eSENTIRE

Service Description: Managed Detection and Response Services with Microsoft Defender for Identity and Cloud Apps

1. Service Overview

eSentire's Managed Detection and Response Services ("MDR") with Microsoft Defender for Identity and Cloud Apps (the "MDICA Service") provides Client with user identity, application control, and visibility to support threat prevention, detection, investigation, and response. The Service enables the eSentire Security Operations Center ("SOC") to prevent, detect and respond to threats based on detection via the Microsoft Defender for Identity ("MDI") sensor, and Defender for Cloud Apps ("MDCA") platform. MDI (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages Clients on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at Clients organization. MDCA (formerly Microsoft Cloud App Security) provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all Clients Microsoft and third-party cloud services. Together, both services help protect against risky behavior across data, users, and – SaaS – applications, and help gain visibility of deployed cloud apps, discover shadow IT, and protect Clients sensitive information. eSentire supports analyzing suspicious identity and cloud application 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.

"Configuration Worksheet" filled out by the Client during deployment that gives eSentire more context into Client environment.

3. 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 Client and 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 utilizing response playbooks by eSentire.

eSentire is responsible for providing guidance on implementing configuration changes to support prevention and visibility within the MDCA portal. This includes custom policies, sanctioning/un-sanctioning applications, session controlled conditional access policies, and detection capabilities via policies.

eSentire will investigate security events identified through the MDICA Services and escalate actionable alerts as appropriate in accordance with the Service Level Objectives (SLOs). eSentire may filter traffic based on volume to optimize service delivery. Once investigated, events are classified, alerted, and escalated to Client if 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 and tuning support on MDI and MDCA, to harden overall security posture and ensure service functionality.
- Knowledge transfer and walkthrough of MDCA portal.
- 24x7x365 Investigation and response into identity/app-based threats.
- Dedicated platform designed for identity/app-based threat investigations.
- Direct API integration for disabling user accounts and revoking refresh/session tokens based on risky identity/app behavior.
- Extended visibility across business-critical SaaS applications and adds user-level threat detection and containment capabilities.

4. Response Actions for Identified Threats

eSentire has the below native capabilities within the MDICA Service:

- Revoke refresh/session token of a user (for M365 apps)
- Disable user in Active Directory
- Reset user password

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 Client. All Alerts are available within the eSentire Insight Portal (the "Portal") for Client's review. All reporting is delivered through the Portal.

6. Deployment

6.1 Access. eSentire will provide the Client with a detailed deployment document (Onboarding Guide) 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 Client environment to operationalize the eSentire MDICA Service

6.2 Configuration. eSentire will assign a consultant, and provide guidance to Client, for implementation of fundamental configurations and various security components within Microsoft Defender portal. The

eSentire consultant will have up to 4 hours allocated to provide guidance to Client for implementation of the main features and functionality that are identified below.

6.2.1 Entra ID Protection:

- Configure risky user policy for automated response actions through Microsoft
- Configure sign-in risk policy for automated response actions through Microsoft

6.2.2 Defender for Cloud Apps:

- Microsoft Defender portal walkthrough and knowledge transfer
- Enable Shadow IT Discovery via MDCA for Endpoint
- Discover and assess cloud apps and app discovery policies
- Connect Office 365 app – establishing actionable governance for Office 365, SharePoint, OneDrive, Teams, Power BI, etc.
- Essential practice configurations

6.3 Tuning. eSentire will monitor 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 Client. Once the protection and detection capabilities are enabled, eSentire will work with Client to ensure the security platform is in a healthy state and security posture before transitioning to production monitoring.

6.4 Reporting and Data Access. eSentire delivers all SOC led investigation reporting through the eSentire Insight Portal. The Client has direct access to the MDICA platform which includes both the raw data and access to custom reporting which natively includes cloud discovery dashboard, app risk levels, app categories and discovered apps, top entities (most active within your network), etc. Client, as the Microsoft license holder, will have the rights to use the Microsoft software which allows them full visibility and access to the data.

7. Maintenance and Support

eSentire will provide support to the Client for both security and system issues related to the MDICA 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:

- Maintaining active paid-up license, during the Service Term, for Microsoft for an E5 license or E5 security addon / or standalone license for Defender for Cloud Apps and Defender for Identity and one Azure ADP2 license.
- 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 Identity and Cloud Apps.
- 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 for Identity and Cloud Apps API setup	R	I
System – Azure AD Account provisioning setup	R	I
System – Data ingest tuning	I	RA
System – Defender for Identity and Cloud Apps 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.