Security Operations Service

What is the Security Operations Service?

The Security Operations Service is a cloud-hosted cyber security solution that can see your organisation's entire IT estate, all the time, enabling complete visibility helping to identify suspicious activity, ensuring you have an up-to-date view of possible threats. Unlike other traditional cyber monitoring systems, the Security Operations Service combines people, process and technology to protect brand and reputation.

There's a growing demand for an end-to-end cyber security solution, given the need to keep pace with the rising expectations for online services such as always-on, hyper connected and secure applications. To meet this expectation, organisations are investing in distributed IT estates underpinned by cloud services, but this increases the potential attack surface and data sprawl across the estate. Whilst this delivers modern applications, it does present a cyber security challenge given this model exposes organisations beyond the traditional data centre, taking them into multi-cloud, hybrid cloud and on-premises deployments.

Utilising e2e-assure's capability performing services such as traffic analysis; deep packet inspections; Intrusion Detection Systems; vulnerability scanning; blacklist monitoring of the assets that matter to you; highly skilled Security Operations Centre (SOC) personnel and UKCloud's highly connected, highly secure cloud platform, we deliver a SOC that can see your entire IT estate and is always available.

What the service can help you achieve

- Provides an end-to-end cyber security capability, continual cyber defence with alerts and incident response, helping you identify threats before they become incidents
- Integrates with existing toolsets to ensure that you're getting best value from your existing cyber investments
- Provides process support for your SOC with a variety of support options available, from online training and helpdesk to managed SOC functions
- Monitors your workloads at OFFICIAL, OFFICIAL-SENSITIVE and Above OFFICIAL classifications
- Simplifies the management of the increasing attack surface of your cyber security environment by providing a consistent security management service for all your workloads
- Improves the level of cyber capability / skills within your own organisation with tailored support options
- Helps you take control of your own security operation monitoring or have events proactively triaged by highly trained remote SOC analysts, reducing resource requirements for a growing threat landscape

Product options

The service is designed to be flexible and enables you to choose from the options below to match your requirements.

Service tier	Description
Premium / Plus SOC as a Service (including Platform Only and Enhanced capabilities)	A complete cyber solution including: • Professional Services - discovery through to delivery and management (priced separately, see Professional Services Service Definition) • Identify root causes providing deeper remediation support as required • Automated Cyber Defence Remediation as agreed • Remote portal, dashboard and case management tools • Expert SOC analysts, includes event and incident reporting, security processes management • Forensic investigation and malware analysis
Enhanced SOC as a Service (including Platform Only capabilities)	• Alerts triaged by highly trained analysts to mitigate risks • Asset Management and Threat Model • Runbook support and development • Remediation support to reduce recurrence of threats • Portal access for reports and dashboards including monthly reviews • In-house security teams supported by highly trained SOC analysts

Platform Only – Basic SOC	• Cumulo protective monitoring dashboard:
	  ○ Collect events, logs and other threat intelligence continuously
	  ○ High priority alerts within 15 minutes of detection
	  ○ Generates alerts on a 24/7 basis
	  ○ SOC triage and filtering of noise gives clear warnings and helps trigger timely responses
	  ○ You choose to create notifications via email
	• Enable your in-house security operation team to investigate events and threats

Pricing and packaging

Security Operations Service pricing can be as low as £1.96 per asset per month. Full pricing with all options is available in the UKCloud Pricing Guide. Customers will also need to purchase the appropriate UKCloud infrastructure to host the Security Operations Service solution.

Premium Plus SOC as a Service			
Number of IP addresses / devices / users monitored	**Setup / onboarding**	**Per band pricing (monthly)**	**12 month SOC (excluding infra)**
1-128	£5,175.00	£6,313.87	£75,766.42
129-256	£8,625.00	£9,217.04	£110,604.52
257-512	£11,443.00	£13,136.33	£157,635.95
513-1000	£20,125.00	£22,136.17	£265,634.06
1001-2000	£29,325.00	£36,282.16	£435,385.93
2001-4000	£40,020.00	£54,423.24	£653,078.89

Premium SOC as a Service			
Number of IP addresses / devices / users monitored	**Setup / onboarding**	**Per band pricing (monthly)**	**12 month SOC (excluding infra)**
1-128	£3,105.00	£3,120.38	£37,444.51
129-256	£4,025.00	£4,717.12	£56,605.46
257-512	£9,200.00	£7,329.98	£87,959.75
513-1000	£17,250.00	£11,975.06	£143,700.71
1001-2000	£24,150.00	£21,766.29	£261,195.43
2001-4000	£34,500.00	£32,649.43	£391,793.14

Enhanced SOC as a Service			
Number of IP addresses / devices / users monitored	**Setup / onboarding**	**PaaS band pricing (monthly)**	**12 month PaaS (excluding infra)**
1-512	£4,025.00	£3,630.51	£43,566.07
513-1000	£11,500.00	£6,088.30	£73,059.59
1001-2000	£17,250.00	£10,989.54	£131,874.50
2001-4000	£26,220.00	£16,484.31	£197,811.76

Platform Only – Basic SOC			
Number of IP addresses / devices / users monitored	**Setup / onboarding**	**PaaS band pricing (monthly)**	**12 month PaaS (excluding infra)**
1-1000	£11,500.00	£2,899.19	£34,790.28
1001-2000	£17,250.00	£5,233.12	£62,797.38
2001-4000	£26,220.00	£7,849.67	£94,196.07

Accreditation and information assurance

The security of our platform is our number one priority. We've always been committed to adhering to exacting standards, frameworks and best practice. Everything we do is subject to regular independent validation by government accreditors, sector auditors and management system assessors. Details are available on the UKCloud website.

