Managed Vulnerability Service – Managed Only

1. Services Description.

Managed Vulnerability Service – Managed Only ("**MVS**" or "**Service**"), is an eSentire managed only service where eSentire assists the Client with vulnerability scan-management and reporting utilizing the Clients Tenable.io Vulnerability Management license instance and platform, to deliver vulnerability reports to the Client. eSentire will provide Services on the number of assets they identify on the Order Form. For the purposes of this Service, an asset is a client endpoint which may include Client owned laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances ("**Assets**").

For this Service, Client must procure and maintain a Tenable.io Vulnerability Management license (the "**License**") with Tenable, Inc. (the "**Product Publisher**"), during the entire Term of the Service, and coordinate proper licensing permissions with the Product Publisher to allow eSentire full administrative access and credentials into the Client's License instance. Client will retain ownership of the License, and will continue to have all access to utilize their License, however, Client acknowledges and agrees that any changes made by the Client in the Licensed environment could negatively impact eSentire's ability to deliver the Services, and any changes made by Client during the term of this Service should be reviewed with eSentire, otherwise eSentire shall be released from any and all obligations to effectively provide the Services as contemplated herein.

MVS includes the following capabilities:

- Vulnerability Scanning. Utilizing Clients Licensed instance, eSentire will perform external scans weekly, and internal scans monthly on Client Assets (including cloud-hosted and on-premise assets), and agent-based scanning, to help identify Client's vulnerability posture and allow Client to guide network/system configuration and controls. Client also has access to their platform to define and direct their own scanning in cooperation with eSentire. The number of Client Assets included in the Service will be identified on the Service Order Form and should match the exact number of Client Assets included in the Clients License with the Product Publisher. eSentire reserves the right to adjust the fees charged to Client, should the number of Licenses exceed the number of Assets identified on the Service Order Form.
- Vulnerability Reporting and Trending. Various reports for external and internal findings are sent by eSentire to Client following each scan conducted above. eSentire may also direct Client to reporting platform portal to receive vulnerability reports in addition to or instead of providing scan report findings.
- Monthly Review. Client may request a review of the findings provided in the reports, up to one time per month, to review the findings of the scans conducted during the month prior. Each review requested will be scheduled, conducted remotely with eSentire, and will not exceed one hour.
- Ad-Hoc Vulnerability Scanning. Client may also direct their own ad-hoc vulnerability scanning via their vulnerability scan-management and reporting portal, provided such scanning does not unduly interfere with eSentire delivery of the MVS or other eSentire supplied services.
- Supported Tenable products. Currently only Tenable.io Vulnerability Management is supported.

2. Sensor.

Client is responsible for providing/provisioning at least one physical or virtual security appliance ("**Sensors**") to the extent required to facilitate the Service, typically one per location. If the Sensor(s) do not meet the requirements for facilitating the Service, Client will be responsible for the costs associated with adequate provisioning, as determined by eSentire. If Client has network sensors supplied by eSentire, for alternate active services, these sensors, at the discretion of eSentire, may be used to facilitate this Service.

3. Client Responsibilities.

In the 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 Service fail to be valid or accurate, then eSentire will not be responsible for

any related delay or damages. Non-compliance with these obligations may result in suspension of the Services. Client is responsible for:

- Maintaining the License during the entire Term of the Service and coordinating proper licensing permissions with Product Publisher to allow eSentire full administrative access and credentials into the Client's Licensed instance.
- Providing the necessary resources, information, documentation and access to personnel, data, equipment, systems and scanning schedules, as reasonably required by eSentire, to allow eSentire to perform the Services.
- Obtaining all necessary licenses, permissions, and consents to enable eSentire to access Client Assets, and Client networks and/or servers (as necessary), in order to provide the Service, including providing any third-party permissions as required.
- Designating a Client project coordinator to work directly with and serve as the primary Client contact with eSentire for the duration of the Service.
- Providing eSentire a complete copy of Clients security (including privacy) policies, as available. Client is solely responsible for the creation, maintenance, and enforcement of its security policies to protect the security of Client data and systems.
- Notifying eSentire of any change or contemplated change to the Client network, that may impact the Service, in advance of Client effecting such change.
- Advising eSentire of Asset changes, or other changes that may impact Service scoping. For the avoidance of any doubt, any material changes to the Client Asset count including overages that are greater than a five percent (5%) increase to the contracted number of Assets, in any sustained manner greater than 30 days, may incur additional costs at the then-current Service rate and shall be calculated by eSentire and billed to Client minus any newly applicable volume discount.
- Ensuring all owned and operated infrastructure (including any Sensors or Agents) related to the facilitation of the Service is kept updated, secured, and protected.

4. Exclusions. MVS excludes the following:

- All issues related to the License, including access to, and issues related to the License or use thereof. Client shall work with the Product Publisher directly for any such issues.
- The design, creation, maintenance, and enforcement of a security policy for Client.
- MVS is an eSentire Managed Risk Service, however, any terms provided at the Managed Risk Service summary link, will not apply to this Service Description.
- eSentire attempting to access Client's servers without Client's express written or verbal consent.