# Service Definition: Managed Security Operations Centre (MSOC)

Crown Commercial Services | G Cloud 15 framework

# Contents

# Document Information

| | |
|---|---|
| **Client name** | G Cloud 15 Service Definition |
| **Project name** | Managed Security Operations Centre (MSOC) |
| **Document author(s)** | Ade Taylor, Gill Brown |

# Document Change Record

| Issue | Date | Description |
|---|---|---|
| V0.1 | 01/12/25 | Draft Template |
| V0.2 | 12/12/25 | Draft Initial Content added |
| V0.3 | 22/01/26 | Draft for review and sign off |
| V1.0 | 27/01/26 | Final for Issue |

# Contact Information

| | |
|---|---|
| This document has been supplied by Roc Technologies Limited, whose registered office is: | Roc Technologies Limited<br>1 Lindenmuth Way<br>Greenham Business Park<br>Greenham<br>Thatcham RG19 6AD<br>United Kingdom |
| Please refer all enquiries to: | **Gill Brown, 0845 647 6000**<br>publicsector@roctechnologies.com. |

Roc Technologies Limited reserves the right to make improvements or changes to this document and information contained within, and to the products and services described at any time, without notice or obligation.
Roc Technologies understands that any award to supply the products and/or provide the services that are the subject of this document is subject to the mutual execution of a definitive written agreement.
All information supplied for the purpose of this Roc Technologies document is to be considered confidential.

# 1 Service Summary

## 1.1 Why Roc for Cyber Security and Operations?

Roc Technologies is an IT and Cyber Security Managed Service Partner specialising in delivering transformational digital solutions to public and private sector organisations across the UK. We are a team of brilliant minds, bringing together highly secure infrastructure, advanced cyber security, intelligent automation and modern cloud services, all supported by our 24/7 Managed Security Services Operations Centre and security cleared engineering force. We work in partnership with the world's leading vendors, implementing leading edge technologies to the benefit of our customers.

Our expertise is backed up by some of the UK's most rigorous data and security accreditations; we've earned the trust of the nation's largest and most critical organisations and have safeguarded their most sensitive data for over a decade.


Through our partnership with UK MOD, Nuclear Restoration Services, and UK Policing, we ensure our platforms and solutions are UK sovereign resilient and are proud to have obtained Facility Security Clearance (previously List X), as well as List-N status. With our customer portfolio expanding beyond high security and into research intensive organisations (including leading high-performance universities) and the Atomic Weapons Institute, Roc is ideally positioned to balance increasing needs for innovation with a never compromising approach to Cyber Security. Our partnership with Google, as one of the leading providers of fully AI enabled Security Operations, demonstrates this.

# 2 Executive Summary

Our Managed Security Operations Centre (SOC) service provides proactive threat detection, incident response, and continuous improvement, delivered with full transparency and sovereign assurance. Roc Technologies proposes a comprehensive Roc delivered Managed SOC service built around Google SecOps technology, combining advanced analytics and automation with our UK-based, Security cleared analyst team operating 24×7×365.

**Our Managed SOC provides:**

- Continuous monitoring, threat detection, and rapid response aligned to the NCSC Cyber Assessment Framework and NIST 800-207 Zero Trust principles.
- A fully managed SIEM/SOAR platform (Google SecOps) that ingests telemetry from across your digital estate—on-premises, cloud, and SaaS—and correlates events in real time.
- Shared visibility and transparency, ensuring your own authorised analysts have direct access to the same dashboards and incident queues as Roc's Security analysts, ensuring true partnership and collaboration.
- UK data sovereignty, certified to ISO 27001 and Cyber Essentials Plus, with all monitoring, storage, and analysis performed within Roc's Facility Security Cleared and List-N accredited UK facilities.
- A partnership model focused on continual service enhancement, compliance assurance, and knowledge transfer.

This proposal sets out how Roc Technologies will deliver a fully managed Cyber service, encompassing Security Operations Centre, SIEM ingestion and monitoring, Threat intelligence, reporting, incident response, and continual improvement. We are confident that our solution will strengthen your cyber resilience, ensure regulatory alignment, and enable data-driven decision-making. Our approach is proven within critical and regulated environments including AWE, City of London Police, and Nuclear Restoration Services, as well as other Government bodies such as the Ministry of Justice, and research-intensive environments including Commercial Defence and Higher Education organisations.

