Fimatix AWS-Native Security Operations Centre (SOC)

G-Cloud 14 Service Description (UK Government)

Service description

The Fimatix AWS-Native Security Operations Centre (SOC) is a managed cloud security monitoring and incident response service for UK public sector organisations operating workloads on Amazon Web Services (AWS). The service provides continuous visibility of security events, detection of cyber threats, and automated response capabilities using AWS-native security services.

The service is designed to support government organisations in protecting sensitive data, maintaining service availability, and meeting security and assurance obligations in line with UK Government and National Cyber Security Centre (NCSC) guidance.

Who this service is for

This service is intended for UK public sector bodies including central government departments, executive agencies, arm's-length bodies, local authorities, NHS organisations, police forces, and emergency services that use AWS cloud services.

Features

- Centralised AWS security monitoring
- Managed threat detection and alerting
- Vulnerability and misconfiguration identification
- Automated incident response workflows
- Security posture and compliance visibility
- Cloud-scale log and event management
- Integrated investigation and forensic tooling
- Multi-account AWS governance support

Benefits

- Faster detection and response to cyber threats
- Improved protection of government data
- Reduced operational burden on internal teams

• Scalable security aligned to cloud growth

• Improved audit, assurance, and reporting

• Use of fully managed AWS services

• Reduced tooling complexity and overhead

Service scope

Included:

• Configuration of AWS-native security services

• Centralised collection of security logs and findings

• Threat detection and prioritisation

• Automated response playbooks

• Security dashboards and reporting

Not included:

• Monitoring of non-AWS environments

• End-user or endpoint device security

• 24/7 staffed SOC unless agreed separately

• Legal or regulatory breach management

How the service is delivered

The service is delivered using AWS-native security services deployed within the buyer's AWS environment. Security data is collected, analysed, and retained in UK AWS regions unless otherwise agreed. Automated workflows are used to respond to defined security events, with customer oversight and approval where required.

Security

The service supports alignment with the UK Government Security Policy Framework, NCSC Cloud Security Principles, CIS AWS Foundations Benchmark, and ISO/IEC 27001-aligned controls. All security data remains under customer ownership.

Data residency

All service data is stored and processed within UK AWS regions unless explicitly agreed otherwise. The supplier does not remove customer data from the AWS environment.

Pricing

Pricing is based on the size and complexity of the AWS environment, the AWS services enabled, and the delivery model selected (implementation-only, co-managed, or managed service). AWS consumption charges are billed separately.

Contract duration

The service is available under standard G-Cloud framework terms. Contract lengths can be agreed in line with buyer requirements.

Onboarding and offboarding

Onboarding includes service setup, configuration, and knowledge transfer. Offboarding includes handover of documentation, dashboards, and configurations to the buyer.

Service levels

Service levels, response times, and escalation procedures are defined and agreed with the buyer during service onboarding.

Dependencies

The service requires access to supported AWS services, appropriate IAM permissions, and where applicable AWS Organisations for multi-account environments.

Assumptions and constraints

The service operates within the AWS shared responsibility model. Detection capability is limited to AWS-native services and their supported regions.