Connectivity options

UKCloud provides one of the best-connected cloud platforms for the UK public sector. We enable access to our secure platform by DDoS-protected internet, PSN, Janet, HSCN, MCN and your own leased lines via our HybridConnect or CrownConnect services. The full range of flexible connectivity options is detailed in the UKCloud Pricing Guide.

An SLA you can trust

We understand that enterprise workloads need a dependable service that underpins the reliability of the application to users and other systems, which is why we offer one of the best SLAs on G-Cloud. As the SLA varies based on the chosen cloud technology, you can find full details on each service's SLA, including measurements and service credits, in the SLA Definition article on the UKCloud Knowledge Centre.

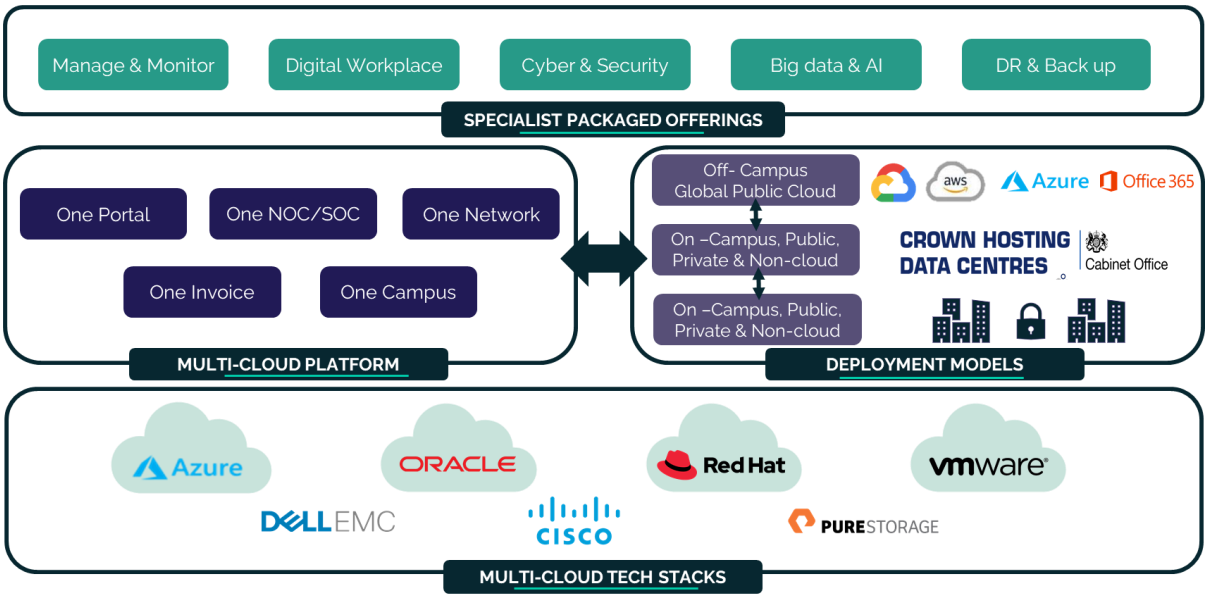
The small print

For full terms and conditions including onboarding and responsibilities, refer to the Terms and Conditions documents.

For full information regarding this product, we have relevant documents on our Knowledge Centre.

Why UKCloud?

UKCloud is dedicated to the digital transformation of our nation's public services through our flexible, secure and cost-effective multi-cloud platform and the expertise of our people and partners. We believe that diversity of technology drives value and innovation and so we bring together different cloud technologies, with different deployment models spanning on-premises (private cloud), on-campus (Government's Crown Campus) and off-campus global public cloud services. This enables you to choose the right cloud for creating new workloads or migrating or replacing existing applications to the cloud with specialist SaaS solutions.



We recognise the importance of public services to UK citizens and businesses, which is why we include the highest level of support to all our customers at no extra cost. This includes dedicated 24/7 UK support, a Network Operations Centre (NOC), utilising protective and proactive monitoring tools, and access to UKCloud's experts. UKCloud can also provide outcome-based professional services or managed services to help you with digital transformation.

UKCloud Ltd
A8 Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX

+44 (0)1252 303300
info@ukcloud.com
www.ukcloud.com