eSENTIRE

Service Description: Managed Detection and Response - Microsoft M365 Bundle

1. Service Overview

eSentire's Managed Detection and Response ("**MDR**") - Microsoft M365 Bundle is a service bundle (the "**Service**") providing threat prevention, detection, investigation, response, and remediation as defined herein, delivered by eSentire's SOC for the entire Microsoft Corporation ("**Product Publisher**" or "**Microsoft**") Defender suite of products available under the Microsoft 365 E5 and similar licensing offered by Microsoft. See Section 4- Subscription Options for licensing information ("**License**" or "**Licensing**").

This Service monitors Clients' endpoint, email, identity, and cloud access security broker ("**CASB**") signals covered by the applicable Microsoft software licensing and investigates, and responds accordingly. In order to provide the Service, eSentire will integrate Client Licensed Microsoft security products with eSentire's platform.

2. Definitions

Capitalized terms contained in this Service Description are as defined herein, or as defined on the Managed Detection and Response ("**MDR**") Services landing page (which can be found under Service Descriptions at: https://www.esentire.com/legal/documents).

3. Service Capabilities

3.1. Description

eSentire will leverage Client's Licensing to obtain email, user identity, application control, and visibility, which will enable the eSentire SOC to identify and investigate potential threats or suspicious activity within Client's environment. The Service is supported by eSentire's SOC on a 24x7x365 basis and will result in human-led investigations of suspicious activity and alerting.

During the Term of the Service, eSentire will provide threat detection, analysis, investigation, escalation, response, and remediation (as described below). In addition, eSentire is responsible for security event analysis and investigation to determine if a security event is considered a legitimate threat and warrants an escalation to Client and a potential response action. If an event is deemed Actionable, due to its behavior and the type of detection, it will be escalated to Client as an Alert. The SOC will perform event triage, assign criticality, and include supporting information and analysis within the Alert and, if necessary, initiate escalation to Client. Malicious or suspicious activity will be identified and resolved by eSentire, utilizing response playbooks. Client will receive access to the eSentire Insight Portal, which will consolidate threat alert reports and investigation details from eSentire SOC analysts. Threat Cases will be visible to Client on their Insight Portal dashboard; however, it is eSentire's responsibility to classify the criticality of Alerts derived from individual events.

eSentire will also provide Client guidance on implementing configuration changes to support prevention and visibility within the M365 Defender Security portal. This may include providing Client advice related to the benefits of custom policies, sanctioning/un-sanctioning applications, session controlled conditional access policies, detection capabilities via policies, email authentication, email protection and detection capabilities via policies, or curation and tuning antivirus ("**AV**") and endpoint detection and response ("**EDR**") policies within the M365 Defender portal.

eSentire will collect events generated by M365 Defender to the eSentire Atlas XDR Platform for machine and human analysis and investigation, and may filter traffic based on volume to optimize service delivery. Once investigated, events are classified, alerted, and escalated to Client if action is required. eSentire will utilize the escalation process, agreed upon during the Deployment process, to contact and relay information to Client. The defined escalation process is a mutually agreed upon process between Client and eSentire.

The following support is included as part of the Services:

- Threat Detection:
  - Collection of detections, metadata and selected raw telemetry to aid in investigation, threat hunting and response activity.
  - Enriching collected Client data with context – such as geolocation of IPs, Client-specific context and threat intelligence.
- Analysis:
  - Analysis of Alerts generated by Clients Licensed platform either through automation in the eSentire Atlas Platform and/or by eSentire (SOC, incident handlers and/or threat hunters).

3.2. Response Actions. At the conclusion of the review of a Work Item, eSentire will classify the item as either a threat or non-threat. The classification of an event as a "threat" will generate a Threat Case and be further evaluated and marked by severity level (Low, Moderate, High, or Critical), which are further defined within the Service Level Objectives (see section 7). A list of classifications, severity levels, and the associated actions, Alerts and follow up expected is as defined in table 1 below:

Table 1:

Classification	Severity Level	Action	Alert	Disposition	Follow Up
Threat	Low/Medium	No Client Action Needed	No Alert	True Positive	Automated remediation actions (SOC can assist with further actions upon request)
		Client Action Needed	Alert with description and relevant data	True Positive	Underlying telemetry and associated data will be available Clients Insight Portal dashboard Subscription to Prevent, Detect, & Respond will result in automated remediation actions (SOC can assist with further actions upon request)
	High/Critical	Client Action Needed	Alert with description and relevant data eSentire threat response • host isolation • identity isolation • remediation actions Escalation procedure (email/phone call with acknowledgement expected)	True Positive	Underlying telemetry and associated data will be available on Insight Portal Subscription to Prevent, Detect, & Respond will result in automated remediation actions (SOC can assist with further actions upon request)
Non-Threat (False Positive / Benign)	N/A	No Client Action Needed	No Alert	False Positive	Recurrences of identical activity will be logged as ignored

