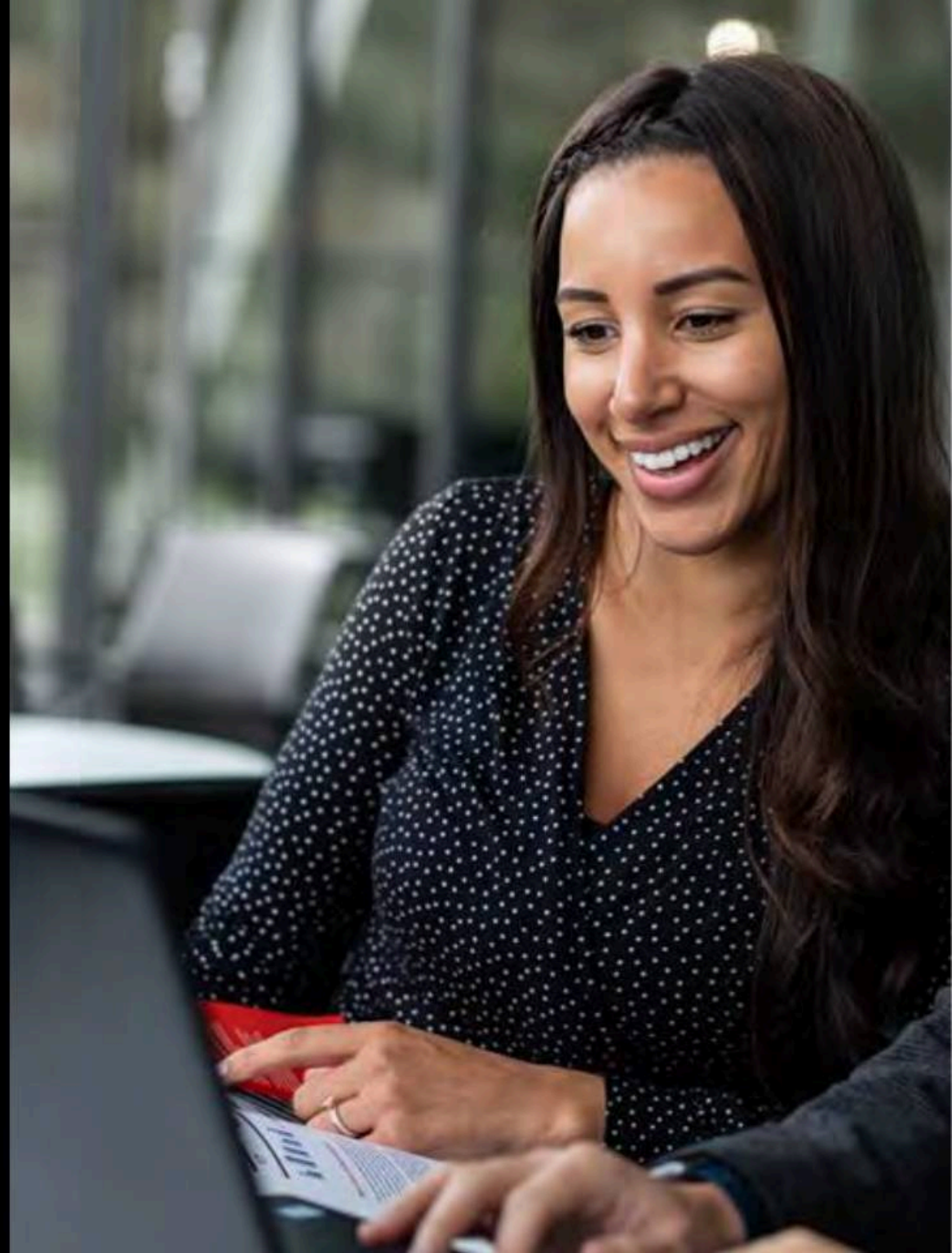




Managed Extended Detection and Response (XDR)

Service guide



About ROCK

ROCK is a technology services group delivering cloud, cybersecurity and managed IT services to public sector, healthcare, education, housing and regulated organisations.

