Cybersecurity Service Descriptions

What we do & how we do it

Dated: 30/05/2024
Version: 3.0
Security: Commercial-in-Confidence

Contents

Version Control 2
Language Disclaimer 3
Introduction 4
1 - Validation & Assessment - Cyber MOT 5
Summary 5
1.1 Cyber Essentials Certification 5
1.2 Cyber Essentials Plus: Validation 6
1.3 Ekco Baseline Cyber-security Assessment 6
1.4 Penetration Test 7
1.5 InTune Policy Management - Basic 7
1.6 External Attack Surface Assessment 8
1.7 Kerberos Reset 9
1.8 Office 365 Security Review (Hardening) 9
1.9 Vulnerability Scan – One Off 10
1.10 Cyber MOT Report 11
1.11 Cyber-security Insurance Questionnaires and Assurance 11
2 – Secure, Detect and Respond 12
Summary 12
Role of the SOC 12
Tasks performed by the SOC 12
2.1 Core Security Monitoring 13
2.2 Managed Detection and Response 14
2.3 Cybersecurity Service Periodic Reporting 15
2.4 Client SIEM (Security Incident & Event Management) 16
2.5 Continuous Vulnerability Scanning 16
2.6 External Attack Surface Scanning (Light) 17
2.7 DNS Filtering 18
3 – Cyber Intelligence Service 19
Summary 19
3.1 Predictive Edge 19
4 – Education & Awareness 21
Summary 21
4.1 Simulated Phishing Attacks 21
4.2 User Behaviours, Cyber Awareness and Education 22
5 – Crisis Response and Recovery 23
Summary 23
5.1 Crisis Response 23
5.2 Disaster Recovery 24

Version Control

This document is electronically version controlled (with each change being tracked automatically). The list of changes below represents significant document releases that are communicated to all Ekco clients. Changes are listed in chronological order.

Version	Date	Changes	Author
0.1	Mar 23	First Draft of New MSSP Service Descriptions	Richard Winter
0.2	May 23	Updated draft incorporating comments and updates from SLT and SOC circulation of V0.1. Reset proofing language to English UK. Additional SDs added: 1.9 - One Month Vulnerability Scanning 1.10 - Insurance Questionnaires and Assurance 2.5 - Secure, Detect & Respond Periodic Reporting Updated Service Map diagram	Richard Winter
1.0	Jun 23	First published edition. Baselined at V1.0 – Updated Service Map – Minor text adjustments. – Removed references to proprietary toolsets Minor amendments and corrections to be saved in DRAFT V 1.1 for Qtrly review in Sep 23 Future Service ambitions to be added to DRAFT V2.0 – ongoing.	Richard Winter
1.1	Sep 23	Addition of new Service Descriptions – Client Tenant SIEM (Msft Sentinel) – Continuous Vulnerability Scan Amendment of Penetration Testing SD and Cyber Essentials SD.	Richard Winter / Kieran Walsh
2.1	Feb 24	Rebrand to Ekco format schema Addition of new SDs: – External Attack Surface Assessment (One off) – External Attack Surface Scanning (Recurring)	Richard Winter
2.2	Mar 24	Addition of DNS Filtering Service	Richard Winter / Chris Poole
3.0	May 24	Rebrand of document to align with Ekco branding	Paige Badham / Hannah Banks

Language Disclaimer

At time of this latest review and update Bluecube Technology Solutions ('Bluecube') is migrating its technical and commercial functions to reflect its new position as a subsidiary within the Ekco group of IT companies. Cyber security services will in future be delivered through the sub-brand "Ekco Security". Throughout this document both 'Bluecube' and 'Ekco' may be found and should be regarded as interchangeable. The cyber-security service continues to be delivered by the former Bluecube security operations centre (SOC), who are becoming an increasingly integrated part of Ekco Security through Q1 and Q2 of 2024.

Future iterations of this document will likely be harmonised and offered as a single Ekco Security service catalogue, applicable across the group.

Introduction

These Service Descriptions are the supporting information to contractual agreements. They are grouped into five sections:

- Validation and Assessment – a 'Cyber MOT'
- Secure, Detect and Respond – real time threat reduction and engagement
- Cyber Intelligence – the proactive edge
- Education and upskilling – your people are your first line of defence
- Recovery and Crisis management – the last resort

Each Service Description provides further details of Ekco's cyber resilience service offerings. Not every client will receive every element of service detailed within this document as each service is designed to be tailored to each clients need, specific details of which services are being delivered to a client can be found within the agreed contract.

These service descriptions ('Service Description') are entered into by the client ('Client') and Bluecube Technology Solutions – An Ekco company ('Supplier') as Identified within the Client contract. By purchasing these Services, the Client agrees to be bound by the terms and conditions associated with that service in addition to the contract Terms.

Ekco also offer certain bespoke and discrete services that are not detailed within this document. These service description Terms and conditions, where at conflict, are superseded by any specific contractual agreement Terms.

Each Service Description contains a link to Ekco's internal processes that relate to the delivery of each service. These links are for internal Ekco reference only and will not work for Clients or any other external parties (this is by design).

