support** throughout the service lifetime to monitor the health of the SIEM and EDR, managing any collector agents and providing log source support.
- **Regular rule tuning** for your environment to reduce false positives. New general detection rules are integrated and tuned as they are added to our foundational content library.
- The creation of up to two additional custom rules upon request from your IT team. Any additional rules requested will be chargeable at the day rate of an engineer in line with our SFIA rate card.
- Where new major critical vulnerabilities are identified, Threat Hunters will search for any evidence of impact in your SIEM.
- **Fortnightly service reviews** led by Reliance Cyber's Customer Success Management.
- **A monthly service report** showing key performance metrics over the preceding month.
- A **Quarterly Business Review**, led by Reliance Cyber's Senior Management. This allows us to ensure that our goals are continually in alignment with your long-term objectives.
- A **weekly personalised Threat Intelligence report**, which tracks all of your public facing artefacts (domains, IP addresses, executive identities, brand logos and brand names) and offers insight into new and emerging threats focused on your organisation and industry. The report also highlights background information on actions we have taken to secure your security posture over the previous week.
- For high-risk threat findings that require immediate attention, ad-hoc reports will be shared the same day to update your IT team of the threat, the risk it poses and the actions we have taken to mitigate and protect against the threat.

Service Onboarding

Our onboarding process ensures rapid security deployment, shielding against up to 80% of risks within just 48 hours, 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 between Reliance Cyber and your key stakeholders. A process of Threat Modelling ensures that 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.

Timescales

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

Week 1 – Deployment and monitoring of EDR tooling, deployment of SIEM and integration of the SIEM with Reliance Cyber SOAR and 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.

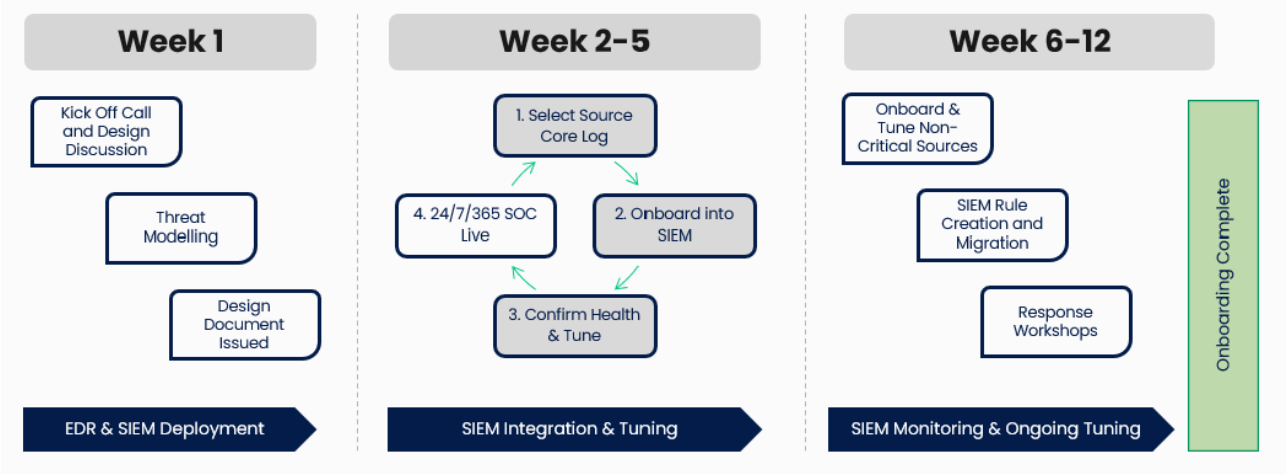

Figure 2: High Level Timescale Overview for XDR Onboarding

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, 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 functionality of current EDR depending on your requirements.

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.

To get the process started please contact one of our experienced team members by email at tenders@reliancecyber.com or call us on 02038729000. We are happy to schedule a scoping workshop to ensure we provide exactly the service you're looking for.

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 XDR service is conducted professionally and reliably. We will plan this when the customer or Reliance Cyber provides a termination notice in line with the agreement terms in the contract. A specific offboarding timeline will be outlined upon receipt of 30 days' notice, as it will vary depending on the customers planned next steps, and the finalisation of activities with the customer and the specific terms of the contract.