Headquartered in the UK, the ROCK Group supports clients globally across and beyond Europe and North America.

The group is structured for scale and resilience, combining disciplined delivery with deep regulatory understanding. This enables ROCK to operate as a trusted partner in complex, high-assurance environments where reliability and security are critical.

The group operates through two focused service disciplines:

- As a Managed Service Provider (MSP), ROCK runs and optimises cloud platforms, infrastructure and modern workplace environments.
- As a Managed Security Service Provider (MSSP), ROCK delivers continuous cyber defence, risk management and compliance-led security operations.

These services can be consumed independently or combined into a unified operating model.

Clients partner with ROCK for clarity and confidence. From a client standpoint, every partnership is shaped by three principles.

Commitment – Through clear ownership and long-term partnership.

Proof – Through measurable outcomes, service metrics and transparent reporting.

Certainty – Through predictable delivery, resilient design and controlled change.

ROCK supports organisations to modernise securely and operate more effectively. We pair technical depth with practical guidance to support informed decisions and keep technology aligned to business priorities.

The group operates within a mature governance framework aligned to ISO 27001:2022, ISO 9001:2015 and Cyber Essentials Plus.

Engineering and service practices are consistent, repeatable and auditable, enabling scale while managing risk.

Ongoing investment in people, platforms and innovation strengthens capability and keeps services responsive to evolving needs. As a strategic partner, ROCK helps clients improve today while building the foundations for long-term change.

Responsible & Sustainable Delivery

ROCK is committed to delivering Social Value alongside high-quality technology services. Our approach is aligned to the UK Government Social Value Model and focuses on creating good jobs, developing skills, supporting inclusive employment, strengthening supply chains, protecting the environment, and promoting workforce wellbeing.

Social Value is embedded into how we operate as an organisation and how we deliver services, including through fair working practices, skills development and training, responsible supply chain management, environmental sustainability, and community engagement.

For each contract, commitments are tailored to customer needs and local context, and agreed during mobilisation and contract governance.



Our Services

ROCK's Managed Extended Detection and Response (XDR) service provides public-sector organisations with a unified, cross-domain security operating model designed to eliminate technical blind spots.

Unlike traditional siloed monitoring, our XDR service integrates telemetry across identities, endpoints, cloud workloads, and networks to provide a single, cohesive truth of your security posture.

The service combines an AI-driven XDR platform with senior Technology Leadership, ensuring that sophisticated threat detection is always paired with strategic business context.

This allows organisations to maintain high-velocity digital transformation while ensuring that security operations are well-governed, resilient, and audit-ready.

The Operational Pillars of XDR

The service operates as a strategic extension of your internal capability, providing the visibility needed to safeguard public value:

Cross-Domain Integrated Protection

We provide continuous, automated detection and response across Microsoft Defender, Sentinel, AWS, and hybrid infrastructures, ensuring threats are contained before they impact service delivery.