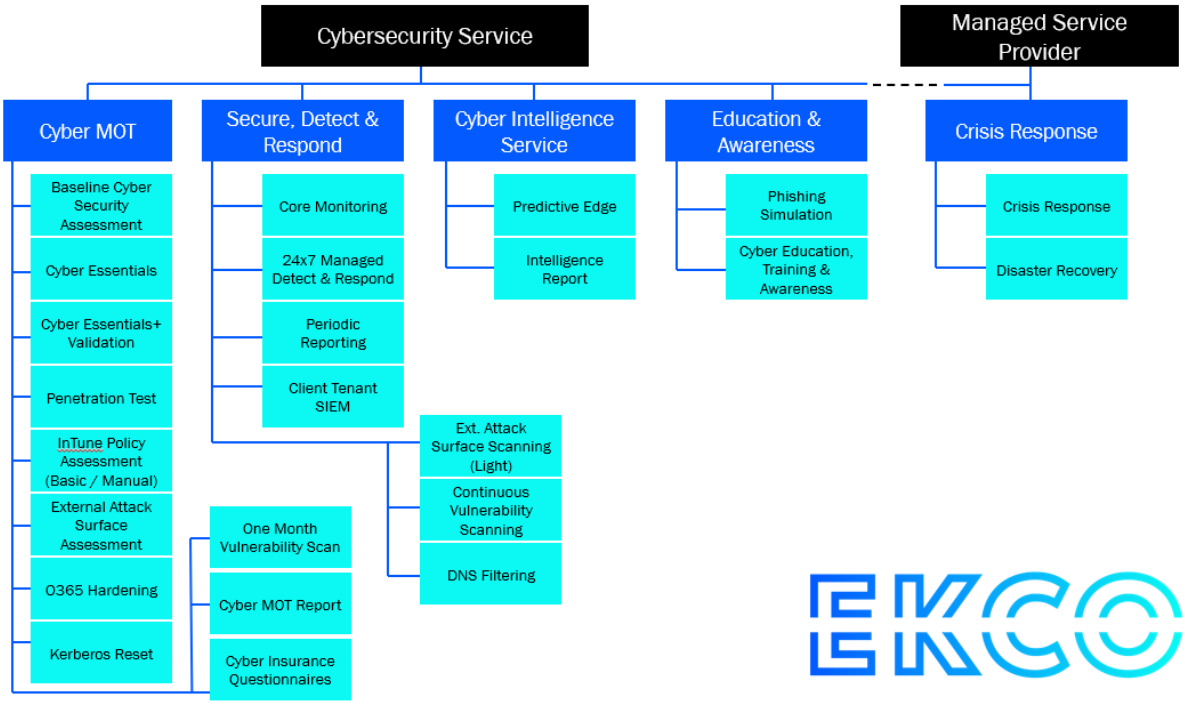

Fig 1 - Cybersecurity Services Map V3 @ May 2024

1 - Validation & Assessment - Cyber MOT

Summary

The Cyber MOT involves an initial deep validation and assessment of the security status of the client IT estate and infrastructure, existing controls and vulnerabilities. The Cyber MOT can include CE/ CE+ certification if desired (the NCSC highly recommends it) as a baseline foundation to a nationally recognised level that provides an increasingly necessary 'kitemark'. For a deeper view we also offer a penetration testing service. Armed with understanding of the client's cyber strengths and weaknesses, we can then remediate any vulnerabilities (within MSP service scope) to bring them up to a known good and defendable state. We will also repeat this process annually if desired, hence the 'MOT' metaphor, and certain elements more frequently as part of our continuous Secure, Detect and Respond service.

1.1 Cyber Essentials Certification

WHAT	
Name	**Cyber Essentials Certification**
Overview	Cyber Essentials is an effective, NCSC backed scheme that helps to protect your business, whatever its size, against a whole range of the most common cyber-attacks. It is increasingly viewed as a cyber-security 'kitemark' for UK businesses of all types and is often required to be able to bid for UK Government contracts.
HOW	
Prerequisites	None
Procedures	A detailed questionnaire-based assessment of your IT systems or services, the answers are assessed by trained, certified cyber-security experts. Bluecube is an IASME Certified Body, authorised to carry out Cyber Essentials evaluations.
Knowledge Base	To be updated and stored in PassPortal
WHEN	
Service hours	A periodic, usually annual, service. The CE certificate is valid for 12 months from date of issue.
TERMS & SLA	
Service Levels	We aim to complete the questionnaire and achieve certification within a calendar month of commission.
Exclusions	None
Billing	Integrated within the Cyber MOT charge or can be offered as a standalone service. The billing will include the certification fees required by IASME, specified for different business sizes.
Client Responsibilities	To maintain an accurate IT asset inventory or asset management system and assist us in identifying and quantifying your IT estate, software and operating systems in use. A board member from the client must certify the submission to say that its true. To remediate shortfalls in the estate as required by the assessment in order to pass. Note that this work may be separately chargeable depending on its complexity and cost.

1.2 Cyber Essentials Plus: Validation

WHAT	
Name	**Cyber Essentials Plus Validation**
Overview	Cyber Essentials Plus still has Cyber Essentials simplicity of approach, and the protections are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out.
HOW	
Prerequisites	Cyber Essentials Assessment Pass
Procedures	We contract an independent cyber-security expert to validate, using hands on methods, the findings of our CE assessment. The CE+ Certificate is issued by Ekco in conjunction with the IASME Consortium.
Knowledge Base	To be updated and stored in PassPortal
WHEN	
Service hours	A periodic, usually annual service.
TERMS & SLA	
Service Levels	After CE is achieved, the validation must be completed within three months.
Exclusions	CE assessment failures or multiple significant non-conformities.
Billing	Integrated within the Cyber MOT charge or can be offered as a standalone service. The validation cost is dependent on the complexity of the client organisation.
Client Responsibilities	As required, arrange access to client HQ/offices to allow the assessor to conduct the tests.

