eSENTIRE

Service Description:
Log Services – Sumo Logic– Managed Only

1. Service Overview

eSentire's Managed Detection Response for Log Service – Sumo Logic – Managed Only is a managed service providing centralized log management with analysis, investigation and alerting based on Log Data leveraging Client owned and managed SIEM platform (the "**Client SIEM**") integrated with the eSentire Atlas XDR platform to detect, hunt, and investigate IT security threats (the "**Services**" or "**Managed-Only Log Services**"). The Client SIEM must be licensed from Sumo Logic, Inc. (the "**Product Publisher**") and implementation and tuning are required to enable integration with the Atlas platform.

The Managed-Only Log Services collect information from assets in Client network and cloud resources (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. A subset of data collected, and usage of the Client SIEM is designated for use for the Managed-Only Log Services (the "**Service Scope**"). Use of the Client SIEM outside of Service Scope is the responsibility of Client.

The Service is scoped/sold using Client provided log data ingestion totals, and the quantity is detailed on the Order Form using a unit measure of GB/Day. Should Client's ingestion usage as a daily average exceed 10% of the daily ingestion quota (measured on an average over one calendar month), notwithstanding any security event (the "**Overage**"), then Client will either (i) take steps to reduce its usage within 30 Days of such Overage, or (ii) move to the next ingestion level, and associated fees, to accommodate its usage for the remainder of the Term.

2. Service Definitions

In addition to the below, 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.

- "**Log Data**" is generated by Client systems and applications for the purpose of recording activity and conditions defined by each specific system and application. Log data is stored in an eSentire-licensed log management platform. The log generating systems are not provided, managed, or supported by eSentire.

3. Service Capabilities

3.1 Log Collection. Managed-Only Log Services accept Log Data from a variety of sources, including syslog, Windows event log (WMI), flat file, and cloud applications and infrastructure. The set of supported log sources is under continuous improvement. Unsupported and/or custom log sources may be nominated for collection; creating support will be evaluated and scheduled on a per-case basis. Alternately, Client may engage with the Product Publisher to facilitate supporting log sources. Logs will be transported from Client Environment to the Client SIEM platform by one of multiple methods as appropriate:

- secure transport direct to the Client SIEM platform via https or secure syslog;

- centralized collection in Client Environment using eSentire-provided collector software installed on Client-managed hosts;
- agent software installed on each monitored host; or
- other collection capabilities as defined by the Client SIEM.

3.2 Log Retention. Client data must be retained for 365 days. All collected data is stored in the Client SIEM. All alerts and metadata transported to eSentire's Atlas platform for analysis and review are stored in eSentire's cloud environment and are subject to administrative, physical, and technical safeguards. Upon termination or expiration of the Service, all collected data in the eSentire environment is securely destroyed or allowed to expire per standard policies.

3.3 Data Access and Reporting. The eSentire Insight Portal is the primary Client interface to access the outcomes of the Service. Insight portal provides an overview of Client's security posture and details on escalated alerts, ongoing investigations, service status and other information. For more detailed interaction with collected Log Data, Client retains direct access to the Client SIEM. This access includes self-service access to:

- ad-hoc searches;
- scheduled searches;
- real-time and scheduled search alerting (direct to Client);
- live dashboards; and
- API queries.

3.4 Alerting Escalation. Collected Log Data may be subject to analysis by eSentire correlation rules, a continuously updating set of logic and intelligence for the purpose of creating alerts for SOC review. The set of eSentire rules will include industry best practices, the results of internal research and intelligence, and suggestions made by other customers. Client may also create additional alerting from log events for direct notification to Client personnel. Monitoring of these alerts are the responsibility of Client. eSentire reserves the right to limit custom alerting configuration to security uses cases and the log sources in scope of the Managed-Log Services. Out of scope activity is the responsibility of Client and Client's Product Publisher.

3.5 SOC Alerting and Investigation. Alerts for potential threats are processed, enriched, and delivered to eSentire's SOC. eSentire uses the data from this Service within the broader MDR Services (sold separately), including other signals, threat intelligence, and investigations to determine the nature and severity of the threat and will notify Client according to defined escalation procedures and service levels. When Client has purchased and implemented other eSentire MDR services, the eSentire SOC may execute proactive response actions.

4. Subscription Types

4.1 Subscriptions. The only Subscription type covered by this service description is Log Standard, as described herein, and Services are delivered to Client by eSentire in a managed only capacity ("**Managed Only**"). This selection will be detailed on the Order Form. In the delivery of the Services, eSentire will manage Client's SumoLogic licensing, which has been procured by Client. Client must procure and maintain its licensing ("**License**") with the Product Publisher, during the entire Service Term, and coordinate proper licensing permissions with 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 the Services in a Managed Only capacity from eSentire:

- Sumo Logic Enterprise Suite

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 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. Throughout the Service Term, Client must provide and eSentire must maintain administrator or equivalent access which enables eSentire staff and systems to execute the tasks included in this service description. Access will only be provided to select, authorized eSentire employees and will be audited.

