eSENTIRE

Service Description: Managed Detection and Response Foundations Bundle

1. Service Overview

eSentire's MDR Foundations is a Managed Detection and Response ("**MDR**") bundle (the "**Bundle**" or "**Services**") which incorporates data ("signals") from both endpoint detection and response ("**EDR**") technologies and general log and audit data from systems in Client's environment.

The Bundle includes both eSentire's Endpoint Services – Prevent, Detect & Respond - Managed Only (the "**Endpoint Services**"), and eSentire's Log Services – Sumo Logic (the "**Log Services**"). The Endpoint Service provides Client with endpoint-level visibility, threat prevention, detection, investigation, response, and remediation as defined herein, delivered by the eSentire SOC using the endpoint Agent chosen and licensed by Client. eSentire will leverage Client owned licensing (see section 4.1) which will be integrated with eSentire's platform in order for eSentire to provide the Service. The Log Service leverages a cloud native SIEM from Sumo Logic, licensed by eSentire, and collects information from assets in Client's network and cloud resources (the "**Client Environment**"), while monitoring and analyzing that data for potential threats, unusual behavior, or other indicators of compromise.

2. Service Definitions

"**Endpoint Agent**" or "**Agent**" means the endpoint software Agent utilized in providing the Services as further described below.
"**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.
"**Product Publisher**" is the approved vendor selected by Client, for which Client procures EDR licensing from (see section 4.1 for the approved vendor list).

In addition to the above, 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).

3. Service Capabilities

3.1 Description

For Endpoint Services eSentire will leverage Client's licensing to obtain visibility which will enable the eSentire SOC to identify and investigate potential threats or suspicious activity within Client's environment. For Log Services, eSentire will leverage eSentire's licensing of a log management platform to collect log data from client nominated sources providing security context, 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, response, and alerting.

During the Term of the Services, eSentire will provide threat detection, analysis, investigation, escalation, response, and limited remediation (as described below). 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

Copyright © 2023 eSentire, Inc. All Rights Reserved.

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 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:

3.1.1 Endpoint Services:

- Threat Detection:
  - Curation and tuning of Agent detections, rules, policies to generate Actionable Alerts.
  - Collection of detections, metadata and selected raw telemetry to aid in investigation, threat hunting and response activity.
  - Enriching collected Client data with context – such as geolocation of IPs, Client-specific context, and threat intelligence.
- Analysis:
  - Analysis of Alerts generated by Clients Licensed platform either through automation in the Atlas Platform and/or by eSentire (SOC, incident handlers and/or threat hunters)

eSentire may filter traffic based on volume to optimize service delivery. Once investigated, events are classified, alerted, and escalated to Client if an action required. eSentire will utilize the escalation process, agreed upon during the on-boarding process, to contact and relay information to Client. The defined escalation process is a mutually agreed upon process between Client and eSentire.

3.1.2 Log Services:

- Log Collection. The Log Services accept log data from a variety of sources, including syslog, Windows event log (WMI), flat file, and cloud applications and infrastructure. Unsupported and/or custom log sources may be nominated for collection, however, creating collection and analysis support for new log sources will be evaluated and scheduled on a per-case basis. Logs will be transported from Client's environment to eSentire's SumoLogic platform by any of the three methods listed below (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.

3.1.3 All Bundle Services:

- Data Access and Reporting. The eSentire Insight Portal is the primary Client interface to access the outcomes of the Services. The Insight Portal provides an overview of Client's security posture and details on escalated alerts, ongoing and past investigations, service status and other information. For more detailed interaction with collected log data, Client can be provided with access to eSentire's SumoLogic platform. With respect to the Endpoint Service, Client can access their raw EDR telemetry from their endpoint licensed instance (provided by their Product Publisher). For both log and EDR access includes Client self-service access to:
  - Ad-hoc searches
  - Scheduled searches.
  - Real-time and scheduled search alerting (direct to Client)

Copyright © 2023 eSentire, Inc. All Rights Reserved.