1.3 Ekco Baseline Cyber-security Assessment

WHAT	
Name	**Ekco Baseline Cyber-security assessment**
Overview	An internal cyber-security baselining assessment without going through the full CE submission and associated costs.
HOW	
Prerequisites	Be a prospective Ekco MSP or MSSP client
Procedures	We run through a basic CE-style questionnaire internally and evidence it through our initial onboarding checks that are most cost effective to complete. We will use our software and cyber-security tooling to scan and identify vulnerabilities and threats to the client IT estate. The tooling will not be resident on the client estate afterwards. A report will be issued to the client with recommendations for remediation where required.
Knowledge Base	To be updated and stored in PassPortal
WHEN	
Service hours	A one off initial validation service. This could be repeated annually but it would be better to do CE or CE+.
TERMS & SLA	
Service Levels	This is a one off check usually conducted prior to onboarding.
Exclusions	Not required for CE or CE+ clients. Award of CE or CE+ is excluded. This check provides no ongoing assurance of cyber-protection, unless Secure Detect and Respond service options are taken.
Billing	Integrated within the Cyber MOT charge or can be offered as a standalone service. Calculated as a per device / user charge, plus a one-off consultancy charge for each deployment and decommissioning of tooling

	agents required.
Client Responsibilities	To assist us in identifying and quantifying the IT estate, software and operating systems in use.

1.4 Penetration Test

WHAT	
Name	**Penetration Test**
Overview	Conduct a penetration test as a standalone task or as part of an annual Cyber MOT using a combination of remote and automated tooling appropriate to the clients need. This can be completed as an in-house service (preferable) or via a third party if demonstrable independence is required by the client – see exclusions below.
HOW	
Prerequisites	None
Procedures	Plan Penetration test, including determination of the type of test (Internal, External infrastructure, Applications etc) Conduct Penetration Test to: • positively identify the exposed attack surface of the systems and applications used by the client • identify vulnerabilities within the attack surface. • produce a prioritised list of the identified vulnerabilities and identify the risk associated with them. • deliver pragmatic remediation advice to enable the client to mitigate the risks. A final report will include an executive summary of the test, details of each vulnerability, and will include advice on remediation.
Knowledge Base	To be updated and stored in PassPortal
WHEN	
Service hours	Takes about a month from commissioning to final report.
TERMS & SLA	
Service Levels	One Off
Exclusions	Customers who wish for, or have a regulatory need for, complete independence. In this case we can commission and manage the process but outsource the actual PenTest to a trusted external provider.
Billing	Costs are dependent on number of Ips (Internal and External) to be scanned and the complexity of the organisation or application in question. Can be billed as a 'one off' activity or as part of Cyber MOT component of a fully manged security service. If a retest is required once the report is produced, then further fees may apply.
Client Responsibilities	To engage with the preparations for the test, advise on timing and risk mitigations.

1.5 InTune Policy Management - Basic

WHAT	
Name	**Intune Policy Management - Basic**
Overview	A manual review of Intune policies in respect of security
HOW	
Prerequisites	N/A

Procedures	Intune is a 'living' product that is updated by Microsoft on a continual basis. As a result, a regular review of the security policies within Intune are required to ensure that a Client's environment is benefiting from the latest available policies within Intune. This is a manual process that is conducted by Ekco SOC team in conjunction with the client.
Knowledge Base	To be updated and stored in PassPortal
WHEN	
Service hours	This is a manual review conducted during normal working hours.
TERMS & SLA	
Service Levels	Conducted annually on the date of the Cyber MOT and then at the intervening six month point, ie twice per year.
Exclusions	Clients that opt for InTune Policy Management - Advanced
Billing	Integrated within the Cyber-MOT per user charge, or as a one-off consultancy charge for any additional manual review.
Client Responsibilities	To ensure availability to discuss, approve and implement (where appropriate) any necessary, or recommended, actions. To ensure that they are purchasing the right type of licensing to allow users to benefit from the security features available.

1.6 External Attack Surface Assessment

WHAT	
Name	**External Attack Surface Assessment**
Overview	External Attack Surface Management (EASM) is a cybersecurity discipline that identifies and manages the risks presented by internet-facing assets and systems. EAS Assessment refers to the processes and technology necessary to discover external-facing assets and any vulnerabilities of those assets. This is a 'one-off' version of the continuous service provided in Section 2 – Managed Secure, detect & Respond.
HOW	
Prerequisites	None
Procedures	The EAS Assessment is initially configured and defined through a consultation and discovery phase with the client. Any vulnerabilities identified through this process will be highlighted to the client (with a view to rectifying).
Knowledge Base	To be updated and stored in PassPortal
WHEN	
Service hours	This is a one off assessment, likely conducted during normal working hours.
TERMS & SLA	
Service Levels	This is an assessment review conducted over one or more days depending on the complexity of the client's estate and extent of any exposed attack surface. From point of commissioning to report being available will be 2 weeks.
Exclusions	-
Billing	Integrated within the Cyber-MOT per user charge, or can be billed as a one-off consultancy charge for any additional or standalone review.
Client Responsibilities	To provide details of externally facing infrastructure, IP addresses and owned web domains/ sub-domains. Ensure availability to discuss, approve and implement (where appropriate) any necessary, or recommended, actions.

