eSENTIRE

Service Description:
Log Services – Sumo Logic

1. Service Overview

eSentire's Managed Detection Response for Log Services – Sumo Logic (the "**Log Service**") is a managed service providing centralized log management with analysis, investigation and alerting based on log data. The Service leverages a cloud-native SIEM platform from Sumo Logic, Inc. (the "**Product Publisher**") combined with the eSentire Atlas XDR platform to detect, hunt, and investigate IT security threats. The Service collects 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.

The Log 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. The Service accepts 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. Logs will be transported from Client Environment to the eSentire's SumoLogic platform by one of three methods as appropriate:

- secure transport direct to eSentire's SumoLogic platform via https or secure syslog;
- centralized collection in Client Environment using eSentire-provided collector software installed on Client-managed hosts; and/or
- agent software installed on each monitored host.

3.2. Log Retention. Client data is retained during the Service for 365 Days. All collected data is stored in the Product Publisher's cloud environment; all alerts and metadata 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 is securely destroyed.

Client-controlled copies of collected Log Data are available by configuring the Service to forward a copy of all collected data to an AWS S3 bucket that is provisioned, managed, and controlled by Client ("**Data Forwarding**"). This feature cannot be applied retroactively.

3.3. Data Access and Reporting. The eSentire Insight Portal is the primary Client interface to access the outcomes of the Service. The 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 can be provided with direct access to the eSentire's SumoLogic platform. 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.

Large volumes of data are collected for a variety of use cases during the Service. Many use cases require continuous monitoring while others may require less frequent real-time analysis. Logs from development, test, pre-production systems, debug/trace logs, and/or specific data excluded from security scope still require collection to be reviewed in digest and support investigation. The Service will direct up to 40% of this low-touch data to alternate storage tiers within the SIEM platform as appropriate to ensure maximum service effectiveness. This data will remain available for ad-hoc searches and API queries and will be in scope for all investigations and threat hunts. The nomination of low-touch logs will be done in collaboration with Client based on the specific set of log sources in scope and based on eSentire's log scoping best practices. eSentire will support Client through access to self-directed training, documentation as well as direct support via email and telephone.

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 eSentire 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 Service.

3.5. SOC Alerting and Investigation. Alerts for potential threats are processed, enriched, and delivered to eSentire's SOC. eSentire uses the data from the 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. Client can subscribe to two Service types ("**Subscription**"), which will be stated on the Order Form, and are further described below:

4.1.1. Log Services – Standard Subscription. This is the standard support model, and includes the items described in section 3 above.

4.1.2. Log Services – Essential Subscription. When ordered by Client, Log Services – Essential, allows a selected subset of data collected for the Service to be designated for a storage-only service option. Data nominated for this service option is collected, stored and available for on-demand searching and threat hunting, however, the data is not system analyzed for the purposes of real-time alerting. Data subject to this Service option is generally data deemed out of scope for security or MDR services or data or systems collected for compliance purposes only. Determination of eligibility and selection is mutually defined by Client and eSentire using industry best practices and specific Client needs. Data subscribed to Log Essentials is not eligible for Data Forwarding.

4.1.3. Additional Data Retention. Additional online storage for log data is available in six-month increments up to two additional years (1095 days). Any additional storage ordered, will be detailed on the Order Form with the associated additional fees.

4.2. Third Party License Requirements. For the Services described in this Service Description, eSentire will procure all required licensing directly from Sumo Logic, Inc. ("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.

For any Service option detailed above, 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 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.

5. Deployment

eSentire will provide and support one cloud-hosted Log instance (an "Log Instance" or "Tenant"). This is a hosted instance of Product Publisher's software used for the purposes of providing log collection, storage, querying, data analytics that is a component of the larger Service. eSentire will also provide support related to the log collectors which will include:

- Installing. eSentire will provide installation software, supporting documentation, guides, and support for installation of on-premise log collectors ("Log Collector" or "Collector(s)").
- Deployment. Collectors will be installed by Client with eSentire's direct assistance during the onboarding period. The Client will be responsible for the ongoing management of the Collectors (see Appendix A) and for ensuring that the Collectors are not prevented from communicating with the applicable Log instance.

