Service Definition: Google SecOPS Cloud Security Licenses

Crown Commercial Services | G Cloud 15 framework

Contents

Document Information

Client name	G Cloud 15 Service Definition
Project name	Google SecOPS Cloud Security Licenses.
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 1 Lindenmuth Way Greenham Business Park Greenham Thatcham RG19 6AD United Kingdom
Please refer all enquiries to:	**Gill Brown, 0845 647 6000** publicsector@roctechnologies.com.

Confidentiality Agreement

All information contained in this document, including any prices quoted, is to be treated as confidential. It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the express written permission of Roc Technologies Limited and shall be held in safe custody.

These obligations shall not apply to information that is in the public domain or becomes known legitimately from some source other than Roc Technologies Limited. All intellectual property rights of products or services provided by Roc Technologies Limited shall remain vested in Roc Technologies Limited.

Non-Disclosure

None of the information may be used by the client for any other purpose, nor may it be disclosed by them otherwise than, firstly to members of its staff who will be engaged in the evaluation and, secondly, to representatives of any organisation acting in the capacity of professional adviser to the client. Before making this document available for evaluation, the client must bring this notice to the attention of those concerned.

Proprietary Information

The information in this document has been reviewed and is believed to be accurate. However, neither Roc Technologies Limited. nor its affiliates assume any responsibility for inaccuracies, errors, or omissions that may be contained herein. In no event will Roc Technologies Limited or its affiliates be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

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 Description

1.1 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, including (Company Name)'s, 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 (Company Name)'s 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 (Company Name)'s change management process.
- Service API exposure allowing integration with (Company Name)'s own reporting or automation systems.

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.

1.2 SecOps SIEM Key Features

Unified Data Model (UDM) for normalized security telemetry

- Google SecOps uses a standardized schema (UDM) to convert raw logs into normalized records – enabling consistent event attributes (e.g., `principal.user.userid`, `network.src.ip`, `target.resource.name`) across many sources.

Massive data ingestion & cloud-scale retention

- Being built on Google infrastructure, the SIEM supports ingesting large volumes of telemetry (logs, alerts, flows) from on-premises, multi-cloud and SaaS systems.

High performance search & modern investigation experience

- Leveraging UDM indexing and enriched context, the platform supports near real-time searching (for indexed fields) and enriched investigation workflows.

Pre-built curated detections & custom rule creation

- The solution provides out-of-the-box detection content and lets organisations author custom rules using a native language (YARA-L or similar) against UDM-normalized data.

Entity context graph & relationship modelling

- The platform includes an entity context graph (users, assets, IPs, domains) capturing relationships (e.g., a user “owns” an asset) and enriches events with that context.

Flexible ingestion (raw logs or already UDM-structured)

- You can ingest logs as “unstructured” and let the platform parse them into UDM, or send data already formatted in UDM (via its ingestion API) for quicker processing.

Cross-environment visibility and multi-cloud/SaaS support

- The SIEM supports telemetry from on-premises, public clouds (GCP, AWS, Azure) and SaaS applications, enabling unified visibility across hybrid enterprise infrastructures.

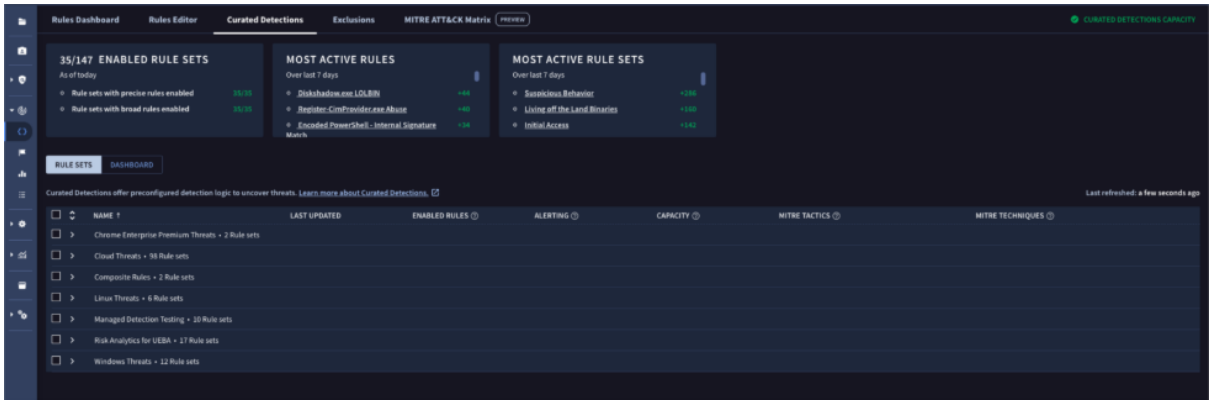
Advanced analytics, enrichment and threat intelligence integration

