eGroup | ENABLING TECHNOLOGIES

ThreatHunter
Comanaged eXtended Detection and Response

PREPARED FOR
Client Name Here

ACCOUNT EXECUTIVE
AE Name Here
Account Executive
email@eGroup-us.com

[Date]

Contents

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

1 Background

CLIENT NAME HERE (“Client” herein) is interested in improving their cyber defense capability. To that end, they are investing in Microsoft security tools and are seeking the assistance of a Managed Security Service Partner.

eGroup Enabling Technologies (“Partner” herein) proposes ThreatHunter, a comanaged security detection and response service. Partner is proposing the following services to Client to meet current and future needs.

2 Objectives

As part of their cyber investments, Client seeks to:

- Augment their team’s capabilities.
- Elevate their cybersecurity posture.
- Ensure 24x7x365 visibility into cyber incidents.
- Respond to incidents before they become impactful.
- Leverage existing security investments without adding proprietary tools.

3 Summary of Solution

ThreatHunter is a comanaged service where Partner monitors and responds to incidents detected by Client's Microsoft security tools. Client retains control of its security logs and tenant settings. Partner has visibility to the Client's environment through a Microsoft-developed API for managed service partners.

Partner will provide:

- Incident detection.
- Auto (and manual) remediation.
- Case management.
- Periodic health checks.
- Guidance to improve posture.
- Regular hardening of in-scope security tools.

Coverage will be valid 7x24x365 and is provided by Partner’s own US-based threat hunters.

4 Incident Severity Levels

Incidents will be classified using Microsoft Sentinel's definitions of incident severity and color-coded as High (Red), Medium (Orange), Low (Yellow) or Informational (Grey). Partner will provide incident response for High and Medium alerts and will log Low and Informational incidents for historical purposes.

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

Severity	Incident Details	Expected Partner Response	Expected Client Response
High (Red)	Alerts commonly seen associated with advanced persistent threats (APT). These alerts indicate a high risk because of the severity of damage they can inflict on devices. Examples: • Credential theft activities • Ransomware or malware activities • Tampering with security sensors • Any malicious activities indicative of a human adversary.	Initial incident response in 60 mins or less by manual or automated interactions Notification to Client's IT Security liaison and, if desired, escalation contact(s) Continuous effort to mitigate as agreed to by the Client and Partner along with Client's Breach Coach or Cyber Insurer Close the incident via manual or automated means and retain for 90 days (by default)	Acknowledgment of incident if notified If applicable, work with internal Client resources to execute incident response plans Perform remediation after threat has been neutralized or mitigated
Medium (Orange)	Alerts from endpoint detection and response post-breach behaviors that might be a part of an advanced persistent threat (APT). Examples: • Observed behaviors typical of attack stages • Anomalous registry changes • Execution of suspicious files • Any incident affecting Domain Controllers or other identified high-value targets	Initial incident response in 90 mins or less by manual or automated interactions Notification to Client's IT Security liaison Continuous effort all day, every day as agreed to by the Client and Partner Close the incident via manual or automated means and retain for historical purposes (in Client's Sentinel)	Acknowledgment of incident if notified If applicable, work with internal Client resources to execute incident response plans Perform remediation after threat has been neutralized or mitigated
Low (Yellow)	Alerts on threats associated with incidents that are auto-quarantined or auto-remediated where intervention isn't necessary. Examples: • Hack-tools like Kali Linux or pen test toolkits • Non-malware hack tools • Running exploration commands • Clearing logs This typically does not indicate an advanced threat targeting the organization.	Initial incident response in 120 mins or less by manual or automated interactions by Partner Escalate incident if determined to cause negative impact Close the incident via manual or automated means to be retained for historical purposes	None
Informational (Grey)	Alerts that might not be considered harmful to the network but can drive organizational security awareness on potential security issues.	Close the incident via manual or automated means to be retained for historical purposes	None

Partner will continue to monitor incidents reported 24x7. When necessary, Partner will escalate incidents to Client for the purposes of gathering additional details, assessing impact, and/or performing remediation steps during or after a security incident.

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

5 Coverage Details and Scope

5.1 Proactive and Managed Services Coverage

Partner will provide security monitoring for the following Microsoft security tools:

Tool	Quantity of users/devices
Defender for Endpoint - Endpoints	XXX
Defender for Office 365 Users	XXX
Defender for Identity	XXX

Every quarter, Partner and Client will confirm the user and device counts documented below. If counts change by more than 10%, the Change Request form and associated pricing adjustments will be presented.

Partner will provide the following managed services based on the frequency outlined in the table below. Partner and Client will preschedule these collaborative activities in advance at a mutually agreeable time.

