EKCO

Managed Extended Detection & Response

G-Cloud 14 Service Definition

Author:	Clare Base
Version:	2.0
Date:	310 July 2025
Document:	EKCO-GEN-447

Table of Contents

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 SOAR 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

- Managed Ekco standard rapid deployment of MXDR technology/technologies
- Log Source onboarding of Azure default log sources (Entra ID, Identity Protection, Defender Alerts, Azure Activity Logs, O365)
- Deployment of Microsoft 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 KQL Detection Alert library in line with Customer requirements
- Design and Implementation of Security Orchestration & Automation (SOAR) playbooks utilising Azure Logic Apps
- 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

Partner Strategic Offering - Service Outlines (Managed Service or Subscription Resale)

Microsoft

- Defender Suite of Services – EDR, MDR and XDR plus Defender 365 and Accelerator
- Sentinel SIEM Security Services - Sentinel SIEM licences utilise the power of Sentinel to collate log data from all of your Microsoft security tools and generate alarms for a SOC team to triage. Microsoft Sentinel can remediate these alarms using powerful automated playbook actions.

Flexible Microsoft Managed Support Service may be tailored to customer requirements.

Arctic Wolf

Service modules include 24x7 Advanced Threat Detection and Response, continuous Vulnerability Management, Security Awareness education, and Digital Forensics & Incident Response

- Fast and Easy Setup - Get up and running quickly and continuously fine-tune configurations to customize your security experience.
- 24x7 Continuous Monitoring Around-the-clock security coverage from security operations experts.
- Security Operations Experts Hundreds of years of combined experience with cybersecurity accreditations like CISSP, HCISPP, CCSP, CISM, CRISC.
- Proactive Threat Hunting Campaign-based threat hunting and sweeps for indicators of compromise.
- Rapid Response Detect and investigate critical events within five minutes. Response Actions and Guided Remediation Rapidly contain incidents and get detailed guidance on remediation.
- Security Journey Guidance Quarterly reviews to help you design, implement, and achieve your security vision

CrowdStrike

Crowdstrike Management and Maintenance security service - monitoring, ongoing maintenance and management of the deployed Crowdstrike platform, in particular using CrowdStrike’s Falcon Suite of products.
Flexible CrowdStrike Managed Support Service may be tailored to customer requirements.