- With normalized data, the platform supports enrichment (e.g., geo-location, user/group info, asset criticality) and applies threat intelligence to detect sophisticated threats. Dashboarding, metrics and SOC operational reporting
- The solution provides built-in dashboards and metrics for SOC operations (e.g., alert counts, analyst performance, incident MTTR) alongside customisable visualisations.

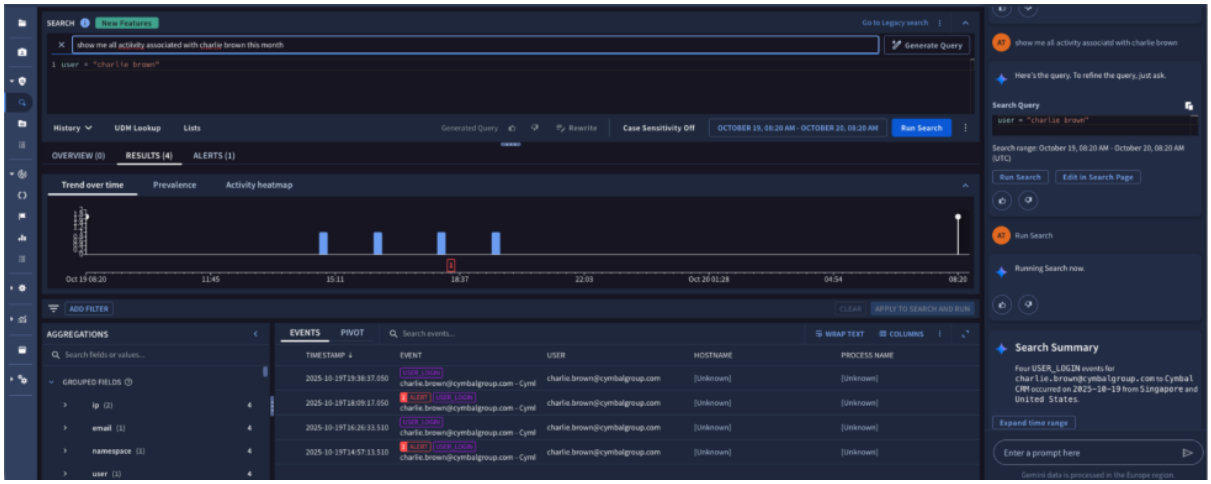
Scalable architecture with long-term retention and unlimited scaling

- Designed for large enterprises, Google SecOps’ SIEM supports years of data retention, petabyte-scale ingestion, and the ability to scale without worrying about infrastructure constraints.

