eSENTIRE

Service Description: MDR for Cloud Services – Cloud Security Posture Management

1. Service Summary

eSentire's MDR for Cloud Services - Cloud Security Posture Management (the "**Service**") provides analysis, investigation and alerting based on threats identified in Client's cloud infrastructure. The Service, delivered by the eSentire's security operations center (the "**eSentire SOC**"), is a fully managed Service leveraging 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. This Service supports the number of Client identified virtual centralized processing unit(s) ("**vCPU(s)**") that represent cloud resources ("Cloud Resources") in the Client environment each as detailed on the Order Form, and as further described below. The Service only supports Cloud Environments hosted within the following cloud infrastructure providers: Amazon Web Services ("AWS"), Google Cloud Platform ("GCP"), or Microsoft Azure.

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 vCPU's within the applicable 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 Security Operations Center ("**SOC**") on a 24x7x365 basis, initiating investigations and Client notification as required. Support includes the following:

3.1 Description

eSentire will leverage Client's licensing to obtain alerts, events, misconfigurations, and findings which will enable the eSentire SOC to identify and investigate potential threats or suspicious activity within Client's environment. The Service is supported by eSentire's SOC on a 24x7x365 basis and will result in human-led investigations of suspicious activity and alerting.

During the Service Term, eSentire will provide threat detection, analysis, investigation, escalation, and response. In addition, eSentire is responsible for security event analysis and investigation to determine if a security event is considered a legitimate threat and warrants an escalation to Client and a potential response action. If an event is deemed Actionable, due to its behavior and the type of detection, it will be escalated to Client as an Alert. The SOC will perform event triage, assign criticality, and include supporting information and analysis within the Alert and, if necessary, initiate escalation to Client. Malicious or suspicious activity will be identified and resolved by Client with the assistance of eSentire, utilizing response playbooks. Client will receive access to the eSentire Insight Portal, which will consolidate threat alert reports and investigation details from eSentire SOC analysts. Threat Cases will be visible to Client on their Insight Portal dashboard; however, it is eSentire's responsibility to classify

the criticality of Alerts derived from individual events. The following support is included as part of the Services:

- Onboarding:
    - Integration of Client environment with eSentire's backend for monitoring and management services.

- Incubation and Tuning Phases:
    - Phase 1 – Facilitate normalization of the machine learning process
    - Phase 2 – Prevention of alert flooding after onboarding
    - Phase 3 – Identification of false positives

- Service Production:
    - Monitoring of Client 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 Cloud Environment.

    - Alerting of events that are non-remediable by eSentire, and 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 Client via email and also posted to the Insight Portal for Client action. eSentire will escalate based on priority level, and defined actions.

- Alerting of events that are non-remediable by eSentire, and 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 Service Term, beginning once the Services are in full production, eSentire will schedule reviews with 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.

3.2 Response Actions

At the conclusion of a review of a Work Item, eSentire will classify the item as either a threat or non-threat. The classification of an event as a "threat" will generate a Threat Case and be further evaluated and marked by severity level (Low, Moderate, High, or Critical). A list of classifications, severity levels, and the associated actions/alerts and follow up expected is as defined in table 1 below:

Table 1:

Classification	Severity Level	Action	Alert	Disposition	Follow Up
Threat	Low/Medium	No Client Action Needed	No Alert	True Positive	Guided remediation actions via alerting and UI.
		Client Action Needed	Alert with description and relevant data	True Positive	Underlying telemetry and associated data will be available Clients Insight Portal dashboard. Guided remediation actions via alerting and UI.
	High/Critical	Client Action Needed	Alert with description and relevant data Escalation procedure (email/phone call with acknowledgement expected)	True Positive	Underlying telemetry and associated data will be available on Insight Portal Guided remediation actions via eSentire SOC-actioned runbooks.
Non-Threat (False Positive / Benign)	N/A	No Client Action Needed	No Alert	False Positive	Recurrences of identical activity will be logged as ignored

3.3 Remediation Actions

eSentire can assist Client with remediation activities for high or critical threats from active hands-on keyboard attackers, in the Client Environment, upon alerting Client. The types of remediation support actions that can be provided by eSentire, in coordination with Client are as follows:

- Guided remediation steps for both UI and CLI workflows.
- SOC-actioned runbooks to mitigate risk in the Client Environment.

4. Subscription Options

The Service contains one service delivery option which is the fully managed Cloud Services for Cloud Security Posture Management. eSentire will maintain the licensing required from Lacework to provide the Service.

4.1 Usage

eSentire Cloud Services are measured by a count of vCPUs or "virtual CPUs". This value is a processor core count of all machines and compute in Clients Cloud Environment. The Lacework platform measures max daily usage over a month, averages the daily values, and takes the 95th percentile of this average as the monthly usage. This measurement style allows for the natural ebb and flow of cloud assets. If Clients environment is not leveraging vCPU as a unit of measure eSentire will work with Lacework to obtain vCPU usage figures, or work with Client and Lacework to transition Client environment to vCPU measurement.

eSentire leverages the normalized Lacework monthly usage value described above. eSentire Cloud Services offer a "grace period" of 10% or 20 vCPUs – whichever value is reached first. If Clients environment exceeds this threshold for two or more months eSentire will initiate a discussion about rightsizing either the deployment or the contract.