Roc's tailored service, which draws on lessons learned, successes, and ongoing engagements should provide you with the confidence in our experience, capability, and governance maturity to progress with this proposal.

# 3 The Service

Roc's Managed Cyber Service and Security Operations Centre delivers comprehensive detection, investigation, and response services to protect your information assets, infrastructure, and users against evolving threats. The service combines experienced analysts, structured processes, and modern automation and deep insights to provide continuous protection with measurable outcomes.

## 3.1 Scope of Service

- Threat Detection & Monitoring – Ingestion and correlation of event data from endpoints, servers, network devices, cloud services, and applications.
- Incident Response – Rapid triage and containment of security incidents according to defined SLAs (with committed 15-minute critical response).
- Threat Intelligence & Hunting – Integration of multiple threat intelligence sources, both open-source and subscription-based, enriched with contextual data.
- Automation & Orchestration – Playbook-driven automation via Google SecOps to accelerate investigation, response, and containment.
- Reporting & Analytics – Real-time dashboards, weekly threat summaries, and monthly performance reports with value-driven, measurable key performance indicators.
- Continuous Improvement – Iterative tuning of detection rules, correlation logic, and workflow automation based on incident trends and lessons learned. This will include localised improvement for you, as well as tuning and refinement based on Roc & Google's wider customer base.

### 3.1.1 Dual Operations Model

You will benefit from a co-managed visibility model, enabling shared access to dashboards, playbooks, and incident data. Roc analysts handle all operational response and tuning, while customer internal security and IT teams can:

- Observe live detections and incident progression.
- Contribute additional context or request escalation.
- Review metrics and historical incidents for audit purposes.

This transparent model ensures you retains control and visibility while Roc carries the operational responsibility of monitoring, triage, and incident management.

### 3.1.2 Integration & Coverage

The service integrates telemetry from your full environment, including:

- Microsoft 365 Defender, Endpoint, and Exchange.
- Network infrastructure (firewalls, switches, proxies, VPN gateways).

- Cloud workloads (Azure, Google Cloud, AWS).
- Critical infrastructure monitoring systems.
- Endpoint protection, vulnerability scanners, and identity providers (AD, Entra ID).

Roc's SOC continuously evolves correlation rules and detection models to match your threat profile, industry intelligence, and compliance obligations.

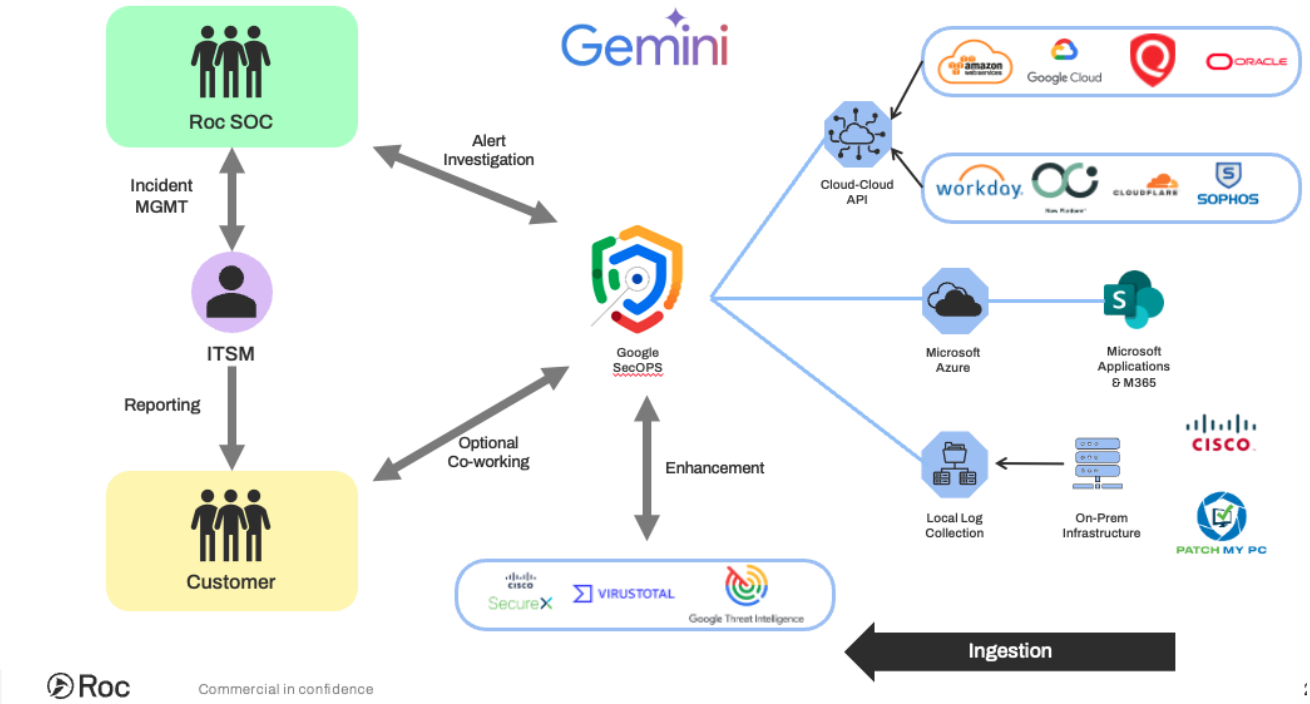
## 3.2 SOC Platform Architecture and Google SecOps Technology Stack

