Cloud Services – Cloud Security Posture Management

1. Definitions

In addition to the capitalized terms defined elsewhere herein or in the Agreement, the following terms will have the meanings ascribed to them below:

"**Actionable**" means a Work Item analysis has concluded that an alert or containment action is required, based on criteria established by eSentire and reviewed with Client.

"**Alert**" means an event that eSentire will escalate to the Client. "Atlas Platform" means eSentire XDR platform which consolidates all data and drives workflow for all eSentire MDR services.

"**Insight Portal**" means the Client interface into the Atlas Platform, where eSentire provides Client summary and detailed reporting and/or event summaries.

"**Security Operations Center ("SOC")**" means the eSentire team which provides 24x7x365 monitoring and reaction to identify, investigate, and where appropriate prevent or contain, threats that are identified as potentially threatening to Client.

"**SOC Dashboard**" means the eSentire SOC interface into the Atlas Platform.

"**Threat Case**" means an Actionable Work Item, which results in a notification or action required.

"**Work Item**" means a collection of one or more events and alerts collected by the Atlas Platform requiring analysis by eSentire SOC Analysts.

2. Service Summary

eSentire's Cloud Services - Cloud Security Posture Management ("**CSPM**" or the "**Service**") provides analysis, investigation and alerting based on threats identified in a client's cloud infrastructure. The Service can be provided to a Client through two different subscription types, a fully managed or managed only capacity, and for the number of Client identified cloud resources ("**Cloud Resources**"), each as detailed on the Order Form, and as further described below. The Service leverages a cloud-native security technology powered by Lacework, Inc. ("**Product Publisher**"), combined with the eSentire Atlas XDR platform to detect, hunt, and investigate IT security threats. The Service collects information from all in scope Client Cloud Resources (collectively the "**Client Environment**") and monitors and analyzes that data for potential threats, unusual behavior, or other indicators of compromise. Suspicious activity detected is monitored by eSentire's 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:

2.1 Deployment

For a new deployment, eSentire will begin by scheduling a kickoff call with Client to collect required information for onboarding. Post data collection/validation, eSentire will provision access to platform and coordinate deployment requirements for the number of in scope Client 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 Client's Cloud Environment changes.

2.2 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 machine learning assets. 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's 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.

2.2 Service Production

Once the Service moves into the production phase, Client's 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 Clients Cloud Environment, at no additional charge.

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

- misconfiguration of Cloud Resources;
- communication to/from IP's on eSentire's proprietary threat blacklist;
- anomalies in typical user and entity behavior analytics ("UEBA");
- 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;
- illicit activity attempting to leverage Client's 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 Client's 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 system 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 Client cloud resource, 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 the Client of their Service environment on a quarterly basis. 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.

3. Subscription Types and Responsibilities

The Client can subscribe to two different Service subscriptions: the Cloud Services - Cloud Security Posture Management subscription and the Cloud Services - Cloud Security Posture Management - Managed-Only subscription, differences are described below:

3.1 Cloud Services - Cloud Security Posture Management subscription, is the fully managed solution. Services are as described above, and responsibilities of each Party is as described below:

Task	Client responsibility	eSentire responsibility
Grant required permissions within Client vCPU's (cloud environment/s), to enable the Service.	X	
Provide required information to support onboarding of Cloud Resources to the Service.		X
Complete configuration of Cloud Resources in the Client Cloud Environment as required by the Service.	X	
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 • Client cloud accounts under protection		X

3.2 Cloud Services - Cloud Security Posture Management subscription – Managed Only is a version of the Service described above, however, eSentire will leverage Client owned Product Publisher licensing which will be integrated with the eSentire's platform in order for eSentire to provide the Service. For this subscription type, Client must procure and maintain an Enterprise Agentless Package (the "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 the Client's License instance. Client will retain ownership of the License, and will continue to have all access to utilize their License, however, Client acknowledges and agrees that any changes made by the Client in the Licensed environment could negatively impact eSentire's ability to deliver the Services, and any changes made by Client during the term of this Service should be reviewed with eSentire, otherwise eSentire shall be released from any and all obligations to effectively provide the Services as contemplated herein. Responsibilities of each Party is as described below for this subscription type:

