eSENTIRE

Service Description:

Atlas MDR Enhanced Package

Overview

eSentire's Atlas MDR EnhancedPackage (the "**Package**") is a managed detection and response ("**MDR**") solution that leverages the Atlas Platform to provide comprehensive cybersecurity protection including threat prevention, detection, response, and proactive threat hunting. eSentire uses Client Data from multiple sources within the Client Environment to provide an MDR solution with telemetry coverage, log collection, and threat hunting. Specific elements of the Package are described in this service description, and the Package is scoped using the total number of Client employees using IT services and in scope of eSentire MDR protection ("**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, any capitalized terms contained in this service description are as defined herein:

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

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

"MDR Services" means the Endpoint Services, Log Services, and other services included in this Package.

"Order Form" means an ordering document, executed by the parties, that specifies services ordered by Client, including any amendments and supplements thereto.

Package Elements

The Package consists of the following elements:

- Collection of endpoint data, log data from the Client Environment;
- Integration with security controls in the Client Environment, including collection and AI-powered investigation of alerts from any source via REST API;
- Pre-emptive security through scheduled penetration tests;
- Atlas Endpoint Agent deployment for endpoint telemetry collection;
- Bring-Your-Own EDR ("**BYO-EDR**") endpoint support (CrowdStrike, SentinelOne, Microsoft Defender for Endpoint or Palo Alto EDR);
- Log collection and investigation from approved log sources with 30-day retention;
- Threat detection and generation of Findings;

- SOC oversight with security investigation of alerts detected via the Atlas Platform;
- Identity and Endpoint Response;
- TRU (Threat Response Unit) Directed Threat Hunting;
- User reported email investigations;
- Threat Intelligence;
- Vulnerability Reporting;
- Dark Web Monitoring – Credentials;
- 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, or installing required eSentire Equipment.

Launch Services will be scheduled with the client 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 pre month.

Pre-emptive Security – Atlas Autonomous Pen Testing

eSentire will schedule with the Client 1 AI-driven penetration test to assess the Client's security posture and improve the detection and response capabilities of the Package. Configuration of this test can be done through self-service in the Atlas UI or by working with the Cyber Resilience Team. Scope of the test can vary based on the cClient Environment.

Endpoint (BYO-EDR)

Client must provide an eSentire-approved endpoint detection and response ("**EDR**") solution already deployed in the Client Environment (referred to as a "**Managed-Only**" solution) or purchased through eSentire as an available add-on. Supported EDR solutions for the Advanced Package include CrowdStrike, SentinelOne, Microsoft Defender for Endpoint and Palo Alto EDR. eSentire will assist the Client in deploying the Atlas Endpoint Agent alongside Client's EDR solution for enhanced telemetry collection. EDR alerts from supported technologies are stored in the Atlas Platform for the Term, while raw telemetry collected by the applicable EDR technologies will be stored on the cloud platform of the applicable third party EDR provider as defined by the Client.

Identity Detection and Response

eSentire will integrate with Client's Okta or EntraID to facilitate identity response by the Atlas Platform.

Integrations

eSentire will configure approved integrations during onboarding to extend detection coverage beyond endpoint telemetry. Integration alerts are ingested into the Atlas Platform for analysis by Atlas AI and eSentire Security Operations Center ("**SOC**") analysts.

SIEM Log Collection and Investigations

eSentire will collect Client log data from approved log sources, to be identified by eSentire during onboarding. The Package includes log collection from those Client security controls, systems and applications deemed relevant by eSentire to its delivery of the Package. Log and audit data is stored in the log module of the Atlas Platform and is retained for 30 days (or until the Package expires, whichever is first). Logs are available for reporting and use in investigations and threat hunts.

Dark Web Monitoring - Credentials

eSentire will collect from Client specific high value credentials and other artifacts and will monitor dark web resources for indicators of these artifacts.

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 SOC will utilize the telemetry gathered from the sources described above to perform detailed security investigations of 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.

Pre-emptive Security - Atlas Autonomous Pen Testing

The Package includes Atlas Autonomous Pen Testing at a frequency of 1 test per year. Autonomous Pen Testing simulates real-world attack scenarios against the Client Environment to identify exploitable vulnerabilities and validate the effectiveness of existing security controls. Test results and remediation recommendations are provided through the Atlas UI. Test results will also be used to enhance detections and investigations.

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 the Atlas Endpoint Agent is deployed alongside client-licensed EDR, Atlas will monitor EDR output as part of Threat Detection. The Atlas Endpoint Agent will collect additional telemetry for Threat Detection

and monitor for EDR bypass behaviors. Response actions will be deployed to monitored endpoints primarily using the capabilities of the EDR technology, with the Atlas Endpoint Agent serving as an alternate method.

SIEM Log Collection and Investigations

Log data from supported sources will be collected to the Atlas Platform and be used to support investigations and threat hunts. Client reporting on collected log data is available in the Atlas UI. Log data is retained for 30 days.

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.

TRU Directed Threat Hunting

eSentire's Threat Response Unit ("**TRU**") will perform directed threat hunting utilizing Client telemetry and evidence data to detect advanced activities such as persistence mechanisms, application usage, network activity, or the tactics, techniques, and procedures ("TTPs") of threat actors. TRU-directed hunts leverage the telemetry available in the EnhancedPackage, including log data and integration sources, to provide threat hunting coverage. When a threat is detected, a security analyst will create a Finding and notify the Client via the Atlas UI.

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.

Dark Web Monitoring – Credentials

The Package includes Dark Web Monitoring – Credentials, which monitors dark web sources for compromised Client credentials. Alerts are generated when Client employee credentials are detected in data breaches, credential dumps, or dark web marketplaces. Findings are delivered through the Atlas UI with recommended remediation actions.

Integrations

The Atlas Platform can integrate with selected security controls. Such Atlas integrations will exist to support one or more of the following use cases:

- Contextual and other supporting data such as asset or identity information.
- High fidelity alerts or incidents to be investigated by Atlas AI.
- Availability of response actions.
- Support for collaboration/interaction with eSentire.

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 core business hours (0800-1600 client's local time).
- Security Support: SOC is available 24X7 via phone, email or Atlas Platform chat.

License Requirements

Endpoint Services being provided in a 'Bring Your Own License' capacity with the Atlas Endpoint Agent supporting co-deployed. Client is responsible for procuring and maintaining the required licensing directly with an approved third party EDR provider during the entire Term and coordinating proper licensing permissions with such third party EDR provider to allow eSentire API access and credentials into Client's licensed environment. Client must purchase one of the following applicable licenses (or an eSentire-approved equivalent):

- CrowdStrike Bring Your Own License – requires Falcon Insight XDR + CrowdStrike Falcon Prevent + Threat Graph Standard
- Microsoft Bring Your Own License – requires Microsoft Defender for Endpoint Plan 2
- SentinelOne Bring Your Own License – requires Singularity Advanced (also recommended at least 14 days retention ("Deep Visibility") to enable threat hunting)
- Palo Alto Bring Your Own License – requires Palo Alto Networks Cortex XDR Pro Endpoint

For Identity Response capabilities, eSentire will leverage Client's existing identity infrastructure – Okta or EntraID – requiring API credentials.

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.

Available Add-Ons

- EDR Licensing
  Licensing for Sentinel One or CrowdStrike EDR are available through eSentire.

Add-Ons will be listed on the Order Form in a separate section outside of the Package fees and service table.