Strategic Governance & Leadership

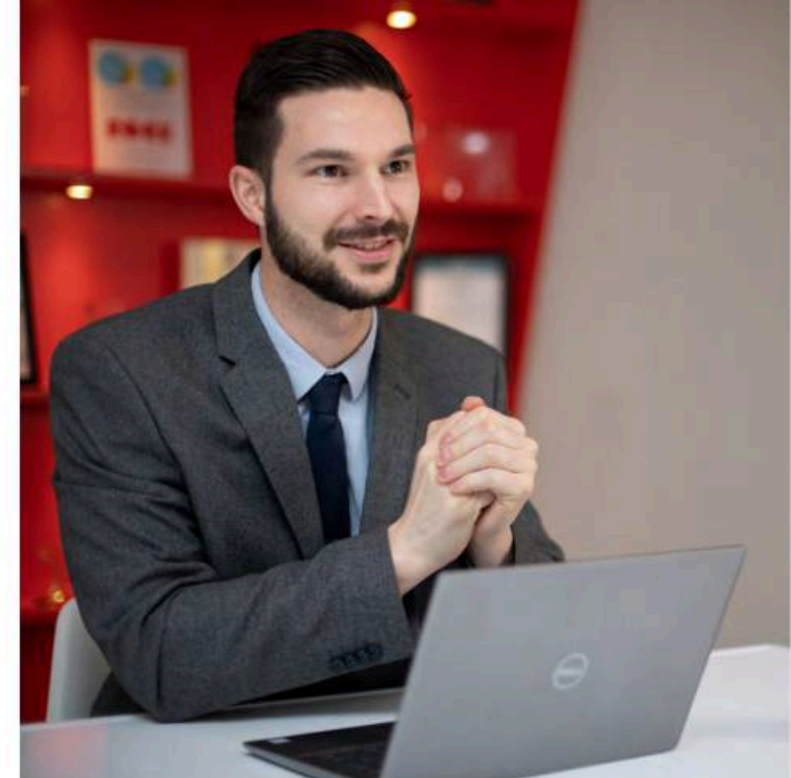
Senior-level oversight (vCTO) translates XDR telemetry into "decision-ready" risk insights, enabling Boards to make informed technology investments based on evidenced risk.

Proactive Resilience Management

Continuous vulnerability assessments and posture governance ensure that environments remain aligned to best-practice baselines, such as the Microsoft Cloud Adoption Framework.

Automated Response & Triage

Using cloud-native playbooks and expert human analysis, we reduce time to resolution and minimise the impact of lateral movement within complex environments.



“Continuous threat detection and response delivered as standard, improving protection without increasing complexity.”

Ian Elsbury, COO at ROCK

Our Approach

Our methodology is designed to move beyond passive monitoring to active exposure management. We apply a structured, evidence-based approach that prioritises the containment of material risk over the simple volume of alerts.

Phase 1: Estate Visualisation & MITRE Alignment

Goal: Eliminate blind spots and create a solid baseline for defence.

Unified Telemetry Onboarding

We integrate Cynet or Microsoft Defender sensors across identities, endpoints, and cloud workloads to create a correlated data fabric.

MITRE ATT&CK® Gap Analysis

We baseline your current visibility against the MITRE ATT&CK framework, producing a heat map that identifies specific gaps in your defensive coverage.

Shadow IT Discovery

We identify unmanaged workloads and unauthorised cloud instances that introduce technical debt and unmanaged risk.

Phase 2: High-Velocity SecOps & Automated Containment

Goal: Reduce the time to respond and eliminate lateral movement.

Cross-Stack Correlation

We leverage the native integration of your XDR tools to correlate disparate signals (e.g., a suspicious login paired with a rare PowerShell command) into a single high-fidelity incident.

Automated Playbook Deployment

We implement pre-approved remediation playbooks (e.g., automated host isolation or password resets) to stop threats at machine speed.

Expert Analyst Validation

Every automated action is reviewed by ROCK's specialists to ensure containment is precise and documented within our ISO 27001 framework.

Phase 3: Strategic Governance & Posture Maturity

Goal: Transform technical telemetry into board-level accountability.

MITRE Maturity Reporting

We provide regular updates on your defensive coverage, showing a traceable link between security activity and the closing of MITRE-identified gaps.

Virtual CTO Risk Advisory

We translate XDR data into decision ready insights for SROs, enabling informed investment in cloud and digital infrastructure.

Continuous Posture Governance

We conduct monthly reviews of policy deviations and technical debt to ensure your estate remains Secure-by-Design.

Key Features

Each feature of our service is designed to deliver a specific, evidenced outcome, ensuring long-term value from your security investment.

Integrated XDR & MDR Operations

Cross-Stack Correlation

Continuous monitoring across identities, endpoints, and cloud workloads to provide a unified "truth" of your security posture.

Automated Remediation & Playbooks

Implementation of pre-approved automated actions (e.g., host isolation, password resets) to stop threats at machine speed, reducing manual burden on internal teams.