- Live dashboards
- API queries

- Alert Escalations. Collected Client data will be analyzed utilizing eSentire developed correlation rules which include a set of logic and intelligence data continuously updated, and utilized to create Alerts. These set of rules are created using both industry best practices, and results of internal research and intelligence.
  - With respect to the Log Services, Client may also create additional alerting from log events for direct notification to Client personnel, however the monitoring of Client created Alerts is 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 Log Services.
  - For Endpoint Services, alerting features are provided by the endpoint Product Publisher and may include:
    - Machine learning ("ML") and artificial intelligence ("AI") are used to detect known and unknown malware and ransomware.
    - Behavior-based indicators of attack ("IOA") are used to prevent sophisticated file-less and malware-free attacks.
    - Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities.
    - Threat Intelligence prevention blocks activities known to be malicious.
    - Continuous raw event recording provides full spectrum visibility at the endpoint.
    - Threat hunting—proactive and managed—with full endpoint activity details.

- SOC Alerting and Investigation. Alerts for potential threats are processed, enriched, and delivered to eSentire's SOC. eSentire uses the data, 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 applicable service level commitments. Where capability exists and where appropriate, the SOC may execute proactive response actions ("Response Actions"). Escalation and response protocols are established at service inception.

- Data Retention
  - Client log data is retained during the Log Services for one calendar year (365 days). Endpoint telemetry generated by the Endpoint Agents are retained within Clients licensed Endpoint platform and retained as prescribed by the Product Publisher. All collected data is stored in the respective SumoLogic (for log), or Endpoint Product Publisher (for endpoint), cloud environment. All alerts and metadata are stored in eSentire's Atlas Platform and are subject to administrative, physical, and technical safeguards. Data collected within the Atlas Platform is retained for the Service Term. Upon Service termination or expiration, all collected Client data in the Atlas Platform is securely destroyed by eSentire. Client-controlled copies of collected log data are available to Client, in the event Client proactively requests that eSentire configure the Log Services to forward a copy of all collected log data to a Client established AWS S3 bucket that is provisioned, managed, and controlled by Client ("Data Forwarding"). This feature cannot be applied retroactively. Copies of Client endpoint raw telemetry may be available depending on the Client's license agreement with their endpoint Product Publisher.

Copyright © 2023 eSentire, Inc. All Rights Reserved.

- Additional online storage for log data is available in six-month increments up to two additional years (1095 days). Additional online storage is subject to fees.
- Additional storage of EDR raw telemetry is subject to the Client's license agreement with the endpoint Product Publisher.

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), which are further defined within the Service Level Objectives (see section 7). 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	Automated remediation actions (SOC can assist with further actions upon request)
		Client Action Needed	Alert with description and relevant data	True Positive	Underlying telemetry and associated data will be available Clients Insight Portal dashboard Subscription to Prevent, Detect, & Respond will result in automated remediation actions (SOC can assist with further actions upon request)
	High/Critical	Client Action Needed	Alert with description and relevant data eSentire threat response • host isolation • identity isolation • remediation actions Escalation procedure (email/phone call with acknowledgement expected)	True Positive	Underlying telemetry and associated data will be available on Insight Portal Subscription to Prevent, Detect, & Respond will result in automated remediation actions (SOC can assist with further actions upon request)
Non-Threat (False Positive / Benign)	N/A	No Client Action Needed	No Alert	False Positive	Recurrences of identical activity will be logged as ignored

Response definitions will be reviewed at service inception and at regular intervals. Response Actions may include:

- isolation of host with release isolation upon confirmation of threat removal or Client orders; and
- block process from execution.

3.3 Remediation Actions

If Client remains an active Endpoint Service customer and maintains Agents in a healthy state, eSentire can assist the Client with remediation activities for high or critical threats from active hands-on

Copyright © 2023 eSentire, Inc. All Rights Reserved.

keyboard attackers, on the endpoint itself, upon alerting Client. The types of remediation support actions that can be provided by eSentire, in coordination with Client are as follows:

- Process or file denylisting on an endpoint
- Block and kill malicious processes.
- Detect and prevent known/unknown bad software (quarantine malicious files)
- Downloading files to an endpoint.
- Isolate an endpoint.
- Initiate a remote shell interactive session on the endpoint to perform a deeper investigation or remediation actions, which can (at our discretion) include:
  - Stop/remove services and registry keys.
  - Perform system reboots to remove malware from volatile memory.
  - Gather files and memory for host.
  - Terminate processes.
  - Delete files on an endpoint.

4. Subscription Options

There is only one Subscription option for this Bundle, which includes Endpoint Services – Prevent, Detect and Respond – Managed Only, and Log Service - Sumo Logic.

