eSENTIRE

Service Description:
Identity Services – Identity Response

1. Service Overview

eSentire's Managed Detection Response ("**MDR**") for Identity Services – Identity Response (the "**Service**") is a managed service providing identity response actions via an eSentire-supported Identity Provider ("**IDP**") to augment existing threat prevention, threat detection and investigation services provided by eSentire within Client's environment (the "**Client Environment**"). The Service is provided based on the number of Client-identified users in each Client-linked IDP ("**Users**"), as detailed on the Order Form, and as further described below.

This Service requires that Client has an active eSentire MDR subscription for an Endpoint, Cloud or Log Service (referred to herein as a "**Managed Source**" and purchased separately). The eSentire Atlas Platform ("**Platform**") will enable identity response actions to mitigate compromised identities and suspicious user behavior surfaced from Managed Sources with identity elements. Identity response actions are taken by members of eSentire's SOC as part of the Managed Source actions.

2. Service Definitions

Any capitalized terms 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.

3. Service Capabilities

3.1. Response. Following successful onboarding of Client IDP(s) within the eSentire Insight portal, eSentire will provide identity response capabilities to address escalated events from Managed Sources in the Client Environment. These capabilities enable response actions to mitigate compromised or suspicious identities. When an event from a Managed Source is deemed Actionable based on behavior and detection type, eSentire will escalate the event to Client as an Alert, implement necessary identity response actions through the eSentire SOC, document actions taken, and communicate with Client through the Managed Source escalation process. Once moved to a service-ready state, the eSentire SOC can perform any of following actions: disable user accounts to prevent lateral movement, re-enable user accounts to un-do eSentire SOC actions, expire user passwords to force creation of new security credentials, and revoke session tokens to immediately force users from Client solutions. Identity response actions may be in addition to eSentire SOC actions taken with respect to a Managed Source.

3.2. Identity Isolation Protocol. Unless Client opts out, eSentire will disable potentially compromised identities via the Client IDP(s), notify Client through established escalation procedures with supporting evidence, and maintain isolation until threat remediation or Client's written acceptance of risk. Under standard operational guidelines, all user entities and identities within the Client IDP(s) are automatically considered authorized for identity response actions unless specifically excluded by the

Client. It is Client's responsibility to identify and communicate any critical identities that require written authorization before isolation can be implemented. eSentire will restrict its isolation actions to non-restricted identities and will only implement such measures when necessary to prevent lateral movement by suspected attackers.

4. Subscription Summary

This Service is provided by eSentire in a managed only capacity, which requires that Client must procure and maintain its IDP licensing ("License") with an eSentire supported IDP.

Additionally, this Service requires Client have at least one separately ordered and active eSentire Managed Source.

5. Deployment

eSentire is responsible for providing Client with the required installation documentation for in scope Client IDP(s). Client is responsible for acting on the documentation to correctly configure and link the IDP(s), via API credentials, to the eSentire Atlas platform. Client is responsible for ensuring the API credentials leveraged for the Service remain present and active in the Client Environment during the Service Term. Once Client onboards an IDP, an end-to-end test is completed by the eSentire SOC to ensure proper configuration and the ability to disable users and take other identity response actions in the Client Environment. Client is responsible for electing and submitting a user account for testing purposes that will be disable and re-enabled by the eSentire SOC.

6. Service Level Objectives

The service levels in the MDR General Information document are only applicable to Client's Managed Source that are ordered separately, as identity response actions are linked to Alerts created as part of such Managed Sources.

7. Client Responsibilities

Client acknowledges that eSentire's ability to deliver the Service and to meet any applicable service levels is dependent upon Client's compliance with the obligations herein. Non-compliance with these obligations may result in suspension of the Service or suspension of service levels. The responsibilities of each party are also summarized in the responsibilities matrix which can be found in Appendix A.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Security – Take identity response action via Client IDP against eSentire-generated findings with an identity element like email addresses or Microsoft Principal IDs	IC	RA
System – Grant access to Atlas platform with properly configured entitlement	I	RA
System – Deploying eSentire-supported IDP	R	ACI
System – Nominating user for end-to-end testing	R	ACI
System – Technology troubleshooting, if necessary	RA	ACI
Health– Uptime monitoring	-	RA
Health – Ensure Client IDP API credentials remain active	RA	CI
Health – Performance or troubleshooting issues	RA	RC

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