eSENTIRE

Service Description:

Atlas MDR Elite Package with Microsoft Defender E5/E7

Overview

eSentire's Atlas MDR Elite Package with Microsoft Defender E5 (the "**Package**") is a managed detection and response ("**MDR**") solution that leverages the eSentire Atlas Platform to provide the most comprehensive cybersecurity protection available, including threat prevention, detection, response, proactive threat hunting, continuous penetration testing, and advanced dark web monitoring. eSentire uses Client data from multiple sources within the Client Environment to provide a premium MDR solution with pre-emptive security, comprehensive telemetry coverage, detection, investigation, response and 24x7 support. 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**"). 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 workflows 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.

"Microsoft Defender E5" means Microsoft's integrated Extended Detection and Response (XDR) solution that provides security across identities, endpoints, applications, email, and cloud data, licensed at the E5 tier, which is required to leverage the services in this Package. See Microsoft licensing documentation for details. This also includes the E7 license level.

"Order Form" means an ordering document, executed by the parties, that specifies services ordered by Client, including any amendments and supplements thereto. "Users" is the number of humans, non-shared identities with interactive log-in capability to the client's IT systems.

Package Elements

The Package consists of the following elements:

- Collection of security data and log data from the Client Environment.
- Integration with security controls in the Client Environment.
- Pre-emptive security through scheduled AI penetration tests.
- Atlas Endpoint Agent deployment to in scope endpoints.

- Atlas Outpost (virtual machines, physical appliances available for a fee) deployment into in scope networks, as required.
- Bring-Your-Own Defender E5 ("**BYO-Defender**") support (E5/E7 licensed Defender for Endpoint, O365, Identity and Cloud Apps).
- Log collection, investigation and eSentire-curated detections from approved log sources using client licensed Microsoft Sentinel SIEM.
- Identity, Endpoint, O365, and Cloud Response.
- Threat detection and generation of Findings.
- SOC oversight with security investigation of Findings detected via the Atlas Platform.
- TRU (Threat Response Unit) directed Threat Hunting.
- Threat Intelligence.
- User reported phishing email investigations.
- Vulnerability Reporting.
- Response Orchestration.
- Digital Forensic and Incident Response.
- Dark Web Monitoring – Credentials.
- Dark Web Monitoring – Advanced.
- 24x7 support from the eSentire Cyber Resilience Team; and
- Access to Atlas 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.
- introduction to a Technical Account Manager, your trusted security consultant.
- installation assistance of Atlas Agents, Outposts 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 should not exceed 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.

Package Capabilities

The following capabilities are included as part of the Package. Each capability below describes how it is enabled as part of Client's onboarding and how it is delivered on an ongoing basis.

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 Penetration Testing and Vulnerability Scanning

eSentire will provide the Client with continuous AI-driven penetration testing and vulnerability scanning to assess the Client's security posture and improve the detection and response capabilities of the Package. Configuration of these tests can be done through self-service in the Atlas UI or by working with the Cyber Resilience Team. Scope of each test may vary as will the schedule and cadence. Client will have complete control over these cadences and scopes.

The Package includes Atlas Autonomous Penetration Testing and Vulnerability Scanning ("**Offensive Security**") on a recurring basis (24 Engagements). Offensive Security simulates real-world attack scenarios against the Client Environment to identify exploitable vulnerabilities and validate the effectiveness of existing security controls. This package includes Penetration Test and Vulnerability scan engagement types. Engagement setup, results and remediation recommendations are provided through the Atlas UI. Results will also be used to enhance detections and investigations. This package entitles the Client to twenty-four engagements per year. Validating Fixes of specific exposures can be executed at any time (up to 100 times/year)

Endpoint (Microsoft Defender E5) + Atlas Agent Detection and Response

Client must provide an E5 licensed Defender solution already deployed in the Client Environment (referred to as a "**Managed-Only**" solution). eSentire will assist the Client in deploying the Atlas Endpoint Agent alongside Client's Defender EDR solution for enhanced telemetry collection from endpoints. EDR alerts are stored in the Atlas Platform for the Term, while raw telemetry collected by the Defender technologies will be stored on the cloud platform of the third-party provider as defined by the Client.

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.

