eSENTIRE

Service Description:
Atlas Essentials Package

1. Overview

eSentire's Atlas Essentials Package (the "**Package**") is a managed detection and response ("**MDR**") solution that leverages the eSentire Atlas Platform to provide cybersecurity insights, along with threat prevention, detection, mitigation, response, and remediation. eSentire uses Client Data from various sources within the Client Environment to provide a comprehensive MDR solution. Specific elements of the Package are described herein, and the Package is scoped using the total number of Client-nominated servers, laptops, and desktop devices with supported operating systems ("**Endpoints**"). The number of Endpoints included in the Client Package are detailed on the Order Form and subject to Overages.

2. Service Definitions

In addition to the below, any capitalized terms contained in this service description are as defined herein:

- "**Atlas Platform**" means eSentire XDR platform which consolidates all data and drives workflow for all eSentire MDR services, including those in this Package. All data on the Atlas Platform, related to the delivery of the Package for Client, is retained for the Term, and deleted upon Package expiration.
- "**Client Data**" means, unless otherwise defined in the underlying terms and conditions referenced in the Order Form, (a) data, records, files of Client including e-mail sent or received by personnel of Client, and (b) all reports generated for or by Client as a result of the provision or use of the services included in the Package, except to the extent such reports contain intellectual property of eSentire.
- "**Indicators of Compromise (IOCs)**" means distinctive elements of data used to detect potential security breaches or malicious actions.
- "**Insight Portal**" means the Client interface into the Atlas Platform, where eSentire provides Client service overview, detailed threat case reporting and/or event summaries.
- "**MDR Services**" means the Endpoint Services, Log Services, and Network Services (if selected) included in this Package.
- "**Order Form**" means an ordering document, executed by the parties, that specifies services ordered by Client, including any amendments and supplements thereto.
- "**Threat Research & Intelligence Briefing**" means a curated monthly brief provided to Client on known and emerging cyber threats (i.e., malware, phishing campaigns, ransomware attacks, and other malicious activities) interspersed with time-sensitive updates about significant developments in the threat landscape.
- "**Term**" is defined on the Order Form during which time eSentire will deliver the Package described herein.

3. Package Elements

The Package consists of the following elements:

- collection of Client Data (including endpoint data, log data, and network data (if selected)) from Client systems (referred to herein as the "**Client Environment**") based on total Endpoints;
  - Limited to not more than 500 total Endpoints (actual quantity ordered detailed on Order Form);
- threat prevention and detection;
- security investigation of alerts detected via the Atlas Platform by eSentire security analysts;
- threat incident handling, reporting, hunting, and response (as required);
- access to Threat Research and Intelligence Briefings;
- support from the eSentire Cyber Resilience Team; and
- access to eSentire Insight Portal for access to reporting, and package features.

Client-specific selections for the Package are identified on the Order Form.

4. Access and Onboarding

Following receipt of a fully executed Order Form, a member of the eSentire Cyber Resilience Team (see **section 6** below) will work with Client to begin Package onboarding activities, which will include:

- assigning an eSentire onboarding manager and scheduling the initial onboarding call;
- establishing the onboarding project plan;

- deploying network appliances (ordered separately if applicable);
- connecting telemetry sources (including logs, enrichment and other data sources); and
- configuring integrations to Client applications.

Client will also be provided with access to the Insight Portal, which provides visibility over all subscribed eSentire services. The Insight Portal acts as a central hub for managing and monitoring security services, allowing Client to configure, integrate, and view eSentire Package elements in real-time. The Insight Portal includes self-service features such as:

- telemetry integration;
- collector configuration; and
- service setup.

Telemetry sources are further detailed below, and if appliances/sensors provided by eSentire ("**eSentire Equipment**") are required as part of Client Data collection, such eSentire Equipment will be listed on the Order Form. Client will be required to assist with accessing telemetry, installing applicable licensed software tools, or installing required eSentire Equipment. Telemetry sources include:

4.1. Endpoint (referred to on the Order Form within the Package as "**Endpoint Services**")

eSentire will collect in-scope Client endpoint data leveraging the eSentire Agent. The eSentire Agent collects endpoint telemetry and will generate endpoint detection and response ("**EDR**") alerts. EDR alerts are stored in the Atlas Platform for the Term. Raw telemetry is stored on the Atlas Platform for 15 days. eSentire Agent is a managed solution whereby eSentire is the license holder (an "**MSSP**" solution).

