Managed Extended Detection & Response

G-Cloud 15 Service Definition

Table of Contents

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**.

Managed Extended Detection and Response

Service Overview

Ekco provides a Managed Security Service (MSS) delivering a Managed Extended Detection & Response (MXDR) Service from the Ekco SOC to support organisations in protecting their cloud services from cyber-attacks. In this dynamic environment, the need for 24/7 detection and response becomes crucial to ensure an organisation's cybersecurity resilience.

Ekco's 24/7 Managed Detection & Response (MDR) Service utilises leading security tools to help identify and neutralise threats and potential security incidents before they escalate into full-blown breaches. Through Ekco's proactive approach to cybersecurity, organisations can minimise the impact of attacks, reduce downtime, and prevent significant financial and reputational damage.

Features

The key features of the Managed Extended Detection & Response (MXDR) Service are:

- Sophisticated Managed Extended Detection & Response (MXDR) Service
- 24/7/365 Threat Protection delivered by the Ekco SOC
- Sophisticated automation capability providing near real time response
- Rapid response SLA to critical Cyber Threats
- Eyes on Screen 'Always on & Always watching'
- Available in 3 flexible service levels to suit customer needs
- Integrated Threat Intelligence
- Proactive Threat Hunting
- Highly Certified Microsoft Partner & Security Operations Centre team

Benefits

The key Benefits of the Managed Extended Detection & Response (MXDR) Service are:

- 24/7 Threat protection ensuring continuous security coverage
- Sophisticated detection capability to protect your organisation
- Automated and near real time rapid response to Cyber Threats
- Provides your organisation with extended 24/7 on demand expertise
- Provides access to highly certified SOC team and Microsoft expertise
- Holistic visibility and security coverage through integration of existing tools

Service Outline

Service Option - Essentials

The **' Essentials'** Service Level is an entry level Security monitoring SOC Service aimed at small / medium sized organisations with a low level of complexity and requirements to provide a rapidly deployed MXDR Service covering a Customers Azure cloud environment and includes the below capability and specification provided to the Customer as part of the service provision.

- Managed Ekco standard rapid deployment of MXDR technology/technologies
- Log Source onboarding of standard Azure log sources (Entra ID, Identity Protection, Defender Alerts, Azure Activity Logs, O365)
- Deployment and configuration of Microsoft's standard built in detection capability
- 24 x 7 x 365 eyes on screen SOC
- Integration of open source Threat intelligence feeds where possible with the defined MXDR Technology/Technologies (Abuse.ch, Virus total etc)
- Quarterly standard MXDR reporting pack

Service Option - Standard

The **'Standard'** Service Level builds on the 'Essentials' Service Level providing additional capabilities to the Security monitoring SOC Service. The 'Standard' Service Level is aimed at small / medium sized organisations with a higher level of complexity covering hybrid, multi-cloud or on premise Customer Operating Environments and requirements to provide a customised deployment of the MXDR Service and includes the below capability and specification provided to the Customer as part of the service provision.

- Managed Ekco customised deployment of MDR technology/technologies
- Deployment of Ekco standard MDR detection capability
- 24 x 7 x 365 eyes on screen SOC
- Ekco SOC standard threat hunting package providing a reactive response to industry critical threats and vulnerabilities
- API Integration of market leading threat intelligence feed to enhance detection and response capability
- Integration of existing Customer owned 3rd party technologies and security tools
- Continued and ongoing 'Service Enhancement' to improve the Customers maturity and detection capability in the provisioned MDR Technology/Technologies
- Aligned Client Success Manager with Monthly/Quarterly option service review
- Monthly /Quarterly option MDR reporting pack

Service Option - Premium

The **'Premium'** Service Level builds on the 'Standard' Service Level providing further additional capabilities to the Security monitoring SOC Service. The 'Premium' Service Level is aimed at medium / large sized enterprise organisations with significant complexity covering hybrid, multi-cloud or on premise Customer Operating Environments and requires a highly complex and customised deployment of the MXDR Service. The 'Premium' Service Level includes the below capability and specification provided to the Customer as part of the service provision.

- Managed Ekco customised deployment of MXDR technology/technologies with aligned Azure Security subject matter expert (SME)
- 24 x 7 x 365 eyes on screen SOC
- Development and deployment of customised use cases and detections in line with Customer requirements
- Design and Implementation of Custom Detections in line with Customer requirements
- Design and Implementation of Security Orchestration & Automation (SOAR) playbooks
- Customised reactive and proactive threat hunting package aligned to Industry and Customer specific threats
- API Integration of market leading threat intelligence feed to enhance detection and response capability
- Integration of existing Customer owned 3rd party technologies and security tools
- Continued and ongoing 'Service Enhancement' to improve the Customers maturity and detection capability in the provisioned MXDR Technology/Technologies
- Aligned Client Success Manager with Monthly service review
- Customised and bespoke reporting capability aligned to Customer requirements

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.