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 that has been created/modified in the course of 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 safely planned offboarding, we recommend a duration of 50% of 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 if all closure action items have been executed successfully, the Customer signs 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) deletion	Deletion of RCIP rules, runbooks, playbooks, SOAR actions and all other IP that has been implemented to support the running of the service.

Service Management

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.

Working hand-in-hand with our technical teams and representing the Voice of the Customer in all internal conversations, the CSM will support your 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. This engagement is delivered through:

- **Process Interlock Document (PID)** – This critical document outlines agreed processes and procedures. It serves as a roadmap for collaboration and streamlines operations through a shared understanding of responsibilities and workflows.
- **Fortnightly Service Reviews** – A platform for open communication, allowing thorough discussion of service performance, challenges and opportunities for improvement. The regular cadence ensures that you remain informed of the latest developments. This includes an overview of any incidents raised, an overview of recent Threat Intelligence and a review of the Customer Service tracker. Service Reviews are attended by Reliance Cyber's Principal XDR alongside the CSM.
- **Monthly Operational Reports** – These reports offer insights into service metrics, key performance indicators and notable security events. By presenting this information in a digestible format, the team ensures that you have a comprehensive view of the cybersecurity landscape, facilitating informed decision-making and strategic planning.
- **Quarterly Business Reviews** – Our senior leadership team will organise a review with you on a quarterly basis to discuss more strategic goals that you're looking to achieve, and how our support can help to enhance these goals. Information gathered by our leadership team will be built into our roadmap, helping us ensure that we continue growing our support with your goals in mind.

Service Level Agreements

As a cloud-based solution, Reliance Cyber's support is provided remotely. 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 XDR 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)** – A widespread breach impacting multiple elements of the organisations 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.

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 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) 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 in for the reporting month for non-adherence.
	P3 - Medium	98% < 4 hours	N/A
	P4 - Low	98% < 12 hours	N/A

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:

- **Sentinel SIEM and Google Security Operations 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 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.

Why Reliance Cyber?

Established in 2003, Reliance Cyber specialises in securing our customers long-term growth through sophisticated technology and the best security analysts on the market. Headquartered in the UK, we provide cyber security services across a myriad of global private and public sector customers.

Proactively supporting your strategic goals: More than just services, we offer a strategic partnership. Our scalable solutions ensure you invest not just in cyber resilience but also in aligning these digital assets with your broader organisational strategy and goals.

Simplified resourcing: Think of us as the architects of your in-house SOC, without the associated overheads. From recruiting the brightest minds in cybersecurity to integrating the latest threat intelligence feeds, we have got you covered.

Technology guidance: Drawing from our breadth of real-world experiences, we ensure you are not just implementing technology, but optimising it to its fullest potential. Our wealth of knowledge allows us to take your existing technology stack and maximise its efficiency and effectiveness.

A truly vendor-agnostic strategy: We do not play favourites. Our only loyalty is to your organisation's security needs. We carefully weave together the very best of industry giants like Microsoft, Google, Zscaler, CrowdStrike, CISCO, Checkpoint, Fortinet and Paolo Alto, ensuring you benefit from a holistic and cost-effective security solution.

Transparent, predictable pricing: No hidden costs, no nasty surprises. Our services come with clear monthly costs, ensuring you always know what to expect. Plus, our onboarding is part of the package, making the transition seamless and scalable.

Enterprise technologies for all: Leading-edge technology is often reserved for the corporate giants. We strive to level the playing field by providing these advanced technologies to companies of all sizes. Our mission is to ensure you are armed with the best, minus the associated excessive costs and extended deployment periods.

We partner with:

Google Microsoft paloalto FORTINET CHECK POINT CISCO

RelianceCyber

Additional Services That Compliment XDR

Where XDR 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.

Incident Response

When XDR alone isn't enough, our Incident Response 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.

Managed Infrastructure Services (MIS)

MIS encompasses comprehensive management of your organisation's IT infrastructure, including networks, servers, and security systems. Our MIS offers tailored solutions that adapt to your unique needs, providing peace of mind and strategic support for your digital journey.

Crest Penetration Testing and Vulnerability Assessment

Our penetration team simulates malicious attacks to test every aspect of your internal and external infrastructure, ensuring your security posture is robust. Following the test, a detailed report containing results, evidence and remediation activities provides reassurance against real threats.