1.7 Kerberos Reset

WHAT	
Name	**Kerberos Reset**
Overview	Kerberos is a computer network security protocol that uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying users' identities. It is the default authorisation technology used by Microsoft Windows. Kerberos is used in Active Directory and is also an alternative authentication system to SSH, POP, and SMTP. The issue (from a security perspective) is that the Kerberos protocol is a target for cybercrime and is often used to create a back door into an environment. In order to mitigate this risk we perform Kerberos resets every six months, and immediately should any suspicious activity be detected.
HOW	
Prerequisites	None
Procedures	The SOC Engineering team will conduct a manual Kerberos reset every six months as per the periodic work schedule. To be recorded in relevant Monday Board on completion.
Knowledge base	To be updated and stored in PassPortal
WHEN	
Service hours	This is a manual reset that is conducted every six months as part of your security service.
TERMS & SLA	
Service Levels	The service will be delivered every 6 months.
Exclusions	-
Billing	Integrated as a per user charge, or a one off consultancy charge for each additional review/ reset.
Client Responsibilities	To take any necessary, or recommended, actions; Ekco can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

1.8 Office 365 Security Review (Hardening)

WHAT	
Name	**Office 365 Security Review (Hardening)**
Overview	Analysing and improving the MS 365 Tenancy Secure Score. Ensuring that your Microsoft Cloud environment is hardened and remains that way; this is an ongoing task as Microsoft are constantly evolving the Office 365 ecosystem and cyber security threats are also ever changing and developing. We recommend that this service is carried out every six months.
HOW	
Prerequisites	A Microsoft 365 based cloud tenancy.
Procedures	Ekco maintain a best practice approach to ensuring that Microsoft 365 tenancies are configured to an ideal blend of security and operability. Increasing the Secure Score of the target tenancy considerably over the 'out of the box' configuration. Looking at all aspects from Exchange Online right through to endpoint management rules.

	A 0365 Hardening report will be issued with recommendations for configuration changes and improvements appropriate to the level of risk.
Knowledge base	To be updated and stored in PassPortal
WHEN	
Service hours	This is a manual review and reporting service that is conducted every six months as part of your security service.
TERMS & SLA	
Service Levels	The service will be delivered every 6 months.
Exclusions	Non-0365 Estates; Issue remediation beyond any actions needed to be performed as your MSP
Billing	Integrated as a per user charge, or a one-off consultancy charge, for each manual review.
Client Responsibilities	To review the report and take any necessary, or recommended, actions; Ekco can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

1.9 Vulnerability Scan – One-Off

WHAT	
Name	**Vulnerability Scan**
Overview	A one month deployment of an advanced vulnerability scanner to identify soft and firmware vulnerabilities requiring patches or updates in the clients IT estate, with opportunity to remediate and retest over the month.
HOW	
Prerequisites	An optional enhancement to Cyber MOT checks, it is not essential but is advisable to take the Cyber MOT as a package if doing the vulnerability scan.
Procedures	An advanced vulnerability scanner agent will be installed on the client's IT estate (end points and servers) for a period of one month. The scanning will identify Critical, High and Medium severity score (CVSS) vulnerabilities and allow either the client or their MSP time to remediate these. The scanning is continuous and produces daily reports, which can be shared with the client; it also reflects real time CVE releases to identify where zero-day vulnerabilities might appear during the month. At the end of the scanning period the agent will be removed (or can be left in operation subject to an ongoing fee as part of Secure, Detect and Respond services, see Section 2).
Knowledge base	Procedure to be stored in Pass Portal.
WHEN	
Service hours	This is a manual review and reporting service.
TERMS & SLA	
Service Levels	The service will be delivered continuously for a period of one calendar month.
Exclusions	Nil
Billing	Integrated as a per device charge for the agent, plus a one-off consultancy charge for each deployment and decommissioning required.
Client	To review the reports and take any necessary, or recommended, actions on

Responsibilities	patching etc; Ekco can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

1.10 Cyber MOT Report

An annual report detailing the outcome of the Cyber MOT activities provided to the client within 2 weeks of the annual assessment.

1.11 Cyber-security Insurance Questionnaires and Assurance

Ekco can assist with the completion of proprietary cyber-security questionnaires that are periodically required for cyber-insurance companies or other regulatory requirements. This service is charged at our standard consultancy rate, on a per-hours basis on request. Alternatively, assistance with an annually recurring questionnaire can be included within an annual Cyber MOT service charge.

In the event that the support desired is deemed deeply specialist, requires the use of new cyber-security tools or third party expertise, a Project will need to be commissioned to manage the work. The project cost, deliverables and timescale will be subject to separate negotiation.

2 – Secure, Detect and Respond

Summary

Secure, Detect and Respond is a 24x7 (or working hours as the client chooses) comprehensive monitoring, alerting and response capability centred on our state of the art Security Operations Centre, best in class toolsets and 'always on' team. Within this we can also offer continuous vulnerability management - a step beyond the norm - we are able to watch the emergence and incidence of vulnerabilities becoming apparent in near real time. In this way we catch the never ending stream of newly discovered vulnerabilities and patch them faster than the routine update cycle, keeping clients safer from no notice attacks than ever before.

Role of the SOC

The SOC is the 'how' Ekco provides the Secure, Detect and Respond services, it is no longer sold as a service in its own right, instead the SOC is assumed to exist for all security clients. The SOC will provide three levels of monitoring service – Core, Managed and Advanced; these are designed to build on each other. For example, a client taking the Advanced service automatically receives the Managed and Core services.

The SOC is a dedicated, centralised team of Security Analysts and Engineers. Their primary responsibility is monitoring client IT system environments for indicators of a possible cyber event, including identifying vulnerabilities, acceptable use and policy violations, unauthorised activity, network intrusions, credential compromises, malware and phishing, and providing direct support to the cyber Incident Response process.

The SOC team will also enact delivery and management of many of the other Security Services that a client receives from Ekco, for example the Cyber-Intelligence service. A notable exception is the Crisis Response service which is closely linked to, but not delivered by, the SOC (see Section 5).

Tasks performed by the SOC

Monitor Security Posture
Monitoring the client's environment for security conditions, alarms and responding through various technical solution(s).

