eSENTIRE

Managed Detection and Response ("MDR")

1. Definitions

In addition to the capitalized terms defined elsewhere in the Agreement, the following terms will have the meanings ascribed to them below for all eSentire MDR service offerings:

"Actionable" means a Work Item analysis has concluded that an alert or containment action is required, based on criteria established by eSentire and reviewed with Client.
"Alert" means an event that eSentire will escalate to the Client.
"Atlas Platform" means eSentire XDR platform which consolidates all data and drives workflow for all eSentire MDR services.
"Business Impact" means any quantification of the reputational, operational, compliance or financial impact to the Client's business.
"Dashboards" means third party technology dashboards, which for some MDR Services Client will have access to view additional reporting and/or event summaries.
"Disaster Recovery and Business Continuity Planning" means assessment, execution and/or building of disaster recovery and continuity planning processes and techniques. Used to help an organization recover from a disaster and continue or resume routine business operations.
"Embedded Incident Response" means where eSentire MDR will identify and contain the attacker (within the visibility and scope of the MDR service) and provide remediation guidance to the customer.
"Emergency Incident Response" means the rapid mobilization and deployment activities aimed at quickly securing Client systems and networks, providing incident response services beyond what MDR provides. Covers the full lifecycle of an incident - containing the full extent of the attack (across all attack surfaces).
"Forensic Investigation" means salvaging as much information as possible from the Client's systems and networks deemed in scope and regression analyzing that information to conclusively determine the full extent of compromised assets.
"Insight Portal" means the Client interface into the Atlas Platform, where eSentire provides Client summary and detailed reporting and/or event summaries.
"Litigation Support" means support, including but not limited to expert and fact witness testimony.
"Notification" means when eSentire notifies the Client via the Insight Portal and email, of an actionable Threat Case.
"Security Operations Center ("SOC")" means the eSentire team which provides 24x7x365 monitoring and reaction to identify, investigate, and where appropriate prevent or contain, threats that are identified as potentially threatening to Client.
"SOC Dashboard" means the eSentire SOC interface into the Atlas Platform.
"Threat Case" means an Actionable Work Item, which results in a notification or action required.
"Work Item" means a collection of one or more events and alerts collected by the Atlas Platform requiring analysis by eSentire SOC Analysts.

2. MDR Services

The eSentire MDR Services, and related Service Descriptions, which include descriptions of the subscription types available for each, can be found below:

- Endpoint Services - SentinelOne
- Endpoint Services - VMware Carbon Black
- Endpoint Services - CrowdStrike
- Endpoint Services - Microsoft

- Managed Detection and Response Services with Microsoft Defender for Office 365
- Managed Detection and Response Services with Microsoft Defender for Identity and Cloud Apps
- Cloud Services – IaaS
- Network Services
- Log Services – Sumo Logic
- Log Services - Sumo Logic – Managed Only
- Log Services - Azure Sentinel – Managed Only

3. MDR Service Level Objectives ("SLOs")

3.1 eSentire measures a set of internal objectives that apply to all eSentire MDR Services. For each SLO, a minimum of 20 Threat Cases must be processed during the month for the SLO to apply. These eSentire standards are further described below.

3.1.1 **Time to Engage ("TTE") – Work Item – SLO target 60 minutes.** The Service Level Indicator (SLI) time starts when a Work Item is created in the SOC Dashboard and ends when an eSentire SOC Analyst changes the state of the Work Item in the SOC Dashboard to "under review". A Work Item is marked "under review" in the SOC Dashboard, when analysis of the Work Item by an eSentire SOC Analyst has commenced. The analysis includes collecting evidence and creating assessment notes against the Work Item. The outcome or duration of the analysis does not impact the TTE SLO target.

3.1.2 **Time to Respond ("TTR") – Actionable Work Item – SLO Target based on Priority Level (Table 1).** As a result of the Work Item analysis described above, eSentire will determine if a Work Item is Actionable, and if so, will create a Threat Case. eSentire will then notify Client via the Insight Portal, and email, of any Threat Case. The SLI starts when a Threat Case has been created in the SOC Dashboard and ends when an eSentire SOC Analyst notifies the Client and provides the Client defined response remediation actions.

Table 1.

Priority Level	TTR SLO Target*
P1	10 minutes
P2	20 minutes
P3	40 minutes
P4	60 minutes
*SLO Target is measured as a monthly aggregate by priority level, taking into consideration all actionable Threat Cases from the previous month.	

The Priority Levels listed above are defined below in Table 2.

Priority Level	Description
P4 (Low)	Minor activity recorded but not alerted, and the presence of likely unwanted activity - for example, adware.
P3 (Medium)	Suspicious activity that might not be deemed malicious by itself, and malicious activity not known to be targeted.
P2 (High)	Malware event, tactics, techniques, and procedure events, or events indicating targeted attack with potential for widespread impact.
P1 (Critical)	Malware infection(s), virus infection(s), and lateral movement, or indications of targeted attack with a high potential to cause grave damage to critical assets.

Of note: eSentire objectives listed above may be impacted by short periods due to scheduled maintenance where updates, patches, are installed and configured (i.e., maintenance windows), or when hardware deployment or replacements are required.

4. Client Responsibilities

General Client responsibilities for MDR Services are listed below. Specific service responsibilities are contained within the applicable Service Descriptions. Client must comply with Client responsibilities in order for eSentire to meet its obligations and deliver MDR Services. Client Responsibilities are as follows:

- Client is responsible for all Client provided third-party equipment, software services, support, or vendors not under the control of eSentire.
- Client should respond to alerts and inquiries from eSentire in a timely fashion.
- Client should identify prior issues with Client's network to the eSentire team prior to MDR Services commencing (including any incidents, problems, errors, or other events subject to an open support ticket from a legacy or other third-party service provider).
- Client is responsible for implementing any recommendations or remediation advice provided by eSentire related to Client incidents, however, Client's decision to not implement any remediation recommendations may adversely impact eSentire's ability to deliver the Services.
- Client should communicate and coordinate any required changes to the Client network or other component required for the MDR services to be delivered, prior to making any changes.