24/7 Expert Analyst Triage

ITIL-aligned service desk support providing human validation and specialist investigation of complex alerts to ensure precise containment.

Strategic Assurance & MITRE Alignment

MITRE ATT&CK® Gap Analysis & Heat Maps

An objective assessment of your defensive coverage against global threat actor TTPs, providing a clear "North Star" for maturity.

Prioritised Vulnerability & Risk Registers

Identification of technology and delivery risks, maintained through structured registers that align findings to business impact.

Continuous Posture Governance

Regular review of security policy and configuration to ensure environments remain Secure-by-Design and aligned to the Microsoft Cloud Adoption Framework.

Executive Leadership & Reporting

Executive Insight & Decision Packs

Monthly board-level reporting that provides regular visibility of delivery progress, risks, and required investment decisions.

Traceable Technology Decision Logs

Clear ownership of technology and security decisions supported by documented accountability structures.

Strategic Security Roadmap

Oversight of technology roadmaps to ensure security investment is traceable to service outcomes and public value.

Key Benefits

Our Managed XDR service, powered by Cynet and Microsoft Defender, provides measurable improvements to risk management and organisational confidence.

Operational Resilience & Delivery Certainty

Reduced Mean Time to Detect and Respond (MTTR)

Achieve rapid containment of threats through automated remediation playbooks that stop lateral movement at machine speed.

Elimination of security blind spots

Gain 360-degree visibility across identities, endpoints, and cloud workloads through cross-stack correlation, ensuring no unmanaged exposure exists.

Reduced internal operational burden

Offload day-to-day alert investigation and triage to ROCK's specialist analysts, allowing internal teams to focus on service delivery and transformation.

Financial Efficiency & Value for Money

Optimised ROI on existing technology

Maximise the value of your current Microsoft Defender or Cynet investments through expert configuration and continuous monitoring.

Avoided costs of incident recovery

Proactively prevent high-impact security breaches and the associated financial and reputational rework through MITRE-aligned proactive defence.

Predictable & scalable expenditure

Access a senior-level security operating model without the overhead of full-time executive recruitment or complex infrastructure lock-in.

Strategic Governance & Public Trust

Evidence based board assurance

Empower SROs and Boards with reporting and MITRE Heat Maps that demonstrate defensive maturity in plain language.

Continuous audit & regulatory readiness

Maintain a Secure-by-Design posture with documentation and decision logs aligned to ISO 27001, UK GDPR, and Cyber Essentials Plus.

Strategic alignment to service outcomes

Ensure that your security roadmap directly supports organisational objectives and public service delivery rather than becoming an operational constraint.

Management & Governance

The Managed XDR service is delivered through a structured, repeatable engagement model designed to support absolute transparency and delivery velocity.

We combine ITIL-aligned service desk disciplines with continuous posture governance to ensure your security environment remains resilient and well-documented.

Engagement Model & Managed SOC

24/7 Monitoring & triage

ROCK provides continuous oversight of alerts from Cynet and Microsoft Defender, with analysts reviewing severity and context to ensure potential threats are triaged and contained promptly.

Automated playbook governance

We manage and refine the library of automated response playbooks, ensuring host isolation and password resets are executed safely and documented for audit trails.

Single point of contact

Access to specialist security engineers is provided through our ITIL-aligned service desk, ensuring clear ownership of all security requests and incidents.

MITRE-Aligned Posture Governance

Defensive maturity reviews

Regular governance sessions focus on your MITRE ATT&CK® coverage, using operational evidence to identify and close visibility gaps.

Policy & baseline compliance

We conduct continuous monitoring of security configurations to ensure they remain aligned to the Microsoft Cloud Adoption Framework and organisational risk appetite.

Technical debt management

We identify and track obsolescence and misconfigurations through risk registers, ensuring remediation is prioritised by impact.