4. Deployment

Client will receive onboarding documentation and assistance from eSentire, where needed, to deploy the solution to their Cloud Environment. There are three main phases to the deployment process: cloud account integration, normalization and tuning.

During the cloud account integration phase, eSentire will schedule time with the client's technical implementor to deploy the solution to one or more of the clients in-scope cloud accounts. Once accounts are successfully onboarded, the solution enters a three-day normalization phase where cloud environment interactions are observed. Following the normalization phase, eSentire will schedule a meeting where a UI walkthrough and training are delivered as well as the start of the tuning process.

5. Tuning and Configuration

eSentire is responsible for configuring and tuning the Service capabilities leveraging Client's Licensing. 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's 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 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 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 that 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.

6. Service Level Objectives

The ability for the eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on Licensing from Product Publisher being integrated and in production in Client's applicable Cloud Environment. The service levels contained on the Managed Detection and Response ("MDR") Services general description found here: https://www.esentire.com/legal/documents?Service=MDR, are only applicable to Cloud Resources that are licensed as part of the Service and are actively communicating with the Service.

eSentire will monitor the in-scope Client 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.

7. Responsibilities

Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the Service is dependent upon Client's compliance with the obligations hereunder, including meeting the service levels above. In the event Client fails to perform its obligations herein, in the time and manner specified or contemplated below, or should any obligation set out herein with respect to the Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

Non-compliance with the responsibilities and obligations may result in suspension of the Service or suspension of service levels. Below are a list of responsibilities, and a responsibilities matrix is located in Appendix A:

8.1 Client Responsibilities

- Onboarding and Maintenance including:
  - Integrate the solution with one or more cloud environments to provide the service access to assess Client assets;
  - Deploy agents to container or VM workloads to enable runtime visibility;
  - Grant required permissions to integrate eSentire SSO with Client License; and
  - Ensure that user account and API key sets leveraged for eSentire service delivery remain intact and unmodified.

- Tuning, Configuration and User Management including:
  - Return incubation report to eSentire, complete with input on each Alert; and
  - When requested, provide contextual information to aid in the investigation of an Alert.

8.2 eSentire Responsibilities:

- Detection Monitoring, Analysis & Resolution including:
  - Ensure all detections from Product Publisher are ingested into eSentire's XDR platform;
  - Provide required information to support onboarding of Client Environment to the Service; and
  - Perform monitoring of the Cloud Environment included in the Service, 24/7/365.

- Investigation, Guided Remediation and Notification including:
  - Preparation of the incubation period report used to implement tuning;
  - Perform Service tuning based on input from Client via the incubation period report;
  - Provide detailed information regarding misconfiguration of Cloud Resources, enabling Client to perform required configuration changes within the Cloud Environment; and
  - Where applicable, perform investigations into the cause of an Alert and provide investigation details to Client.

- Policy and Environment Configurations and Consulting including:
  - Introductory walkthrough and professional support;
  - Answer Client questions about the Service, Alerts, configuration, or other items;
  - Post-deployment policy tuning and support; and
  - Provide Client with the opportunity to review Service status including items such as:
    - Alerts
    - Number of Alert triggered for reporting period
    - Client cloud accounts under protection

8. Service Terms.

9.1 Exclusions

The Services do not provide Emergency Incident Response including but not limited to deep Forensic Investigation, recovery support, Litigation Support, Disaster Recovery and Business Continuity Planning, and/or the quantification of the Business Impact, with respect to all Client assets, whether currently under embedded Incident Response or not. Additionally, the Services are limited to eSentire's management of the following Lacework capabilities:

- CSPM – monitoring and alerting of misconfigurations.
- UEBA – monitoring and alerting on anomalies found in cloud platform API logs.

Of note, there are additional capabilities often included with licensing provided by Lacework which are not managed by eSentire as part of the Services. Client may be able to leverage these capabilities, but they are not managed or monitored by eSentire, and require direct interaction with Lacework if support is required. A list of non-managed capabilities include, but are not limited to:

- Agentless side scanning in AWS and GCP
- Container image evaluation via repository, registry, or CI/CD
- CI/CD integration for container vulnerability assessment during build process

Appendix A: Responsibilities Matrix

Task	Client responsibility	eSentire responsibility
Integrate the solution with one or more cloud environment to provide the service access to assess client assets.	X	
eSentire to assist customer with deployment of cloud accounts.		X
Ensure that user account and API keyset used for eSentire service delivery remain intact and unmodified.	X	
Grant required permissions within Client vCPU's (cloud environment/s), to enable the Service.	X	
Provide required information to support onboarding of vCPU's to the Service.		X
Complete configuration of cloud resources in the Client Cloud Environment as required by the Service.	X	
Ensure all detections from Product Publisher are ingested into eSentire's XDR platform.		X
Provide required information to support onboarding of Cloud Resources to the Service.		X
Perform monitoring of the Cloud Environment included in the Service, 24x7x365.		X
Preparation of the incubation period report used to implement tuning.		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
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	
Introductory walkthrough and professional support.		X
Answer Client questions about the Service, Alerts, configuration, or other items.		X
Post-deployment policy tuning.		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