eSENTIRE

Service Description:

Atlas MDR Professional Package

Overview

eSentire's Atlas MDR Professional Package (the "**Package**") is a managed detection and response ("**MDR**") solution that leverages the Atlas Platform to provide foundational cybersecurity protection including threat prevention, detection, and response. eSentire uses Client Data from sources within the Client Environment to provide essential MDR coverage. Specific elements of the Package are described in this service description, and the Package is scoped using the total number of Client employees ("**Employees**"). Employees are defined as those using IT services and in scope of eSentire MDR protection. The number of Employees included in the Client Package are detailed on the Order Form and subject to Overages.

Service Definitions

In addition to the below, capitalized terms have the meaning given to such terms in this service description. Capitalized terms used but not defined in this service description have the meaning given to such terms in the Master Security Services Agreement between eSentire and Client that governs this service description.

"Atlas Platform" means the eSentire security operations platform which consolidates all data and drives workflow for all eSentire MDR services, including those in this Package. All data on the Atlas Platform related to the delivery of the Package for Client is retained for the Term and deleted upon Package expiration.

"Atlas AI" means the Atlas agentic AI framework, designed to enrich and investigate alerts in the Atlas Platform.

"**Atlas UI**" means the user interface of the Atlas Platform where interaction with and configuration of the Atlas platform and MDR services is performed.

"Client" means the entity ordering the MDR Services described in this service description.

"Client Environment" means the Client systems from which Client Data is collected for the delivery of the Package.

"Indicators of Compromise" or **"IOCs"** means distinctive elements of data used to detect potential security breaches or malicious actions.

"MDR Services" means the endpoint services and other services included in this Package.

"Order Form" means an ordering document that specifies the eSentire services ordered by Client, including any amendments and supplements to such ordering document.

Package Elements

The Package consists of the following elements:

- Collection of log data from the Client Environment;
- Integration with security controls in the Client Environment;
- Atlas Endpoint Agent deployment for endpoint telemetry collection;
- Bring-Your-Own AV ("**BYO-AV**") endpoint support (Microsoft Defender AV);
- Threat detection and generation of findings
- SOC oversight with security investigation of alerts detected via the Atlas Platform;
- Endpoint Response;
- User reported pemail investigations;

- Threat Intelligence;
- Business Hours support from the eSentire Cyber Resilience Team; and
- Access to the Atlas UI for reporting and package features.

Launch & Optimization Services

Following receipt of a fully executed Order Form, a member of the eSentire Cyber Resilience Team will work with Client to begin Package onboarding activities, which will include:

- assigning an eSentire onboarding manager and scheduling the initial onboarding call;
- establishing the onboarding project plan;
- installing agents and connecting telemetry sources (including logs, enrichment and other data sources);
- configuring integrations to Client applications.

Client will also be provided with access to the Atlas UI which provides visibility over all subscribed eSentire services. The Atlas UI acts as a central hub for managing and monitoring security services, allowing Client to configure, integrate, and view eSentire Package elements. The Atlas UI includes self-service features such as telemetry integration, and service setup.

Telemetry sources are further detailed below. Client will be required to assist with accessing telemetry, installing applicable licensed software tools, and/or installing required eSentire Equipment.

Launch services will be scheduled with Cient and eSentire at a mutually acceptable time. The launch project plan will be jointly developed. Nominal project plans will consume 10 eSentire resource hours operating over 5 business days. Launch services will not exceed 15 eSentire resource hours or 15 business days.

Optimization services will continue at a regular cadence of quarterly configuration reviews, to be agreed upon during onboarding, not exceeding 2 hours per month.

Endpoint (BYO-AV)

Client must provide a supported antivirus ("**AV**") solution already deployed in the Client Environment. The supported AV solution for the Professional Package is Microsoft Defender AV. eSentire will assist the client in deploying the Atlas Endpoint Agent alongside Client's AV solution. eSentire Atlas Agent will be deployed to endpoints with the supported AV to deliver detection, investigation and response.