Roc Technologies' Managed SOC for you is underpinned by a dedicated Google SecOps Platform-as-a-Service (PaaS) environment.

The Google platform delivers both the technology foundation for our managed SOC operations and a secure, collaborative workspace where your analysts and authorised users can directly access dashboards, investigations, and playbooks.

This dual-consumption model provides transparency, knowledge transfer, and a measurable uplift in operational maturity.

### Roc's Integrated SOC Platform




*Note: Integrations shown as illustrations. There are hundreds of supported integrations & log sources in addition to custom connectors*

### 3.2.1 Platform Service Model

Roc operates Google SecOps as a managed, multi-tenant but logically isolated PaaS hosted entirely within UK sovereign data centres.

Each customer environment is provisioned as a dedicated logical tenancy with separate storage, encryption keys, and role-based access controls.

The platform is managed by Roc's Cyber Security Service Analyst team, who are responsible for configuration, maintenance, scaling, and integration, while nominated users are granted delegated access through secure Single Sign-On with MFA.

**The service provides:**

- 24×7 platform availability with >99.999% uptime SLA.
- Elastic ingestion and compute scaling to support surges in event volume.
- Quarterly release cadence managed by Roc engineers with controlled change windows aligned to your change management process.
- Service API exposure allowing integration with your own reporting or automation systems.

### 3.2.2 Data Ingestion and Correlation Pipeline (SIEM)

All log and telemetry sources—network devices, servers, cloud workloads, security appliances, and SaaS platforms—are securely forwarded to Google SecOps via TLS-encrypted collectors or directly via API or connectors provided by Google and Roc.

Roc's engineers design the ingestion pipeline to ensure high-fidelity, timestamp-synchronised data and minimal latency.

| Pipeline Stage | Description |
|---|---|
| Collection | Agents or API connectors gather logs from M365, firewalls, EDR, IDS/IPS, identity providers, and OT/ICS devices where applicable. |
| Normalisation | Events are parsed and standardised into the Google SecOps data schema for consistent correlation. |
| Enrichment | Threat-intelligence feeds, asset data, and vulnerability information are automatically added to each event. |
| Correlation & Detection | ML-driven models and rule-based logic identify patterns across datasets. |
| Alerting & Case Creation | Confirmed detections generate incidents within the SOAR module for triage and response. |

Changes to detection logic, playbooks, or connectors will follow a controlled change-management process with review and approval.

### Integration with your Ecosystem

The platform supports bi-directional integration with operational systems to ensure seamless workflow:

- Ticketing: Incidents synchronised with ITSM (Ivanti, Service Now etc.) for tracking and closure.
- Asset Inventory: supported continuous synchronisation with CMDB and vulnerability scanners for accurate context.
- Threat Intelligence: Subscription and government feeds ingested to tailor detection rules.
- Reporting: Custom Power BI or Google Looker dashboards for executive visibility.

Roc provides interface documentation and tailored training to enable you to extend or adapt integrations as its environment evolves.

## 3.2.3 Resilience and Business Continuity

The Google SecOps environment operates across dual UK data centres with active-active redundancy.

Event data is replicated in real time, and recovery objectives are:

| Metric | Target / Description |
|---|---|
| RPO | < 15 minutes |
| RTO | < 1 hour |
| Failover Testing | Quarterly failover testing to validate recovery and service continuity. |

Quarterly failover testing will demonstrate service continuity and will be planning in line with BCDR planning and Change control processes. Defined success criteria will be identified ahead of each failover test, and results will be communicated within two working days. As part of Roc's commitment to a transparent and collaborative service offering – we welcome analysts to observe failover and resiliency testing.

