Cyber **security**

MANAGED SENTINEL XDR

Intelligent cloud security for rapid detection and response

THREAT READY



LRQA
Your Risk Management Advantage

CONTENTS

3 Managed Sentinel XDR

4 What is Microsoft Sentinel?

5 Microsoft Sentinel SIEM capability

6 Microsoft Defender for endpoint capability

7 What do leading industry analysts say?

8 LRQA's Sentinel XDR capability

9 Managed Sentinel XDR – service features

10 Value proposition

MANAGED MICROSOFT SENTINEL XDR SOC

The need for scalability and flexibility is increasing and as more organisations move to the cloud, this means thinking about cybersecurity in a new way.

Microsoft Sentinel collects data from all your applications, devices, and cloud services to quickly spot suspicious behaviour and eliminate threats.

But to realise this, you need the right people with the time to configure, manage and tune the technology. Plus, they must have the expertise to understand what the alerts mean and how to build on the intelligence and insights gained.

LRQA specialises in Microsoft Sentinel and Defender security tools. Our UK based SOC delivers round-the-clock sophisticated managed detection and response (MDR) services that leverage Microsoft's leading security tools. Microsoft Sentinel combines security orchestration automation and response (SOAR) and user entity behavioural analytics (UEBA) with the power and flexibility of the cloud to secure you against sophisticated cyber threats. This provides you with a high level of assurance that your organisation is protected.

LRQA SOC SECURITY OPERATIONS CENTRE

Microsoft Solutions Partner
Security



MICROSOFT SENTINEL SIEM CAPABILITY

In today's interconnected world, it is increasingly difficult for organisations to protect their data.

Technology and cloud environments continue to rapidly evolve and change the working practices of organisations and people.

Microsoft Sentinel combines the latest in security innovation and advanced AI to provide near real-time intelligent security analytics giving a bird's-eye view of your entire IT estate.

Sentinel allows you to consume security-related data from almost any source, not just your cloud environments. This removes the need to manage multiple pieces of complex and costly infrastructure components, whilst providing a cloud platform SIEM solution that can easily scale to your needs.



COLLECT

Collect data at cloud-scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.



DETECT

Detect previously undetected threats and minimise false positives using Microsoft's analytics and unparalleled global threat intelligence.



INVESTIGATE

Investigate threats with artificial intelligence and hunt for suspicious activities at scale, tapping into years of cybersecurity work at Microsoft.



RESPOND

Respond to incidents rapidly with built-in security orchestration and automation of common tasks.



Customisable data storage options available providing cost-effective hot, warm, and cold storage in any region.

MICROSOFT DEFENDER FOR ENDPOINT CAPABILITY

Microsoft Defender is an enterprise multiplatform security solution designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats across all assets.

The Microsoft Defender suite provides advanced threat protection including antivirus, antimalware, ransomware mitigation, and more, together with centralised management and reporting.

Defender for endpoint uses the following combination of technology and Microsoft's robust cloud service to deliver a leading EDR and endpoint security platform:

ENDPOINT BEHAVIOURAL SENSORS

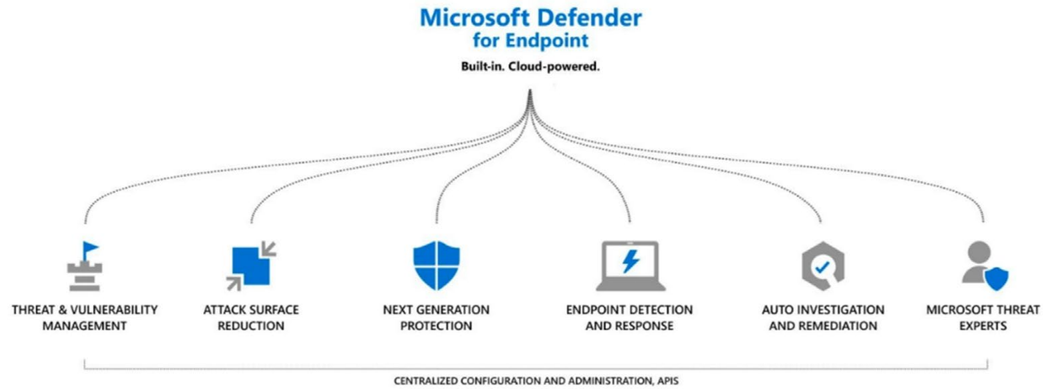
Embedded in deployed agents, these sensors collect and process behavioural signals from the operating system, sending this sensor data to your private, isolated, cloud instance of Microsoft Defender for endpoint.