Service	Frequency
Provide reporting and metrics of Sentinel incidents and threats	Monthly
Defender Portal Reporting Review	Monthly
Attack Simulation Training - Phishing Simulations	Quarterly
Configuration improvements to in-scope Microsoft security tools	Quarterly

5.2 Services in Scope

Partner Security Operations Center will provide the following services:

a. Monitor incidents created by the following security tools, and respond within the timelines outlined in **Incident Severity Levels**:
    i. Entra ID
    ii. Defender for Endpoint
    iii. Defender for Identity
    iv. Defender for Office 365
    v. Intune
    vi. Exchange Online
    vii. Windows 10/11 (OS Only)
        1. Surface Area Reduction
        2. OS updates
    viii. Defender for Cloud
    ix. Defender for Cloud Apps
    x. Sentinel
    xi. 3rd Party systems and/or Log Collectors
b. Assist with Response and Remediation

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

i. Eradicate incidents where possible (manually or via automation).
ii. Security orchestration and automated response at the Client's pre-approval or direction.
iii. Maintain and develop playbooks to respond to new threats.
iv. Perform Microsoft Sentinel and Defender maintenance as needed.

c. Hunt for Threats
   i. Use KQL queries developed by Microsoft or Partner to hunt for known threats.
   ii. Maintain indicators of compromise as provided by Client and Microsoft.

d. Respond to incidents, in cooperation and at the direction of the Client's IT Security Delegate
   i. Partner will leverage Microsoft Sentinel to perform automated incident response.
   ii. Participate in Client's Incident Response plans as agreed upon during onboarding.
   iii. Work with Security Delegate to determine if incidents are false positives.
   iv. Notify the Client's IT Security Delegate of incidents which indicate the following:
      1. Security breach
      2. Compromised accounts
      3. Data loss
      4. Negative user impact
      5. Productivity loss
      6. Uncovered persistent threats
      7. Application or service outages
   v. Provide access to Microsoft's analysis to assist in determining the root cause of the incident when requested by Client's IT Security Delegate

e. Manage Intune's configurations of (in-scope) Client workstations and laptops:
   i. Configure and monitor Policy and Profile Management settings:
      1. Compliance Policies
      2. Patching Profiles
         a. Windows OS Update Rings
         b. Windows OS Feature Updates
   ii. Configure and monitor Endpoint Security settings:
      1. Security Baselines
      2. Defender for Endpoint Policies
         a. Endpoint Detection and Response
         b. Attack Surface Reduction
         c. Automated Threat Remediation
      3. Account Protection
      4. Conditional Access
   iii. Wipe, retire or delete devices to protect company data

f. Conduct periodic phishing simulations using Microsoft Attack Simulation
   i. Deploy and run phishing simulation campaigns on Client's behalf to promote Security Awareness and Zero Trust concepts.
   ii. Provide reporting at the conclusion of each campaign
   iii. Assign training to users who fail phishing simulations, from the content within Defender for Office P2's library.

g. Escalate technical issues with Microsoft security tools to Microsoft Support as needed, and work with Microsoft on Client's behalf to resolve bugs or other unexplained errors.

h. Provide executive-level advisory services on a periodic basis for a total of eight (8) hours to understand and recommend relevant improvements about:
   i. The scope of Client's IT estate, regulatory requirements for disclosure and compliance, policies, and procedures (Incident Response Plan, acceptable use document, data governance policy), cyber insurance and data forensics incident response preparation.
   ii. Road-mapping, advisement, or covering specific topics of Client interest (i.e., audit preparation, board communication, internal training, reporting metrics).

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

5.3 Areas out of Scope

Anything not expressly in scope, including but not limited to:

1. Contacting **users** beyond the Security Delegate(s) to inquire or notify about a breach, phishing attempts, or other security events or threats.
2. Setting up **new** services, policies , connectors, features, or any additional functionality that Microsoft adds to their Defender Suite of products.
3. Configuration and feature updates that require **greater than two (2) hours** of effort. Other or longer tasks can be handled by Partner as a Change Request.
4. Any activities that would require design, planning, or architecture of the solution. These will be handled by Partner's Professional Services team as one-time projects, under a separate agreement upon request.
5. Any Microsoft license administration, including manual or dynamic licensing, as it relates to the Defender Suite.
6. Issues with 3rd party integrations to Microsoft Sentinel. These will be handled as "best reasonable effort support" and may require a Change Request for detailed troubleshooting.
7. Microsoft Intune policies and configurations not related to the Defender Suite.
8. Application Management and Packaging via Intune, or Intune Suite features.
9. Onsite assistance.
10. Management or security of smartphones and tablets.
11. Penetration testing.
12. Specific compliance attestations.
13. Detailed training documentation.
14. Information Governance and Data Loss Protection settings or policies including but not limited to:
    a. Microsoft 365 and Teams DLP Policies
    b. Purview Information Protection
    c. PII and Sensitive Information Policies
    d. Email Message Encryption
15. Post incident forensics and remediation efforts after a threat has been mitigated. These will be handled by Partner's Professional Services team as one-time projects, under a separate agreement upon request, or by Client's Cyber Insurance or Breach Coach.
16. Client access to Partner's intellectual property. Partner will own the intellectual property rights in all workbooks, playbooks, and other automations to use in other deployments.
17. Any task or deliverable not specifically listed as in-scope in this document.

