Cloud/Security Monitoring & Incident Response

Service Definition

G-Cloud 15 – Lot 3: Cloud Support Services

Spirit UK Managed Services Ltd

---

1. Service Overview

Cloud/Security Monitoring & Incident Response is a managed support service that provides continuous monitoring, triage, investigation, and response support for security and technology events affecting cloud environments.

Spirit UK delivers this service to help organisations detect and respond to outages and cyber security threats within platforms such as Google, Amazon, Microsoft Azure and Microsoft 365. The service focuses on early detection, rapid response, and operational containment, reducing the likelihood and impact of all incidents.

This service is designed as a support-led, SOC-lite capability, suitable for organisations without an in-house security operations centre.

---

2. Service Objectives

The objectives of this service are to:

- Detect security threats and suspicious activity early

- Reduce time to identify and respond to incidents
- Support effective containment and remediation actions
- Improve visibility of cloud security posture
- Reduce operational and reputational risk

---

3. Scope of Service

3.1 In-Scope Platforms

The service typically supports:

- Microsoft Azure
- Microsoft 365
- Microsoft Entra ID (Azure AD)
- Google Cloud Services
- Amazon Services
- Supported cloud-hosted workloads and services
- Integrated security tooling such as Microsoft Defender and Microsoft Sentinel (where deployed)

3.2 In-Scope Activities

Security Monitoring

- Continuous monitoring of security & general alerts generated by supported platforms
- Review of identity, access, endpoint, and workload-related alerts
- Identification of suspicious or anomalous activity

Incident Triage and Investigation

- Initial triage of security events to determine severity and impact
- Investigation of potential security incidents
- Correlation of related alerts and activities

Incident Response Support

- Guidance on containment actions such as account isolation
- Support for remediation actions in coordination with the customer
- Assistance with recovery and service restoration

Escalation and Communication

- Escalation of confirmed incidents based on agreed severity levels
- Clear communication with nominated customer contacts
- Support for decision-making during incidents

Reporting and Improvement

- Regular security incident reporting
- Trend analysis and review of recurring issues
- Recommendations to improve security posture

---

4. Service Delivery and Management

The service is delivered as an ongoing managed support service, integrated with Spirit UK's service desk and incident management processes.

Security incidents are managed using an ITIL-aligned incident response approach, ensuring structured handling, escalation, and resolution.

The service complements, but does not replace, formal governance, audit, or compliance services.

---

5. Support Levels and Escalation

- Security events are logged and managed via Spirit UK's service desk
- Incidents are prioritised based on severity and potential impact
- Escalation to senior security engineers is available where required
- Out-of-hours response support is available by prior agreement
- Post-incident stabilisation support is provided where required

Response times and escalation paths are agreed in the Statement of Work.

---

6. Security and Data Protection

Security and data protection are integral to service delivery:

- Data is handled in accordance with UK GDPR and applicable legislation
- Spirit UK acts as a Data Processor where applicable
- Access to customer environments is restricted and controlled
- Activity is logged for audit and accountability purposes

The customer remains responsible for data ownership and lawfulness.

---

7. Customer Responsibilities

Customers are responsible for:

- Maintaining supported cloud platforms and licences
- Providing Spirit UK with appropriate access and permissions
- Nominating authorised contacts for escalation and approvals
- Implementing agreed remediation actions
- Notifying Spirit UK of significant environment changes

Failure to meet these responsibilities may affect service effectiveness.

---

8. Service Constraints

- Effectiveness depends on supported security tooling being enabled
- Third-party platform limitations may affect monitoring depth
- Incident prevention cannot be guaranteed
- Scope limited to environments defined in the Statement of Work
- Formal forensic or legal investigations are excluded

---

9. Pricing Model

Pricing is defined in the applicable Pricing Pack or Statement of Work and typically includes:

- Per-user/service pricing for ongoing security monitoring
- Time-based pricing for incident response and specialist support

All prices are exclusive of VAT.

---

10. Service Outputs

Typical service outputs include:

- Security incident notifications and updates
- Incident investigation summaries
- Regular security reports and trend analysis
- Recommendations for security improvements

---

11. Exit and Offboarding

Upon termination of the service:

- Monitoring and response activities will cease
- Final reports will be provided where applicable
- Access to customer systems will be securely removed
- Knowledge and documentation will be handed over as agreed