Roc's internal BCDR team will maintain alignment organisational continuity planning, ensuring a coordinated response during major incidents.

While not a requirement of the day one service, Roc have the ability to run Major Incident Exercises both virtually and in person. Regular MIEs would provide continual evolution and a measurable baseline by which to develop continual service improvement, training, and business cyber change workstreams.

### 3.2.4 Innovation Roadmap

Roc continuously evolves our Cyber platform, leveraging Google's product roadmap and have introduced features such as:

- Generative AI Assistant for automated investigation summaries.
- SOAR Marketplace for rapid integration of new response modules.
- Post-Quantum Cryptography pilot for encrypted telemetry channels.
- Digital Twin Simulation for attack emulation and resilience testing.

By engaging with Roc, you will benefit from early-adopter access and joint roadmap reviews, ensuring the platform remains future-proof and compliant with evolving government mandates.

### 3.2.5 Service Operations and Incident Management

Roc's SOC operates under a continuous, outcome-based model aligned to the detect, contain, eradicate, and recover framework.

#### Incident Lifecycle

1. Detection & Triage – Continuous alert monitoring via Google SecOps. Analysts prioritise alerts by severity, confidence, and asset criticality.

2. Containment – Isolation of affected endpoints, users, or systems through automated and manual actions.

3. Eradication & Recovery – Elimination of malicious artefacts and validation of restoration media.

4. Post-Incident Review – Root cause analysis, reporting, and application of new detection logic.

#### Response Times and SLAs

Critical alerts: triaged within 15 minutes, containment initiated within 30 minutes.

High-severity incidents: investigation initiated within 1 hour.

| Severity | MTTD Target | MTTA Target | MTTM Target |
|---|---|---|---|
| Critical | <15 minutes | <15 minutes | <1 hour |
| High | <30 minutes | <30 minutes | <2 hours |
| Medium | <1 hour | <1 hour | <4 hours |
| Low | <4–6 hours | <4–6 hours | <3 days |

#### Definitions

- MTTD: Mean Time To Detect.
- MTTA: Mean Time To Acknowledge.
- MTTM: Mean Time To Mitigate.

Routine events: handled according to agreed daily operational schedule.

**Collaboration and Communication**

Incident notifications are issued via secure channels and integrated into internal escalation processes. Roc's analysts collaborate directly with technical teams to coordinate containment and resolution, maintaining detailed audit trails for every action.

### 3.2.6 SOC Account & Service Delivery Team

| Role | Function |
|---|---|
| CEO | The highest point of escalation. |
| CTO | Executive sponsor and overall technical lead. |
| Head of Cyber Services | Practice lead with responsibility for all Roc cyber services. |
| Service Delivery Manager | Roc will allocate a dedicated/named Service Delivery Manager to oversee SOC operations and Service Delivery as a whole, acting as a vital central point between the live service and your own delivery and service teams. Through regular meetings and service reviews, Roc will ensure the service taken live continually meets and exceeds expectations. |
| Account Manager | Ensuring continuity, Roc will engage a single account manager to oversee activity and drive initiatives across all workstreams, allowing a more unified experience for the business and better information shared across the stakeholders and project teams. |
| Head of SOC | Escalation points for P1 incidents & operational SOC customer queries/concerns<br>The Head of SOC oversees training, service escalations, acts as the SOC Service Subject Matter Expert (SME), supervises the Engineering function and architecture, serves as the primary Incident Responder, and ensures quality assurance and compliance with SOC policies. The Head of SOC is also responsible for holding monthly service delivery meetings and reporting. |