The Endpoint Service requires that Client secures appropriate endpoint licensing with one of the product publishers listed in section 4.1 below. The Log Service requires licensing with Sumo Logic, which will be procured and licensed by eSentire.

The Service is sold in tiers based on the number of Client endpoint licenses in scope. The endpoint license count maps to an entitlement of log ingestion expressed in GB/day. See Order Form for details.

4.1 Third Party License Requirements

Client must procure and maintain endpoint licensing ("License") with any of the listed Product Publishers, 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 must purchase at least one of the following licenses:

- SentinelOne Singularity Complete
- CrowdStrike Falcon Insight + CrowdStrike Falcon Prevent + Threat Graph Standard
- VMware Carbon Black Hosted EDR
- VMware Carbon Black Cloud Enterprise EDR + Endpoint Standard
- VMware Carbon Black Cloud Workload Enterprise
- Microsoft M365 E5, Microsoft M365 E5 Security Add-On, Microsoft Business Premium (plus x1 Azure AD P2 license), or Microsoft Defender for Endpoint Plan 2 standalone (plus x1 Azure AD P2 license).

Client will retain ownership of the License and will continue to have all access to utilize their endpoint License. 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 Term of the Service, Client must provide and eSentire must maintain administrator or equivalent access which enables eSentire staff and systems to execute

Copyright © 2023 eSentire, Inc. All Rights Reserved.

the tasks included in this service description. Access will only be provided to select, authorized eSentire employees and will be audited.

There are no additional licensing requirements for Log Services as Sumo Logic licenses will be procured and owned by eSentire.

5. Deployment

eSentire will provide access to an onboarding manager, who is a project manager responsible for scheduling, tracking, and driving the installation and configuration of all elements of the Service ("**Onboarding Manager**").

5.1 Endpoint Service Deployment

For Endpoint Services, Client is responsible for Agent deployment related to the Clients Product Publisher Licensing. eSentire will provide Clients with the required installation documentation for the Endpoint Agent.

5.2 Log Service Deployment

For Log Services, eSentire will provide and support only one cloud-hosted Log instance (a "**Log Instance**" or "**Tenant**"). This is a cloud hosted instance of Sumo Logic software used for the purposes of providing log collection, storage, querying, data analytics that is a component of the larger Log 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-premises log collectors ("**Log Collector**" or "**Collector(s)**").
- Deployment. Collectors will be installed by Client with eSentire's direct assistance during the onboarding period. Client will be responsible for the ongoing management (see RACI in Appendix A) of the Collectors and for ensuring that the Collectors are not prevented from communicating with the applicable Log instance.

Log data is explicitly nominated for the Log Services by source host or application. Scoping of the Log Service is performed prior to sale to ensure compatibility and that expected log volume is within the pre-set allocation determined by the size of the environment, as defined by the license tiers dictated by the number of EDR licenses in scope. The eSentire professional services team (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 Log Services onboarding service time allocation varies by size of Client's SIEM instance. Deployments generally require four to six weeks of calendar time. The 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 Professional Services - Service Description for more details. Table 2 below shows approximate deployment times depending on Clients ingest quota.

Table 2:

Ingest Quota	Approximate Deployment Time
1-5 GB/day	10 hours
6-20 GB/day	10 hours
21-99 GB/day	20 hours

Copyright © 2023 eSentire, Inc. All Rights Reserved.

100-249 GB/day	30 hours
>250 GB/day	40 hours

6. Tuning and Configuration

eSentire is responsible for configuring and tuning leveraging Clients Licensing for Endpoint Services, and eSentire's licensing for Log Services. This requires a special configuration and tuning process due to the automated blocking/killing capabilities that will need to be established. The eSentire support team during this tuning process will include the Onboarding Manager, and a technical team. eSentire requires that Client has 80% of the contracted Agents deployed prior to completing the eSentire tuning process and moving the Service into production. Detections utilizing Clients Licensing capability are handled by the eSentire (Prevent) during the tuning and configuration period(s). All detections provided pursuant to the Detect and Respond portion of the Service are handled by the eSentire SOC immediately upon Agent install, however, all Service activities related to the Prevent portion of the Service require tuning before sent to the SOC for real time. Once tuning has been completed, the Service will be live and transitioned to the SOC for real-time monitoring at which time the Service is considered fully deployed and in-production. Additional details related to tuning and configuration are as follows:

- Data required for detection begins streaming immediately after Client has installed the Agents.
- eSentire begins monitoring detection events immediately after an end-to-end verification test is successfully completed.
- The configuration of the Prevent portion of the Service is a phased approach.
- A tuning period of four weeks for tuning the Prevent portion of the Service begins once 80% of Agents are installed. Weekly meetings to take Client through configuration and tuning will happen over the four-week period.
- Once the tuning period is completed, Prevent with necessary exclusions will be fully active.
- Hosts must remain under eSentire's configured prevention policies to ensure compatibility and continued Service support.

Log tuning is an ongoing process throughout Log Service Term, rather than a discrete post-deployment period. This is considered part of Maintenance and Support and is detailed in Section 8.2

7. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on Licensing from Product Publisher (for Endpoint), and Agents being installed, integrated, and in production in Client's applicable 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 Clients environment in scope that are licensed as part of the Service, and are actively communicating with the Service.

8. Maintenance and Support

eSentire shall provide support to Client for both security and system issues related to the Services.

8.1 Endpoint Service Maintenance and Support

Endpoint License support and maintenance is the responsibility of Client, however, eSentire will perform any maintenance and support associated with connecting the endpoint licensed technology to the eSentire Services, such as data streaming, connections to the Agents for response, connection to the Licensed EDR platform for investigation.

8.2 Log Service Maintenance and Support.

Copyright © 2023 eSentire, Inc. All Rights Reserved.

Log Services include ongoing maintenance support and Table 3 below outlines the support time limits based on the Clients ingest quotas.

Table 3:

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

8.2.1 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.

8.2.2 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 Client's security team, change in escalation procedures, change in working relationship.

Blue Team ongoing support is to be used as required and agreed upon between Client and eSentire. Support time in intended to be approximate is not budgeted/metered per month; it may be used as required in any increments and do not carry over at end of contract. For additional details refer to the Blue Team Professional Services Service Description.

eSentire will also support Client through access to self-directed training and documentation. Support is available via email, telephone, or by contacting the Client's eSentire customer success manager.

9. 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. Should the ingestion usage for Log, on a monthly average basis, be more than ten percent of the daily ingestion limit (identified on the Order Form), notwithstanding any security event, for more than two consecutive months,

Copyright © 2023 eSentire, Inc. All Rights Reserved.

Client will move to the next ingestion level to accommodate its usage for the remainder of the Service Term.

Non-compliance with these obligations may result in suspension of the Service or suspension of service levels. A responsibilities matrix is located in Appendix A below.

9.1 Client Responsibilities

Client obligations include:

- Deployment and Endpoint Maintenance including:
  - installing Agents on endpoints in scope of the Service and working with eSentire to confirm Agents are operational within 30 days;
  - granting eSentire access to all data and systems required for the Service;
  - ensuring there are no firewall rules, network configurations or other infrastructure issues that prevent communication from Agents to the Product Publisher's management server;
  - ensuring there is sufficient network bandwidth and access to perform the Service;
  - assisting eSentire with troubleshooting related to the installation of Endpoint Agents, including providing logs when requested.
  - ensuring devices meet the minimum hardware and software requirements prior to installing the Agents.
  - notifying eSentire of newly added machines to the Endpoint Service during the deployment phase.
  - notifying eSentire of newly added machines to the Service during the Service Term. Should the ingestion usage on a monthly average basis be more than 10% of the daily ingestion limit (identified on the Order Form), notwithstanding any security event, for more than two consecutive months, Client will move to the next ingestion level to accommodate its usage for the remainder of the Service Term;
  - working with eSentire 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 Log Services including necessary licenses, permissions, consents, and tokens to enable eSentire to access Client's network, servers, and cloud service providers.
  - 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 Log Services.

- Tuning, Configuration and User Management including:
  - being available for weekly meetings to discuss detections identified during tuning;
  - ensuring Client authorized contacts remain current, including approved access and all associated information (note: Clients authorized contacts are provided to eSentire by Client during Service inception and can be maintained through contact with the SOC or Client's CSM. Authorized contacts are individuals allowed to approve changes to services, configurations and to respond to escalated alerts); and
  - administering and maintaining user access within Client's Endpoint Licensed instance.

