Log Services - Azure Sentinel - Managed Only

The Service name was updated by eSentire from "esLOG Services (Managed Only) for Azure Sentinel", to "Log Services – Azure Sentinel – Managed Only". 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 for MDR is a service providing centralized log management with analysis, investigation and alerting based on log data leveraging a 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 "**Managed-Only Log for MDR Services**", the "**Service**"). This service description describes the services as implemented in conjunction with Microsoft Azure Sentinel.

The Managed-Only Log for MDR Services collect log, audit and other telemetry 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. This is fully managed and available on a subscription basis.

A subset of data collected and usage of the Client SIEM is designated for use for the Managed-Only Log for MDR Services (the "**Service Scope**"). Use of the Client SIEM outside of Service Scope is the responsibility of the Client.

The configuration and support of the es service will target MDR and general cybersecurity best practices. This scope is the collection of log data beneficial to the detection and investigation of cybersecurity threats. The primary goal of Log is real time monitoring of high fidelity, high value and sources contributing to alerting logic defined in eSentire content for the purposes of alerting the SOC and supporting their investigations. Additional log data is collected to support deeper investigations, threat hunts and threat sweeps.

Adjacent use cases such as Compliance, DevOps/DevSecOps, host metrics and Observability are not considered core MDR use cases but can be supported through client self-service.

Service Features

Log Collection

Managed-Only Log for MDR Services accept log data from a variety of sources, including syslog, Windows event log (WMI), flat file, and cloud applications and infrastructure. Specific data connectors will vary and the set of supported log connectors is under continuous improvement. New and/or custom log sources support requires Client engagement with their SIEM vendor.

Logs will be transported from the Client environment to the Client SIEM platform by one of multiple 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;

Configuration of log sources and transport to the SIEM is the responsibility of the Client; eSentire will advise and assist as appropriate.

Log Retention

Data considered within the scope of the service, as defined at service inception, 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 is subject to administrative, physical and technical safeguards. Upon termination of the Log for MDR Services, all collected data in the eSentire environment is securely destroyed or allowed to expire per standard policies while remaining under standard safeguards.

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 the Client retains direct access to their Client SIEM. This access includes self-service access to:

- Ad-hoc searches
- Scheduled searches
- Real-time alerting (direct to Client)
- Dashboards and workspaces
- API queries

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. eSentire Tactical Threat Response creates and maintains a library of content which detects potential threat activity or behaviour in log data to drive alerts to SOC and support investigations by eSentire Analysts – known as Runbooks. eSentire content also includes saved searches, dashboards and other features as supported by the host SIEMs.

Content inputs include:

- Threat Research (internal and external)
- SOC Incidents and Investigations
- Macro cybersecurity events
- Customer requests and feedback
- Market
- Blue Team customer-specific work during deployments or maintenance
- Content repositories

The Client may also create additional alerting from log events for direct notification to Client personnel. Triggering playbooks from alerting configuration is also an option. Monitoring of these alerts and defining automation 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 Managed-Only Log for MDR Services. See the Blue Team Services Description for more details. Out of scope activity is the responsibility of the Client and the Client's SIEM vendor.

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, 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. Sentinel Playbook automation/response is not utilized for SOC-driven actions.

Deployment, Maintenance and Support

eSentire Blue Team consulting and professional services are required for planning, strategy, and integration of the Client SIEM into the Managed-Only Log for MDR service. The SIEM will be evaluated for general health, availability and current configuration and a project plan for integration will be created in collaboration with the Client. The SIEM will be configured with eSentire-developed content such as rules, Runbooks, searches, and dashboards for the purposes of facilitating eSentire MDR services. Clients may also develop and maintain their own content.

Log data is explicitly nominated to be in Service Scope by source host or application. Scoping of the service is performed prior to sale to determine the contracted managed scope and 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 Managed-Only Log for MDR Services onboarding service time allocation varies by size of the SIEM instance. Please refer to the Blue Team Services Description for details.

Additional professional services time is available for a fee.

eSentire shall provide support to the 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 the client. All SIEM platform specific issues or issues for data outside Services Scope are the responsibility of the Client and their SIEM vendor. The Managed-Only Log Services include ongoing maintenance and change service hours.

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 MDR 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
    - quota management; data filtering and tuning

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	Microsoft
Azure Active Directory B2B Permissions	RA	CI	
Threat Detection - content creation, evolution and management (standard library)	I	RA	C
Threat Detection - deploy content	I	RA	
Threat Detection - content tuning	A	R	
Threat Detection- custom use cases	RA	R limited	RA
Threat Detection - submit new use cases to eSentire	CI	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	

Function	Client	eSentire	Microsoft
System – SIEM setup	R	I	
System - Collection of data to SIEM	R	I	
System – Data storage and quota management	RA	C	A
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	R
Health - Collector uptime & patching	R	I	R
Health - General troubleshooting	RA	C	R
Data - Source device logging config	RA	C	
Data - Resolving collection issues	RA	C	R
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, parsing	RA	C	R

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:

- Procuring and maintain appropriate SIEM licenses
- 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 term of the Log Services
- 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 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.

MDR Service Level Objectives

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

eSentire will monitor 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 ENDPOINT or NETWORK, 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 Managed-Only Log Services excludes the design, creation, maintenance, and enforcement of a security policy for Client.

The Managed-Only Log Services exclude procurement, initial installation, licensing and maintenance of the Client SIEM.

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.