



Managed Cyber Threat Intelligence Services

G-Cloud 15 Service Definition



Table of Contents

Introduction.....2

Service Overview.....3

 Features.....3

 Benefits.....3

Service Outline.....4

 Service Option - Standard.....4

 Service Option - Premium.....4

Project Implementation.....6

Why Ekco.....7



Introduction

Ekco Cloud & Security is an ideal partner for public sector organisations seeking a **secure, compliant, and scalable provider** via G Cloud 15.

We make it easier for IT teams to innovate, scale, manage, troubleshoot and secure. Across cloud, business continuity, security and workspace solutions, we enable the growth our customers want with the team they already have.

Through our security-first approach, large specialist workforce, AI-enhanced operations, and proven delivery capability, we help organisations:

- Modernise securely
- Strengthen cyber resilience
- Reduce operational risk
- Improve service continuity
- Deliver safer, more reliable digital services for our customers and their stakeholders.

Ekco's end-to-end cloud and cyber services are well matched to **G Cloud purchasing needs and public sector transformation goals**.

Service Overview

To support organisations that are seeking to protect their cloud services against cyber-attacks, Ekco provides a Managed Security Service (MSS) delivering a Managed Cyber Threat Intelligence (MCTI) service utilising from the Ekco SOC.

The Ekco MCTI service utilises a combination of market-leading intelligence tooling to monitor and alert on security events and/or report on information discovered about an organisation across open, closed, and dark web sources. This capability is complimented with Ekco's skilled and experienced Cyber Threat Intelligence team who will respond and investigate to capture comprehensive information about the alert/event to provide actionable and timely intelligence giving a clear understanding of the alert/event and possible follow-on actions.

This output enables organisations to make informed decisions, maintain their desired security posture and effectively employ their technologies to detect and prevent attacks.

Features

The key features of Ekco's MCTI service are:

- Sophisticated managed intelligence service
- Monitoring across dark web for brand images, corporate credentials, domains, users, etc.
- Monitors for vulnerability and supply chain intelligence
- 24/7/365 threat protection delivered by the Ekco Team
- Rapid response SLA to critical cyber threats
- Available in flexible service levels to suit customer needs
- Highly Certified Partner, SOC and Threat Intelligence team

Benefits

The key benefits of the Ekco's MCTI service are:

- Uses intelligence to identify external threats and prevent cyber attacks
- Provides extended 24/7 on-demand expertise to your organisation
- Provides organisations access to highly certified SOC and CTI teams
- Holistic visibility of risks and threats through eyes of adversaries
- 24/7 threat protection ensuring continuous security coverage
- Reduces the risk of real attacks against your organisation
- Enhanced prioritisation and threat detection capability to protect your organisation
- Cost effective service designed to adapt to evolving cyber threats

Service Outline

Ekco MCTI services are designed to be flexible and customisable in order to meet customer requirements.

Service Option - Standard

The '**Standard**' service level is a Managed Cyber Threat Intelligence Service aimed at small- and medium-sized organisations with a lower level of complexity, maturity, and intelligence requirements providing a Cyber Threat Intelligence and monitoring capability to enable organisations to make informed decisions, maintain its desired security posture and effectively employ its technologies to prevent and detect attacks.

- Managed Ekco standard rapid deployment of MCTI technologies
- Organisational data monitoring and alerting using the Recorded Future intelligence platform, covering the following modules:
 - Brand & supplier intelligence
 - Threat indicator intelligence
 - Vulnerability intelligence
 - Identity intelligence
 - Third-party intelligence (for an additional fee)
- 24/7/365 Threat Protection delivered by the Ekco Team
- Standard Monthly Operational Intelligence Report
- Geopolitical threat bulletins

Service Option - Premium

The '**Premium**' service level is aimed at medium to large sized organisations with a higher level of complexity, maturity, and intelligence requirements providing a Cyber Threat Intelligence and monitoring capability to enable organisations to make informed decisions, maintain its desired security posture and effectively employ its technologies to prevent and detect attacks.

- Managed Ekco standard rapid deployment of MCTI technology/technologies
- 24/7/365 threat protection delivered by the Ekco team
- Intelligence enrichment of Ekco SOC services
- Organisational data monitoring and alerting using the Recorded Future intelligence platform, covering the following modules:
 - Brand intelligence

- Threat indicator intelligence
 - Vulnerability intelligence
 - Identity intelligence
- Standard Monthly Operational Intelligence Report
- Geopolitical threat bulletins
- Ad-hoc threat intelligence flash notices
- Annual Threat Assessment & Report
- Takedown Services (for an additional fee)

Project Implementation

Onboarding a client into their new contracted services requires a structured process to ensure a smooth transition and clear expectations. The following process provides a high-level overview of our bespoke implementation plan.