- Investigation, Analysis and Response including:
  - responding to the escalated alerts and validating the legitimacy of the content contained within the Threat Case;
  - updating eSentire of any changes altering agreed upon escalation procedures; and

Copyright © 2023 eSentire, Inc. All Rights Reserved.

- promptly providing information and assistance during SOC investigations conducted by eSentire when additional information is required.

10. 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 are 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.

Any eSentire-developed configuration content on the Client EDR systems will be removed and the Client will disable eSentire access.

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.

11. Service Terms

11.1. 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.
- Services are limited to in-scope Endpoints and do not extend to any Product Publisher license add-on, module, or feature unless mentioned in the above description. eSentire operationalizes the Anti-virus (Prevent) and EDR (Detect and Respond) modules/features of the Product Publishers Agent technology for the purposes of preventing, responding to, or remediating threats. Examples of out-of-scope modules include, but are not limited to, Device Control, Firewall Control, Workloads, Identity, or other optional services that may be available to Client.
- Log Services are limited to in-scope collected logs and do not extend to any Product Publisher license add-on, module, or feature unless mentioned in the above description. eSentire operationalizes the log collection, searching, dashboard/workbook and basic rules/analytics modules/features of the Product Publishers technology for the purposes of preventing, responding to, or remediating threats. Examples of out-of-scope modules include, but are not limited to Cloud SIEM Enterprise, AWS Observability, Cloud SOAR, Automation. The Log Services exclude the design, creation, maintenance, and enforcement of a security policy for Client.

11.2 Log Provisions

By using the Services, Client agrees to the following Log provisions required by Sumo Logic, Inc. (the "Product Publisher"):

a) 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)

Copyright © 2023 eSentire, Inc. All Rights Reserved.

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 Log Services, the development, provision or use of a competing software service or product or any other purpose that is to the Log Product Publisher's detriment or commercial disadvantage; or (iv) use the software other than in accordance with the Log Services description.

b) Client hereby grants to the Log 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 Log Services for internal purposes and for purposes of providing the Log Services; 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 Log Services including all intellectual property rights therein.

c) Client acknowledges and agrees that the Log 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.

d) If required, Client will cooperate with Log Product Publisher in connection with the performance of the Log Services by making available such personnel and information as may be reasonably required and taking such other actions as Log Product Publisher may reasonably request. Client will also cooperate with Log 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 Log Services.

e) Unless otherwise specified by the Log Product Publisher, Client will use Log Product Publisher's then-current names, marks, logos, and other identifiers for the Services and Software ("Trademarks") and Log 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 Log Product Publisher specifically prescribes and only in connection with the Log Services; 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 Log Services 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 Log 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.

f) Client acknowledges and agrees that the Log Services 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

Copyright © 2023 eSentire, Inc. All Rights Reserved.

applications such as third party collection devices and the like. Log 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. Log 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.

g) Client agrees that during the term of this Agreement and for a period of one (1) year after the termination thereof it shall not solicit or assist anyone else to solicit any person who is then or at any time during the then preceding year was an employee or consultant of Log Product Publisher.

h) 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 Log Services, Log 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.

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

Copyright © 2023 eSentire, Inc. All Rights Reserved.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Security – Detection monitoring, analysis	I	RAC
Security – Investigation	-	RAC
Security – Notification	I	RAC
Security – Remediation procedures	AI	RAC
Security – Detection resolution	I	RAC
Security – Threat Intelligence integrations	I	RAC
Security - Supply evidence to Incident Response	RA	RA
Threat Detection – ad hoc threat sweeps for IOCs	-	RA
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
System– custom alerts, dashboards, or workflows	RA	-
System – Initial product walkthroughs and/or guides	A	R
System – Deploying initial endpoints	RA	CI
System – Initial policy and environment configurations	CI	RAC
System – Post-deployment installation or host group management	RA	C
System – User account management and administration	RA	C
System- End user training*	RA *	C
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 - Operations and metrics use cases	RA	-
System - Compliance use cases	RA	-
System - Observability use cases	RA	-
Health– Data ingestion, uptime monitoring and tuning	-	RA
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
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.
*= Self service

Copyright © 2023 eSentire, Inc. All Rights Reserved.