eSENTIRE

Service Description: Managed Detection and Response Services with Microsoft Defender for Office 365

1. Service Overview

eSentire's Managed Detection and Response Services ("**MDR**") with Microsoft Defender for Office 365 (the "**Service**") provides Client with email-level visibility and control to support threat prevention, detection, investigation, and response. The service enables the SOC to prevent, detect and respond to threats based on detection via the Microsoft Defender for Office 365 platform. Microsoft Defender for Office 365 (formerly Office 365 Advanced Threat Protection) helps protect organizations against sophisticated attacks such as phishing and zero-day malware. Microsoft Defender for Office 365 also provides actionable insights by correlating signals from a broad range of data to help identify, prioritize, and provide recommendations on how to address potential threats. eSentire supports analyzing suspicious O365 security events and uncovering additional context in multi-signal MDR investigations depending on supported services. The service is supported by eSentire's SOC on a 24x7x365 basis. The Service is scoped by the number of Client users, and the number of users included in the Service are outlined on the Order Form.

2. Definitions

Any capitalized terms below, contained in this Service Description are as defined herein, or as defined in the "Managed Detection Response ("**MDR**") Services - General Information" document (referred to herein as the "**MDR General Information**" document) which can be found under the "Managed Detection and Response ("MDR") Services" section found on this webpage: https://www.esentire.com/legal/documents. The MDR General Information document contains information applicable to all MDR services, including this Service.

"**Domain Keys Identified Mail (DKIM)**" confirms received email was sent/authorized by the owner of that domain.

"**Domain-based Message Authentication, Reporting and Conformance (DMARC)**" uses SPF and DKIM to determine the authenticity of an email message.

"**Sender Policy Framework (SPF)"** helps receiving servers confirm mail sent from your domain is from Clients organization.

3. Service Features / Service Capabilities

3.1. Investigation and Analysis. eSentire is responsible for threat detection, analysis, investigation, escalation, and response. 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 the Client and potential response action. If an event is deemed as actionable, due to its behavior and the type of detection, it will be escalated to the Client as an Alert. The SOC will perform event triage, assign criticality, and include all supporting information within the Alert and, if necessary, initiate escalation to the Client. Malicious activity will be identified and resolved immediately utilizing response playbooks by eSentire.

eSentire is responsible for providing guidance on implementing configuration changes to support prevention at the Microsoft Defender for O365 email gateway. This includes email authentication, email protection and detection capabilities via policies.

As part of the Service, eSentire will investigate all security events identified and escalate actionable alerts as appropriate in accordance with the service levels detailed below. eSentire holds all rights to filter traffic based on volume to optimize service delivery. User escalated phishing emails are considered security events. Once investigated, events are classified, alerted, and escalated to the Client if there is an action required. eSentire will utilize the escalation process, agreed upon during the on-boarding process, to contact and relay information to the Client. The defined escalation process is a mutually agreed upon process between the Client and eSentire.

3.2 Key Benefits

- Configuration hardening to prevent social engineering, malware, and other email-based threats.
- Implementation of security configuration for SharePoint, OneDrive, and Microsoft Teams.
- 24x7x365 Investigation and response into email-based threats.
- Dedicated platform designed for email-based threat investigations.
- Investigate and respond to escalated suspected phishing emails.
- Direct API integrations for blocking and removing identified malicious content.

4. Response Actions for Identified Threats

eSentire has the below native capabilities within the Service:

- Delete / quarantine malicious email
- Add IPs/domain/email sender to blocklist
- Isolate compromised user

If Client is subscribed to multiple eSentire services, additional response actions can be utilized based on the most effective response action. This can include endpoint, network, identity, and cloud response.

5. Incident Alerts and Reporting

eSentire sends Alerts via email for Medium, High, and Critical severity events followed by escalation(s) for High and Critical severity events, as necessary, based on agreed upon escalation procedure in the configuration worksheet. A member of the eSentire customer success team will be assigned to review the overall Alerts with the Client. All Alerts are available within the eSentire Insight Portal for Client's review. All reporting is delivered through the Insight Portal.

6. Deployment

6.1 Access. eSentire will provide the Client with a detailed deployment document outlining the access required and configuration that is necessary for eSentire to connect to the Client. This is a requirement for eSentire resources to securely access the customer environment to operationalize the Service.

6.2 Configuration. eSentire will assign a consultant and provide guidance for implementation of email authentication security components and various email security policies which are the main ways to filter out potentially malicious content. The eSentire consultant will have 4 hours allocated to provide guidance for implementation of the main features and functionality that are identified below.

6.2.1 Email Authentication:

- SPF
- DKIM
- DMARC

6.2.2 Defender for Office 365:

- Anti-malware Policy
- Anti-spam policy
- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams
- Anti-phishing protection in Defender for Office 365
- Real-time detections
- External Email Warning

6.3 Tuning. eSentire will monitor all preventions and detections that are triggered within the platform and make the necessary changes to allow legitimate emails to reach the Client's infrastructure during the tuning phase. During the tuning phase, an assessment will be made on whether minor policy changes are needed depending on the specific requirements of the Client. Once the email authentication, protection and detection capabilities are enabled eSentire will work with the Client to ensure the email security platform is in a healthy state before transitioning to production monitoring.

6.4 Reporting and Data Access. eSentire delivers all SOC led investigation reporting through the eSentire Portal. The Client has direct access to the Microsoft Defender for O365 platform which includes both the raw data and access to custom reporting which natively includes URL Protection Report, Compromised User Report, Spam Detection Report, Safe Attachment Report, etc. Client has the right to use the Microsoft software which allows them full visibility and access into the data.

7. Maintenance and Support

eSentire will provide support to Client for both security and system issues related to the service, as defined below.

8. 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 in the MDR General Information document are only applicable to Client's environment in scope Licensed as part of the Service, and that are actively communicating with the Service.

9. 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.

9.1 Client obligations include:

- Working with eSentire staff to implement the proper security protections to limit the attack exposure of their email footprint.
- Ensuring changes to 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 eSentire MDR with Microsoft Defender for O365 Services
- 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.

10. Exclusions

The Service does not include any Microsoft licensing.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Threat Detection – deploy content	I	RA
Threat Detection – content tuning	A	R
Threat Detection – custom use cases	RA	I
Threat Detection – submit new use cases to eSentire content teams	I	RA
Threat Detection – Alert monitoring, analysis	I	RA
Threat Detection – Notification	I	RA
Threat Detection – Resolution	RA	RA
System – Microsoft Defender O365 API setup	R	I
System – Azure AD Account provisioning setup	R	I
System – Data ingest tuning	I	RA
System – MDO365 knowledge transfer session	I	RA
System – User account management	RA	RA
Health – Data ingestion uptime monitoring	I	RA
Health – General troubleshooting	RA	C
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.