CNAPP Services – Tenable One

1. Service Overview

eSentire's Cloud-Native Application Protection Platform ("**CNAPP**") Services – Tenable One (the "**Service**") provides analysis, investigation and alerting based on threats identified in a client's cloud infrastructure. The Service can be provided to Client, in two different subscription types, a co-managed or managed only capacity, and for the number of Client identified Tenable One cloud resources (each a "**Cloud Resource**" or "**Resources**"), each as detailed on the Order Form, and as further described below. The Service leverages a cloud-native security technology powered by Tenable, Inc., (the "**Product Publisher**"), combined with the eSentire Atlas XDR platform (the "**Platform**") to detect, hunt, and investigate IT security threats.

2. Service Definitions

Any capitalized terms contained in this Service Description are as defined herein, or as defined on the Managed Detection and Response ("**MDR**") Services landing page (which can be found under Service Descriptions at: https://www.esentire.com/legal/documents?Service=MDR).

3. Service Capabilities

The Service collects information from all in scope Cloud Resources (collectively the "**Cloud Environment**") and monitors and analyzes the data for potential threats, unusual behavior, or other indicators of compromise. Suspicious activity detected is monitored by eSentire's Security Operations Center (SOC) on a 24x7x365 basis, initiating investigations and Client notification as required. The Service only supports Cloud Environments hosted within the following cloud infrastructure providers: Amazon Web Services ("**AWS**"), Google Cloud Platform ("**GCP**"), or Microsoft Azure. The Service includes the following:

3.1. Deployment. For a new deployment, eSentire will begin by collecting the required information for onboarding. Following data collection/validation, eSentire will provision access to the Platform, schedule a kickoff call with Client, and coordinate deployment for the number of in scope Cloud Resources. A Client contact with administrator access to the Client Cloud Environment is required to complete integration. eSentire will review the configuration worksheet with the Client during this initial deployment of the Service to confirm Client has included key areas of their Cloud Environment to maximize coverage and visibility. Following initial deployment, eSentire will provide ongoing hardening guidance as the Cloud Environment changes.

3.2. Incubation and Tuning Phases. After onboarding is completed, the Service will enter an incubation phase to fine tune the security Alerts. eSentire will work through the incubation and tuning phases with Client and work to move them into a production state. Until incubation and tuning are complete, events generated by the Cloud Environment will not be monitored by the eSentire SOC. Additional details for this phase are:

- **Phase 1 - Facilitate normalization of tooling**. The solution leverages both rule-based detection and anomaly-based detection; the latter needs time to baseline the Cloud Environment configured so that Alerts can be triggered if the baseline is exceeded.
- **Phase 2 - Prevention of Alert flooding after onboarding**. Depending upon the Client Cloud Environment configuration, after the initial onboarding, there is potential for a flood of Alerts. During the incubation and tuning phase, all alerting will be turned off, and neither Client nor the eSentire SOC will receive notifications. After initial onboarding, to optimize the Alerts based

on severity and relativity to Client, eSentire will manually review Alerts with Client. When this phase closes, Alerts will flow into the eSentire SOC.

- Phase 3 - Identification of false positives. eSentire will review the Service with the Client, including the eSentire Insight Portal, as well as any other applicable user interface ("UI"), and/or features. eSentire will also review the alerting, specifically the workflow for managing false positives. During this time, eSentire will provide Client an incubation phase report outlining all Alerts starting from Phase 1 and 2 above. After review, Client and eSentire will identify false positives contained in the report and agree on which Alerts should no longer be reported. eSentire will apply Client changes, and dismiss Alerts for the specific policy, on the specific Cloud Resource, ensuring that subsequent Alerts for that policy do not fire for the specific Cloud Resource. Of note, in the event a Cloud Resource is configured to be compliant with a policy but is subsequently modified to be non-compliant, an Alert may report again. Alerts from the incubation report which Client indicates are legitimate Alerts, will be passed on to the production service phase. The incubation report will include instructions to assist Client with remediation of these specific Alerts.