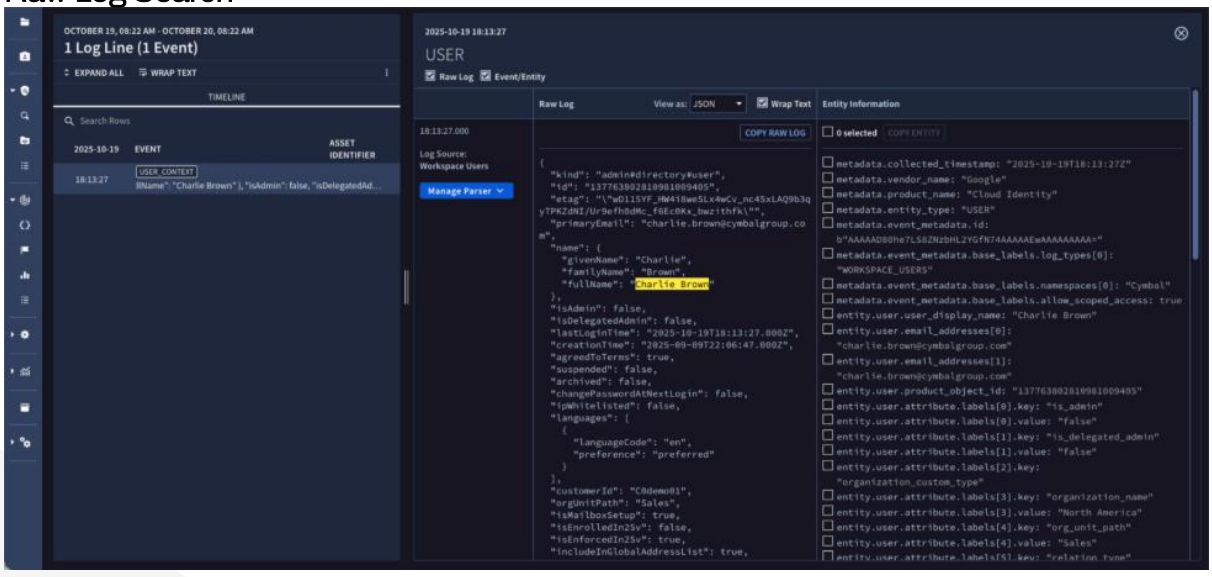
Curated SIEM Detection Rules



Gemini Powered SIEM UDM Search



Raw Log Search



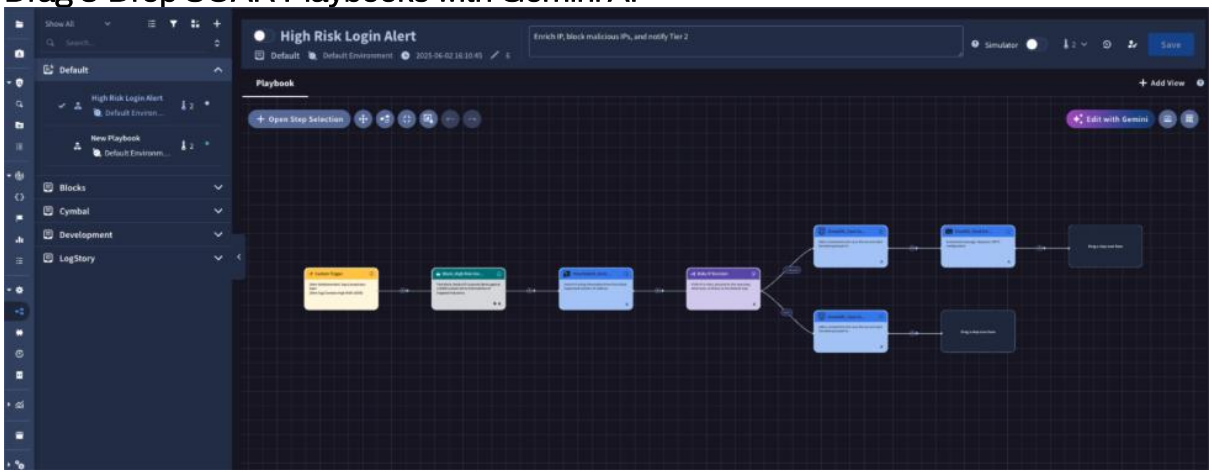
SOAR and Automation Framework

The integrated Security Orchestration, Automation and Response (SOAR) capability enables real-time containment and remediation.

Roc maintains a library of over 150 automation playbooks covering common attack types, credential compromises, phishing, malware containment, and insider-threat scenarios.

Playbooks can be triggered automatically based on event confidence scores or manually by analysts from either Roc or (Company Name), whether playbooks are automated or require manual (human-in-the-loop) triggering, will be assessed during onboarding, and then continually reviewed as part of continual service improvement and enhancement.

