Insider Services

In this "**Services Description**", capitalized terms used and not otherwise defined shall have the meanings given in the Terms and Conditions ("**Terms and Conditions**"), and any capitalized terms used in this Services Catalogue that are not defined in this Services Catalogue or the Terms and Conditions will have the generally accepted industry or technical meaning given to such term.

1. STANDARD MAINTENANCE and SUPPORT

If Client is provisioned with eSentire Equipment, eSentire shall maintain the hardware and software for all eSentire-provided devices including appliances. eSentire will ship replacements of failed components the next business day with priority express shipping, 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.

eSentire shall provide support to Client for both security and system issues related to eSentire Equipment. eSentire will communicate with Client's IT personnel by the following methods:

Email Support. Email support is provided by the SOC on a 24x7x365 basis for inbound enquiries by Client. Email response is provided in accordance with the severity level of the incident or inquiry. The eSentire incident response email address is:

Method	Contact Information	Location
Email	esoc@esentire.com	Worldwide

eSentire SOC initiates outbound email alerts following detection of security events within the Client network. Alerts are escalated in accordance with the severity level of the incident.

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.

If a ticketing system is in use by the Client's IT group, a ticket number should be included in communications with eSentire so that eSentire can reference the Client's ticket number in the eSentire ticket.

Escalation Process. During initial deployment, the parties may agree upon the terms and conditions of appropriate attack/risk/response levels in writing from time to time. Notification/response process will be determined according to Client's requirements and will be agreed upon in writing by the parties. For example, if an active and serious attack occurs outside business hours, Client must be available for consultation. In such a case, eSentire will define appropriate actions based on factors such as level of attack sophistication and risk, during specified time periods, and will provide an opinion to Client's organization as to the best response. eSentire will also provide advice with respect to the hands-on level of incident management required. In the event that Client requires implementation of any response strategy to be performed by eSentire, such implementation terms, conditions and rates will be agreed upon in writing in advance and additional fees will apply.

2. Insider Services

Definitions

"Software" means eSentire's applicable software-as-a-service product hosted and co-managed by the Client and eSentire to which Client is provided access. Insider means the Software and any related documentation, information, technical assistance or training provided by eSentire to Client pursuant to this Insider Addendum ("Insider Services" or "Services").

"ThreatCases" mean maps of potential adversary campaigns unfolding inside a network that highlight elevated business risk.

Services Description.

Insider Service is a managed service that allows adversary campaign detection. The Services generate ThreatCases, which are maps of potential adversary campaigns unfolding inside a network that highlight elevated business risk based on the automated analysis of internal network data including flow and variants thereof. With the identification of multiple hosts and various behaviors linked into a single narrative, the gap between identification and response is dramatically shortened, reducing the potential damage that can be inflicted by sophisticated adversaries. eSentire will provide access to Insider's user interface, in which network coverage information and ThreatCase reports are available for review and response.

The Insider Services are configured to generate ThreatCases within its console, allowing the Client to monitor alerting and activity at any time.

eSentire will also provide any related documentation, information or training reasonably necessary to the Client in order to evaluate and use the Services.

eSentire will be responsible for providing the initial installation, configuration and ongoing maintenance of the Insider, as well as interpretation of the output from time to time as part of the Insider Services.

Premises

The Services shall be hosted by eSentire within a Client-specific AWS subaccount. Depending on technical requirements, the Client may be responsible for deploying and managing services or systems, including but not limited to data collection machines. The Services may be accessed by Client from within the United States and from other jurisdictions reasonably necessary for Client to use the Software. The Services will be accessed by eSentire personnel for initial installation, configuration, ongoing maintenance, and interpretation of the output.

The Services are configured to generate ThreatCases within its console, allowing the Client to monitor alerting and activity at any time.

Support

In addition to the Standard Maintenance and Support, eSentire provides security reviews and support by its Insider Threat Review Team and technical support via telephone and online, from its Seattle, WA, USA location between 9AM and 5PM PT Monday through Friday excluding holidays.

eSentire is willing to schedule calls outside of those hours to accommodate Client scheduling preferences.

Exclusions. The Insider Services exclude the design, creation, maintenance, and enforcement of a security policy for Client.

Access. eSentire will not attempt to access Client's servers without express written or verbal consent.

Client Responsibilities. Client is responsible for:

- any and all data and systems which Client grants access to for receipt of the Insider Services;
- obtaining all necessary licenses, permissions and consents to enable eSentire to access the Client's network and servers in order to provide the Insider 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 Insider 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 Insider Services;
- communicating all network infrastructure changes to eSentire so that the Services can be configured. eSentire is not responsible to provide network hardware required to acquire flow data and has no liability or responsibility in the event of inability to acquire flow logs from the Client's network.
- notifying eSentire of any change or contemplation of change to its network in advance of or within four (4) hours following such change. In the event that the client fails to notify eSentire then eSentire is released from any and all obligations of the Services to effectively make detections in the Client's network.

In event Client fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption outlined herein with respect to the Insider Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages. For the avoidance of any doubt, the Client will be using the Services for its internal business purposes only.

Reports and Confidentiality

The Insider Services will generate reports within its console related to the detections it has made. Except for the purpose of fulfilling eSentire's obligation under this Insider Addendum, eSentire shall not disclose the information derived to any party for any purpose without express written consent from the Client. All Client information is bound by the Confidentiality provisions set out in the MSSA.