KHIPU CYBER SECURITY

KHIPU Networks

Google SecOps, Cloud SIEM and SOAR

G-Cloud 15 Service Definition Document

Crown Commercial Service

By Royal Appointment to
His Majesty The King
Cyber Security Provider
KHIPU Networks Limited
Hampshire

VERSION: 1.1
DATE: 30th January 2026

All information disclosed within this document is confidential. It shall not be disclosed in whole or part to any third party or to any employees other than those who have a need to know such information.

Date of Issue:	30th January 2026
Document Version and Reference:	1.1
Controlling Author(s):	Steven Pearson
Approval:	Matt Ashman

KHIPU Networks is a fully certified company to the following quality standards:

- ISO9001 Quality Management
- ISO27001 Security Management
- ISO14001 Environmental Management
- ISO45001 Occupational Health and Safety Standard
- Cyber Essentials Plus

KHIPU Networks supports the National Apprenticeship Scheme and employs and develops apprentices within all sectors of the company.

KHIPU Networks Limited
Company Number: 5218573
Switchboard: +44 (0)345 272 0900
Support: +44 (0)345 272 0910

UK Office
3 Waterfront Business Park
Fleet
Hampshire
GU51 3TW

sales@khipu-networks.com
@KHIPUNetworks
www.khipu-networks.com

KHIPU Networks South Africa (PTY) Limited
Company Number: 2012/180716/07
Switchboard: +27 (0)41 393 7600
Support: +27 (0)41 393 7601

Gqeberha Office
Office 1 Block 1, Greenacres Office Park
2nd Avenue
Newton Park
Gqeberha

Cape Town Office
13 Waterford Mews
Century City
Cape Town

TABLE OF CONTENTS

What is the Service?

Service Name

Google SecOps, Cloud SIEM and SOAR

Service Description

Google SecOps (formerly Chronicle) offers a unified experience across SIEM, SOAR, and threat intelligence to drive better detection, investigation, and response. Collect security telemetry data, apply threat intel to identify high priority threats, drive response with playbook automation, case management, and collaboration.

Service Categories

Systems Infrastructure Software

Security

Security analytics

- Security analytics

Governance, risk and compliance

- Governance, risk and compliance

Service Features

- Ingest data from SaaS and on-prem. Store for 12 months
- Monitor the ongoing health of your data pipelines
- Correlate petabytes of telemetry with predefined rules
- Map alerts to specific threats MITRE ATT&CK security framework
- Simplify detection authoring with YARA-L to build custom content
- SIEM and SOAR functionality
- Unify and enrich telemetry onto a single, correlated timeline view
- Get actionable threat information with sub-second search
- Integration with 3rd party products into SecOps SOAR

Service Benefits

- Hyper-scale, fast, and cost-efficient data lake and analytics platform
- Leverage Google curated detections to find the latest threats
- Manage, prioritise and assign work with unique threat-centric case management
- Investigation views, visualisations, threat intel insights, user aliasing
- Investigate with full context, including anomalous assets and domain prevalence
- Enterprise Package includes Enriched Threat Intelligence and UEBA
- Enterprise Plus Package includes Premium Threat Intelligence

Service Scope

Cloud Deployment Model

- Public cloud

Constraints

Log data is limited to 365 days, unless a separate GCP bucket is configured for longer term retention. Advanced functionality is included at additional cost.

System Requirements

- Connectivity to the internet from the on-premise SecOps forwarder
- VM or PAAS environment SecOps Forwarders (Docker/Linux image)
- Connectivity to the internet from the SecOps SOAR Remote Agent
- VM or PAAS environment for SecOps SOAR Remote Agents

Reselling

Supplier Type

I’m a reseller providing extra features and support not available from the original supplier

Organisation whose services are being resold

Google SecOps

Compliance and Certifications

Certifications

KHIPU can confirm that we are Cyber Essentials Plus certified.

KHIPU adhere to ISO policies and procedures. We are certified to:

- ISO9001 (Quality Management)
- ISO27001 (Information Security Management)
- ISO14001 (Environmental Management)
- ISO45001 (Occupational health and safety)

Any potential breach or risk of security or process is highlighted to senior management including the board of directors immediately.

We comply fully with UK GDPR and the Data Protection Act 2018. All personal data is processed lawfully, fairly, and transparently, with appropriate technical and organisational measures in place to ensure confidentiality, integrity, and availability. Data is stored and processed within secure environments that meet ISO27001 standards, and encryption is applied to data at rest and in transit. We maintain strict access controls, role-based permissions, and multi-factor authentication to prevent unauthorised access. Our processes include regular security audits, penetration testing, and adherence to NCSC guidance. We support data subject rights, including access, rectification, and erasure, and provide clear procedures for handling data breaches, notifying customers within agreed timelines.

We are committed to achieving Net Zero by 2050 in line with UK Government policy and PPN 06/21. Our Carbon Reduction Plan (CRP) is published on our website and includes:

- Remote service delivery and reduced travel.
- Energy-efficient equipment.
- Collaboration through initiatives like Techies Go Green.
- Regular ISO 14001 audits for environmental sustainability

Social Value

KHIPU fully comply with the Public Services (Social Value) Act 2012 and the CCS Social Value Model. Our commitments include:

- Creating employment and apprenticeship opportunities, particularly for underrepresented groups.
- Supporting skills development and in-work progression through training and mentoring.
- Promoting equality, diversity, and inclusion in recruitment and supply chains.
- Delivering environmental benefits by reducing carbon emissions and supporting clean energy initiatives.
- Engaging with local communities and stakeholders to co-design and deliver social value outcomes. We have governance processes in place, including a nominated CCS Social Value Contact, to ensure delivery and reporting of social value commitments throughout the contract lifecycle.

Operational Details

User Support

Traditional Services

As with all of our supplied and installed solutions, our Technical Assistance Centre (TAC) is available to provide maintenance, support and managed services with a number of different levels (SLA's) to our customers. The following is available within our support, maintenance and managed service options:

- Network Operations Centre (NOC): Monday to Friday, 24x7x365(6) and bespoke days / hours of cover.
- Security Operations Centre (SOC): Monday to Friday, 24x7x365(6) and bespoke days / hours of cover.
- Pro-active monitoring, alerting and support "KARMA™".
- Telephone, email, SMS and remote access support.
- Next Business Day, 4-hour hardware replacement (with / without engineer) options.
- Flexible tailored managed services "adds, moves and changes" of a customer's environment (OPEX, CAPEX and flexible models).
- Configuration management and change control.
- Updates, upgrades and software releases (major and minor).
- Quarterly health checks and preventative maintenance.
- Professional services / Support Tokens such as for onsite and offsite (remote) configuration, changes and upgrades, assistance to cover staff shortages, an "extra pair of hands" etc.
- Annual or Multi-year 'Pre-paid' Service packages.

Using our unified communications platform, our 24x7x365(6) manned NOC and SOC, our TAC provides a single point of contact for the following

- Reporting issues and faults.
- Technical queries and general requests for information.
- Progress updates on KHIPU TAC calls.
- Remote problem investigation e.g. remote support.
- Upgrades / Software Releases (major and minor).
- Advanced hardware replacement
- Escalating issues to the Escalations Manager.

After Sales Account Management

Account management is one of our key strengths when working in partnership with our customers, to support the commercial and technical aspects within the service delivery team. For all projects, we allocate the following senior account management team to the customer:

- **Chief Commercial Officer**; responsible for future strategies and overall relationship between KHIPU and the customer
- **Account Manager**; responsible for day to day queries, general updates, generate quotes, organising account management and service review meetings, providing product updates, invitations to events, new features, new solutions and offerings
- **Chief Information Officer**; Similar to the Chief Commercial Officer's role but from a technical perspective
- **Technical Account Manager**; responsible for the day-to-day relationship from a technical perspective.

We also provide effective account management through:

- Regular email and phone calls
- Quarterly onsite account management meetings

As part of our extensive after sales support, regular service review meetings are held with our customers. These are extremely important in the on-going successful management of our deployed solutions, maintenance, support and managed services. We believe this is the best mechanism to review all commercial aspects of the relationship including charges throughout the lifetime of the maintenance contract, based upon experience of product reliability and service performance.

More in-depth information regarding our account management process and our service review agenda is available upon request.

Email or Ticketing Support

KHIPU delivers support packages with associated SLAs. The response time SLA is linked to the priority of the incident. Response times can vary from 30 minutes (Priority 1) to 4 hours (Priority 4), depending upon the severity of the support call logged. We can also offer bespoke support packages that allow the initial response time to be tailored to the environment if required. The initial response time does not differ based upon the time of day nor day of the week.

Phone Support

Yes, phone support is available 24x7.

Web chat Support?

No

Onsite Support

Onsite support is available but at an extra cost.

Support Levels

KHIPU's ethos is to provide outstanding technical and after sales support, both during and after a project implementation. To evidence this, we have a number of exceptional customer references should customers wish to speak with them. For all supplied solutions we provide maintenance and support services, with all of the proposed equipment being supported and maintained by KHIPU to the required level based upon the customers' cover. The following is included within our available support/maintenance services:

- Maintain Services: Break-fix support with 1st, 2nd and 3rd line troubleshooting for all KHIPU delivered solutions. KHIPU holds top-level certifications and works directly with manufacturers as required.
- Monitor Services: Proactive monitoring, alerting and analysis.
- Fully Managed Service: Complete responsibility for device management.
- Co-Managed Service: Shared responsibility for device management.
- SOC Service: Comprehensive detection and response to protect critical infrastructure from cyber threats.

All services are available 24x7x365 or during business hours (08:00–18:00) and include support via telephone, email, secure portal and remote access.

KHIPU would also assign a Technical Account Manager to every customer, who would be responsible for ensuring that SLA's are met in the event that customers call upon the agreed support service.

Support Available to Third Parties?

Yes

Asset Protection

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

- United Kingdom
- European Economic Area (EEA)

User control over data storage and processing locations

Yes

Penetration testing frequency

At least every 6 months

Data sanitisation process

Yes

Data sanitisation type

Explicit overwriting of storage before reallocation / Secure Erase

Security and Compliance

Staff Security Clearance

Staff screening performed which conforms to BS7858:2019

Government Security Clearance: Up to Security Clearance (SC)

KHIPU adhere to ISO policies and procedures. We are certified to ISO9001 (Quality Management), ISO27001 (Information Security Management), ISO14001 (Environmental Management) and ISO45001 (Occupational health and safety). Any potential breach or risk of security or process is highlighted to senior management including the board of directors immediately.

Cyber Essentials

KHIPU can confirm that we are Cyber Essentials Plus certified.

Exit Planning

End-of-contract data extraction

KHIPU End-of-Contract Data Handover Checklist:

When a contract ends, KHIPU ensures a secure and compliant process for returning customer data if requested:

1. Data Identification Confirm all customer-owned data, including logs, reports, configurations, and backups, across systems covered by the agreement.
2. Data Extraction Prepare data in the agreed format (e.g., encrypted files, CSV, PDF) and verify completeness and integrity before transfer.
3. Secure Transfer Use encrypted channels such as secure portals or physical media. Apply encryption for data at rest and in transit, and confirm authorised recipient access with multi-factor authentication.
4. Customer Confirmation Obtain written confirmation that the data has been received and validated for integrity and usability.
5. Data Destruction Remove all residual copies from KHIPU systems and confirm deletion within the agreed timeframe.
6. Compliance Ensure all steps comply with GDPR and Data Protection Laws. The process is documented for audit purposes.

This structured approach guarantees security, transparency, and legal compliance during the data handover process.

End-of-contract process

At the end of the contract, if the organisation chooses not to renew and continue with the service, all data pertaining to the organisation is deleted. If the organisation chooses to renew then the service continues as normal. 90-days prior to the contract expiration date an initial reminder email is sent, followed up by gradually increasing reminders until the date of expiration. Included in the Price Data extraction and secure transfer in standard agreed formats. Customer confirmation and validation process. Secure deletion of residual data. Compliance with GDPR and legal requirements. Additional Costs Bespoke data formats or media (e.g., physical drives, custom encryption). Accelerated timelines for data handover or destruction. Extended storage beyond the agreed retention period. Consultancy or technical support for data migration to third-party systems.

Change Management

Configuration and change management standard

Supplier-defined controls

Configuration and change management approach

All service configuration changes follow an ITIL-based Change Control Process. Requests must be logged via the KHIPU Support desk and submitted by authorised personnel only. Each change is assessed for technical suitability, security risks, and service impact. Findings are clearly communicated to the customer, who makes the final decision to proceed, including consideration of any commercial implications. This process ensures a full audit trail and that all aspects of the change are reviewed before implementation.

Vulnerability management type

Supplier-defined controls

Vulnerability management approach

KHIPU uses continuous scanning tools like Tenable Nessus and Qualys to identify vulnerabilities across servers, applications, and networks. Findings are assessed using CVSSv3 and prioritised from Low to Critical. Asset and service owners remediate issues with critical/high vulnerabilities within 14 days of discovery. The process includes identification, classification, remediation, and verification, with reports provided within five business days post-remediation. Threat intelligence is sourced from vendor advisories, industry platforms, and external feeds, ensuring timely updates and compliance with ISO27001 and Cyber Essentials Plus. This proactive, risk-based approach enables rapid response and strong security across all services.

Protective monitoring type

Supplier-defined controls

Protective monitoring approach

KHIPU provides 24x7x365 protective monitoring via its Security and Network Operations Centre using Cyber Managed Detection and Response (CMDR). Servers, firewalls, and critical assets are continuously monitored for abnormal behaviour, trend anomalies, and suspicious logs. Potential compromises trigger real-time alerts, followed by immediate triage, severity validation, and escalation to technical teams. Customers are informed through agreed channels. Response times meet strict SLAs: critical within one hour, high within two, and medium/low within four. This proactive approach, combining automated monitoring, early indicators, and structured escalation, ensures rapid detection and resolution while maintaining compliance and service integrity.

Incident management type

Supplier-defined controls

Incident management approach

KHIPU's approach to incident management is ITIL-aligned and prioritises rapid resolution. Customers log incidents via telephone, email or support portal with required details. Cases are categorised by priority in agreement with the customer: P1 – Urgent: Critical outages or major incidents requiring immediate attention P2 – High: Significant issues affecting functionality, not completely halting operations. P3 – Medium: Moderate impact, e.g. warnings or non-critical alerts. P4 – Low: Minor issues, or informational requests with negligible operational impact. Service-affecting incidents are escalated to 2nd/3rd line teams and account/technical managers. Escalation procedures and SLAs are provided during onboarding, ensuring transparency and accountability.

Version History

Version	*Date*	Change
1.1	30th January 2026	Approved release

Confidentiality Statement
The information set out in this document that is marked 'Customer / Company Confidential' may include, but not be limited to, information such as itemised prices, design documents, plans and any information relating to KHIPU Networks' clients. This information is communicated in confidence, and disclosure of it to any person otherwise than with KHIPU Networks' consent will be treated as a breach of confidentiality.

Furthermore, the disclosure of information that is commercially confidential to KHIPU Networks may, or may be likely to, prejudice KHIPU Networks' commercial interests. Such commercially confidential information will be exempt from the duty to confirm or deny and from disclosure under the Freedom of Information Act 2000.

Disclaimer
This document is provided for information purposes only. KHIPU Networks accepts no responsibility for any errors or omissions that it may contain.

This document is provided without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In no event shall KHIPU Networks be liable for any claim, damages or other liability (either direct or indirect or consequential), whether in an action of contract, tort or otherwise, arising from, out of or in connection with this document or the contents thereof. All goods and services are supplied subject to KHIPU Networks / G-Cloud 15 framework terms and conditions.

Freedom of Information
For the purposes of the Freedom of Information Act 2000, itemised price information contained in this document (but not the total price) is communicated in confidence. Without prejudice to the foregoing, KHIPU Networks acknowledges that third parties may be required to release into the public domain KHIPU Network's name or the total price submitted (or both). KHIPU Networks does not normally object to the release of this information.

KHIPU