Initiate & Manage Incident Response
Validating security incidents based on alerts and network monitoring activities. Initiate IR support from vendors, forensic, regulators and other third party sources as required.

Reporting
Run reports to support IT General Controls monitoring and compliance requirements. Run reports to support alarms, incidents and respond to additional data requests.

When an action is required an 'Event' ticket will be created in Lighthouse (or our SIEM toolset) to track all activities in relation to an Event. The SOC team will often work in conjunction with other Ekco teams to resolve an issue.

2.1 Core Security Monitoring

WHAT	
Name	**Secure, Detect & Respond – Core**
Overview	We check regularly using our proprietary tooling that basic security controls are in place and conforming to an agreed security policy baseline.
HOW	
Prerequisites	An IT platform that includes AV, disk encryption and supports MFA in a reportable format, for instance Microsoft 365; a compatible directory-based core IT platform, eg Microsoft Azure Active Directory. (Google Directory Services can be checked but may be subject to an additional charge.)
Procedures	The Core Service includes proactive: • Anti-Virus Monitoring - to confirm Anti-Virus protection and coverage is in place. To stop known viruses and malware. • Encryption Status Monitoring - to confirm all devices are encrypted, to ensure that if a laptop is stolen or lost, all data on it is subject to encryption in order to mitigate unauthorised access. • Password Status Monitoring - to confirm that passwords meet the complexity requirements as recommended by Microsoft or the client's chosen policy. • Multi-Factor Authentication Status monitoring - to confirm that all accounts have MFA enforced. MFA enforcement policy will be pre-defined with the client. • Patch Status Monitoring - to monitor the patch health of client IT estate or services. This includes both Microsoft and 3rd party application patch status. For Ekco MSP customers tickets will be raised in Lighthouse to trigger patch management/ update. • Privileged Account (eg Administrator) monitoring – a monthly review not real time. • Credential Audit - user account usage and status. This is to ensure that the estate does not have 'stale' or old accounts still active. • GPO Changes monitoring - to alert when new GPO's are created or existing ones changed (malicious actors often change GPO's once they have compromised an environment).
Outputs	Alerts when AV, Encryption, Password, MFA, patching status and GPO status deviate from the agreed baseline. A summary report will be created and shared monthly (from Power BI).
Knowledge Base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	Monitoring is an 'always on' service. This means that the solution is designed to be available and operational at all times. Typically these checks will be carried out once per day or more frequently. Auditing of privileged accounts and credential audits takes place monthly.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Any device that does not have the Ekco Monitoring Agent installed or that is not enrolled into Intune.

	Monitoring for MFA if MFA is not enforced or applied. Remediation of patch status alerts – this is performed by Ekco Ops for MSP customers or by clients if they have their own IT or 3rd party service provider. Technology Platforms that do not provide a centralised directory in a supported format.
Billing	Integrated as a per user or per device charge as appropriate.
Client Responsibilities	Allow the Poseidon agent and N-able to be installed on all devices. Prior notification of any non-Windows/Linux devices requiring monitoring. Support in installing the agent on standalone machines or workgroups. Ensure Lighthouse is kept up to date with all new starters and leavers for MFA monitoring. To review the monthly report and take any necessary, or recommended, actions; (Ekco can assist with this process if there is an IT Support contract in place over and above the Managed Security Service).

2.2 Managed Detection and Response

WHAT	
Name	**Secure, Detect & Respond – Managed Detection and Response**
Overview	Ekco will deploy a state of the art endpoint protection agent to the client's estate (on prem, 3rd party or Ekco MSP) and integrate it with our other tooling and the Ekco SIEM (Security Incident & Event Management) toolset.
HOW	
Prerequisites	Secure, Detect & Respond - Core is recommended but not essential. Microsoft Defender for Cloud Apps (previously called Cloud App security) is required for impossible travel.
Procedures	The SOC team leverage a best in class XDR toolset in order to identify unusual, suspicious or malicious activity on client devices and cloud infrastructure. When an incident is detected a ticket will be created in Lighthouse to track remediation. The SOC team will often work in conjunction with other Ekco or external teams to resolve an issue. EDR will be set to 'detect only' mode for an agreed period of time (to allow the Artificial Intelligence engine to learn about normal behaviours and an exclusion list to be created by Ekco). Following this the EDR will be switched to 'Protect mode' which will provide real-time protection for all devices with the agent. The Managed Service includes proactive: • Advanced Endpoint Protection, Detection & Response (EPP / EDR) • Advanced Cloud app protection using XDR and Azure Defender • Event monitoring through O365/ Azure, for example, detection of suspicious sign on, eg from foreign countries and impossible travellers, multiple failed logins etc, suspicious inbox rules, unusual file deletions. • Event Monitoring in Active Directory, detecting indicators of an attack often seen in AD. • 24 x7 AI assisted 'human in the loop' analysis, event triage, alerting and threat remediation

	• Incident escalation to client service provider (eg Ekco Ops) and incident triage, management and prioritisation by SOC senior staff. • Access to Ekco cyber-security expertise, for example post incident, lessons identified and remediation discussions.
Outputs	Incident reports will be provided for each major incident.
Knowledge Base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times. Ekco operates a resilient SOC across multiple sites to prevent power outages or natural disaster from interrupting the MDR service.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%.
Exclusions	Any device that does not have the EDR/XDR Agent installed. Managing or responding to events that are not deemed to be a Security alert or alerts outside of the scoped, agreed data sources being monitored.
Billing	Can be delivered for a monthly fee or integrated as a per user charge, or per device (as stated in the contract). Subject to a minimum term commitment of 12-months.
Client Responsibilities	To take any necessary, or recommended, actions.

