eSENTIRE

Insider Services

1. Definitions

"Software" means eSentire's applicable software-as-a-service product hosted and co-managed by 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 as described herein.
"ThreatCases" mean maps of potential adversary campaigns unfolding inside a network that highlight elevated business risk.

2. Services Description

The Insider Service (the "Service") is a managed service that allows adversary campaign detection. The Service generates threat cases, 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 (each a "Threat Case", as used in this document only). 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 a user interface, in which network coverage information and ThreatCase reports are available for review and response.

The Insider Service is 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 Client in order to evaluate and use the Service.

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

3. Premises

The Service 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 Service may be accessed by Client from within the United States and from other jurisdictions reasonably necessary for Client to use the Software. The Service will be accessed by eSentire personnel for initial installation, configuration, ongoing maintenance, and interpretation of the output.

4. Support

In addition to the Standard Maintenance and Support described on the eSentire Service Catalogue main page, eSentire will provide Client security reviews and support, and technical support via telephone and online, from its Seattle, Washington 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.

5. Exclusions.

The Insider Services exclude the design, creation, maintenance, and enforcement of a security policy for Client. MDR Service Level Objectives do not apply to this Service.

6. Access.

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

7. 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.
- Choosing 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.

8. Reports and Confidentiality

The Insider Service will generate reports within the Service console related to the detections it has made. Except for the purpose of fulfilling eSentire's obligations described herein, 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 terms and conditions executed between Client and eSentire.