5. Deployment

Log data is explicitly nominated to be in Service Scope by source host or application. Scoping of the service is performed prior to execution of an Order Form, to determine the contracted managed scope and quota, expressed in GB per Day. The eSentire professional services (referred to as "The Blue Team") in collaboration with Client will complete an inventory of all in-scope logging and auditing devices, applications and cloud services and assist with configuring data acquisition. The Blue Team is comprised of experienced security industry practitioners, trained, and certified in multiple SIEM technologies and cybersecurity and engineering disciplines. Log data to collect will be prioritized by data types providing maximum service effectiveness. The Blue Team's services are required for planning, strategy, and integration of the Client SIEM into the Managed-Only Log service. The Client SIEM will be evaluated for general health, availability and current configuration and a project plan for integration will be created in collaboration with Client. The Client SIEM will be configured with eSentire-developed content such as rules, Runbooks, searches, and dashboards for the purposes of facilitating the Services

The Managed-Only Log Services onboarding service time allocation varies by size of the Client's SIEM instance. Deployments generally require two to three weeks of calendar time. It is assumed the Client SIEM is operational prior to eSentire's management overlay." Actual project plan will be set during kick-off. Hours are approximate and must be used in the agreed-upon project timeline. See the Blue Team Service Description for more details. See the "Blue Team Service Description" for more details, which can be found on the following webpage under "Additional Offerings": https://www.esentire.com/legal/documents for more details ("Blue Team Description"). Table 1 below shows approximate deployment times depending on Clients ingest quota.

Table 1:

Ingest Quota	Approximate Deployment Time
1-5 GB/Day	10 hours
6-20 GB/Day	10 hours
21-99 GB/Day	20 hours
100-249 GB/Day	30 hours
>250 GB/Day	40 hours

Additional professional services time is available for a fee.

6. Maintenance and Support

eSentire shall provide support to Client for both security and system issues related to data within Services Scope. eSentire will assume administrative control of the Client SIEM in a co-managed model, sharing this responsibility with Client. All SIEM-specific related issues or issues for data outside Services Scope are the responsibility of Client and their SIEM vendor. The Managed-Only Log Services includes additional Blue Team availability for ongoing maintenance and enhancements beyond standard support and monitoring. See the Blue Team Description for more details. Log Services include ongoing maintenance support and Table 2 below outlines the support time limits based on the Clients ingest quotas.

Table 2

Ingest Quota	Support time
1-5 GB/Day	1 hour / month
6-20 GB/Day	1 hour / month
21-99 GB/Day	2 hours / month
100-249 GB/Day	4 hours / month
>250 GB/Day	8 hours / month

6.1 Included Activities

- Define Service scope, data collection requirements, retention policies
- Prioritize log sources by security/threat detection value
- Identify data sources and types for inclusion in the Services
- Identify non-standard sources or collection methods
- Outline available Runbooks (relevant to in scope sources)
- Outline Runbook roadmap and processes
- Collect 'custom' requests
- Define and implement initial scope of standard runbooks, auto-notifications, dashboard charts and saved searches
- Ongoing operational tasks:
  - add new standard content created by eSentire, apply updates to existing content
  - adjust thresholds for existing content
  - update allowlists, denylists, lookup tables and other reference data
  - update contact info/escalation procedures

6.2 Available post-deployment for additional fees

- Connect new type of data source
- Deploy new collector nodes, move collection transport in any way
- New charts or custom rules for a new type of data source
- Onboard acquired company or accommodate a major infrastructure overhaul
- New or significant change to customer security team, change in escalation procedures, change in working relationship

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 below. 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.

7.1 Client is responsible for:

- working with eSentire staff to enumerate and define in scope log sources and the required service level for each;
- ensuring changes to logging applications or their collection is communicated to eSentire;
- designating a project coordinator to work directly with and serve as the primary Client contact with eSentire for the Service term;
- choice of equipment, systems, software, cloud service providers, and online content; and
- providing the necessary resources, information, documentation and access to personnel, equipment, and systems, as reasonably required by eSentire, to allow eSentire to perform the Services.

8. Service Level Objectives

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

eSentire will monitor 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 Client may be needed depending on the information available to the analyst at the time of the investigation.

9. Service Turndown

Upon termination or expiration Service, eSentire will sever all connections to the Client SIEM and remove all access by eSentire employees. As part of turn-down all eSentire proprietary content added for Service delivery is removed. Any content developed in conjunction with the Client will remain.

Upon termination of the Services, all collected data in the eSentire Atlas XDR environment is securely destroyed or allowed to expire per standard policies while remaining under standard safeguards.

10. Service Terms.

10.1 Exclusions: The Service excludes the design, creation, maintenance, and enforcement of any security policies for Client.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Threat Detection - content creation, evolution, and management (standard library)	I	RA
Threat Detection - deploy content	I	RA
Threat Detection - content tuning	A	R
Threat Detection- custom use cases	RA	R - limited
Threat Detection - submit new use cases to eSentire content teams	I	RA
Threat Detection - Alert monitoring, analysis	I	RA
Threat Detection - Notification	I	RA
Threat Detection - Resolution	RA	RA
Threat Detection - Threat Intel integration	I	RA
System – SIEM setup	R	I
System - Collector	R	I
System - Usage (data quota) management	RA	C
System - Data ingest tuning	RA	C
System - End user training	RA	C
System - User account management	RA	RA
System - Operations and metrics use cases	RA	-
System - Compliance use cases	RA	-
System - Observability use cases	RA	-
System - ad hoc search, report, and dashboards (outside standard library)	RA	R - limited
Health - SIEM uptime & patching	R	I
Health - Collector uptime & patching	R	I
Health - General troubleshooting	RA	C
Data - Source device logging config	RA	C
Data - Resolving collection issues	RA	C
Data - Monitoring collection (in scope data)	I	RA
Data - Notification of lack of collection	A	R
Data - Source Category definition	RA	C
Data - Verify data correctness (for in scope data)	RA	C

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.