Log Services

The Service name was updated by eSentire from “esLOG Services”, to “Log Services”. All other content remains the same.

Definitions

Cloud Services – The collective cloud-based service offerings, including all services related to Log Services.
Product Publisher - The publisher of any third-party software utilized as part of the Log Services.
Alert - An event or set of events that eSentire will escalate to the Customer.
Emergency Incident Response - The rapid mobilization and deployment activities aimed at quickly securing Client systems and networks, providing incident response services beyond what MDR provides. Covers the full lifecycle of an incident - containing the full extent of the attack (across all attack surfaces).
Embedded Incident Response - MDR will identify and contain the attacker (within the visibility and scope of the MDR service) and provide remediation guidance to the customer.
Forensic investigation – Salvaging as much information as possible from the Client’s systems and networks deemed in scope and regression analyzing that information to conclusively determine the full extent of compromised assets.
Litigation support – Any litigation support, including but not limited to expert and fact witness testimony.
Disaster recovery and business continuity planning – Assessment, execution and/or building of disaster recovery and continuity planning processes and techniques. Used to help an organization recover from a disaster and continue or resume routine business operations.
Business impact – Any quantification of the reputational, operational, compliance or financial impact to the customer’s business.

Service Description

eSentire's Log Service is a service providing centralized log management with analysis, investigation and alerting based on log data (the “**Log Services**”). Log Services leverage a cloud-native SIEM platform from Product Publisher combined with the eSentire Atlas XDR platform to detect, hunt, and investigate IT security threats. Log Services collect information from assets in the 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 Security Operations Center (SOC) on a 24x7x365 basis, initiating investigations and Client notification as required. The Log Services are fully managed and available on a subscription basis.

Service Features

Log Collection

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 and is included in the Log Services.

Logs will be transported from the Client environment to the Product Publisher’s hosted cloud SIEM platform by one of three methods as appropriate:

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

- Centralized collection in the Client environment using eSentire-provided collector software installed on Client-managed hosts;
- Agent software installed on each monitored host.

Log Retention

Client data is retained by Log Services 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 is subject to administrative, physical and technical safeguards. Upon termination of the Log Services, all collected data is securely destroyed.

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

Data Access and Reporting

The eSentire Insight Portal is the primary Client interface to access the outcomes of MDR services, including Log. Insight portal provides an overview of the Client's security posture and details on escalated alerts, ongoing investigations, service status and other information.

For more detailed interaction with collected log data Log Services provide Client with direct access to their Log SIEM tenant. This access includes self-service access to:

- Ad-hoc searches
- Scheduled searches
- Real-time and scheduled search alerting (direct to Client)
- Live dashboards
- API queries

Large volumes of data are collected for a variety of use cases for Log Services. 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. Log Services 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 to 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 the Client based on the specific set of log sources in scope and based on eSentire's log scoping best practices.

eSentire will support the Client through access to self-directed training, documentation as well as direct support via email and telephone.

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 Clients.

The Client may also create additional alerting from log events for direct notification to Client personnel. Monitoring of these alerts are the responsibility of the client. eSentire reserves the right to limit custom alerting configuration to security uses cases and the log sources in scope of the Log Services.

SOC Alerting and Investigation

Alerts for potential threats are processed, enriched, and delivered to eSentire's SOC. eSentire uses the data from Log Services within the broader MDR Services, including other signals, threat intelligence, and investigations to determine the nature and severity of the threat and will notify the Client according to defined escalation procedures and SLOs. Where other MDR services are in place, the SOC may execute proactive response actions.

Log Essentials Service Option

A selected subset of data collected for the Log Services may optionally 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 the Client and eSentire using industry best practices and specific Client needs. Data subscribed to Log Essentials is not eligible for Data Forwarding.

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 Log Service.

Log Collectors

- 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 the Client with eSentire's direct assistance during the onboarding period. The Client will be responsible for the ongoing management 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 service is performed prior to sale to determine the contracted ingest quota, expressed in GB per day. The eSentire professional services in collaboration with the Client will complete an inventory of all in-scope logging and auditing devices, applications and cloud services and assist with configuring data acquisition. Log data to collect will be prioritized by data types providing maximum service effectiveness.

The Log Services onboarding service time allocation varies by size of the SIEM instance. Deployments generally require 4-6 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.

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

Maintenance and Support

eSentire shall provide support to the Client for both security and system issues related to the Log Services. The Log Services include ongoing maintenance and change service hours. See the Blue Team Service Description for more details.

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

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

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

For additional details refer to the Blue Team Professional Services Service Description.

Responsibilities

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

Function	Client	eSentire
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

Function	Client	eSentire
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

The 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 Log Services including necessary licenses, permissions, consents, and tokens to enable eSentire to access Client's network, servers, and Cloud Service providers in order to provide Log Services
- 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
- Installing of on-premise log collectors to enable log collection for sources within the 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
- Providing the necessary resources, information, documentation and access to personnel, equipment and systems, as reasonably required by eSentire, to allow eSentire to perform the Log Services.

In the event Client fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption set out herein with respect to the Log Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

Service Level Objectives

The service levels below are only applicable to log data that has been included in the scope of Log services.

eSentire will monitor the Log service for potential threats and notify accordingly. When potentially malicious activity is identified eSentire will perform an investigation. If available through response-capable services such as eSentire's Endpoint or Network services, eSentire 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.

Severity/Priority	Description	Notification/Escalation
N/A	Informational or custom alerts – direct to client with no real-time SOC review.	Automated alert (via email) within 20 minutes of events arriving at the log platform.
Low (P4)	Minor activity recorded but not alerted.	None. Accessible on demand through Insight portal and saved searches.

Medium (P3)	Unusual activity which requires further investigation or confirmation.	Email notification within 90 minutes of determinations of the security event by the SOC.
High (P2)	Potential threat activity that does not require immediate attention but if left unchecked may lead to more severe security incidents	Email notification within 60 minutes of determination of the security event by the SOC.
Critical (P1)	Threat activity identified in log data that requires immediate attention. These items may indicate that a severe security incident is underway or is imminent. *Log events supporting investigations triggered from eSentire's Network and Endpoint Services are tracked to the SLOs of those service lines.	Alert (via email) within 40 minutes of the determination of a security event followed by phone call to the Client per defined escalation procedures.

Exclusions

The Log Services exclude the design, creation, maintenance, and enforcement of a security policy for Client.

The MDR service does not provide emergency incident response (as defined above) 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 customer assets, whether currently under embedded incident response or not.