Log data is explicitly nominated for the Service by source host or application. Scoping of the Service is performed prior to execution of an Order Form, to determine the contracted ingest 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. Client is responsible for configuration of the logging sources and ensuring network transport to the Log Collector.

The Service onboarding service time allocation varies by size of Client's SIEM instance. Deployments generally require four to six weeks of calendar time. 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, 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

6. Maintenance and Support

eSentire shall provide support to Client for both security and system issues related to the Service. The Service 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	2 hour / month
21-99 GB/Day	4 hours / month
100-249 GB/Day	6 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 non-standard sources or collection methods
- Outline available Runbooks (relevant to in scope sources)
- Outline Runbook roadmap and identify Runbooks to add in maintenance
- 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;
- granting access to required data and systems to configure log collection for the Service including necessary licenses, permissions, consents, and tokens to enable eSentire to access Client's network, servers, and cloud service providers in order to provide the Service;
- 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 term of the Service;
- installing of on-premise log collectors to enable log collection for sources within Client Environment;
- ensuring no firewall rules or other network blocking exists that would prevent the communication from log collectors to the log server
- Client's 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 Service.

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 expiration of the Service Term, Client's Log Service platform instances will be destroyed as part of offboarding processes, removing all collected log data and all configurations. If Client wishes to retain collected log data for archive purposes or to move to an alternate provider Client is required to proactively configure data forwarding to client-controlled AWS S3. Retroactive bulk export of data is not available. Client also has the option to take over ownership of the log platform, and if Client wishes to do so they must initiate a relationship with Sumo Logic and secure licensing sufficient to carry the instance. Upon confirmation of appropriate relationship and licensing, upon Service expiration, eSentire will co-ordinate with the Client contact and Sumo Logic to remove all eSentire-proprietary configuration, disable all eSentire users, make Client contact the instance owner, and sever the instance from the eSentire parent instance.

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.

10.2. Product Publisher - Flow Down Provisions: Unless other terms have been negotiated and attached or referenced on the Client's Order Form, the following terms are required by Sumo Logic, Inc. ("**Product Publisher**") to be agreed to by Client, for the MSSP Services described herein. eSentire owns the licensing directly with the Product Publisher, and as an MSSP eSentire has an obligation to ensure Client agrees to flow down provisions applicable to the licensing. Defined terms this section are solely for the purposes of this section. In such case, Client agrees to the following Product Publisher required flow down provisions:

10.2.1. Client will not, directly or indirectly, and will not permit or enable any third party to: (i) input, upload, transmit or otherwise provide to or through the software any information or materials that are unlawful or injurious or contain, transmit or activate any malicious code; (ii) damage, destroy, disrupt, disable, impair, interfere with or otherwise impede in any manner the software, in whole or in part; (iii) access or use the software for purposes of competitive analysis of the Service, the development, provision or use of a competing software service or product or any other purpose that is to the Product Publisher's detriment or commercial disadvantage; or (iv) use the software other than in accordance with this Service Description.

10.2.2. Client hereby grants to the Product Publisher: (A) a non-exclusive, royalty-free, worldwide, transferrable, sub-licensable license and right to use, copy, modify, create derivative works of, and disclose data, information or other material provided, uploaded or submitted by Client in the course of receiving the Service for internal purposes and for purposes of providing the Service; and (B) a non-exclusive, irrevocable, perpetual, royalty-free, full paid-up, worldwide, transferable, sub-licensable license and right to generate anonymized data for any business purposes (including, without limitation, for purposes of eSentire or its Product Publisher, improving, testing, operating, promoting and marketing products and services). Client shall retain all right, title and interest in and to the any data, information or other material provided, uploaded, or submitted by Client in the course of using the Service including all intellectual property rights therein.

10.2.3. Client acknowledges and agrees that the Product Publisher, may anonymize and use Client's Anonymized Data, share Anonymized Data with third parties for business and analytic purposes, combine Client's Anonymized Data with data from other sources to an aggregate dataset, use the resulting information for business and analytic purposes. Anonymized Data means data that has had all Client and Personally Identifiable Information ("**PII**") removed. Client's Anonymized Data will not be disclosed in any manner that would identify Client as the source of the data. The aggregate Anonymized Data will be separated from Client's data.

