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 (as defined below) to provide a comprehensive MDR service. 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 is 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:

- "**Client Data**" means, unless otherwise defined in the Agreement, (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, except to the extent such reports contain intellectual property of eSentire.
- Overages
- "**Atlas Platform**" means eSentire XDR platform which consolidates all data and drives workflow for all eSentire MDR services.
- "**Insight Portal**" means the Client interface into the Atlas Platform, where eSentire provides Client service overview, detailed threat case reporting and/or event summaries.
- "**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.
- "**Indicators of Compromise (IOCs)"** means distinctive elements of data used to detect potential security breaches or malicious actions.

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 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);
- 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;
- 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. Details around retention of Client Data can be found in section 8 below. Telemetry sources include:

4.1. Endpoint (referred to on the Order Form as "Endpoint Services")
eSentire will collect in-scope Client endpoint data leveraging the eSentire Agent (an "**MSSP**" solution). License requirements and support model are described below.

4.2. Log (referred to on the Order Form as "Log Services")
eSentire will leverage Client log data and will perform real-time analytics on up to 5 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 MDR services. The Package includes a MSSP log solution whereby eSentire is the license holder.

4.3. Network (referred to on the Order Form 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 whereby eSentire is the license holder. Client will be required to install eSentire network sensors to capture a TAP or SPAN of network traffic. 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).

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.

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 3 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 8x5 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 thorough 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 complete 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 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: eSentire will procure all required licensing directly with the third-party provider of the applicable solution (each a "**Product Publisher**"); eSentire will be the licensee of record with each Product Publisher; and eSentire will manage any such licensed solutions provided by third parties. 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 all eSentire packages, including 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 MDR 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 Services.
- Client should communicate and coordinate any required changes to the Client network or other component required for the MDR services to be delivered, prior to making any changes.
- Client may be provided with a level of administrative access to MDR 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 MDR 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 MDR Services may impair eSentire's ability to provide the MDR Services. 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 MDR Services or (ii) liability for the failure to provide such MDR Services.

8.2. MDR Service Level Objectives ("SLOs"). eSentire measures a set of internal objectives that apply to all eSentire 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. Data Storage. <need intro here>

At the end of the Service Term ALL DATA is destroyed

Technology/Component	Data Type	Term
Atlas Platform	Incidents, Work Items, Threat Cases and associated collected data	Service Term
Sumo Logic Atlas Log	Log Data	365 days during the Term additional log retention up to 5 total years can be purchased
Tenable	Vulnerability Data	365 days
CrowdStrike	endpoint telemetry and EDR alerts	EDR Alert / Metadata 365 days Raw Telemetry 15 days (when eSentire owned instance, under Client license, retention defined by Client)
Atlas Agent (co-deploy or EDR)	endpoint telemetry and EDR alerts	Service Term

8.5 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 pursuant to a package, 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 service 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 24x7x365, 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 AICPA 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.

If Clients environment exceeds this threshold for two or more months eSentire will initiate a discussion about rightsizing either the deployment or the contract. Entitlements for alert volumes, number of network users monitored, bandwidth processed by network sensors and total log volume ingested and analyzed are calculated from this number of Endpoints value based on observed usage and averages across the eSentire customer base (see "Fair Use" below). Fair Use – eSentire reserves the right to limit data volumes of captured network traffic and log data collected to reasonable amounts linked to the number of Endpoints in scope. Entitlements of network and log volume are calculated as ample for the 90th percentile of existing eSentire customers' usage. eSentire will not charge retroactive "overage" fees and will not implement any modifications or filters without consultation with the client.