Service Description:
Dark Web Monitoring

1. Service Overview

eSentire's Dark Web Monitoring (the "**Service**") is an exposure management service, which continuously searches the clear, deep, and dark web for Client information, indicating potential exposure. Service deliverables and findings are provided to the Client at a method and cadence determined by the service tier selected by Client, further described herein and identified on the Order Form (the "**Service Tier**").

2. Service Definitions

Any capitalized terms contained in this Service Description are as defined in the Order Form, below or herein:

"**Dark Web**" means the part of the Deep Web that requires specific software or authorization to access.

"**Deep Web**" are internet sites which are not indexed by search engines, generally due to technical restrictions put in place to prevent indexing, are password protected or require specific software to access.

"**Clear Web**" means the section of the internet that is publicly accessed and includes sites that are indexed by a search engine.

"**Compromised Credentials**" means login information, such as usernames and passwords, which have been stolen or improperly obtained and are available for sale or use.

"**Insight Portal**" means the Client interface into the Atlas Platform, where eSentire provides Client summary and detailed reporting alert and event summaries. Client may be provided access to the Insight Portal depending on other eSentire Services Client has purchased.

"**Monitored Data**" is Client-specific information which will be monitored as part of the Service, which is determined by the Service Tier ordered.

3. Service Capabilities

3.1 Service Onboarding. During Service kickoff, Client will meet with an eSentire project manager, who will be responsible for scheduling, tracking, and driving the installation and configuration of all elements of the Service ("**Onboarding Manager**"). In order for eSentire to configure the Service, Client will be required to provide eSentire Monitored Data, which can be provided to eSentire by Client either within a Service onboarding worksheet ("**Worksheet**"), or within the Insight Portal. For the Credentials Only Service Tier, a completed Worksheet submission (or submission via the Insight Portal) will constitute the start of service. . For the One-time and the Advanced Service Tier, the service date begins when the Worksheet is submitted (or there is submission via the Insight Portal). Additional information may be gathered during a phone call between eSentire and Client, followed by initiation of the tuning phase.

3.2 Service Features. Following Service activation and during the Service Term, eSentire will regularly query Client-provided Monitored Data against a continuously updated database of clear, deep, and dark web data. If Client information is identified, the findings will be communicated to the Client as further detailed in Table 1 below (depending on Service Tier):

Table 1.

Monitored Data	Type of Notification	Service Tier
Email addresses from Client's domain and domains similar to Client's (typo squatting)	Report	One-time
Email addresses from Client's domain	Automated email and Threat Case	Credentials Only, One-time and Advanced
Domains similar to Client's (typo squatting)	Automated email and Threat Case	One-time and Advanced
Public facing IPs	Report	One-time and Advanced
Executive contacts	Report	One-time and Advanced
Third party vendors	Report	One-time and Advanced

In the event Client has separately purchased Managed Detection and Response (MDR) Services from eSentire, this information will supplement MDR service tasks as contextual information, such as investigations, response, and incident handling.

4. Subscription Options (Service Tiers)

The Service offers three service delivery options ("**Service Tiers**") which include: One-time, Credentials Only and Advanced. The features of each Service Tier and are as detailed below:

4.1 Credentials Only – Service Tier. This Service Tier includes:

- Automated alerts & Threat Cases for potentially Compromised Credentials;
- MDR service augment (if Client is subscribed to MDR services); and
- Quarterly change/update to Monitored Data.

4.2 Advanced – Service Tier: This Service Tier includes all features of the Credentials Only Service Tier, and the following additional features:

- Additional automated alert notifications and threat cases for:
  - typo-squatted domains; and
  - potential impersonation domains.
- eSentire will perform an investigation into alerts related to potential breaches ("**Breach Alerts**") and will escalate to Client if such Breach Alert is validated. Breach Alerts are defined as:
  - Shell/General/Initial Access Broker selling access – a threat actor is selling access to Client's infrastructure;
  - Ransomware mentions – ransomware group has mentioned Client organization on their site; and/or
  - Compromise of organizational data – a threat actor mentioned Client organization in a discussion of data compromise.
- eSentire will schedule call touchpoints at a cadence determined by Client user count, and on business days between 0800-1800 Eastern Standard Time (see Table 2 below for touchpoint cadence).
- eSentire will email reports (in a .PDF format), at a cadence determined by Client user count (see table 2 below for report cadence). Reports may include a summary of the following information (as applicable, and referred to herein as the "**Findings Report**"):
  - Initial Access Broker, ransomware, and shell access mentions;
  - Credentials being shared;
  - Access to organization being sold;
  - Compromised organizational data;

- Hackitivist targeting;
- Underground discussion of organization;
- Detection of open S3 buckets;
- Organizational content on GitHub;
- Relevant executive mentions;
- Relevant mentions of organization of external IP addresses on underground sites, open sources, new sites, social media/messaging platforms; and/or
- Relevant data associated with third party vendors.

Historical data will not be available for the following categories:

- Typo-squatted/potential impersonation domains; and
- Detection of open S3 buckets.

- Additional tuning and alterations to Monitored Data.

Table 2: Meeting, Report Cadence & Limitations for Advanced Dark Web Monitoring

Knowledge Worker Count (detailed on Order Form)	Cadence	Max unique domains	Max executive names	Max 3rd-parties
< 250	Quarterly	10	15	10
250-999	Quarterly	20	20	10
1,000-4,999	Monthly	30	30	20
5,000+	Monthly	50	50	20

4.3 One-time – Service Tier. This Service Tier is provided one-time, on a non-recurring basis, and will run for a period of 30 days. Over the 30-day period, eSentire will monitor Client-provided Monitored Data, provide auto-alerts for credentials, typo-squatted, and potential impersonation domains, and at the end of the 30-day period, eSentire will email a final report containing any findings (in a .PDF format). The findings in the report will provide same types of findings that would be provided in the Advanced Service Tier Findings Report. The max number of domains and executive names is the same as in Table 2 above.

6. Responsibilities

Client responsibilities include ensuring any changes to Monitored Data are communicated to eSentire in a timely fashion. In addition, a responsibilities matrix can be found at Appendix A.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Submission and Maintenance of Monitored Data	R	I
Detection of Client Monitored Data on Clear, Deep, and/or Dark Web	I	RA
Automated Notification	-	RA
Onboarding and Tuning	CI	RA
Initial Policy and Environment Configurations	CI	RA
Post-deployment updates	RA	RI

R = Responsible; responsible for action and implementation. Responsibility can be shared.
A = Accountable; ultimately answerable for the activity or decision. This includes “yes” or “no” authority and veto power.
C = Consulted; typically, the subject matter experts, to be consulted prior to a final decision or action.
I = Informed; needs to be informed after a decision or action is taken.