CLOUD SECURITY ANALYTICS

Using big data, device-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Microsoft 365), and online assets, the system translates behavioural signals into insights, detections, and recommended responses to advanced threats.

THREAT INTELLIGENCE

Generated by Microsoft hunters and security teams, before scaling by partners, threat intelligence enables the Microsoft Defender suite to identify attacker tools, techniques, and procedures, generating alerts when they are observed in collected sensor data.



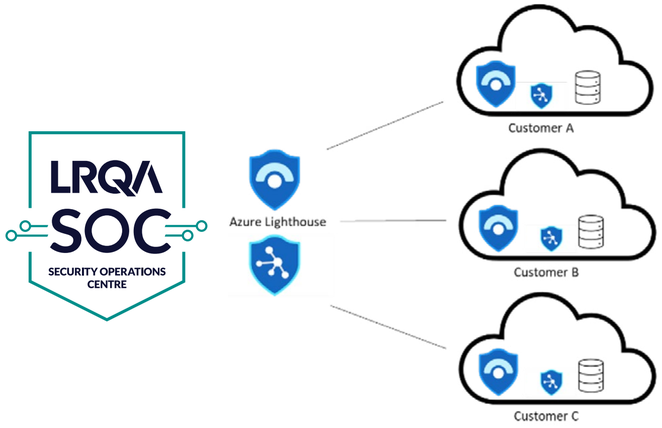
LRQA'S SENTINEL XDR CAPABILITY

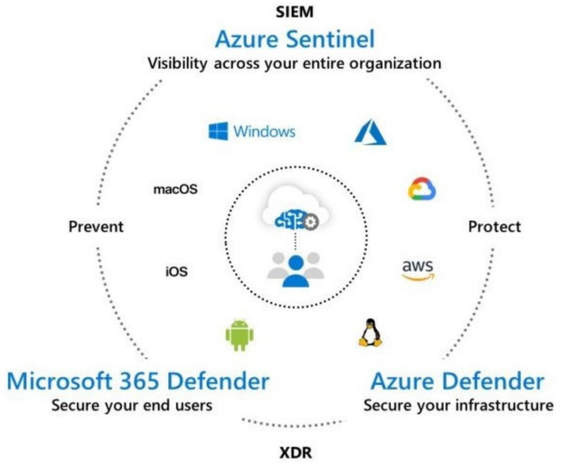
LRQA has been a leading, award-winning SOC and SIEM provider for many years. Combining our talents and using the powerful Azure Lighthouse solution delivers a world-class Managed Sentinel detection and response capability to our clients.

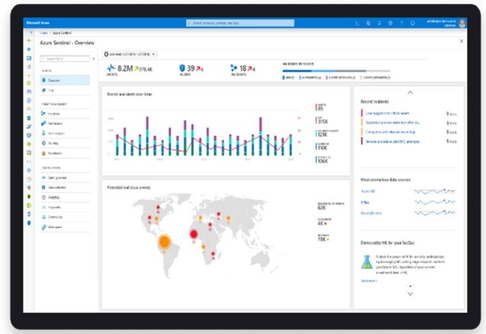
Azure Lighthouse manages multiple subscriptions across different tenants with granular delegated resource management from a single pane of glass. Azure Lighthouse is fully flexible to manage Azure entities across multiple environments and clients securely.

Microsoft Sentinel combined with integrated threat protection products like Defender for Azure and Defender for Endpoint, empowers defensive teams to defend against modern attacks with cloud-native SIEM, SOAR and XDR capability.

Sentinel has many out-of-the-box configurations and use cases available. Organisations struggle to collect the right data to ensure alarms and use cases provide high-fidelity threat detection. Built over many years with our expertise in offensive and defensive cyber operations LRQA can provide a sophisticated alarm, use case, and threat detection suite. This is combined with the capability of Microsoft Sentinel and Microsoft Defender suite to protect you against sophisticated cyber-attacks.







