Blue Team Professional Services

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

The eSentire professional services Blue Team provides a set of services to plan, design, build and maintain the SIEM technology component of esLOG and the eSentire Managed Detection and Response (MDR) services. The Blue Team is comprised of experienced security industry practitioners, trained, and certified in multiple SIEM technologies and cybersecurity and engineering disciplines. This service description will detail tasks which are included in standard deployments of esLOG and tasks which are available for additional fees.

Deliverables in the setup and ongoing maintenance of the SIEM technology are primarily performed by the Blue Team with the assistance of supporting teams such as Client Success, Threat Response Unit or others as required.

The Blue Team does not perform monitoring, investigation, or response/remediation tasks for the MDR service. See the esLOG and other MDR services Service Descriptions for details.

The configuration and support of the esLOG 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 esLOG 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

Included in initial deployments of the LOG Service

Ingest Quota	LOG Services	Managed Only LOG Services
1-5GB/day	10 hours	10 hours
6-20GB/day	10 hours	20 hours
21-99GB/day	20 hours	30 hours
100-249GB/day	30 hours	40 hours
>250GB/day	40 hours	50 hours

Tasks to be performed by eSentire staff in collaboration with the Client. eSentire team may be comprised of Blue Team (SIEM consulting), Customer Success, Deployments and others as required.

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.

PLAN – 20%

- Scope review workshop - inventory all log sources and document
    - Update and notate pre-sales scoping document
    - Finalize source scope document, sign off and check in
- Service outcomes workshop - review goals of log service within MDR
    - Review service:
        - log value, priority and appropriate data tier;
        - alerts to SOC and resulting investigations;
        - use of log data for multi-signal investigations;
        - use of log data for asynchronous threat hunts;
        - alerts direct to client – auto-notifications;
        - co-management & self-service options
    - Overview of Runbook and content library
    - Overview of additional custom (Blue Team) content options
    - Overview of bundled SIEM content options
    - Outline content pipeline from custom to library
    - Review content roadmap
    - Collect content feedback - submit to Product Management
    - Overview of SIEM usage: dashboards, workbooks, searches and other content
    - Provide training links for self-service
    - Create content scope document, sign off and check in

Deliverables: Project plan, log source scope document, kickoff presentation, SIEM training links

BUILD – 70%

- SIEM instance setup
- SIEM onboarding to Atlas and eSentire infrastructure
- Guidance to customer: how to deploy collectors (if required)
- Standard (library) content deployment and verification
- Log source setup on SIEM, guidance to customer: configuring log sources
- Filtering, data routing

- Ingest monitoring setup
- User setup
- Blue Team content deployment and verification
- SIEM bundled content deployment and verification
- Set automated notifications if in scope
- Additional custom content creation (as time allows and within scope defined)

Deliverables: Completed implementation,

RUN – 10%

- Basic training – hand off
- Project hand off
- Maintenance and maturity planning

Deliverables: Verification of completed project plan, documented next steps

Ongoing tasks included in service

SOC and Support

- Rule tuning (standard content library)
- New users/Access controls
- Deploy new library content
- General support – uptime, troubleshooting
- Log collection monitoring

Client self-service

- Self-service data access
- Add new sources (to existing categories)

Blue Team

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

Blue Team ongoing support is to be used as required and agreed upon between the Client and eSentire. Support time is not budgeted/metered per month; it may be used as required in any increments and do not carry over at end of contract. Examples of Blue Team ongoing support tasks:

- Review source and content scope documents, edit/expand as necessary
- Add new source type
- Quota monitoring
  - bi-weekly review for overages
  - email communication of overage from Customer Success
  - minor filtering by Blue Team to maintain quota
  - recommendations to increase quota

- Use cases outside of MDR/real time cybersecurity monitoring scope:
  - o Compliance reports
- New custom cybersecurity content

Additional Services

Additional Blue Team resources may be contracted by Client as required.
$2000 USD/day (8 working hours, remote)

Service	Description	Deliverable	Time
Hourly	Blue Team time to be applied to tasks as defined prior to engagement which may include: • Custom content • Logs source support • Training	As defined	Day increments as required

Client Responsibilities

Client is responsible for:

- obtaining all necessary licenses, permissions and consents to enable eSentire to access the Client's network and servers in order to provide the services;
- designating a project coordinator to work directly with and serve as the primary Client contact with eSentire for the duration of Client's receipt of the services;
- providing eSentire a complete copy of its security (including privacy) policies, as available. Client is solely responsible for creating, maintaining and enforcing its security policies to protect the security of Client Data and Systems;
- its choice of equipment, systems, software 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;
- providing a current network topology diagram;
- notifying eSentire in advance of any network changes that will affect Client's network.

Exclusions

- the design, creation, maintenance and enforcement of a security policy for Client;
- eSentire attempting to access Client's servers without Client's express written or verbal consent;
- eSentire configuring Client sources to output logs;
- Consult on acquiring new security controls;
- Any changes to client environment such as networking, users, permissions;
- Non security-related content, including DevOps, Metrics, Operational monitoring.

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.

Definition and Limitations for Log Content

eSentire's Tactical Threat Response creates and maintains a library of content which detects potential threat activity or behavior in log data to drive alerts to SOC and support investigations by eSentire Analysts-

Runbooks. eSentire default 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

Blue Team's mission is to create real time detections for direct-to-customer notification plus other views and configurations in the SIEM dashboard for clients that deliver extended (not yet in standard library) or site-specific security value and provide co-managed access to the log service.

Blue Team content will generally focus on client-specific needs and will not overlap with existing eSentire content delivered to all clients automatically.

eSentire has services directly integrated with Atlas and the SOC for select types of data and sources to deliver MDR outcomes. These include:

- EDR (Endpoint with CbR, CbTH, Crowdstrike, Defender);
- IDS, packet and flow capture and analysis (Network and Insider Services);
- the Microsoft Defender suite (Defender for Endpoint, o365, CAS, Identity);
- Vulnerability scanners (MVS via tenable.io)

Most content surrounding EDR, IDS, VA or Defender is found in the eSentire Endpoint, Network, Insider, MVS and the Microsoft services as appropriate.