eSENTIRE

Managed Vulnerability Service

Service Overview

eSentire's Managed Vulnerability Service (the "Service"), is an eSentire service which provides Client with visibility and management of security vulnerabilities across the Client's information technology ("IT") environment. The Service leverages a vulnerability management license (the "Platform") (options detailed below) with Tenable, Inc. ("Tenable" or "Product Publisher"). The Services are delivered on the number of Client assets detailed on the Order Form. For the purposes of this Service, an asset is an endpoint which may include Client-owned laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances ("Assets"). The Service is scoped/sold using the number of Client-provided Assets, and the quantity is detailed on the Order Form using a unit measure of "Asset". For the avoidance of any doubt, any material changes to the Asset count including overages that are greater than a five percent increase to the number of Assets identified on the Order Form for a period greater than 30 days may may incur additional costs calculated by eSentire, inclusive of updated license pricing and volume discounts. 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.

1. Definitions

In addition to the below, capitalized terms contained in this Service Description are as defined herein. • "Customer Success Manager" or "CSM" means eSentire resources that provide Client with ongoing support and relationship management to drive value and maximize benefits of eSentire's Services. • "Insight Portal" means the Client interface into the Atlas Platform, where eSentire provides Client summary and detailed reporting and/or event summaries.

2. Service Capabilities

The Service includes the following capabilities:

2.1 Vulnerability Scanning. eSentire will perform external scans weekly, and internal scans monthly, on the in-scope Assets. Client has the ability to define and direct their own scans within the Platform, in cooperation with eSentire, however, Client shall not interfere or otherwise modify agreed scanning policies and scan frequencies as defined by eSentire and shall not utilize Platform access in a manner that adversely affects the delivery of the Service without prior written consent by eSentire.

2.2 Vulnerability Reporting. Following each eSentire-scheduled vulnerability scan (identified above), results are validated, and findings are captured in various vulnerability reports provided to Client via the eSentire Insight Portal. Additionally, Client will be notified of newly identified critical, externally facing vulnerabilities.

2.3 Remediation Guidance: eSentire will provide remediation guidance to Client, which will include actionable insights to help address identified vulnerabilities, as well as recommendations with respect to prioritizing and implementing effective remediation strategies.

2.4 Critical Asset Identification (TenableOne Subscription option only). Assets are inventoried and prioritized based on indicators of business value and criticality.

2.5 Asset Risk Score (TenableOne Subscription option only). Asset risk is quantified based on level of criticality (or impact) to the business and likelihood factors that indicate breach probability.

2.6 Monthly Review. Client may request a meeting, up to one time per month, to review the findings and remediation guidance for the scans conducted during the month prior. Each review requested will be scheduled in advance and conducted remotely.

2.7 Ongoing Support. Client must open a support ticket (via the Insight Portal) to contact a member of the eSentire team for assistance with the following issues:

2.7.1 Scan Management:
- Rescheduling failed and/or prolonged scans
- Optimizing existing scans
- Scanning new or sensitive infrastructure
- Custom scan policies for zero-day/high priority vulnerabilities
- Creation of target groups/tags
- Recasting (changing the severity) of vulnerabilities

2.7.2 Environment Changes:
- Addition/removal of subnets
- Installation of cloud scanners for vulnerability scanning
- Changes to credentialed scans/agent deployments

2.7.3 General Support:
- Creation and scheduling of reports
- Unexpected network and system impact
- Vulnerability management platform-specific issues (features, functionality, etc.)

3. Subscription Options

3.1 Subscriptions. Client has the ability to order the Service leveraging either:

a) a license to the Tenable.io Vulnerability Management module, or

b) a license to TenableOne Vulnerability Management (each a "Subscription").

The Subscription selected is detailed on the Order Form. Each Subscription option includes the features detailed in section 3 above (unless otherwise stated). Additionally for each Subscription option, Client may request the optional offerings listed below (the "Options"), and if included in the Service, additional fees will apply, and such Option will be listed on the Order Form:

3.1.1 Quarterly PCI Attestations: With this Service Option, eSentire will submit external scan results from this Service only, to the approved scanning vendor for PCI-ASV attestation. Such scanning shall be performed once per calendar quarter, provided it is Client's sole responsibility to request that scan results are submitted for ASV certification as needed. This Service option is sold on an annual basis (as a fixed price per year).

3.1.2 Web Application Scanning ("WAS"): With this Service Option, eSentire will scan external facing web applications for known vulnerabilities to determine Client's web application posture and allow Client to guide web configuration and controls. Client can also leverage Client's access to the Platform to define and direct their own scanning in cooperation with eSentire. This Service option is ordered on a per URL basis.