Reporting & Executive Insight

Reporting is structured to support both technical action and board-level assurance:

- MITRE coverage heat maps: Visual representation of defensive maturity against global threat actor techniques.
- Automated remediation logs: Detailed evidence of all automated containment actions taken by the XDR platform.
- Decision ready summaries: Executive-level reports outlining material risks, dependencies, and recommended technology investment priorities.

Reporting & Executive Insight

Senior stakeholder engagement

Our senior advisors engage with SROs and Executives to translate technical telemetry into informed, risk-based technology decisions.

Strategic roadmap alignment

We ensure that the security evolution of the estate is traceable to organisational objectives and value-for-money obligations.

Security & Data Protection

Security is embedded throughout our Managed XDR service. We combine cloud-native security controls, disciplined operational processes, and ISO-aligned governance to protect environments and data.

ISO-Aligned Security Governance

The service operates within ROCK's ISO 27001:2022 certified Information Security Management System, ensuring consistent and auditable control of information.

Our operations are aligned to recognised standards for information security, quality management, and environmental responsibility.

Handling of all telemetry complies with UK GDPR and Cyber Essentials Plus requirements.

Data Handling & Privacy

ROCK processes only the operational metadata required to deliver the service, such as XDR alerts, logs, and configuration metadata.

Customer production data remains within the client's own environment (Azure/AWS/On-premise) and is not extracted or stored by ROCK.

Only information required to deliver agreed outcomes is processed, such as architecture documentation and delivery plans.

Identity & Access Controls

Access to sensitive security information is restricted to authorised personnel using least-privilege controls, with mandatory access logging and review.

Identity is governed through Microsoft Entra ID using Multi-Factor Authentication (MFA).

All staff undergo background screening aligned to BS7858:2019 for roles with access to client systems.

Secure Monitoring & Threat Visibility

We collect and analyse security alerts from Cynet, Microsoft Defender, and Sentinel via encrypted, secure mechanisms.

Security monitoring leverages cloud-native tooling to identify suspicious activity, misconfigurations, and policy deviations.

All access is approved, logged, reviewed regularly, and removed promptly when no longer required.

Data Retention & Secure Disposal

Service-related data is retained only for the duration required to support outcomes.

At contract end, data is securely disposed of in line with ISO-aligned sanitisation practices



Values & Outcomes

Our Managed XDR service delivers evidenced value by transforming cross-domain telemetry into a strategic roadmap for resilience. Outcomes are achieved through structured governance, automated containment, and proportionate oversight.

Operational Value

Reduced Internal Workload

ROCK assumes responsibility for 24/7 XDR operations, monitoring, and triage, allowing internal teams to focus on service delivery rather than alert fatigue.

Accelerated Mitigation (MTTR)

Achieve faster issue resolution and recovery through automated playbooks and SRE-aligned practices that prioritise prevention and rapid restoration of service.

Elimination of Blind Spots

Improved visibility and stability are achieved through cross-stack correlation and proactive monitoring, reducing the likelihood and impact of unplanned outages.

Clear Operational Accountability

Defined service roles, governance structures, and regular reviews provide transparent ownership of security outcomes.

Financial Value

Optimised ROI on Existing Tech

Ensure robust value for money by making full use of existing Microsoft Defender or Cynet licenses through expert configuration and continuous validation.

Predictable & Controlled Expenditure

Consistent tagging and FinOps practices align security spend to services and outcomes, providing clear cost attribution and improved budgetary control.

Avoided Capital Expenditure

Scalable, cloud-native security services enable organisations to pay only for what is required, avoiding the cost of a full-time executive appointment or internal SOC infrastructure.

Reduced Waste

Ongoing optimisation of resources and consumption management ensures security efficiency as organisational demand evolves.

Security & Compliance Value

Stronger & Consistent Security Posture

Embedded governance, identity controls, and policy enforcement across the digital estate reduce the risk of unmanaged technical debt.

Continuous Audit Readiness

Logging, reporting, and evidence-based insights align to ISO 27001, UK GDPR, and Cyber Essentials Plus requirements.