4.2. Log (referred to on the Order Form within the Package as "**Log Services**")

eSentire will leverage Client log data and will perform real-time analytics on up to five approved log sources, to be identified by eSentire during onboarding. The Package includes unlimited log collection from those Client security controls, systems and applications deemed relevant by eSentire to its delivery of the Package. Log and audit data is stored in the SIEM/log module of the Atlas Platform and is retained for 365 days (or until the expiration of the Term, whichever is first). Client may order additional online log storage retention for up to five years (expiration of the Term, whichever is first) and, if requested will be listed on the Order Form in a separate section outside of the Package fees, and service table. The Package includes an MSSP log solution.

4.3. Network (referred to on the Order Form within the Package as "**Network Services**" or "**Threat Intelligence**")

In the standard Package configuration, eSentire will access the Client Environment in order to provide real-time capture and monitoring of network traffic, leveraging an MSSP network solution. Client will be required to install eSentire network sensors to capture a TAP or SPAN of network traffic. Network sensors capture network packets and metadata, which are stored on the network sensor inside the network environment where each sensor is deployed (physical appliance or virtual machine). Each network sensor will generate network alerts, which are stored in the Atlas Platform for the Term. Such sensors are eSentire Equipment and will be either physical or virtual appliances located at select locations in the Client Environment (generally co-located with Client firewalls), and if required/requested will be listed on the Order Form in a separate section outside of the Package fees, and service table.

Alternatively, if Client elects not to provide network telemetry, Client may receive eSentire's Threat Intelligence feed in a standardized format. Client may then ingest such feed into Client's security tools such as a TIP, firewall, email server, or endpoint technology, to enhance such tools with high value and up-to-date IOCs.

Client selections are detailed on the Order Form.

5. Package Deliverables

The following will be delivered to Client as part of the Package:

5.1. eSentire SOC and Security Analysts. An eSentire security analyst operating in an eSentire Security Operations Center ("**SOC**") will utilize the telemetry gathered from the sources described in **section 4** above to perform detailed security investigations of alerts detected via the Atlas Platform. Security analysts provide 24x7x365 monitoring and reaction to identify, investigate, and (where appropriate) prevent or contain potential Client threats. eSentire technical support is also available for Client assistance with the technologies directly linked and supporting the delivery of Packaged services. Such technical support is available 8am x 5pm EST, with the availability of support outside of these defined hours.

5.2. Unlimited Incident Handling. eSentire security analysts will perform incident handling for all security incidents. Incident handling includes detecting, analyzing, containing, and assisting in the recovery from security incidents, and may involve attempted isolation of compromised assets, disruption of attacker activities, termination of malicious processes, and severing of command-and-control connections. Security analysts also provide remediation guidance, investigate the initial access vector, and check for potential data exfiltration. Core objectives include:

- suppressing and containing threats before further damage occurs;
- investigating and neutralizing threats to prevent their continued operation;
- utilizing the deployed MDR Services to conduct investigations; and
- identifying root causes where possible.

In addition, eSentire also provides containment and remediation recommendations and, when necessary, defers to eSentire or third-party digital forensics/incident response ("**DFIR**") services (not included in the Package) when an incident cannot be fully contained through MDR alone or has other complicating factors (e.g., litigation, visibility, forensics, etc.).

5.2.1. Incident Handling Process:

When the Atlas Platform generates an indicator of a potential threat eSentire begins an investigation. An investigation includes validating the presence of a threat via Client telemetry and evidence data, threat intelligence, and other data and information sources within the Atlas Platform. Using this information and the automation capabilities of the Atlas Platform, a security analyst then determines the nature and extent of any compromise that may have occurred. Depending on the nature of the potential threat, activities conducted during the incident handling process may include:

- Threat analysis:
  - Assessment of the malicious nature of a threat and its potential impact.
  - Categorization according to industry essential practice frameworks including MITRE ATT&CK.
  - Contextualisation of validated threats based on factors such as industry vertical and geopolitical context.
- Threat hunting across Client's telemetry data which has been ingested into the Atlas Platform.
- Threat response actions taken per Client's previously configured response protocols.
- Recommendation to Client of a suggested response covering suggested next steps, and remediation activities as required.

After remediation, a summary of findings will be provided to Client, detailing evidence, and timelines. Throughout the process, corrective action tracking will be maintained. Upon completion of the incident handling processes, should Client defer to eSentire DFIR services or engage a third-party DFIR firm, eSentire will provide the Advanced findings of its investigation, including acquired forensic artifacts (if possible).

6. Cyber Resilience Team Support

As part of the Package, Client will receive ongoing service support and technical and commercial relationship management by eSentire's Cyber Resilience Team, which will assist Client with maximizing the benefits of the Package ("**Support**"). The Support deliverables provided as part of the Package will include:

6.1. Onboarding Support: eSentire's Cyber Resilience Team will provide guidance and a personalized setup of the Package elements ordered. This Support will assist Client with the deployment, integration of Package services

into Client's existing infrastructure, establish meeting cadences, and set clear expectations. See **section 4** above for additional details.