3.3 Service Production. Once the Service moves into the production phase, Client's Cloud Environment will be monitored in real-time, against policies contained within the eSentire solution, which define the criteria to send an Alert. eSentire's security operations center ("SOC"), will monitor the Cloud Environment 24x7x365, and will investigate and escalate identified critical severity events to Client. The Service tools will also be tuned to send automated notifications directly to Client for non-critical events that still require remediation. New threat detections (as applicable) are consistently being added to the Service and applied to the Client Cloud Environment, at no additional charge.

During production, eSentire will monitor Cloud Resources in the Cloud Environment for items such as:

- misconfiguration of Cloud Resources;
- threats present in VM and container-based workloads;
- communication to/from IP's on eSentire's proprietary threat blacklist;
- anomalies in typical user and entity behavior analytics;
- identity issues stemming from over-permissioning and / or unused accounts;
- threats discovered in audit logs;
- anomalous activity, including deviations from baseline behavior correlating changes to cloud API interactions, user privileges, group policies, access keys, and other configurations;
- critical service exposures;
- misconfigurations in cloud automation tooling;
- illicit activity attempting to leverage the Cloud Environment to mine cryptocurrencies such as Bitcoin and Ethereum;
- potential account hijacking attempts by monitoring for unusual login activities such as concurrent attempts, peculiar geo-locations, and unknown browsers or operating systems; and
- sensitive modifications to the Cloud Environment.

The Service policies are categorized into two classifications, and depending on the classification, eSentire will handle Alerts as follows:

- Alerts that are non-remediable by eSentire, investigable by eSentire. Such Alerts are mainly the result of policies which identify potentially malicious behavior. These Alerts will be identified as requiring investigation by the eSentire SOC, and eSentire will investigate and attempt to identify information related to such Alert such as (as applicable):
  - user account which made a potentially sensitive configuration change to a Cloud Resource;

- unusual user activity, which occurred at the same time as a potentially sensitive configuration change (identification of potential account compromise);
- identification of abnormal cloud resource utilization, as a result of malicious activity such as crypto mining;
- identification of false positive Alerts, filtering these out from Alerts reported to Client; and/or
- determine the threat actor, impacted Cloud Resources, and severity of threat.

Once the SOC has completed collecting information related to the Alert, if required, eSentire will send Client the Alert summary along with recommended remediation activities. This information will be sent to the Client via email and also posted to the Insight Portal for Client action. eSentire will escalate based on priority level, and defined actions, described in the MDR Service Level Objectives (link provided in section 3 below).

- Alerts that are non-remediable by eSentire, non-investigable by eSentire. Such Alerts are mainly mis-configuration items that will be sent to Client directly by eSentire, via email and also posted to the Insight Portal for Client action. These types of Alerts can only be corrected by Client as they require account configuration changes and/or review. The details included in the Alert sent to Client will include information on the policy criteria that caused the Alert, details on the violating Cloud Resource and specific steps to remediate the condition.

  The Alerts that are sent to Client, and identified for Client action on the Insight Portal, will remain unresolved until Client either performs the recommended remediation steps, or advises eSentire that the Alert was a false positive and should be suppressed.

During the Term of the Service, beginning once the Services are in full production, eSentire will schedule reviews with Client on a quarterly basis, to review the Cloud Environment. Ad hoc system generated reporting can be run on a predefined basis as requested by Client, and such reporting will cover automated events and be utilized by Client as needed to assist in system hardening in their Cloud Environment.

4. Subscription Types and Responsibilities

The Services are limited to eSentire's management of the following Tenable One capabilities:

- Tenable One Cloud – CNAPP (Standard or Enterprise licensing)

Client may request the Service to be provided by eSentire in one of the following ways: a) as a co-managed service with bundled licensing ("MSSP"), or b) in a managed only capacity ("Managed Only"). This selection will be detailed on the Order Form. Licensing requirements for each are detailed below:

4.1 MSSP Licensing Requirements. In this Service option, eSentire will procure all required licensing directly from Product Publisher, will be the licensee of record with Product Publisher, and provide management. As the Licensee, eSentire may grant Client enhanced access into eSentire's license instance, and if so granted, Client acknowledges and agrees that any changes made by Client in the licensed environment could negatively impact eSentire's ability to deliver the Services. Responsibilities of each Party is as described below for this subscription type:

Function	Client	eSentire
Grant required permissions within Client Cloud Resources, to enable the Service.	X	
Provide required information to support Service onboarding of Cloud Resources.		X
Complete configuration of Cloud Resources in the Cloud Environment as required.	X	

Function	Client	eSentire
Preparation of the incubation period report.		X
Return incubation period report to eSentire, complete with input on each Alert.	X	
Perform Service tuning based on input from Client via the incubation period report.		X
Perform monitoring of the Cloud Environment included in the Service, 24x7x365.		X
Provide detailed information regarding misconfiguration of Cloud Resources, enabling Client to perform required configuration changes within the Cloud Environment.		X
Where applicable, perform investigations into the cause of an Alert and provide investigation details to Client.		X
When requested, provide contextual information to aid in the investigation of an Alert.	X	
Answer Client questions about the Service, Alerts, configuration, or other items.		X
Provide Client with the opportunity to review Service status including items such as: • Alerts • Number of Alerts triggered for reporting period • License utilization • Cloud Resources under protection		X

4.2 Managed Only Licensing requirements. In this Service option, eSentire will manage Client's Product Publisher licensing, which has been procured by Client. Client must procure and maintain its cloud licensing ("License") with Product Publisher, during the entire Term of the Service, and coordinate proper licensing permissions with the Product Publisher to allow eSentire full administrative access and credentials into Client's License instance. Client must purchase the following applicable licenses, in order to receive Cloud Services in a Managed Only capacity from eSentire:

- Tenable One Cloud Standard or Enterprise entitlement

Responsibilities of each Party is as described below for this subscription type:

Function	Client	eSentire
Grant required permissions to allow re-parenting of Client Tenable One container under eSentire management.	X	
Grant required permissions within Cloud Resources, to enable the Service.	X	
Provide required information to support Service onboarding of Cloud Resources.		X
Complete configuration of Cloud Resources in the Cloud Environment as required.	X	
Preparation of the incubation period report.		X
Return incubation period report to eSentire, complete with input on each Alert.	X	
Performing Service tuning based on input from Client via the incubation period report.		X
Perform monitoring of the Cloud Environment included in the Service, 24x7x365.		X
Provide detailed information regarding misconfiguration of Cloud Resources, enabling Client to perform required configuration changes within the Cloud Environment.		X
Where applicable, perform investigations into the cause of an Alert and provide investigation details to the Client.		X
When requested, provide contextual information to aid in the investigation of an Alert.	X	
Answer Client questions about the Service, Alerts, configuration, or other items.		X
Provide Client with the opportunity to review Service status including items such as: • Alerts • Number of Alerts triggered for reporting period • License utilization • Cloud Resources under protection		X

5. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on an active Tenable One Cloud license from Product Publisher being integrated and in production in the Client Cloud Environment. The service levels contained on the Managed Detection and

Response ("MDR") Services general description found here (https://www.esentire.com/legal/documents), are only applicable to hosts that are licensed as part of the Service and are actively communicating with the Service.

eSentire will monitor the in-scope Client Tenable One Cloud Resources included in the Service, for potential threats and respond accordingly. When potentially malicious activity is identified, eSentire will perform an investigation and will respond according to the identified threat. Additional confirmation from the Client may be needed depending on the information available to the analyst at the time of the investigation.

6. Service Terms

Of note, Tenable One Cloud is a portion of the overall Tenable One Exposure Management Platform. For this Service, eSentire will only Manage, and in the case of MSSP support, Client only receives entitlement for Tenable One Cloud Licenses but can purchase additional Tenable One entitlement in an un-managed, entitlement-only model. Client may be able to leverage these capabilities, but they are not managed or monitored by eSentire, and require direct interaction with Tenable if support is required. A list of these optional additional licenses and modules include, but are not limited to:

- Tenable One - Just-in-Time (JIT) Cloud Permissions Management
- Tenable One – Identity Exposure
- Tenable One – Attack Surface Management
- Tenable One – OT Security