Unless Client opts-out, as part of the Service, eSentire will by default isolate potentially compromised machines and user identities. eSentire will isolate endpoints and user identities using the native capabilities of the Microsoft 365 Defender Security Portal and notify Client of the isolation via the agreed upon escalation procedure including evidence to support the action. The endpoint or user identity will remain in isolation until the threat has been remediated or Client has accepted the risk and removes the endpoint or user identity from isolation. Details of the isolation process are as follows:

- All endpoints and user identities are considered authorized for isolation unless otherwise communicated by Client.
- eSentire will escalate all Alerts that require isolation to Client for their visibility and active feedback on the Alert.
- Client commits to allowing eSentire's default isolation response action on potentially compromised endpoints and identities or forfeits this response capability – Isolation response action is used to prevent the spread of malicious code and lateral movement by suspected attackers.

Clients subscribed to this Service are hereby advised that the eSentire SOC has the functionality to isolate endpoints and user identities on Clients' network, the ability to use this function to protect the network, and that the isolated endpoint or user identity will lose all connectivity to all other devices or resources.

3.3. Remediation Actions

eSentire can assist Client with remediation activities for high or critical threats from active hands-on keyboard attackers, on the endpoint itself, upon alerting Client. The types of remediation support actions that can be provided by eSentire, in coordination with Client are as follows:

- Process or file denylisting on an endpoint.
- Block and kill malicious processes.
- Detect and prevent known/unknown bad software (quarantine malicious files).
- Downloading files to an endpoint.
- Isolate an endpoint not included in the permitted automatic isolation policy noted in 3.2.
- Initiate a remote shell interactive session ("Real Time Response") on the endpoint to perform a deeper investigation or remediation actions, which can (at eSentire's discretion) include:
  - stopping or removing services and registry keys;
  - performing system reboots to remove malware from volatile memory;
  - gathering files and memory for host;
  - terminating processes; and/or
  - deleting files on an endpoint.

3.4. Reporting and Data Access

eSentire delivers all SOC led investigation reporting within the eSentire Insight Portal. Client will have access to both the raw data and custom reporting through Clients Licensed Microsoft platforms. This natively includes a cloud discovery dashboard, app risk levels, URL protection reports, compromised user reports, safe attachment reports, device list, etc.

4. Subscription Options

4.1. Third-Party Licensing Requirements

Client must procure and maintain one, or more, of the applicable Microsoft licensing during the entire Term of the Service, and coordinate proper Licensing permissions with the Product Publisher to allow eSentire full administrative access and credentials into Client's License instance.

The minimum requirement for the MDR Microsoft M365 Bundle requires Client to procure all the following modules from Microsoft:

- Defender for Endpoint Plan 2
- Defender for Office 365 Plan 2
- Defender for Identity
- Defender for Cloud Apps
- Azure AD Premium 2 (P2) licensing

These modules are all included in the following Microsoft M365 Licensing bundles:

- Microsoft 365 E5
- Microsoft 365 E3 + E5 Security add-on

Client will retain ownership of the License and will continue to have all access to utilize their License. Client acknowledges and agrees that any changes made by Client in the Licensed environment could negatively impact eSentire's ability to deliver the Services. In addition, Client acknowledges and agrees that any changes made by Client during the term of this Service should be reviewed with eSentire, otherwise eSentire shall be released from any and all obligations to effectively provide the Services as contemplated herein. Throughout the Term of the Service, Client must provide and eSentire must maintain administrator or equivalent access which enables eSentire staff and systems to execute the tasks included in this service description. Access will only be provided to select, authorized eSentire employees and will be audited.

5. Deployment

eSentire will provide Client with deployment documentation (the "Onboarding Guide") outlining the access required and configuration that is necessary for eSentire to connect to Clients Licensing. This is a requirement for eSentire resources to securely access Clients environment to operationalize the Services. eSentire will provide support to assist with any questions related to the deployment process and the requirements for the Service.

6. Tuning and Configuration

eSentire is responsible for configuring and tuning the Service capabilities leveraging Clients Licensing. The Client is responsible for the M365 Defender technology implementation. Service deployment methodologies can take up to 30 days to fully tune. This requires a special configuration and tuning process due to the automated blocking/killing capabilities that will need to be established.

eSentire will provide guidance for the implementation of Defender for Endpoint, Defender for Office 365, and Defender for Identity & Cloud Apps policies for the purposes of ensuring Defender configuration is compatible with eSentire services. The eSentire consultant may offer up to one hour per Microsoft Defender service to provide guidance for implementation of the main features and functionality that are identified below.