| | |
|---|---|
| SIEM Engineer | Responsible for tuning customer environments, beginning at the on-boarding stage, as part of our baselining activities they will track all the alarms, looking for false negatives, they will test the effectiveness of the ruleset, we are looking for the rules to trigger as we have intended them too.<br>Our engineers will monitor which alarms are triggering most often and collaboration from the analyst's investigation, we will determine the cause, where there is no concern for the activity taking place, an expectation may be put in place, this exception will be as specific to the activity as possible. |
| Senior SOC analyst | Assumes a leadership role within the security team, with an expanded set of responsibilities that reflect their advanced expertise and experience. They are the first point of escalation within the SOC. In addition to performing the core functions of monitoring, detecting, and responding to security incidents, a senior SOC Analyst takes on tasks such as mentoring and training junior analysts, providing guidance on complex investigations, and overseeing the development and implementation of security policies and procedures. They are often involved in the strategic planning of security operations, including threat intelligence analysis, risk assessment, and security tool evaluation and deployment. |
| SOC Analyst | Their main responsibilities revolve around monitoring, detecting, and responding to security incidents in real-time. This involves continuously analysing security alerts generated by various monitoring systems, investigating potential security breaches, and determining the appropriate course of action to mitigate risks. SOC Analysts conduct in-depth analysis of security events to identify patterns and trends that may indicate a larger threat landscape. |

### 3.2.7 Incident Analysis and Reporting

All incidents undergo documented review, with evidence preserved for compliance and investigation purposes. Monthly incident trend reports summarise:

- Number and type of incidents.
- Mean time to detect and respond (MTTD/MTTR).
- Root cause and remediation actions.
- Lessons learned and new rule implementations.

Major incidents will be reported on outside of the usual monthly cycle, with Roc providing a Major Incident Report (MIR) within 2 business days.

### 3.2.8 Governance, Security, and Compliance

Roc's Managed Cyber service is governed through a comprehensive security framework that ensures you receive full assurance, traceability, and alignment with statutory and regulatory obligations. Governance is embedded through policies, accreditations, and an operational model built to exceed public-sector assurance requirements.

### 3.2.9 Certifications and Accreditation

*Roc Technologies maintains:*

- ISO 27001 – Information Security Management
- Cyber Essentials Plus – independently validated annually without exceptions
- ISO9001 – Quality Management
- FSC (formerly List X) – for handling classified data
- SC-cleared analysts and engineers within UK-based facilities
- List-N – Accredited by the Office of Nuclear regulation to provide IT and Data services to the Nuclear industry

These certifications underpin every operational process within Roc, extending to our Managed Services Operations Centre, ensuring auditable compliance with assurance frameworks.

### 3.2.10 Policy and Controls Framework

All SOC operations are governed by Roc's Information Security Policy, which mandates:

- Multi-Factor Authentication (MFA) for all administrative accounts
- Role-based access control and privilege segregation
- 24×7 monitoring of system and audit logs
- Strict patch management cadence and vulnerability scanning
- Quarterly internal audits and annual external penetration testing
- Secure data retention and disposal aligned to GDPR, NIS2

Incident response procedures are formally documented and rehearsed. Analysts follow predefined playbooks for critical incident categories, ensuring consistent response and escalation.

### 3.2.11 Reporting and Transparency

**Customers will receive:**

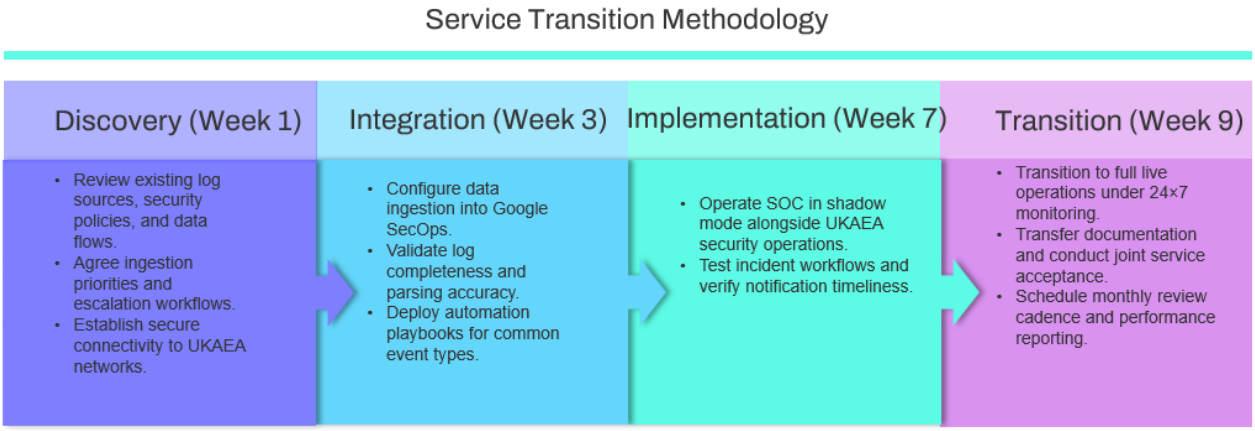
- Monthly Compliance Dashboard: visibility of SLA adherence, incident volume, and measurable performance metrics.