Task	Client responsibility	eSentire responsibility
Grant required permissions within Client vCPU's (cloud environment/s), to enable the Service.	X	
Grant required permissions within Client Cloud Resources, to enable the Service.		X
Provide required information to support onboarding of Cloud Resources to the Service.		X
Complete configuration of Cloud Resources in the Client Cloud Environment as required by the Service.	X	
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

Task	Client responsibility	eSentire responsibility
Provide Client with the opportunity to review Service status including items such as: • Alerts • Number of Alerts triggered for reporting period • License utilization • Client cloud accounts under protection		X

General Client responsibilities for all MDR Services are listed below. Client must comply with these Client responsibilities in order for eSentire to meet its obligations and deliver the Services. Client Responsibilities are as follows:

- Client is responsible for all Client provided third-party equipment, software services, support, or vendors not under the control of eSentire.
- Client should respond to Alerts and inquiries from eSentire in a timely fashion.
- Client should identify prior issues with Client's network to the eSentire team prior to Services commencing (including any incidents, problems, errors, or other events subject to an open support ticket from a legacy or other third-party service provider).
- Client is responsible for implementing any recommendations or remediation advice provided by eSentire related to Client incidents, however, Client's decision to not implement any remediation recommendations may adversely impact eSentire's ability to deliver the Services.
- Client should communicate and coordinate any required changes to the Client network or other component required for the MDR services to be delivered, prior to making any changes.

4. Service Level Objectives

4.1 eSentire measures a set of internal objectives that apply to all eSentire MDR Services. For each SLO, a minimum of 20 Threat Cases must be processed during the month for the SLO to apply. The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on an active Enterprise Agentless Package license from Product Publisher being integrated and in production in Client's Cloud Environment. These eSentire standards are further described below and are only applicable to hosts that are licensed as part of the Service and are actively communicating with the Service.

4.2 **Time to Engage ("TTE") – Work Item – SLO target 60 minutes.** The Service Level Indicator (SLI) time starts when a Work Item is created in the SOC Dashboard and ends when an eSentire SOC Analyst changes the state of the Work Item in the SOC Dashboard to "under review". A Work Item is marked "under review" in the SOC Dashboard, when analysis of the Work Item by an eSentire SOC Analyst has commenced. The analysis includes collecting evidence and creating assessment notes against the Work Item. The outcome or duration of the analysis does not impact the TTE SLO target.

4.3 **Time to Respond ("TTR") – Actionable Work Item – SLO Target based on Priority Level (Table 1).** As a result of the Work Item analysis described above, eSentire will determine if a Work Item is Actionable, and if so, will create a Threat Case. eSentire will then notify Client via the Insight Portal, and email, of any Threat Case. The SLI starts when a Threat Case has been created in the SOC Dashboard and ends when an eSentire SOC Analyst notifies the Client and provides the Client defined response remediation actions.

Table 1.

Priority Level	TTR SLO Target*
P1	10 minutes
P2	20 minutes
P3	40 minutes
P4	60 minutes
*SLO Target is measured as a monthly aggregate by priority level, taking into consideration all actionable Threat Cases from the previous month.	

The Priority Levels listed above are defined below in Table 2.

Priority Level	Description
P4 (Low)	Minor activity recorded but not alerted, and the presence of likely unwanted activity - for example, adware.
P3 (Medium)	Suspicious activity that might not be deemed malicious by itself, and malicious activity not known to be targeted.
P2 (High)	Malware event, tactics, techniques, and procedure events, or events indicating targeted attack with potential for widespread impact.
P1 (Critical)	Malware infection(s), virus infection(s), and lateral movement, or indications of targeted attack with a high potential to cause grave damage to critical assets.

Of note: eSentire objectives listed above may be impacted by short periods due to scheduled maintenance where updates, patches, are installed and configured (i.e., maintenance windows), or when hardware deployment or replacements are required.