MITRE-Aligned Assurance

Reduced risk of misconfiguration or exposure through standardised patterns and continuous oversight mapped to global threat actor techniques.

Strategic & Organisational Value

Improved Leadership Insight

Clear visibility of performance, cost, and risk provides executive stakeholders with decision-ready insights to support long-term planning.

Greater Organisational Readiness

Aligning people, process, and technology ensures teams can operate and evolve cloud services with confidence during periods of change.

Scalable Leadership Model

A flexible leadership model that adapts as organisational needs, services, and constraints evolve.

Accreditations & Certifications

ROCK maintains a proven, independently assessed way of working that underpins every service, helping us provide the best IT solutions to our clients. Our certifications and partnerships show that we take security, governance and quality seriously, strengthening our credibility through best-practice services, recognised standards, and ongoing accreditation.

Security Clearances

BS7858:2019 Screening

All staff undergo background screening aligned to BS7858:2019 for roles with access to client systems or sensitive information.

Security Check

Staff can hold UK Government Security Check clearance where required by the service scope, buyer requirements or contractual obligations.

Enhanced DBS Checks

Enhanced DBS checks are performed for staff supporting regulated or sensitive environments where required by client contracts or service scope.

Strategic Partnerships

ROCK works with a range of leading cloud and technology providers to deliver secure, resilient and well-governed services.



Microsoft Partner

Cloud, identity, security and productivity services across Azure, Microsoft 365, Microsoft Entra ID and Microsoft Defender.



AWS Partner

Infrastructure and platform services including compute, storage, networking and security.



Cisco and Meraki

Cloud-managed networking, SD-WAN and secure connectivity solutions.



Cloud Security & SASE

Secure access, firewalling, SD-WAN and ZTNA capabilities, including cloud security.



Backup & Recovery | N-Able & Cove

Cloud-based backup, replication and disaster recovery solutions supporting cloud, hybrid and endpoint environments.



Endpoint & Device Management

Endpoint security, configuration, monitoring and lifecycle management tooling across user devices and servers.



SonicWall

Network security, firewalling, secure remote access and SD-WAN capabilities for on-premise and cloud-connected environments.

Certifications & Compliance



ISO 27001:2022

Certified information security management system demonstrating effective controls for data protection, access management and operational security.



ISO 9001:2015

Certified quality management system supporting consistent service delivery, continuous improvement and effective governance.



Cyber Essentials Plus

Independently verified assurance of strong baseline cybersecurity controls across all operational systems.



ICO registration

Fully registered with the Information Commissioner's Office for data processing compliance.

How To Buy

This service can be procured quickly and compliantly through the Crown Commercial Service (CCS) G-Cloud 15 Framework under the Cloud Support lot.

This provides a streamlined route for public-sector organisations to access high-quality managed support without needing to run a full tender.

What Buyers Can Expect

- Fast mobilisation, with service commencement scheduled quickly after award.
- No contract negotiation, as all terms follow the standard G-Cloud framework.
- Transparent pricing, published and fixed in accordance with the G-Cloud catalogue.
- Clear onboarding processes, including asset discovery, documentation intake and communication setup.

Purchasing Steps

1. Search for ROCK on the Digital Marketplace under: Managed IT Services - Cloud Support
2. Review the Service Definition, pricing document and terms.
3. Shortlist ROCK based on your technical, operational and commercial criteria.
4. Evaluate shortlisted suppliers following CCS guidance.
5. Award a Call-Off Contract directly to ROCK through G-Cloud 15.
6. Agree service scope and onboarding timelines with our mobilisation team.

Support with Procurement

ROCK can support buyers with:

- Responding to clarification questions
- Helping shape scope within the boundaries of G-Cloud
- Providing guidance on service levels, onboarding and shared responsibilities
- Supporting internal approvals or business case preparation

We remain fully compliant with CCS rules - no pre-award customisation of terms.





Your cybersecurity partner to reduce risk,
strengthen resilience and build trust.

rock.co.uk