- Quarterly Governance Review: discussion of improvements, technology updates, risk posture, threat intelligence review, successes and lessons learned.
- Audit Evidence Pack: anonymised audit trails, training logs, and testing summaries.

Roc's approach ensures full visibility of our operations while maintaining the confidentiality and integrity of data.

### 3.2.12 Transition and Onboarding

A structured, low-risk transition process enables you to adopt the Managed Cyber service efficiently and without operational disruption. Roc applies a stage-gate transition methodology, proven across government and defence onboarding programmes:




### 3.2.13 Knowledge Transfer and Training

Roc will deliver training sessions and access workshops to the internal Cyber Security team, focusing on:

- Navigating Google SecOps dashboards and analytics.
- Understanding SOC alert classification and escalation.
- Reviewing and tuning detection rules.

Through a partnership approach, Roc will ensure that you gains not only a managed service and comfort in 24x7x365 monitoring, alerting, detection, and response but also the operational insight to verify and audit outcomes. We will commit to ensuring customers are able to be effective as a smart customer.

### 3.2.14 Collaboration and Service Management

Roc's partnership model ensures proactive collaboration and shared accountability. Governance, communication, and continual improvement are embedded throughout the service lifecycle.

Our service will be managed by a dedicated Service Delivery Manager (SDM) who acts as a single point of contact. The SDM ensures:

- Regular service reviews and KPI reporting.
- Coordination of improvement initiatives.
- Escalation management and contractual compliance.
- Adherence to SLAs and contractual obligations.
- Access to Roc SMEs, Practice Leads, and Senior Management.
- A single, holistic understanding of all customer change initiatives, in flight projects, and live services.
- Alignment and understanding of Customer processes and governance.

### 3.2.15 Performance Measurement

*The following Key metrics will be reported on monthly:*

- Incident volume and categorisation.
- Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- Number of automation playbooks executed.
- Threat coverage improvements and false positive rates.
- Progress on improvement initiatives
- Change control reporting
- Commercials (as appropriate)

*The following Collaboration Channels will be made available:*

- Monthly Service Review: As above
- Monthly SOC Steering Meeting: jointly chaired by Roc and Customer stakeholder leads.
- Quarterly Technology Review: roadmaps, innovation pipeline, and threat landscape updates.
- Quarterly Governance Review: discussion of improvements, technology updates, risk posture, threat intelligence review, successes and lessons learned.
- Ad-hoc Incident Review Workshops: post-event analysis and corrective actions.

### 3.2.16 Innovation and Continuous Improvement

Roc's Cyber service is not static. It evolves continuously to counter emerging threats and leverage technological advances, by leveraging AI and ML capabilities, we are able to access the necessary resources on a near-immediate basis to continually tune and amend our policies, processes, and ingestion rulesets.

#### Automation and AI Integration

- Use of Google SecOps AI capabilities for anomaly detection and risk scoring.
- Automated correlation of threat intelligence and contextual enrichment.

- Playbook-driven remediation for recurring or low-complexity incidents.
- Human-in-the-loop and fully automated playbooks.

### Proactive Threat Hunting

Roc's analysts perform structured threat hunts based on the MITRE ATT&CK framework, identifying latent threats that evade traditional detections. Findings are translated into new detection rules, improving future response.

### Learning and Development

Roc's Cyber Security analysts undertake continuous professional development in digital forensics, malware analysis, and cloud security. Insights are shared through regular knowledge-transfer sessions with clients. Through our strategic partnership with Google, we have access to exclusive training bootcamps, national, and international events – with early visibility and input into roadmap feature sets and training opportunities.