6 Client Prerequisites

The following section describes actions Client must take to obtain successful technical support from Partner:

- Pay for any Azure consumption to support the service
- Provide contact information for primary and secondary Security Liaisons.
- Grant Granular Delegated Administrative Privileges access to Partner for the following within client tenant:
    - Azure Tenant where Microsoft Sentinel is configured.
    - M365 Tenant with access to the entire Defender suite (Identity, Endpoint, Cloud Apps, O365).
- Obtain Microsoft licenses required for monitored workloads (i.e., M365 E5/A5/G5, or E5/A5/G5 Security).
    - Attack Simulation Training requires Defender for Office for 365 P2.
    - Servers require ala carte Defender for Endpoint licenses
- Provide and maintain necessary on-premises infrastructure.
    - AD Domain Controllers that are being monitored by Defender for Identity sensors.

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

    - If applicable, the Virtual Machine (VM) containing the log collector to forward logs from on-premises devices into Client's Sentinel (this VM could also reside in Azure).
    - Log Analytics agents running on-premises machines from which logs are being sent to Sentinel.
- Configure firewall rules (to be provided during onboarding) to enable traffic from on-premises log sources to Sentinel.
- Hold and maintain (and provide Partner documentation for):
    - Cyber insurance provider information, declaration of coverage, and insurance policy.
    - Breach Coach/Incident Response contractors, if applicable.
    - Backup and Incident Response Plan for the covered assets, including Data Recovery Plan.
    - Completed Partner Security Questionnaire.

7 Roles and Responsibilities

While Partner is taking a primary role in monitoring and managing security events in Client's environment, a shared responsibility model is still in place.

Partner is primarily responsible for:

a) Monitoring the (in-scope) environment for security alerts.
b) Classifying certain (groups of) alerts as incidents of interest.
c) Identifying, triaging, isolating, and advising customer of recommendations to remediate the issue.
d) Remediating the issue with automated responses.
e) Tracking the incident with the Client until it is resolved.

Notifications and escalations will follow an agreed upon process to be documented during onboarding. In some cases, Client will be required to take action to respond, remediate, and recover. For instance, if the incident involves systems Partner has no administrative privilege nor day to day management responsibility (i.e. firewalls), Partner is not responsible for remediating the issue. Instead, Partner will advise Client and assist in (but not own) the recovery.

The following table outlines the responsibilities of each party for the services/systems covered in this Service Level Agreement. The tables are organized in RACI format, with:

R = The **R**esponsible Party (the group / person assigned to *perform the work*)

A = The **A**ccountable Party (the decision maker with *ultimate ownership*)

C = The **C**onsulted Party (stakeholders *involved before a decision* is made/action taken)

I = The **I**nformed Party (person(s)/party informed about decisions or actions that *were taken*)

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

The stages are based on the NIST Cyber Security Framework, where Identify and Protect are proactive motions taken by client. Detect and Respond are chiefly Partner functions, and Recover is a Client responsibility.

NIST CSF Stage	Client	Partner
Govern	RA	CI
Identify [1]	RA	CI
Protect [1] & Patch	RA	RCI
Detect, Analyze, Identify, Triage, and Notify	CI	RA
Respond		
Initial Response & Classification [2]	ACI	R
Escalated Response Investigation [3]	RA	CI
Recover		
Remediate & Restore [4]	RA	CI
Forensic Analysis & Postmortem [3]	RA	CI
Reports [5]	CI	RA

Footnotes are described as follows:

1. There is a shared **R**esponsibility for Identifying and Protecting against issues.
    a. Client is **R**esponsible for identifying vulnerabilities (CVEs, open ports, etc.) *and* to make corrective protections in all systems that are beyond Partner's scope (i.e., network equipment and firewalls).
    b. Partner is **R**esponsible for identifying vulnerabilities and proactively protecting the following services:
        i. Entra ID
        ii. Defender for Endpoint
        iii. Defender for Identity
        iv. Defender for Office 365
        v. Intune
        vi. Exchange Online
        vii. Windows 10/11 (OS Only)
            a. Surface Area Reduction
            b. OS updates
2. Upon detecting an incident, Partner is **R**esponsible for:
    a. Logically isolating affected Client machines that are at risk of spreading malicious code or that could be used for lateral movement. Isolation occurs via Defender for Endpoint, and will prevent compromised machines from communicating to other network devices (in the customer's network or on the Internet). The isolated machine will maintain connectivity to Client's Defender portal, allowing continued investigation without putting other network devices at risk.
    b. Downloading investigation packages from impacted and/ or isolated devices. Such packages will enable Partner's security personnel to conduct a safe and separate investigation on the impacted machine.
    c. Uploading impacted files (and/or binaries) from Client's environment to Virus Total (via the MSFT Defender portal) for investigation. Virus Total assesses the file and makes a judgment on if it's malicious. Partner assumes no responsibility for binaries once uploaded to Virus Total, which at the time become subject to Virus Total's Terms of Service and Privacy. Partner will not make the file(s), nor the fact that they're coming from Client's environment, publicly available.
    d. Communicating to Client about the status of the issue, until it is resolved.
3. When an incident is confirmed and warrants escalation:

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

a. Client is **R**esponsible to conduct escalated response steps under the advisement of Client's cyber insurance provider and/or breach coach/legal counsel.
b. Partner will participate and provide information to Client's insurer and/or breach coach.
c. Client's counsel or its forensics partners may not have direct access to Partner's monitoring systems, so as to protect the confidentiality of other customers.

4. Client is **R**esponsible to conduct the restoration of the affected system(s) with their own resources or contractors, unless:
    a. Partner is also Client's Managed Service Provider for the affected system(s).
    b. Partner is contracted (under a separate retainer) to conduct the restoration of systems
    c. If a. or b. are the case, the ThreatHunter team will escalate to Incident Response and Remediation resources after determining and agreeing that restoration or mitigating controls are needed.
5. Partner is **R**esponsible for creating and delivering timely reports about:

Report	Purpose	Frequency
Vulnerable Systems (identified by Defender for Endpoint)	Alert customer of systems at risk, as seen by Partner's monitoring systems	Monthly, unless agreed upon. If a system is known to be vulnerable but cannot be patched due to application incompatibility, Partner a) Bears no responsibility b) Can reduce frequency of such reports
Active Incidents	Alert customer of present/active risk	As it is happening and at pertinent update intervals
Incident History	Catalog of all incidents that were auto remediated or manually investigated.	Monthly

8 Assumptions

The Services, fees, and delivery schedule for this SLA are based on the following assumptions:

1. **Partner strongly encourages Client to have a validated and regularly tested Incident Response Plan and to perform Tabletop Exercises to validate recovery processes.**
2. **All data recovery efforts due to failures or security related incidents are Client's responsibility.**
3. Partner cannot guarantee security or that your organization will not be breached when using Microsoft 365 and Azure security products and services.
4. The Client's personnel will perform their roles and provide responses in a timely manner.
1. None of the Client's logs, files, nor data (outside of event logs and security signals) will be transmitted to nor stored by Partner. All files and content will remain in the Client's Azure or Microsoft 365 tenant.
5. This SLA is generated based upon information currently known as provided by the Client and deemed to be accurate and correct.
2. If the existing environment or solution requirements dictate a change in this Scope of Work, a change request form may be executed by both parties.

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com

9 True Up / Change Request Process

Client or Partner can request a change to the scope and counts identified in this agreement. For all change requests, regardless of origin, Partner shall submit to the Client a standard Change Request Form. The Change Request Form shall describe the proposed change(s) to the SLA, including the impact of the change(s) on the agreement scope, schedule, fees, and expenses. No change to this scope shall be made unless it is requested and accepted, and partner shall have no obligation to perform or commence work on any proposed change until a Change Request Form is approved and signed by both parties.

Every quarter, Partner and Client will confirm the user and device counts documented in Section 1, Summary of Services. If counts change by more than 10%, the Change Request form and associated pricing adjustments will be presented.

10 Contact and Escalation Process

Partner provides a designated email address (incidents@enablingtechcorp.com) and telephone support number **(863-279-0744)** for Client to ask questions, report incidents, or request follow-up.

The standard escalation process for issue review, approval and/or dispute resolution is as follows:

	Partner Escalation Matrix
Level 1	Submit ticket to incidents@enablingtechcorp.com
Level 2	Security Engineer on Duty 443-625-5199
Level 3	Managed Services Technical Team Lead Derek MacDonald 443-625-5218
Level 4	Director of Managed Services Fred Barzycki 443-625-5121
Level 5	Vice President of Technical Services Joshua Shoemaker 443-625-5158

482 Wando Park Blvd. Mt. Pleasant, SC 29464 | p 877.347.6871 | f 843.284.0150 | info@eGroup-us..com