3.2 Third Party License Requirements. Client may request each Service Subscription to be provided by eSentire in one of the following delivery methods: a) as a co-managed service with bundled licensing ("MSSP"), or b) in a managed only capacity ("Managed Only"). This selection will be detailed on the Order Form. Licensing requirements for each are detailed below:

3.2.1 MSSP Licensing requirements: In this Service delivery option, eSentire will procure all required licensing directly from Product Publisher, will be the licensee of record with Product Publisher, and will provide management. eSentire will provision a dedicated instance of the Platform, leveraging Asset details provided by Client up to the total number of Assets identified on the Order Form. Additionally (if required), eSentire will provide at least one physical or virtual security appliance (a "Sensor") as specified on the Order Form. eSentire will configure and remotely manage the Sensor and its embedded software. Client may only access the configuration of such Sensor with eSentire's prior written authorization. As part of this license, eSentire may grant Client enhanced access into eSentire's license instance, and if so granted, Client acknowledges and agrees that any changes made by Client in the licensed environment could negatively impact eSentire's ability to deliver the Services.

3.2.2 Managed Only Licensing requirements: In this Service delivery option, eSentire will manage Client's Tenable licensing, which has been procured by Client. Client must procure and maintain its licensing ("License") with Tenable, during the entire Service Term, and coordinate proper licensing permissions with Tenable to allow eSentire full administrative access and credentials into Client's License instance. Client must purchase one of the following licenses (as applicable) in order to receive the Service in a Managed Only capacity from eSentire:

• Tenable.io Vulnerability Management, or

• TenableOne - Vulnerability Management module In the event Client's managed only order includes one of the Service Options described in section 4.1 above, the following License is required (as applicable, and must match the Vulnerability Management licence type above):

• Tenable.io Quarterly PCI Attestations license, or TenableOne Quarterly PCI Attestations, or

• Tenable.io Web Application Scanning license, or TenableOne Web Application Scanning Module In addition to the licensing required above, in a Managed Only delivery model, Client is responsible for providing/provisioning at least one Sensor 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, then such sensors may be used to facilitate this Service at the discretion of eSentire.

3.2.3 Other Tenable Licensed Offerings: In the event Client has ordered the TenableOne Service Subscription in an MSSP support model (for certainty, this does not apply to Tenable-io Subscriptions nor to Managed –Only Subscriptions), Client may order additional TenableOne licensed modules from eSentire outside of those included in or required or supported by the Service ("Add-Ons"). 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. 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. Client can request assistance with such MSSP Add-ons from eSentire, and eSentire will open a ticket with Product Publisher.

Add-Ons are made available by eSentire to Client on an "as-is" basis and eSentire specifically disclaims all representations and warranties with respect to Add-Ons, express or implied, including the implied warranties of merchantability, operability, and fitness for a particular purpose. With respect to either option above, eSentire does not provide the setup, configuration, and/or management of any Add-On.

A list of available TenableOne License modules/Add-Ons are as follows:

- Attack Surface Management
- OT Security
- Identity Security
- Tenable Patch ManagementFor any Service option, Client acknowledges and agrees that any changes made by Client in the licensed environment could negatively impact eSentire's ability to deliver the Services. In addition, Client acknowledges and agrees that 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. Throughout the Service Term, Client must provide and eSentire must maintain administrator or equivalent access which enables eSentire staff and systems to execute the tasks included in this service description. Access will only be provided to select, authorized eSentire employees and will be audited.

4. Client Reponsibility

With respect to the Service, Client is responsible for:

- Any and all data and systems to which Client grants access for the Service;
- Obtaining all necessary licenses, permissions, and consents to enable eSentire to access Client's network and servers in order to provide the Service, including any third party permissions as required;
- Designating a Project Coordinator to work directly with and serve as the primary Client contact with eSentire for the Service Term;
- Providing eSentire with a complete copy of its 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 its network in advance of Client effecting such change;
- Advising eSentire of network and Asset changes.

With respect to WAS, in addition to the above Service responsibilities, Client shall also be responsible for:

- specifying one valid web application address/port for each web application being scanned. Each additional web application being scanned will be billed to Client minus any newly applicable volume discount; o accessing WAS service reporting via the Platform; and
- conducting and remediating identified risks and vulnerabilities for each respective web application.

With respect to Quarterly PCI Attestations in addition to the above Service responsibilities, Client shall also be responsible for:

o being proactive towards the remediation of discovered vulnerabilities, contacting eSentire ahead of submission deadlines and in responding to communications regarding PCI compliance;

o providing all documentation required for their PCI compliance submission a minimum of three weeks before submission, providing updates as required, until documentation is formally submitted; and

o requesting one scan per calendar quarter so that eSentire submits external scan results to the approved scanning vendor for PCI ASV validation and certification. It is Client's responsibility to request that scan results are submitted for ASV certification as needed.

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 Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages. If Client fails to notify eSentire of network changes as contemplated above, then eSentire shall be released from all obligations to scan Client's network until Client has notified eSentire of such change.

5. Exclusions

These Services exclude the following:

- The design, creation, maintenance, and enforcement of a security policy for Client;
- Support for third party API integrations;
- Tenable compliance and audit file library support;
- Patching of vulnerable devices; and
- Vulnerability and exposure management program development and implementation.