10.2.4. If required, Client will cooperate with Product Publisher in connection with the performance of the Service by making available such personnel and information as may be reasonably required and taking such other actions as Product Publisher may reasonably request. Client will also cooperate with Product Publisher in establishing a password or other procedures for verifying that only designated employees of Client have access to any administrative functions relating to the Service.

10.2.5. Unless otherwise specified by the Product Publisher, Client will use Product Publisher's then-current names, marks, logos, and other identifiers for the Services and Software ("**Trademarks**") and Product Publisher designated intellectual property related notices provided that Client will: (a) only use Trademarks in the form and manner, and in accordance with the quality standards and usage guidelines that Product Publisher specifically prescribes and only in connection with the

Service; and (b) upon termination of this Agreement for any reason, immediately cease all use of the Trademarks. None of Client or any affiliate will (a) otherwise brand the Service or(b) otherwise use or register (or make any filing with respect to) any trademark, name or other designation relevant to the subject matter of this agreement anywhere in the world, whether during or after the term of this Agreement or (c) contest anywhere in the world the use by or authorized by the Product Publisher of any trademark, name or other designation relevant to the subject matter of this Agreement or any application or registration therefore, whether during or after the term of this Agreement.

10.2.6. Client acknowledges and agrees that the Service operate on or with or using application programming interfaces (APIs) and/or other services operated or provided by third parties ("Third-Party Services"). For purposes of clarification, these Third-Party Services include applications and the like that are not incorporated into the Log Service directly and consist of applications such as third-party collection devices and the like. Product Publisher is not responsible for the operation of any third-party services nor the availability or operation of the Services to the extent such availability and operation is dependent upon Third-Party Services. Client is solely responsible for procuring any and all rights necessary for it and its customers to access Third Party Services and for complying with any applicable terms or conditions thereof. Product Publisher does not make any representations or warranties with respect to Third-Party Services or any third-party providers. Any exchange of data or other interaction between Client and a third-party provider is solely between Client and such third-party provider and is governed by such third party's terms and conditions.

10.2.7. Client agrees that it shall not make, or cause to be made, any untrue statement or communicate any untrue information (whether oral or written) that disparages or reflects negatively on the Service, Product Publisher or its management or employees. This paragraph shall not, however, prohibit the Client from testifying truthfully as a witness in any court proceeding or governmental investigation.

10.2.8. During the term of this Agreement, the Client agrees that it shall not embed or utilize with the Service-related software in any service substantially similar in functionality to or identical in functionality to the Service.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Threat Detection – research, risk review, log identification	I	RA
Threat Detection – content creation (standard library)	I	RA
Threat Detection – content deployment (standard library)	I	RA
Threat Detection – content management (standard library)	I	RA
Threat Detection - custom or new content	RA	R*
Threat Detection - content tuning	RA	RA
Threat Detection - submit new content	I	RA
Threat Detection – ad hoc threat sweeps for IOCs	I	RA
SOC - Alert monitoring (standard library), analysis	I	RA
SOC - Alert monitoring (custom use cases)	R	-
SOC - Investigation	RA	RA
SOC - Notification via ticket + escalation SLO	I	RA
SOC - Resolution	RA	RA
SOC - Supply evidence to Incident Response	RA	RA
SOC - Threat Intelligence integration	I	RA
System - SIEM cloud instance setup	I	RA
System - Hosted Collector setup	RA	RA
System - Installed Collector setup	RA	C
System - Usage (data quota) management	RA	C
System - Data ingest tuning	RA	C
System - End user training	RA **	C
System - User account management	A	RA
System - Operations and metrics use cases	RA	-
System - Compliance use cases	RA	-
System - Observability use cases	RA	-
System - ad hoc search, dashboards (not in standard library)	RA	R *
Health - Cloud instance uptime & patching	I	RA
Health - Hosted Collector uptime & patching	I	RA
Health - Installed Collector uptime	RA	C
Health - Installed Collector patching	RA	C
Health - General troubleshooting	RA	C
Data - Source device logging configuration	RA	C
Data - Resolving collection issues	RA	C
Data - Monitoring collection	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
Data - Add new data source	RA	CI

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.
* Limited scope
** self-service