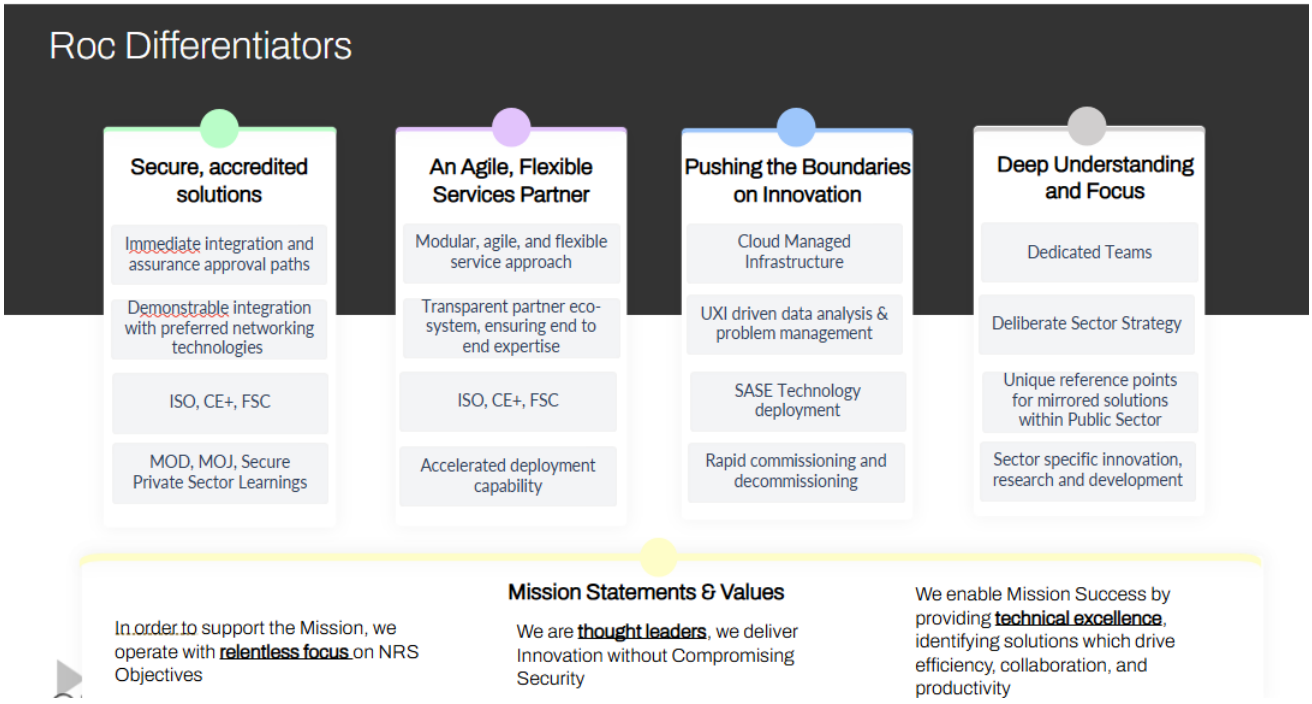
### Technology and Process Innovation

- Integration of SOAR workflows with case management and vulnerability systems.
- Continuous evaluation of new Google SecOps features and API integrations.
- Implementation of AI-assisted phishing analysis and behavioural analytics.

Roc's commitment to innovation ensures customers benefit from a SOC that remains state-of-the-art throughout the contract term and evolves to meet emerging, not just point in time, threats.

### Value Proposition and Differentiators

Roc Technologies provides a trusted, sovereign, and proven partner capable of delivering measurable security outcomes. Overall, we position ourselves as highly differentiated within the sectors the customer is aligned to, both across our portfolio and specifically within Cyber Security:




*Key Cyber Service Differentiators*

- UK Sovereign Operations: All monitoring, data processing, and support are performed within Roc's UK FSC and List-N accredited facilities.
- Government Provenance
- Google Partnership: Deep technical alignment with Google's SecOps engineering and strategy teams, enabling advanced feature deployment and use-case optimisation.
- SOC + NOC Integration: Combined monitoring enables faster anomaly detection and reduced downtime.
- Outcome-Focused Model: SLAs based on security outcomes and risk reduction, not merely activity levels.
- Human + Machine Synergy: AI automation accelerates response while SC-cleared analysts provide expert validation.

*Quantified Benefits*

- Reduction in mean time to detect and respond (target <30 minutes for critical incidents).
- Enhanced visibility across hybrid infrastructure.
- Improved compliance efficiency through automated reporting.
- Reduced total cost of ownership through integrated tooling.
- Continuous service uplift with zero operational downtime.
    - With a commitment to 100% availability of service

### 3.2.17 Summary and Next Steps

You requires a SOC and Cyber Services partner who can deliver resilience, transparency, and assurance while operating within the strict governance frameworks of a national research and innovation body. Roc Technologies' Managed Cyber service, underpinned by Google SecOps, provides this capability through proven technology, UK-based operations, and experienced personnel.

