Service Description:
Incident Response Readiness Service

1. Service Overview

eSentire's Incident Response ("**IR**") Readiness Service ("**IR Readiness**" or the "**Service**") is a planning and preparation service during which eSentire will assess Client's IR readiness, identify potential barriers, and work with Client to optimize a future incident response. The Service includes a) a walkthrough of the eSentire IR process, b) the collection of key configurations, architecture, and services information, c) the creation of templates for Client to expedite administrative tasks, d) guidance on proactive log configuration, and e) forensic tool deployment/staging. The Service also includes the deployment of eSentire Agents (defined below) to collect critical forensic artifacts on a rolling seven-day window to provide eSentire Incident Response personnel with data to enable rapid incident response if an investigation is subsequently and separately requested by Client and contracted for with eSentire.

2. Service Definitions

Capitalized terms contained in this Service Description are as defined below or herein:

"**Agent**" refers to eSentire digital forensics agents**.**

"**Incident Response**" or "**IR**" means an organization's process of reacting to information technology ("**IT**") threats such as a cyberattack or security breach.

"**Insight Portal**" is a web-based portal managed by eSentire, and during the Service Term, Client will be provided with access for secure document exchange and collaboration.

"**PCI**" is "**Payment Card Industry**," data associated with payment processing.

"**PHI**" is "**Protected Health Information**," data created in the delivery of health care.

"**RACI**" is a matrix of tasks and functions identifying the parties Responsible, Accountable, Consulted, and Informed of each item.

3. Service Capabilities

The Services include the following:

3.1 Service Initiation. Following the Order Form - Service Commencement Date, and annually for each Renewal Term thereafter, eSentire will schedule a kick-off call with Client to collect necessary information for Service setup ("**On-boarding Call**"). eSentire will also provide Client a scoping document to complete ("**Assessment Questionnaire**"), which is used to collect information related to Client's environment. eSentire will work with Client to gain an understanding of key configuration, architecture, and other information which may include the identification or collection of some or all of the following:

- Client repositories containing Client intellectual property and regulated data,
- complete list of all Client endpoints, servers, and IP addresses,
- log sources relevant to IR (to allow for optimization guidance as applicable),
- all ingress/egress points and public IP addresses,
- forensic tools that are deployed currently in Client environment,
- Client documentation outlining current IR processes and timelines,
- any special considerations, and
- patch levels on Client key servers and applications where possible.

Following the On-boarding Call, eSentire will work with Client on the following additional Service elements:

3.1.1 Readiness Assessment (the "**Assessment**").

Using information collected pursuant to the activities in section 3.1 above, eSentire will perform a Readiness Assessment of Client's preparedness for an IR event. eSentire will begin to schedule and identify requirements for this Assessment during the On-boarding Call with Client. The Assessment will include a review of information provided by Client and contained in the Assessment Questionnaire. eSentire will interview Client's internal team to understand the rules and policies that have been implemented throughout their environment and provide guidance on cyber security essential practices. Information will be evaluated by eSentire, and eSentire will review the results of the Assessment with Client and guide Client on the most efficient and practical actions that can be taken in the event of a security incident. The results from this Assessment will provide Client with information that will assist and expedite IR processes reducing time lost to negotiation, administration, onboarding, and forensic tool deployment when responding to an active threat. In addition to the results of the Assessment, eSentire will use the findings from this Assessment, to create an IR process RACI matrix slide, an IR engagement process and workflow slide, and a cyber investigation order form (further described below), each of which will be reviewed with Client and posted to the Insight Portal.

The cyber investigation order form listed above, is a a sample contract, signable in the event of a security incident (the "Cyber Investigation Order Form"). The Cyber Investigation Order Form will include a general scope a cyber investigation, a pre-set hourly rate, payment terms, terms and conditions, and an expiration date/sign by date. The Cyber Investigation Order Form created and provided by eSentire may be used by Client in the event of a cyber related emergency and will only be acted on if signed by Client by the expiration date. Client will have the opportunity to review the Cyber Investigation Order Form and seek internal pre-approvals, so that Client may sign urgently if emergency incident support is required. Client pre-approvals may include seeking review from Client's executive team, Client counsel, and/or insurers, for example. The final Cyber Investigation Order Form will also be stored in Clients Insite Portal instance, for easy access/use. After the expiration date on the Cyber Investigation Order Form, information contained in the document is subject to change, and a new Cyber Investigation Order Form will be required.

All Assessment activities described in this section will run for a period of no longer than 90 days following the On-boarding Call and will be limited to five hours of eSentire support. If the Assessment activities are not completed within 90 days (following the On-boarding Call) due to Client delays, the Assessment will be considered complete.