6.2. Reporting and Reviews: In addition to eSentire's Threat Research and Intelligence Briefings, Client will receive regular reporting provided by the Cyber Resilience Team through:

- automated reports available via the Insight Portal; and
- support from a pooled relationship manager.

7. License Requirements

All Packaged services hereunder are being provided in a MSSP capacity: where applicable, eSentire will procure all required licensing directly with the Product Publisher; eSentire will be the licensee of record with each Product Publisher; and eSentire will manage any such licensed solutions provided by Product Publisher. As the license holder for MSSP solutions, eSentire may grant Client enhanced access into eSentire's licensed environment. In the event such access is granted: Client acknowledges and agrees that any changes made by Client in the licensed environment could impair eSentire's ability to deliver the Package; Client accepts responsibility for such changes; and Client releases eSentire from its obligations to deliver the Package to the extent of such impairment.

8. Package Services General Information

The following information applies to this Package:

8.1. Client Responsibilities. General Client responsibilities for Packages are listed below. Client must comply with Client responsibilities in order for eSentire to meet its obligations and deliver services. Client Responsibilities are as follows:

- Client is responsible for all Client provided third-party equipment, software services, support, or vendors not under the control of eSentire.
- Client should respond to alerts and inquiries from eSentire in a timely fashion.
- Client should identify prior issues with Client's network to the eSentire team prior to Packaged services commencing (including any incidents, problems, errors, or other events subject to an open support ticket from a legacy or other third-party service provider).
- Client is responsible for implementing any recommendations or remediation advice provided by eSentire related to Client incidents, however, Client's decision to not implement any remediation recommendations may adversely impact eSentire's ability to deliver the Package.
- Client should communicate and coordinate any required changes to the Client network or other component required for the Packaged services to be delivered, prior to making any changes.
- Client may be provided with a level of administrative access to Packaged services for Client and its affiliates, professional advisors, service providers and agents (collectively, "**Representatives**"). Such administrative access may include, by way of example, access to portals or dashboards used to access Client Data or configure and control the Packaged services. Client acknowledges that, in addition to actions Client takes with respect to its own systems, actions that Client or its Representatives take utilizing such administrative access to Packaged services may impair eSentire's ability to provide the Package. In such case and to the extent of any such impairment, Client assumes full responsibility for such actions and releases eSentire from any (i) obligations to provide the impaired Packaged services or (ii) liability for the failure to provide such Packaged services.

8.2. MDR Service Level Objectives ("**SLOs**"). eSentire measures a set of internal objectives that apply to MDR Services. For each SLO, a minimum of 20 Threat Cases must be processed during the month for the SLO to apply. These eSentire standards are further described below. Defined terms for this **section 8.2** are as follows:

- "**Work Item**" means a collection of one or more events and alerts collected by the Atlas Platform requiring analysis by eSentire SOC Analysts.
- "**Actionable**" means a Work Item analysis has concluded that an alert or containment action is required, based on criteria established by eSentire and reviewed with Client.
- "**Threat Case**" means an Actionable Work Item, which results in a notification or action required.

- "**SOC Dashboard**" means the eSentire SOC interface into the Atlas Platform.

8.2.1. Time to Engage ("**TTE**") – Work Item – SLO target 60 minutes:
The Service Level Indicator ("**SLI**") time starts when a Work Item is created in the SOC Dashboard and ends when an eSentire SOC Analyst changes the state of the Work Item in the SOC Dashboard to "under review". A Work Item is marked "under review" in the SOC Dashboard, when analysis of the Work Item by an eSentire SOC Analyst has commenced. The analysis includes collecting evidence and creating assessment notes against the Work Item. The outcome or duration of the analysis does not impact the TTE SLO target.

8.2.2. Time to Respond ("**TTR**") – Actionable Work Item – SLO Target based on Priority Level (Table 1):
As a result of the Work Item analysis described above, eSentire will determine if a Work Item is Actionable, and if so, will create a Threat Case. eSentire will then notify Client via the Insight Portal, and email, of any Threat Case. The SLI starts when a Threat Case has been created in the SOC Dashboard and ends when an eSentire SOC Analyst notifies the Client and provides the Client defined response remediation actions.

Table 1.

Priority Level	TTR SLO Target[1]
P1	10 minutes
P2	20 minutes
P3	40 minutes
P4	60 minutes
[1]SLO Target is measured as a monthly aggregate by priority level, taking into consideration all actionable Threat Cases from the previous month.	