By partnering with Roc for this opportunity, Customers will:

- Achieve continuous 24x7x365 threat detection and rapid incident response.
- Maintain full visibility through shared access and transparent reporting.
- Strengthen compliance and reduce audit overhead.
- Leverage automation and AI to stay ahead of evolving threats.
- Build a sustainable, scalable security capability aligned to national standards.
- Benefit from successes and lessons learned across a wider, industry aligned customer base.
- Be positioned as a strategic customer of Google SecOps, benefitting from additional input into and visibility of future development roadmaps.
- Benefit from analyst training, provided by Roc as part of our commitment to partner enablement.

We welcome the opportunity to discuss this proposal further and demonstrate our platform's capabilities through a technical workshop or proof of concept.

#### Resource Augmentation for Complex Work Packages

Roc employs a wide ranging and highly skilled team aligned to the customer. Depending on the area of involvement, we are required to provide a blend of onsite and remote personnel with security clearances ranging from BPSS, SC and DV clearance to ensure seamless access and compliance. The team is comprised of the following personnel:

- SDM for service delivery oversight.
- Solution Architect technical architecture roadmap management.
- 1st-3rd Line Support Analyst teams for comprehensive operational support, incident and threat detection, and 24x7 support.
- Professional Service Consultants for specialised expertise.
- Data Architects and Automation Architects for play and run book automation, policy and configuration tuning.

# 4 Service Pricing

Refer to Roc's pricing document.

## 4.1 Onboarding Fees

For each new service provision, a one-time on-boarding charge will apply. This fee is charged to cover transition activity such as process definition, toolset configuration, system discovery, remote access configuration and knowledge management tasks. This charged will be in line with Roc's published Rate card and will vary based upon the nature and complexity of the environment to be on-boarded.

During the on-boarding process, Roc will review the configuration of each in-scope item. Where in-scope items have not been configured in-line with best practice, remedial actions may be required before the item can be on-boarded or covered by Roc's SLA's. Such remedial activity can be performed by the client or Roc. Where performed by Roc it can be funded via Roc's published Rate card or the Additional Service Points purchased as part of the service.

Roc follow a mature service transition process for on-boarding new Managed Services:

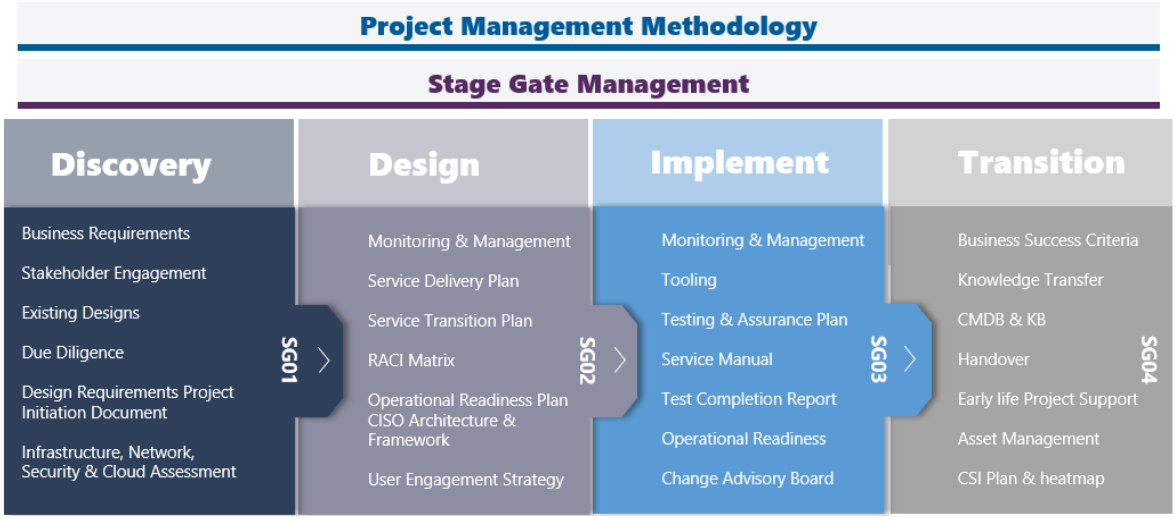



*Figure 1 – Roc Service Transition Process*

# 5 Terms and Conditions

Refer to Roc's Terms and conditions documents included with the submission. Standard terms are relevant to smaller one-off purchases, and the Master Service Agreement (MSA) is applicable for longer term contracts.