6.1 Defender for Endpoint

- Defender EDR Advanced Features configurations
- Defender AV custom policy configuration within Intune (Endpoint Manager)
- Attack Surface Reduction ("ASR") rule policy configuration and knowledge transfer within Intune (Endpoint Manager)

6.2 Defender for Office 365

- Sender Policy Framework ("SPF"), Domain Keys Identified Mail ("DKIM") and Domain-based Message Authentication ("DMARC"), Reporting & Conformance
- Anti-malware, anti-spam, anti-phishing, safe attachments, safe links
- Safe attachments for SharePoint, OneDrive, and Microsoft Teams
- External email warning

6.3 Defender for Identity & Cloud Apps

- Connect Office 365 application as a connected application
- High-level knowledge transfer of environment
    - Azure identity protection policy
    - Conditional access policy for session controls
    - OAuth applications
    - Discovered applications – sanctioning/un-sanctioning
- Defender for Identity - sensor validation
- Enable rile monitoring.
- Enable synchronization between Microsoft Defender applications

7. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on Licensing from Product Publisher being integrated and in production in Client's applicable environment. The service levels contained on the Managed Detection and Response ("MDR") Services general description found here (https://www.esentire.com/legal/documents), are only applicable to Clients environment in scope that are Licensed as part of the Service, and are actively communicating with the Service.

8. Responsibilities

Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the Service is dependent upon Client's compliance with the obligations hereunder, including meeting the service levels above. In the event Client fails to perform its obligations herein, in the time and manner specified or contemplated below, or should any obligation set out herein with respect to the Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

Non-compliance with these obligations may result in suspension of the Service or suspension of service levels. A responsibilities matrix is located in Appendix A below.

8.1 Client Responsibilities

Client obligations include:

- Working with eSentire to implement the proper security protections to limit attack vectors and increase security posture.
- Ensuring changes to application programming interface ("API") and/or access into the environment is communicated to eSentire.
- Designating a project coordinator to work directly with and serve as the primary Client contact with eSentire for the term of the Service.
- Providing the necessary resources, information, documentation and access to personnel, equipment, and systems, as reasonably required by eSentire, to allow eSentire to perform the Services.

- Ensuring appropriate licensing is procured (see section 4.1).
- Ensuring that there are not any firewall rules or other network blocking in place that would negatively impact communication between endpoints and the Microsoft Licensing.
- Deploying Endpoint/Defender AV policies via Group Policy Objects ("GPO"), System Center Configuration Manager ("SCCM"), and Intune.
- Notifying eSentire of newly added machines to the Service during the Service Term. Should the ingestion usage on a monthly average basis be more than 10% of the daily ingestion limit (identified on the Order Form), notwithstanding any security event, for more than two consecutive months, Client will move to the next ingestion level to accommodate its usage for the remainder of the Service Term.

8.2 eSentire Responsibilities

eSentire is responsible for the Services as described in this Service Description.

9. Service Terms

9.1 Exclusions

- The Service does not include any Microsoft licensing.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Security – Detection monitoring, analysis	I	RAC
Security – Investigation	-	RAC
Security – Notification	I	RAC
Security – Remediation procedures	AI	RAC
Security – Detection resolution	I	RAC
Security – Threat Intelligence integrations	I	RAC
Security – content tuning during deployment	RA	R
Security – custom use cases for client-specific implementation/direct-to-client notification	RA	I
Security – submit new use cases to eSentire for potential inclusion in SOC Runbook library	RA	RA
Threat Detection Security – ad hoc threat sweeps for IOCs	-	RA
System– custom alerts, dashboards, or workflows	RA	-
System – Initial product walkthroughs and/or guides	A	R
System – Deploying initial endpoints	RA	CI
System – Initial policy and environment configurations	CI	RAC
System – Post-deployment installation or host group management	RA	C
System – User account management and administration	RA	-
System- End user training*	RA *	C
System – eSentire API permission consent for alert ingestion	RA	I
System – Data ingest tuning	I	RA
System – Onboarding policy configuration	RA	RAC
Infrastructure – environment and product changes	RA	CI
Health– Data ingestion, uptime monitoring and tuning	-	RA
Health – Managing sensor updates	RA	-
Health – Adding and removing hosts from isolation	RAI	RA
Health – Performance or troubleshooting issues	RA	CI
Data – Resolving collection issues	RA	C
Data – Monitoring collection (in scope data)	I	RA
Data – Notification of lack of collection	A	R

R = Responsible; responsible for action and implementation. Responsibility can be shared.
A = Accountable; ultimately answerable for the activity or decision. This includes “yes” or “no” authority and veto power.
C = Consulted; typically, the subject matter experts, to be consulted prior to a final decision or action.
I = Informed; needs to be informed after a decision or action is taken.
*= Self service