2.3 Cybersecurity Service Periodic Reporting

WHAT	
Name	Cybersecurity Service Periodic Reporting
Overview	A textual and statistical report supplied to the client at the desired frequency, for example bi-annually, quarterly but no more often than monthly. The report will summarise cybersecurity service delivery metrics (drawn from our tooling) and add contextual narrative (provided by our SOC staff). It is designed to enable the client to determine whether their cyber-security risk appetite is being exceeded or their risk exposure is within tolerance.
HOW	
Prerequisites	Secure, Detect & Respond – Basic, Managed or Advanced is required.
Procedures	Template for Basic (TBD) – this will consist of a PowerBi presentation slide of actions undertaken by the SOC and basic statistical information drawn from in-house toolsets relevant to the SD&R Basic Service. Template for Managed (TBD) – As above per 'Basic' but with contextual narrative and to include additional information about alerts and remediated events from S1.
Knowledge Base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	Normal working weekdays.
TERMS & SLA	
Service Levels	A periodic report delivered electronically to the client at an agreed frequency.
Exclusions	Any cyber incident or additional activity that generates a separate report,

	for example Cyber MoT, CE/CE+ or specific threat assessment.
Billing	Included within each Secure Detect & Respond service, at a cost determined by the level of SD&R service contracted (Basic, Managed or Advanced).
Client Responsibilities	Availability to discuss, approve and implement (where appropriate) any necessary, or recommended, actions.

2.4 Client SIEM (Security Incident & Event Management)

WHAT	
Name	**Client SIEM**
Overview	For Clients who wish to yield maximum value from their 365 Defender licensing XDR/EDR, and On-Premises security appliances, Ekco can setup a client instance of Microsoft Sentinel, a cloud native SIEM (Security Information and Event Management) solution that empowers SOC with the ability to proactively detect, investigate, and respond to cybersecurity threats at scale. Ekco will configure the initial connectors in line with your current licensing and products for enhanced visibility of your security events (telemetry) and real-time query's will be configured for additional alerting enrichment. (Analytics) The initial build will be treated as a SOC engineering project, that will take place within your Azure Cloud Tenant. Access to your Security Resource Group will be securely delegated via Azure Lighthouse to allow the SOC to centrally manage all incidents and alerts from a single pane of glass.
HOW	
Prerequisites	Secure, Detect & Respond – Managed is required.
Procedures	
Knowledge Base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	This is an always on service.
TERMS & SLA	
Service Levels	SIEM management and incident monitoring is an always on service for MDR clients - availability should be above 99%.
Exclusions	Non-Microsoft SIEMs (eg Splunk)
Billing	Included within the chosen Secure Detect & Respond level of service, at an additional cost determined by the complexity of the client environment.
Client Responsibilities	To work with Ekco in the initial configuration of the SIEM and to agree reporting lines of responsibility for alerts and incident management.

2.5 Continuous Vulnerability Scanning

WHAT	
Name	**Vulnerability Scan**
Overview	Deployment of an advanced vulnerability scanner to identify soft and firmware vulnerabilities requiring patches or updates in the clients IT estate, with opportunity to remediate via accelerated patching where beneficial.
HOW	
Prerequisites	An optional enhancement to the MDR or Core Monitoring service.

Procedures	An advanced vulnerability scanner agent will be installed on the client's IT estate (end points and servers). The scanning will identify Critical, High and Medium severity score (CVSS) vulnerabilities and allow either the client or their MSP time to remediate these. The scanning is continuous and produces daily reports, which can be shared with the client; it also reflects real time CVE releases to identify where zero-day vulnerabilities might appear during the month. At the end of the scanning period the agent will be removed (or can be left in operation subject to an ongoing fee as part of Secure, Detect and Respond services, see Section 2).
Knowledge base	Procedure to be stored in Pass Portal.
WHEN	
Service hours	This is an automated service that runs 24x7, 365. Reports are generated at intervals set in consultation with you, to balance scanning activity against patching cycle these are normally weekly outputs for a full internal or external surface scan. Emergent vulnerability scans are conducted every 24 hours.
TERMS & SLA	
Service Levels	The service will be delivered continuously to 99% availability.
Exclusions	Vulnerability Remediation is not included with this service but the SOC will alert your MSP (which might be Ekco) and work to accelerate patching of discovered critical vulnerabilities.
Billing	Billed as a per device charge for the agent, plus a one-off consultancy charge for deployment and tuning. Minimum license period is Six months.
Client Responsibilities	To review the reports and take any necessary, or recommended, actions on patching etc; Ekco can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

2.6 External Attack Surface Scanning (Light)

WHAT	
Name	**External Attack Surface Assessment**
Overview	External Attack Surface Management (EASM) is a cybersecurity discipline that identifies and manages the risks presented by internet-facing assets and systems. EAS scanning refers to the processes and technology necessary to continuously discover external-facing assets and any vulnerabilities of those assets. This is a continuous service within the group of MDR services designed as a value EASM offering. A more comprehensive Attack Surface Intelligence service is provided under Section 3, Predictive Edge.
HOW	
Prerequisites	None but it will be helpful if the client subscribe to monthly service reporting, otherwise a standalone one-two page report will be produced.
Procedures	The EAS Assessment is initially configured and defined through a consultation and discovery phase with the client. Any vulnerabilities identified through this process will be highlighted to the client (with a view to rectifying). An EAS toolset, cloud based rather than Agent based, will periodically scan the clients external attack surface for vulnerabilities and potential exposure.
Knowledge Base	To be updated and stored in PassPortal

WHEN	
Service hours	The tool scans on a predefined schedule with periodicity and timing configured by the SOC.
TERMS & SLA	
Service Levels	99.9% with outputs included in monthly cyber security service reporting.
Exclusions	-
Billing	Integrated within the MDR Charge.
Client Responsibilities	To provide details of externally facing infrastructure, IP addresses and owned web domains/ sub-domains. Ensure availability to discuss, approve and implement (where appropriate) any necessary, or recommended, actions.