The Priority Levels listed above are defined below (see Table 2).

Table 2.

Priority Level	Description
P4 (Low)	Minor activity recorded but not alerted, and the presence of likely unwanted activity - for example, adware.
P3 (Medium)	Suspicious activity that might not be deemed malicious by itself, and malicious activity not known to be targeted.
P2 (High)	Malware event, tactics, techniques, and procedure events, or events indicating targeted attack with potential for widespread impact.
P1 (Critical)	Malware infection(s), virus infection(s), and lateral movement, or indications of targeted attack with a high potential to cause grave damage to critical assets.

eSentire objectives listed above may be impacted by short periods due to scheduled maintenance where updates, patches, are installed and configured (i.e., maintenance windows), or when hardware deployment or replacements are required.

8.3. Add-on's. Client may order from eSentire additional licensed offerings outside of those included in or required or supported by the Packaged services ("**Add-Ons**"). Any such Add-Ons will be provided for Client use, but other than as described below, do not include any eSentire support or configuration assistance. Such Add-On's are only available to Client, when Client is being supported in an MSSP support model, eSentire is considered the licensee of such Add-Ons (referred to on the Order Form as an "**MSSP Add-on**" or "**Add-on**") and eSentire will provide access and documentation to Client. Client can request assistance with such MSSP Add-ons from eSentire, and eSentire will open a ticket with Product Publisher. Add-on's will be listed on the Order Form in a separate section outside of the Package fees, and service table.

8.4. eSentire Equipment. If Client is provisioned with eSentire Equipment, eSentire shall maintain the hardware and software for all eSentire-provided devices including any sensor. eSentire will ship replacements of failed components and receipt of replacements or failed components is subject to local custom or similar procedures. This maintenance policy does not apply to hardware provided by Client's organization. Shipping of replacement parts or systems for eSentire provided devices is included with the existing sensor fees. This replacement policy does not apply if the eSentire-provided hardware is damaged or lost through fire, theft or misuse. In the event of loss of eSentire-provided hardware through fire, theft or misuse, Client is responsible for the cost and shipping

of the replacement. When eSentire Equipment is required to facilitate access to certain telemetry, such eSentire Equipment will be listed on the Order Form in a separate section outside of the Package fees, and service table.

8.5. eSentire Support. Client may contact the eSentire SOC related to eSentire services at any time by any of the following methods:

Method	**Contact Information**
Phone (North America)	+1-844-552-5837(Toll Free)
Phone (Direct-to-SOC Toll Outside of North America)	+353 21 4757102 (toll)
Phone (United Kingdom)	0800-044-3242 (Toll Free)
Email (Worldwide)	esoc@esentire.com
Mobile Application	per downloaded mobile application and associated instructions

Issue Tracking. eSentire maintains a ticketing system to handle all incoming contact from Clients. As such, eSentire keeps a log of all support calls and emails received from Client. Information to be included in this log include the name and location of the Client employee or contractor, eSentire security analyst involved, the date and time of the contact, the time to resolve the logged issue and details of the issue. This process is audited each year by eSentire's external auditors for SOC2 compliance.

8.6. Package Overages. Packages are scoped/sold using Endpoint totals, and the quantity is detailed on the Order Form. Should Client's number of Endpoints active as a daily average exceed 10% of the purchased value (measured on an average over one calendar month), notwithstanding any security event (the "**Overage**"), then Client will either (i) take steps to remove Endpoints within 30 Days of such Overage, or (ii) move to the next Package tier, and associated fees, to accommodate its usage for the remainder of the Term.

8.7. Product Publisher Flow Down Terms. If Client has ordered Services to be delivered in an MSSP fashion, 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. These flow down provisions are not negotiable, as they are listed below, as specifically required by the Product Publisher. In such case, Client agrees to the following Product Publisher required flow down provisions:

8.7.1. Product Publisher – Sumo Logic, Inc. flow down provisions for Log Services (newly defined terms in **section 8.7.1** shall only apply to this section):

8.7.1.1 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 Log Services, 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.

8.7.1.2 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 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.

8.7.1.3 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.

8.7.1.4 If required, Client will cooperate with 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 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 Log Services.

8.7.1.5 Unless otherwise specified by the Product Publisher, Client will use Product Publisher's then-current names, marks, logos, and other identifiers for the Log 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 Log Services; and (b) upon termination of these terms and conditions 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 section 8.7.1 anywhere in the world, whether during or after the Term 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 section 8.7.1 or any application or registration therefore, whether during or after the Term.

8.7.1.6 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 Services 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 Log 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.

8.7.1.7 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 Log Services, 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.

8.7.1.8 During the Term, 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.