Service Description:
Endpoint Services – Palo Alto Networks

1. Service Overview

eSentire's Endpoint Services – Palo Alto Networks (the "**Service**") is a managed service providing endpoint-level visibility and control to support threat detection, investigation, and response leveraging the Palo Alto Network's Cortex XDR ("**Cortex Platform**") agent/license ("**Agent**") installed on servers and workstations with supported operating systems within Client's environment (the "**Client Environment**"). The eSentire Atlas Platform will capture available telemetry from in-scope Endpoints, enrich signals from available sources, analyze suspicious or threatening indicators, and support eSentire's Security Operations Center ("**SOC**") in delivering appropriate investigations and response. The eSentire SOC will perform all investigations within the Atlas Platform and not directly within the Client Environment and will support the Service on a 24x7x365 basis. All detections, analysis, investigation and other capabilities rely on the Application Programming Interface ("**API**") capabilities of Cortex Platform, and a continuous integration between the Client Environment and the Atlas Platform throughout the term of the Service. The Service is provided to Client in a managed only capacity, and for the number of Client-identified endpoints (each an "**Endpoint**"), as detailed on the Order Form, and as further described below.

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

eSentire is responsible for security event analysis, investigation to determine if a security event is true positive and warrants an escalation to Client, and potential response action (which may include Endpoint isolation). If an event is deemed Actionable, due to its behavior and the type of detection, Client will be notified with a corresponding Threat Case in eSentire's Insight Portal. Identified malicious activity will be contained (isolated) immediately by eSentire once identified. It is eSentire's responsibility to classify the criticality of the Alerts derived from individual events as part of the Service. The below tasks are included in the Service:

- Detection Monitoring, Analysis & Resolution including:
  - ensuring threats captured within the Cortex Platform are ingested into the Atlas Platform;
  - processing, enrichment and continuous tuning within the Atlas Platform of detection and asset data to identify, patterns, flag anomalous activity and reduce false positives; and
  - automatic writebacks to resolve ingested alerts.

- Investigation, Response and Notification including:
  - 24/7 human-led investigations of Cortex Platform security events, utilizing available tools and information;
  - Threat Cases, including recommendations, upon determination of an actionable security event, escalated alerts in accordance with policy for high and critical severity Threat Cases, a summary of which will be available on the Insight Portal for Client; and

- at SOC analyst discretion, immediate host isolation for all confirmed high or critical threats, interrupting any active attacks.

4. Response Actions for Identified Threats

eSentire will isolate potentially compromised machines and notify Client of the isolation via the agreed upon escalation procedure including evidence to support the action. The machines will remain in isolation until the threat has been remediated, or Client has accepted the risk and has requested the eSentire SOC to remove the host from isolation.

- All Agents are considered authorized for isolation unless otherwise communicated by Client.
- eSentire will escalate all alerts that require isolation to Client for visibility and active feedback on the Alert. Client commits to identifying critical assets that are NOT to be isolated unless Client has given written authorization.
- eSentire commits to isolating machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.

If Client has purchased other eSentire services, response may be implemented at multiple enforcement points, including but not limited to network, identity, and cloud (if applicable).

The eSentire SOC has the functionality to isolate machines from Client's network, the ability to use this function to protect the network. Isolated machines will lose all connectivity to all other devices or resources on the network. eSentire is limited to endpoint response actions through the API capabilities.

5. Incident Alerts and Reporting

eSentire ingests detections from the Cortex Platform. Activity that is determined to be an actionable threat will appear as a Threat Case in the eSentire Insight Portal. All high and critical threats as determined by eSentire will result in escalation(s), as necessary, based on agreed upon configured escalation procedures in the Insight Portal. All Threat Cases and observed detection signals are available within the Insight Portal for Client review. All reporting is delivered through the Insight Portal.

6. Deployment, Support & Configuration

eSentire is not responsible for the installation, troubleshooting or support of Agents. eSentire will only be responsible for providing support for eSentire tooling (Insight Portal, Atlas Platform).

In order for eSentire to deliver the Service, Client must install the Agent on all in scope endpoints. eSentire will provide documentation and support for integrating the Cortex Platform with the Atlas Platform.

6.1 Third Party License Requirements. The Service subscription is provided by eSentire in a managed only capacity ("**Managed Only**") and thus requires that Client secures appropriate endpoint licensing with Palo Alto Networks, Inc. ("**Product Publisher**"). See Order Form for details. Client must procure and maintain endpoint licensing ("**License**") with Product Publisher, during the entire Service Term, and coordinate proper licensing permissions with the Product Publisher to allow eSentire full connectivity to the Cortex Platform via API. Client must purchase the following applicable licenses in order to receive the Services:

- Palo Alto Networks Cortex XDR® Pro per Endpoint

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 to API or previously agreed upon configuration during the Service term 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 Service Term, Client must configure integration which enables eSentire staff and systems to investigate detections and execute response actions. Access to API secrets will be stored securely for system use only and not provided to eSentire employees; access will be audited.

7. Responsibilities

The responsibilities of each party are summarized below and in the responsibilities matrix which can be found in Appendix A.

7.1 Client Responsibilities: To maximize the effectiveness of the Service, Client is responsible for performing the obligations listed below. Client acknowledges that non-compliance with these obligations may interfere with eSentire's ability to deliver the Service in accordance with the applicable service levels agreed to and result in suspension of the Service. Client's obligations include:

- Ensuring any changes to access into the Client Environment are communicated to eSentire.
- Ensuring in-scope Client Endpoints have the Agent installed.
- Granting required API access to all data and systems required for the successful delivery of the Service.
- Ensuring that no firewall rules or other network blocking exists that would negatively impact communication by the Agent between Endpoints and the eSentire SOC.
- Validate and respond to the eSentire SOC for escalated Threat Cases; and
- Providing information and assistance during investigations conducted by eSentire when additional information is required.
- Ensuring that authorized contacts remain current, including approved access and all associated information.

8. Excluded Services

eSentire SOC will not implement, change, consult, or otherwise modify any setting with the Cortex Platform.

9. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on a supported Agent being installed on a licensed host in Client's Environment. The service levels contained on the MDR Landing Page are only applicable to hosts that are licensed as part of the Service and are actively communicating with the Service.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Security – Detection ingestion, monitoring, analysis	I	RAC
Security – Investigation for in-scope detections	-	RAC
Security – Notification and Escalation	I	RAC
Security – Host containment (isolation)	I	RA
Security – Detection resolution	-	RAC
System – Custom alerts, ad-hoc or post-alert investigations.	RA	-
System – Deploying endpoints	RA	-
System – Initial policy and environment configurations	RA	CI
System – Exclusions, detection or correlation rules, policy or host settings	RA	-
Health – Data ingestion and uptime monitoring	-	RA
Health – Managing sensor updates	RA	-
Health – Troubleshooting	C	RA*

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.

***Insight Portal only**