2.7 DNS Filtering

WHAT	
Name	**Domain Naming Service (DNS) Filtering**
Overview	DNS filtering is a method of controlling access to online content by intercepting DNS queries and determining whether to permit or deny access to specific domain names. It operates through DNS-based 'blocklists', which block known malicious or undesirable domains, or 'allowlists', which allow access only to approved domains
HOW	
Prerequisites	Client must be signed up to DNSFilter
Procedures	Ekco have a predefined list of allowed/blocked websites that are applied to all clients, A custom policy will be created for the client through a consultation and discovery phase. Any additional blocked websites can be added by raising a ticket to the SOC
Knowledge Base	To be updated and stored in PassPortal
WHEN	
Service hours	This is a 24/7 service that can be updated via requests to the SOC
TERMS & SLA	
Service Levels	The DNS Filtering service operates 24x7, 265 with an estimated availability of over 99.9%.
Exclusions	TBC
Billing	Typically integrated within the MDR Charge.
Client Responsibilities	To provide details of IP addresses and web domains/ sub-domains they are likely to need access to (for populating the allow lists) To discuss and agree any specific categories of website that the client would not wish users to access (in addition to the standard list). Ensure availability to discuss, approve and implement (where appropriate) any necessary, or recommended, actions.

3 – Cyber Intelligence Service

Summary

The Cyber Intelligence service gives Ekco SOC a predictive edge. Clients do not receive intelligence directly but benefit from our ability to see into the Deep web and Dark web, draw on global intelligence monitoring agencies and open source media reporting, and the fusion of these sources into actionable information. The SOC then gets the earliest notifications of potential and building attacks, before they are initiated. Accordingly, the Cyber Intelligence service is only of benefit to clients that take Managed Detection and Response, or ideally the Advanced MDR service.

Cyber Intelligence Services: To include (these can be discrete but are best packaged together):
- Cyber Threat Intel
- Brand Intel
- Vulnerability Intel
- Attack Surface Intel
- Open Source Intel

Whichever sources are selected, you will benefit from our intelligence fusion that brings these analytics together to provide a predictive and focussing edge to our Secure, Detect and Respond services.

3.1 Predictive Edge

WHAT	
Name	**Cyber Intelligence Service – Predictive Edge**
Overview	Cyber Intelligence Service – Predictive Edge fuses multiple sources of intelligence about threat, incidents, attack surface, adversaries, trends and geo-political and other contextual information. This can be pulled together into a periodic report on request but is mainly used to gain a predictive edge to the SOC detection and response activity. Empowers the SOC team with the most up-to-date intelligence and insights relevant to the client.
HOW	
Prerequisites	Managed Detection & Response
Procedures	Accelerate Detect & Respond functions to make faster, confident decisions based on external intelligence automatically correlated with internal threat data in real time. Sources: - Cyber Threat Intel – to understand adversary capability and intent better, focussing analysis and detection spotlights on those who are assessed as likely to be interested in harming a particular client. Pairs well with Threat Hunting. - Brand & Identity Intel - to monitor and analyse web domain abuse, typosquat websites, credential leakages, impersonation – for example of key executives, logos and identifiable brand images. - Vulnerability Intel - monitoring for new vulnerabilities; avoids wasting time and resources on vulnerabilities that are low risk. Vulnerability Intelligence focuses attention on the vulnerabilities that actually matter. Augments Vulnerability Scanning in Advanced MDR. - Attack Surface Intel - Continuous scanning of the internet to identify all internet (public) facing assets; discover unknown shadow IT and out of policy devices; build a persistent view of the potential attack surface. - Open Source Intel – Monitoring of key industry feeds, social media and

	regular media outlets for indicators and warnings, contextual information and correlation with trusted sources.
Knowledge base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Clients that do not take MDR
Billing	A per client charge, billed monthly.
Client Responsibilities	Provide details of domains owned, key staff online persona and other publicly relatable/ discoverable information.

4 – Education & Awareness

Summary

Education and upskilling of client staff, to become other than the weakest link, and ideally the first line of defence. Delivered through cyber awareness training and phishing simulation. There is no better anti-phishing tool than the human eyeball and a critical mind; education and training are essential enablers of a strong first line of defence.

4.1 Simulated Phishing Attacks

WHAT	
Name	**Simulated Phishing Attacks**
Overview	The provision of the tooling and configuration to allow for the simulation of a real phishing threat, delivered to the client directly. The purpose of which is to both understand end user behaviours and / or deliver targeted training.
HOW	
Prerequisites	None
Procedures	A phishing attack will be built based on client requirements. All campaigns tend to differ. The result is a 'fake phishing attack' delivered by Ekco. The output of this exercise is a report that will identify any users that engaged with the email and clicked on links. This will allow for greater awareness of these attacks and will also highlight individuals who would benefit from further training / awareness.
Knowledge base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	08:30 – 17:30 excluding weekends and bank holidays
TERMS & SLA	
Service Levels	One off event or can be repeated periodically at client determined frequency.
Exclusions	-
Billing	Integrated as a per user charge with campaigns quoted for separately, based on requirements.
Client Responsibilities	To engage with the set up, initiation and go-live process, to conduct internal awareness and follow up activity with employees.

