eSENTIRE

Service Description:

Cloud Services — User Reported Phishing

Service Overview

eSentire's Managed Detection and Response ("MDR") for Cloud Services — User Reported Phish (the "Service") is a managed service that investigates and triages user-reported phishing emails within Client's Microsoft Office 365 environment. The Service leverages Microsoft Defender for Office 365 P1 or P2 ("MDO"; purchased separately) to deliver analyst-driven phish investigation and triage.

The Service is provided based on the number of "Users" which is measured by non-shared Client-licensed Microsoft 365 mailboxes ("Mailboxes"), as detailed on the Order Form, and as further described below.

The Service will be offered as an add-on to an existing qualifying eSentire MDR service subscription (a "Managed Service"; purchased separately). User reported phish triage actions supplement the investigation and response actions provided by the Managed Service.

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.

Service Capabilities

Investigation

Following successful onboarding of Client's Microsoft Office 365 environment, eSentire will provide phishing investigation capabilities for emails reported by end users via the Microsoft Outlook Report button. When an end user reports an email as phishing, the eSentire SOC retrieves the alert generated by the report and performs analysis to determine whether the email is a genuine phishing threat or a false positive.

Response

When a reported email is determined to be a confirmed phishing threat, the eSentire SOC will take the following response actions as appropriate:

- **Alert Classification** — classify the phishing alert as a true positive with appropriate determination, documenting the investigation findings. When a reported email is determined to be a false positive (legitimate email reported by the user in error), the eSentire SOC will classify the alert accordingly.
- **Escalation** — if the phishing email is associated with credential compromise, malware delivery, or other indicators of intrusion, the eSentire SOC will escalate the event through the established Managed Service escalation process for further investigation and containment.

Phishing Simulation Filtering

The Service automatically identifies and filters phishing simulation emails generated by third-party Security Awareness Training providers (e.g., KnowBe4, Proofpoint, Cofense, Beauceron). Simulated phishing emails reported by users are classified as simulations and closed without SOC investigation, ensuring that analyst time is focused on genuine threats.

Subscription Summary

This Service is provided by eSentire in a managed-only capacity. Client must procure and maintain Microsoft Defender for Office 365 Plan 1 (minimum). The Service is offered as an add-on to an existing eSentire MDR subscription for a Managed Service.

Deployment

eSentire is responsible for providing Client with the required installation documentation for in-scope Microsoft Office 365 configuration. Client is responsible for acting on the documentation to correctly configure and link the Client's Microsoft Office 365 environment, via API credentials, to the eSentire Atlas platform.

Once Client onboards, an end-to-end test is completed by the eSentire SOC to ensure proper configuration and the ability to investigate and respond to user-reported phishing emails in the Client Microsoft Office 365 environment. Client is responsible for electing and submitting a test phishing report for verification purposes.

Service Level Objectives

The service levels in the MDR General Information document apply to this Service. User-reported phishing alerts are triaged within the applicable SLO for the alert severity. Phishing simulation emails identified by the automated filtering logic are excluded from SLO measurement.

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 — Investigate and respond to user-reported phishing emails via eSentire-supported Microsoft 365 environment	IC	RA
System — Grant access to Atlas platform with properly configured entitlement	I	RA
System — Deploying eSentire-supported Microsoft 365 configuration	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 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.