MANAGED SENTINEL XDR – SERVICE

LRQA offers a globally recognised, CREST-accredited Security Operations Centre (SOC), strengthened by our Microsoft partnership status.

It delivers industry-leading configuration, protection, and support for your organisation.

Our approach is proactive and threat-led; informed by our offensive and threat intelligence teams to shape our defensive stance. It protects against the latest industry threats to provide an in-depth defence with unrivalled detection and alerting capability where it is needed most.

24/7/365 ALWAYS ON

Our SOC provides 24/7 x 365 expert security analysis; always there, monitoring & advising for your peace of mind.

GLOBAL DELIVERY

LRQA has been at the forefront of cybersecurity SOC operations since 2003. Our SOC services can be deployed and managed globally.

GLOBAL EXPERTISE

Certified expert defensive SOC team on hand 24/7 as an extension of your teams to provide advice, guidance and remediation where required.

FLEXIBLE COMPONENT-BASED

Our component modular-based approach provides flexibility for your business requirements. We understand things can change over time and new features or components can be added at any time to enhance your cyber maturity.

TECHNOLOGY & THREAT INTELLIGENCE

Leading industry technologies and sophisticated threat intelligence is available to our SOC to ensure they always remain ahead of the latest cyber threats.

PERFORMANCE & REPORTING

Through the use of LRQA's custom Aperture cybersecurity operations platform, we deliver industry-leading performance & reporting on alerting and response SLA's covering MTTR and MTTE across your service.

CERTIFICATION

Our SOC services are certified to ISO27001, ISO9001 and CREST SOC standards. We take our certification levels seriously and ensure we always maintain the highest certification for our SOC and the staff.

OPERATIONAL DELIVERY

Our services are proactively delivered to the structured process and governance models of ISO20k. All clients have an aligned SOC consultant and service delivery manager ensuring you get the support you need.

VALUE PROPOSITION

The LRQA SOC provides advanced 24/7 detection and response services to protect your organisation. We can deliver leading cloud and security expertise, advice and guidance to cover all your technical and security needs.

We provide a consultative threat-led approach acting as an extended part of your team for cloud, security, and technology requirements. We do this by combining sophisticated security technology with our highly accredited people to deliver best-in-class outcomes and value for your organisation.

We can provide a range of additional enhancing services that complement your Managed Sentinel XDR service, including Managed Vulnerability Scanning, Incident Response, and aligned dedicated expertise. Our services ensure predictable value-based outcomes for you on what matters most.

SERVICE VALUE

SERVICE DELIVERY

- ISO20000 aligned service delivery model
- Aligned service delivery manager
- Optional technical account manager

VALUE OUTCOMES

- Reduced Detection & response times
- Improved visibility
- Proactive security and threat stance

SERVICE ASSURANCE

- Custom SIEM dashboards
- Sophisticated service performance & security reporting
- Proactive security and threat stance

MICROSOFT SENTINEL

ENRICHMENT & ANALYTICS & ML

- Built-in intelligent machine learning (ML) behavioural analytics to increase early visibility and near real-time response
- Built-in threat intelligence, processing 6.5 trillion security signals daily
- Sophisticated integration capability
- Fusion correlation engine with scalable ML algorithms

ORCHESTRATION, AUTOMATION & RESPONSE

- Microsoft Sentinel provides integrated automation & orchestration delivering near real-time threat mitigation & remediation
- Highly customisable integrated response playbooks and escalations delivered through Azure Logic apps

24x7 GLOBAL SECURITY OPERATIONS CENTRE

- Fully accredited SOC (ISO27001, Crest, PCI)
- Multi tenant & dedicated SIEM management
- Industry leading technology support and management
- 24/7 eyes on glass
- UK-based SOC, security cleared
- Multi skilled & certified analyst team
- Proactive threat hunting
- Sophisticated security and service reporting
- Best in class SLA response times (average MTTR 0.5 hours P1/2/3)

LRQA SOC SECURITY OPERATIONS CENTRE

DETECTION LAYER

LRQA threat intelligence cell

- SIEM
- EDR
- EPP

LRQA labs custom TTPs

- NDR
- Cloud protect
- Deception

CLIENT

- Cloud environments
- End user compute
- Applications
- Infrastructure
- Identity & access management
- Networks

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **enquiries.uk@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage