

G-CLOUD 14 BY LRQA

G-Cloud 14 SOC-as-a-Service Pricing

Prepared for G-Cloud 14

Cloud Support Services
2024

LRQA



Contents



- 3 SOC-as-a-Service Pricing
- 4 Endpoint Detection and Response
- 5 Service Configuration
- 6 Additional Optional Components
- 7 CIRT Incident Response Retainer

SOC-as-a-Service Pricing



The Core component of the Service Offering is based on the volume of data and logs ingested to LRQA Security Information and Event Management (SIEM). The LRQA SOC then performs 24/7 Analysis, Monitoring and Detection of events, logs and alerts.

MPS/EPS	Annual Cost	Year One Setup Cost
50	£43065	£13487.50
100	£50475	£13487.50
250	£73545	£15725
500	£107295	£18425
750	£133545	£22175
1000	£154095	£28950
1250	£175845	£28950
1500	£195195	£32900
2000	£248895	£38300
2500	£302595	£38300

- Includes 24/7 SOC service, all software required, quarterly management reports and service delivery reporting with a dedicated service delivery manager, dedicated account manager.
- LRQA will work with you to best size the required SOC-as-a-Service solution to meet your exact needs.
 - The SOC-as-a-Service solution will be subject to assumptions regarding scale and complexity and/or additional options as listed in the accompanying service description and in this document.
 - We will regularly invoice in advance on the invoice schedule defined in the Service Order.
 - All invoices will be payable within 30 days.
 - VAT is not included in our rates.

Endpoint Detection and Response



An optional component of the Service Offering is based on number of assets protected. The LRQA SOC then performs 24/7 Analysis, Monitoring and Detection of events, logs and alerts.

MPS/EPS	Annual Cost	Year One Setup Cost
50	£4,057.50	£2,700
100	£6,115.00	£2,700
250	£12,287.50	£3,375
500	£22,575.00	£4,050
750	£32,862.50	£4,050
1000	£43,150.00	£4,725
1250	£53,437.50	£4,725
1500	£63,725.00	£4,725
2000	£84,300.00	£4,725
2500	£89,875.00	£5,400



Service Configuration



SOC-as-a-Service Configurations

SOC-as-a-Service Configurations		Included
CORE SERVICE		
1	Business Intelligence Workshop with Threat modelling and detection design included as part of Service Implementation	✓
2	Deployment and configuration of MDR tooling, and onboarding of log sources and devices	✓
3	24/7/365 Sophisticated Managed Detection & Response delivered by LRQA SOC	✓
4	Next-Gen Industry leading SIEM Technology (LogRhythm) Unified platform with advanced AI engine, Threat Detection and Analytics	✓
5	Continuous review of events, alarms and health Management of all incidents and events raised	✓
6	Online Dashboard Web console showing health status, trends and incident information	✓
7	LRQA Custom developed and designed detections	✓

SOC-as-a-Service Configurations		Included
CORE SERVICE		
8	3 years (36 months) Log and Data Archive retention	✓
9	Design & Implementation of Playbooks and SOAR automation	✓
10	Integration & configuration of Threat Intelligence and 3rd party security services & tools	✓
11	Enhanced Security and service level reporting	✓
12	Aligned Service Delivery Manager with regular reviews	✓
13	Initial Incident Assessment and Management - 30 min review and investigation of High priority Incidents	✓
14	Pro-Active Indicator of Compromise (IoC) Search and Investigation Conducted by SOC Analysts	✓

Additional Optional Components



SOC-as-a-Service Additional Components	
ADDITIONAL COMPONENTS	
1	CIRT Incident Response Retainer <ul style="list-style-type: none">Cyber Response Onboarding24 x 7 IR Retainer with 4 hour response SLA, Cyber Response engagement & Incident ManagementAnnual Tabletop exercises
2	CIRT Incident Response Professional Services <ul style="list-style-type: none">Digital Attack Surface AssessmentRansomware Resilience assessmentCyber Response Planning and exercisingIncident response Policy assessmentThreat Hunting
3	Technical Cyber Account Manager <ul style="list-style-type: none">Aligned Security Expert providing enhanced technical and service supportAssist with the design and implementation of new services, scope and detectionsDedicated client technical escalation point
4	Managed EDR & EPP <ul style="list-style-type: none">Fully Managed Endpoint Protection, Detection and response technologies provided by Crowdstrike

SOC-as-a-Service Additional Components	
ADDITIONAL COMPONENTS	
5	Managed NDR – Network Detection & Response <ul style="list-style-type: none">Real time deep packet analysis, analytics and capture of Network traffic providing enhanced and additional protection seamlessly integrated to LRQA SOC
6	Managed Vulnerability Scanning <ul style="list-style-type: none">Continuous vulnerability scanning of your environments and services utilising the powerful tenable cloud solutionProactive Vulnerability alerts and notificationCustom dashboard and risk reporting
7	Managed Network Services <ul style="list-style-type: none">Managed NOC services providing 24/7/365 support of network security products (such as Firewalls, IPS/IDS, 2 factor, etc)

CIRT Incident Response Retainer



Managed IR		Bronze	Silver	Gold
CIRT RETAINER				
1	24 x 7 IR Retainer with 4-hour Response SLA	✓	✓	✓
2	Bank of Retained DFIR Hours in the Event of a Cyber Incident*	30 Hours	60 Hours	90 Hours
3	Crisis & Incident Management with Aligned Cyber Response Incident Manager	✓	✓	✓
4	Aligned Cyber Response Engagement Manager	✓	✓	✓
5	Annual 2-day IR Simulation & Tabletop Exercise	✓	✓	✓
6	Incident Response Policy Review & Assessment	✓	✓	✓

* Cyber Incident Response Service Options. Key: ✓ Optional ✓ Standard

Important:

- Bank of Retained hours does not roll over annually.
- Bank of Retained Hours can be used flexibly for other Incident response professional services activities.





Get in touch

Visit www.lrqa.com for more information



UK Head Office 1 Trinity Park Bickenhill Lane Birmingham B37 7ES	Americas 810 Seventh Avenue Suite 1110 New York NY 10019	Asia Pacific 460 Alexandra Road #15-01 mTower Singapore 119963	Europe Fidiou 9 Athina 106 78 Greece
---	---	---	---