1. Pre-Implementation Preparation

Initiate internal communications with internal stakeholders, confirming contracted deliverables, and bespoke scope of works. Confirm dedicated resource across the business depending on function.

2. Client Engagement

Initiate communication with the customer's key stakeholders to discuss the onboarding process, timescales (including support go live date), expectations, and roles.

3. Business Intelligence Discovery

Conduct a thorough assessment of the client's internal processes, gather key information regarding end users, business requirements, 3rd party data, user account management and operational workflows.

4. Technical Deliverables

Complete a detailed assessment of the customer's existing IT infrastructure, cloud, network, applications, and systems. Identify different user roles and access requirements. Deploy and document toolsets. Develop a comprehensive knowledge base containing FAQs, troubleshooting guides, and best practices based on their current environment.

5. NOC and SOC Deliverables

Configure and deploy and contracted NOC and SOC toolsets, complete basic security checks such as MFA and password policies.

6. Points of Attention

Based on technical audits and client concerns, create a Points of Attention document with the assigned account manager to review with the client

7. Acceptance into Service

Schedule and complete the acceptance into service with the required internal departments.

8. "Go Live"

Handover to our required internal stakeholders and departments to take on the clients contracted deliverables. Implementation team to provide 2 weeks of enhanced support to our internal teams and the client, ensuring support, access and processes are running smoothly.

Why Ekco

Why UK Public Sector Organisations benefit when they Partner with Ekco Cloud & Security

Security-First Cloud Services Aligned to Government Standards

Ekco Cloud & Security is a leading UK and European **security-first managed cloud provider**, delivering deep expertise across cyber security, identity, and cloud. Our services align with **NCSC guidance, the Cyber Assessment Framework (CAF), NHS DSPT**, and wider public sector assurance requirements.

Our proven **Assess → Protect → Detect → Respond** model supports secure-by-design digital transformation across hybrid and distributed environments—directly addressing public sector risk and resilience priorities.

End-to-End Capabilities Mapped to G Cloud 15

Public sector buyers need suppliers that can deliver migration, protection, management, and optimisation through a single, accountable partner. We provide a **fully integrated cloud and security portfolio**, including:

- Cloud migration and managed cloud operations
- Security and infrastructure management
- Identity security and privileged access management
- Secure modern architecture design
- Real-time threat detection and incident response

These services align directly with **G Cloud 15 lots and purchasing criteria**, enabling organisations to modernise securely while managing complex legacy estates.

Scalable Expertise and Sovereign Delivery

With **1,000+ cloud and security specialists across the UK and Europe**, we offer the scale, depth, and resilience required to support mission-critical public services. A dedicated **identity security practice** provides mature capability for access control and Zero Trust adoption—an increasingly critical requirement across government organisations.

Tailored Solutions for Resource-Constrained Organisations

Recognising the challenges faced by councils, NHS trusts, education, and blue-light services, we offer **cost-effective, scalable cloud and cyber security solutions** designed for organisations with limited internal capacity.

These services protect against phishing, ransomware, and social engineering while meeting G Cloud's expectations for solutions that are secure by default, rapidly deployable, and low overhead.

AI-Enhanced Security Operations

We embed **AI into daily security operations**, improving analyst productivity and response effectiveness. AI-assisted services accelerate:

- Incident triage and prioritisation
- Threat analysis and vulnerability summarisation
- Reporting accuracy and audit readiness

This enables faster outcomes and stronger protection for public bodies operating with limited staffing.

Public Sector-Focused Engagement Model

Our partnership-led approach aligns with government procurement expectations, offering:

- Dedicated, accountable delivery teams
- Transparent SLAs and service reporting
- 24/7 support with local expertise
- Predictable commercial and contract models

This ensures we act as a **strategic long-term partner**, not a transactional supplier.

Global Recognition and Strategic partnerships

These global accreditations partnerships show our commitment to customer satisfaction, data safety, security and overall quality. We're independently audited every year to give our customers confidence in our approach.



From agile managed cloud platforms to next-gen security services that supercharge defences, our local team of specialists provide proactive, round-the-clock management. With one Ekco Cloud & Security team delivering a combination of services, our customers quickly gain control and visibility over their technology.