3.1.2 Cyber Threat Intelligence.

eSentire will provide Client with summarized threat intelligence from the eSentire Threat Research Unit (TRU) Threat Intelligence brief at a cadence determined by eSentire. Threat intelligence is not specific to any one customer, but instead is based on relevant threats to the eSentire customer base.

3.1.3 Insight Portal Access.

eSentire will provide Client with access to the eSentire Insight Portal. The Insight Portal is the primary Client interface to access the eSentire Agent installation files and to monitor the health/connectivity of the Client's installed eSentire Agent base. The Insight Portal also provides generalized threat information extrapolated from the overall eSentire client base, provides a ticketing system for service inquiries, and offers a file repository in which documents related to the Service will be stored.

3.1.4 eSentire Agent.

eSentire will provide Client installation files and instructions for installing the eSentire Agent via the Insight Portal. Up to 50 eSentire Agents are included with the Service, however, Client may purchase additional Agents up to a maximum of 3,500 total Agents (pursuant to a signed order). Client will be responsible for deployment of the Agents by using the installation instructions. During the Service, the eSentire Agent is not being used as a monitoring tool, nor is it being used as a breach prevention tool; rather, for the purposes of this Service the tool is providing ongoing collection of forensic artifacts which can be used to support IR activities (per a signed Cyber Investigation Order Form). Data collected as part of this Service includes process monitoring, network metadata monitoring, and/or login/logout monitoring functions and is used to enhance a subsequent IR activity. Under normal operation of this service, there is no collection of PCI/PHI data. The Service will capture the aforementioned telemetry and retain this collected data for a rolling seven-day window, and such information is for use by the eSentire team if engaged by way of a Cyber Investigation Order Form. Further details on the Agent are as follows:

- **Self-Service Install**. Client will access the Insight Portal to download binaries and installation instructions to deploy eSentire Agents to its in-scope endpoints.
- **Data Capture**. From in-scope endpoints, the Agent will collect system information such as IP addresses, logged in users, running processes, and other data points critical to response activity. Such telemetry data will be securely transported to and stored by eSentire to be used in analysis and investigation during a separately contracted IR activity.
- **Data Retention.** Telemetry data gathered will be retained for seven days. All data transported to eSentire for storage is subject to eSentire’s administrative, physical, and technical safeguards. Client Data is encrypted in transit and at rest. The data storage platform is a multi-tenant platform, and all Client Data is logically separated from the data of other clients. Upon expiration or termination of the Service, Client Data in the eSentire environment is securely destroyed or allowed to expire per standard retention policies while remaining under standard safeguards.

4. Deployment

4.1 Installation. Client shall be responsible for the installation of the eSentire Agent on in-scope endpoints, pursuant to the information provided to them and further defined in section 3.1.4 above.

4.2 Service Renewal & Turndown. Following the initial Contract Year, in the event Client renews the Service, Client will be responsible for reviewing and providing eSentire any updates to the Assessment Questionnaire, and eSentire will review the updated results with Client. If Services do not renew, all data, including delivered documentation and data collected through the eSentire Agent will be deleted within thirty (30) days of Service expiration or termination.

5. Maintenance & Support

eSentire will be responsible for providing updates to the eSentire Agent. Notification of updates will be issued at least two weeks prior to Agent updates being pushed out to endpoints in the Client environment. Installation cadence of updates may be selected by Client to include automatic updating or manual updating by Client. Updates requiring reboot or other disruptions to the host endpoint will be scheduled with Client.

6. Service Level Objectives

There are no Service Level Objectives or Agreements as part of this service.

7. Responsibilities

7.1. Client Responsibilities. Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the Service is dependent upon Client’s compliance with the obligations hereunder. In the event Client fails to perform its obligations herein, in the time and manner specified or contemplated below, or should any obligation set out herein with respect to the Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages. Client responsibilities include:

- Completion of the Assessment Questionnaire within 30 days of the On-boarding Call, or 30 days from the start of any Renewal Term as applicable.
- Providing availability for, and attending, the On-boarding Call and any Assessment meetings.
- Installation of the eSentire Agent on all in-scope endpoints.
- Timely cooperation and engagement as necessary.

8. Service Terms

8.1. Exclusions. This Service prepares both Client and eSentire's IR team for quick response during a Client IR event (following a separately signed Cyber Investigation Order Form). The Service does not provide Emergency Incident Response, including but not limited to, forensic investigation, recovery support, litigation support, disaster recovery, or business continuity planning, and/or the quantification of the business impact, with respect to all Client assets, whether currently under embedded Incident Response or not. Such services are available pursuant to a separately executed order.

NOTE: If Client is experiencing a security event or breach and chooses to initiate Incident Response services, Client should call 1-866-579-2200 and select the option for "Emergency Incident Response." Emergency Incident Response Services will only be provided pursuant to a separate Cyber Investigation Order Form.