Drag & Drop SOAR Playbooks with Gemini AI



Key features include:

- Automated Response: Isolation of endpoints, account disablement, and IOC blocking within <5 minutes.
- Adaptive Playbooks: Parameterised workflows tailored to (Company Name)'s systems and authorisation boundaries.
- Integration Breadth: Hundreds of pre-built connectors including HPE-Aruba, Fortinet and most Linux distributions.
- Closed-loop Feedback: Post-playbook validation updates detection logic and reporting metrics.

This automation layer accelerates response, reduces human error, and allows (Company Name) analysts to witness every step of the incident lifecycle.

1.3 Analytics and Machine Learning

Roc have selected Google SecOps based on its advanced analytics engines and Google's search infrastructure, which gives it the ability to perform large-scale data correlation and anomaly detection.

Roc leverages built-in ML models to identify behavioural deviations, lateral movement, and rare process executions across millions of events per day.

Custom Roc-developed algorithms supplement these models for (Company Name) -specific telemetry, ensuring threat detections align to the MITRE ATT&CK and NCSC CAF frameworks.

Analytics outputs are visualised through dashboards accessible to both Roc and (Company Name) teams, enabling:

- Real-time risk scoring and trend analysis.
- Attack-path visualisation and contextual drill-down.
- Predictive modelling of emerging threats.
- Roll-up reporting
- Auditing and external evaluation

Live MITRE Mapping (Detections to ATT&CK Framework)

1.4 Platform Security and Compliance

The SecOps platform is secured through multiple defensive layers:

Control Area	Implementation
Access Control	RBAC integrated with Roc IdP and MFA for (Company Name) users
Data Protection	AES-256 encryption at rest; TLS 1.3 in transit
Audit and Logging	Immutable logs retained for 12 months and archived for 7 years
Segregation	Dedicated project namespace and VPC for (Company Name)
Vulnerability Management	Weekly scanning and monthly patch cycles
Backup & Recovery	Daily snapshots; 30-day point-in-time restore
Compliance Alignment	ISO 27001 Cyber Essentials Plus, NCSC Cloud Principles, NIST SP 800-207

2 Service Pricing

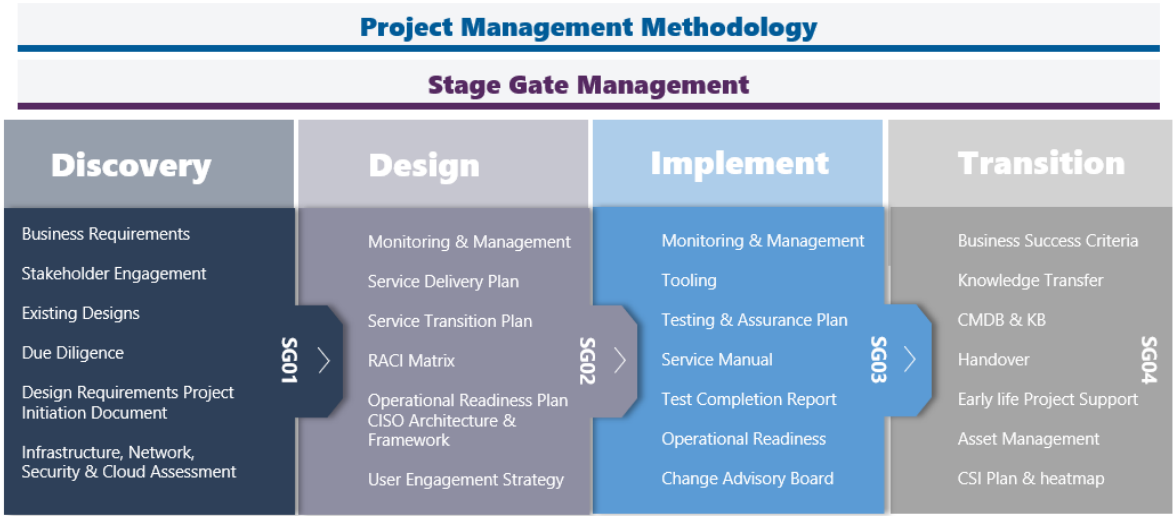
Refer to Roc's pricing document.

2.1 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 SFIA 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 SFIA 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:



Roc Service Transition Process

3 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.