4.2 User Behaviours, Cyber Awareness and Education

WHAT	
Name	**Cyber awareness, education and training**
Overview	The provision of world leading training and learning tools to continuously educate client staff in the cyber-safe use of IT. Award-winning, cloud-based software will be deployed, built on the understanding that traditional security awareness and training doesn't successfully influence security behaviours. The training package educates, nudges, and supports people, and gives you both measurable change and measurable value.
HOW	
Prerequisites	None
Procedures	Deployment of the chosen product set to a client – potentially pure reseller activity but can also be integrated with Microsoft 365 for reporting, identity and with MSft Defender. Ideally clients administer the training, for example maintaining records, monthy status reports etc, themselves as part of their own HR ad training function. However Ekco can perform this service as well on request, at additional cost.
Knowledge base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	08:30 – 17:30 excluding weekends and bank holidays
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	Integrated as a per user charge with specific campaigns,for example to run a focussed event or series of events for Cyber Awareness month, quoted for separately, based on requirements.
Client Responsibilities	To engage with the set up, initiation and go-live process, to conduct internal awareness and follow up activity with employees.

5 – Crisis Response and Recovery

Summary

Finally, in event that it all goes wrong, Bluecube is recognised by the UK's leading cyber-insurance company as pre-eminent in immediate crisis response scenario. We don't intend that any of our cyber-resilience service clients ever need this, but nonetheless, it is the most reassuring insurance back stop they can possibly have. We will get clients up and running again faster than the competition can.

Recovery involves the engagement of our Crisis Response team. This is a fast moving, agile and hugely experienced team whose sole purpose is the recovery and rebuild of systems and environments following a Cyber incident. Ekco has a privileged position in matters of Cybersecurity. We are the exclusive partner with the UK's leading Cyber-insurance provider and with one of the world's leading Cyber-risk consultancies. We are engaged directly by the insurer to help companies who have suffered from a Cyber-attack to recover their systems as quickly as possible. We are experts in this style and type of engagement.

5.1 Crisis Response

WHAT	
Name	**Crisis Response**
Overview	A dedicated Crisis Response team who will respond to any major incident or crisis (typically, but not exclusively, following a cyberattack). The goal of the team is to reduce the time and disruption suffered by organisations that have fallen victim to a Cyber Incident and recover their systems as quickly as possible.
HOW	
Prerequisites	None
Procedures	A Crisis / Incident Response by its very nature is agile. It requires rapid and dynamic thinking and each engagement is unique. It is for that reason that we have a dedicated Crisis Response team that will lead all engagements to address incident classification, triage, containment, eradication and business recovery activities. This dedicated team will be supported by other delivery functions within Ekco, such as our SOC, NOC and Technical Specialists.
Knowledge Base	This is an 'always available' service. This means that the service is designed to be available clients at all times.
WHEN	
Service hours	N/A
TERMS & SLA	
Service Levels	N/A
Exclusions	Any specialist third party (external) fees required e.g. Forensics, Data Recovery or new hardware. Provision of the service where a client has chosen NOT to adopt or take specific security related advice/recommendations provided by Ekco (in this scenario the service can still be made available to the client, however a fee for the service will be charged, even if the contract states that it is included).
Billing	Typically delivered for an agreed one-off fee or provided as an integrated service for those client taking the Security Operations Centre (SOC) service. The associated Service Contract will confirm if this service is included (if it

	is there are no additional fees for the utilisation of this service).
Client Responsibilities	To ensure availability of key personnel including stakeholders to discuss (and approve) any necessary, or recommended, actions

5.2 Disaster Recovery

WHAT	
Name	**Disaster Recovery**
Overview	Disaster Recovery is defined as the restoration of your key IT systems onto the Microsoft Azure platform to a known time frame (referred to as a Recovery Time Objective) and a known maximum window of data loss (referred to as a Recovery Point Objective).
HOW	
Prerequisites	In order to deliver the service a client must be subscribed to Microsoft Azure through Ekco. In order to provide access to the Disaster Recovery environment it will be necessary for you to have a Remote Desktop Server or a network link into Azure to provide access.
Procedures	In order to calculate the Recovery Time Objective and Recovery Point Objectives we conduct a full Disaster Recovery test. We use the results of this test to confirm the timings and service levels that you can expect. These are formally communicated as part of a documented Disaster Recovery plan. Disaster recovery is invoked by logging of a service request via the Service Desk.
Knowledge base	Procedures to be stored in PassPortal in due course.
WHEN	
Service hours	Disaster Recovery is an 'always on' service. This means that the solution is designed to be available and operational at all times. Please note that invocation of Disaster Recovery can only be requested during normal working hours (Monday to Friday, 08:30 – 17:30, excluding Bank Holidays) due to the requirement to have 3rd line engineers available throughout the process. Outside of normal UK working hours we will make a best endeavours attempt to invoke a Disaster Recovery plan, however this will be subject to senior engineer availability.
TERMS & SLA	
Service Levels	Recovery Time Objective – Subject to specific contract, agreed and defined as part of the testing process. Recovery Point Objective – Subject to specific contract, agreed and defined as part of the testing process. An annual test is provided as part of the service (additional tests can be conducted for an additional charge).
Exclusions	Any servers / systems not included in the Disaster Recovery solution.
Billing	The Disaster Recovery service will attract an initial set-up fee; this fee is based on the complexity of your environment.

	The monthly service charge is based on the amount of reservation of computing power and storage within Microsoft Azure. Typically the charge for Disaster Recovery will be included within the IaaS charges made by Ekco. However, the cost for ongoing Azure charges should Disaster Recovery be invoked (other than for testing) are not included and will be passed onto the client..
Client Responsibilities	Client's must provide written notice of any infrastructure changes not carried out by Ekco.