Package Deliverables

The following will be delivered to Client as part of the Package:

eSentire Atlas AI, SOC and Security Analysts

eSentire Atlas AI and security analysts operating in an eSentire Security Operations Center ("SOC") will utilize the telemetry gathered from the sources described above to perform detailed security investigations of indicators and alerts. Security analysts provide SOC oversight and monitoring to identify, investigate, and (where appropriate) prevent or contain potential threats. Investigations are delivered to the Client in the form of "Findings" in the Atlas UI.

Threat Detection

The Atlas Platform detects threats and suspicious behavior using detections generated by eSentire's Threat Response Unit and native detections from select technologies. The detections use a combination of traditional threat detection techniques, advanced analytics, machine learning and threat intelligence to detect threats.

eSentire continuously makes detection-tuning decisions based on the validity and relevance of alerts and security incidents. Detection alerts are subject to a spectrum of possible outcomes, including automated notification direct to Client, automated AI-led investigation and response, and/or human-led review and analysis by the eSentire SOC.

Endpoint

On endpoints where eSentire Atlas Agent is deployed alongside client-licensed AV (Defender AV), Atlas will monitor AV output as part of Threat Detection. Atlas Agent will collect additional telemetry for Threat Detection, and Agent will be used to deploy response capabilities.

Unlimited Incident Handling

eSentire security analysts will perform incident handling for all security incidents. Incident handling includes detecting, analyzing, containing, and assisting in the recovery from security incidents, and may involve attempted isolation of compromised assets, disruption of attacker activities, termination of malicious processes, and severing of command-and-control connections. Security analysts also provide remediation guidance, investigate the initial access vector, and check for potential data exfiltration. Core objectives include:

- suppressing and containing threats before further damage occurs;
- investigating and neutralizing threats to prevent their continued operation;
- utilizing the deployed MDR Services to conduct investigations; and
- identifying root causes where possible.

In addition, eSentire also provides containment and remediation recommendations and, when necessary, defers to eSentire or third-party digital forensics/incident response ("DFIR") services (not included in the Package) when an incident cannot be fully contained through MDR alone or has other complicating factors (e.g., litigation, visibility, forensics, etc.).

Threat Intelligence

eSentire delivers threat intelligence content at the strategic, operational, and tactical levels. At the strategic level, a monthly Threat Research & Intelligence Briefing is provided to Client on the latest trends and updates. At the operational level, a threat intelligence feed of known IOCs is provided via API in STIX format. At the tactical level, security advisories are provided in response to significant events in the threat landscape.

User Reported Email Detection and Response

The Atlas Platform will consume suspected phishing emails from a shared inbox (Microsoft O365 email), investigate the email to determine if it is malicious and report in a Finding as a threat or benign.

Cyber Resilience Team Support

As part of the Package, Client will receive ongoing service support and technical and commercial relationship management by eSentire's Cyber Resilience Team, which will assist Client with maximizing the benefits of the Package ("Support"). The Support deliverables provided as part of the Package will include:

- Onboarding Support: eSentire's Cyber Resilience Team will provide guidance and a personalized setup of the Package elements ordered, assisting Client with deployment and integration into existing infrastructure.
- Automated Reporting: Automated reports available via the Atlas UI providing visibility into security operations and threat activity.
- Technical Support: Phone and email support is provided in the Client's core business hours (0800-1600 client's local time).

- Security Support: SOC is available 24X7 via phone, email or Atlas chat.

License Requirements

The Professional Package leverages the Atlas Endpoint Agent for endpoint detection alongside Client's existing Microsoft Defender AV deployment. Client is responsible for procuring and maintaining its Microsoft Defender AV licensing during the entire Term. For Identity Response capabilities, eSentire will leverage Client's existing identity infrastructure – Okta or EntraID.

Usage Policies

Fair Use policies will be in effect to enforce reasonable usage of the Services. The employee count scoped for the service package will be mapped to expected volumes of endpoints, log data, storage and identities. "Reasonable usage" means the range of these volumes will fall within 4x the average for customers of similar employee count. Averages are measured on 30 day rolling averages. In the event volumes of usage are outside expected bounds, eSentire will work with the Client to investigate and recommend alternate configurations or other service packages. Service will not be interrupted. Alerts, investigations and other security monitoring and assistance is not capped.

.