Response – Endpoint, O365, Identity

Integration to the Microsoft Defender E5 suite will enable eSentire to enforce response actions in the Client Environment from the Atlas Platform using Defender APIs. Response includes those actions available via the Microsoft Graph API for Defender Endpoint, O365, and Identity, where authorized by Client. Capabilities are subject to change based on capabilities of the Microsoft API. Response actions can include endpoint isolation, account password reset and locking out accounts.

Identity telemetry is monitored as part of the Microsoft Defender E5 suite integration described above, and response actions are deployed per the capabilities of the Microsoft Graph API (see Response above).

Integrations

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

Log Collection and Investigations (Microsoft Sentinel)

eSentire will integrate the Atlas platform with a client-licensed Microsoft Sentinel instance. Log data from approved log sources to be identified by eSentire during onboarding. The Package includes eSentire-developed analytic rules deployed to Sentinel for threat detection using those Client security controls, systems and applications deemed relevant by eSentire to its delivery of the Package. Log and audit data is stored in Sentinel as defined by client administrators. Logs are also available for use in investigations and threat hunts.

Log data stored in Client-licensed Microsoft Sentinel instance is used to support investigations and threat hunts. eSentire-managed detections will run as Sentinel analytics rules.

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.

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 telemetry available in the Elite Package, 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. Threat Hunting hypotheses are developed from observed behaviors in Atlas and from TRU threat research.

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

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

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.

Dark Web Monitoring – Advanced

In addition to credential monitoring, the Elite Package includes Dark Web Monitoring – Advanced, which extends monitoring to include broader threat intelligence gathering from dark web forums, marketplaces, and communication channels for mentions of the Client organization, infrastructure, or proprietary information. Advanced monitoring provides early warning of targeted threats, planned attacks, or data exposure beyond credential compromise. Findings are delivered through the Atlas UI with contextual analysis and recommended response actions.

Atlas Response Orchestration

Response Orchestration is a client and eSentire-configured, eSentire-managed rule engine in the Atlas Platform that defines and executes response actions for telemetry and Findings based on set conditions. Response Orchestration is intended to enable automated response where required/permitted and influence/control eSentire SOC response. Configuration may be updated at any time; changes will be applied to all new telemetry and Findings generated from the time the configuration is saved. Response actions may be triggered when telemetry is first ingested to Atlas, before processing, or when a Finding is created, post enrichment and Atlas AI investigation.

Incident Response & Digital Forensics

eSentire SOC includes full Incident Response (IR) processes for every investigation initiated by MDR services. Onboarding will include development of an IR plan and playbook.

eSentire security analysts will perform incident response for all security incidents detected through the MDR services. Incident response 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 vectors, and check for potential data exfiltration. Core objectives include:

- suppressing and containing threats before further damage occurs – see Response above.
- 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 (Only included in Elite Package) when an incident cannot be fully contained through MDR alone or has other complicating factors (e.g., litigation, visibility, forensics)

IR functions included with MDR Services:

- IR plan & playbook development
- IR retainer setup
- Log source & telemetry gap assessments.
- Advance tooling deployment
- Initial scoping calls
- Timeline reconstruction
- Patient zero identification
- True positive validation

- Isolation actions
- Credential remediation guidance.
- Malware & persistence removal
- C2 blocking.
- Real-time coordination
- Log analysis
- Network traffic analysis.
- Attribution (TTP-level)
- Clean validation
- Backup restoration strategy
- Hardening recommendations
- Re-entry monitoring
- Executive summary report
- Threat intelligence integration
- Compromise assessments
- BEC investigations

Digital Forensics and Incident Response Retainer and Advisory Services

Escalation of an investigation to Digital Forensics and Incident Response (DFIR) services, available via Retainer include these requirements:

- Tabletop exercises & breach drills
- Disk, memory & volatile acquisition; memory forensics.
- Forensics requiring data/systems not integrated with Atlas.
- Malware analysis & reverse engineering
- Data exfiltration analysis
- Extended technical finding reports; lessons-learned sessions
- Regulatory / breach notification
- Litigation support & expert witness
- Insurance claim documentation
- On-site support
- Insider threat investigations
- Compliance-driven investigations
- Other non-incident-driven investigations

Security Consulting & Advisory

- As part of the Package, Client will receive ongoing technical consulting and support by their named Technical Account Manager (TAM). The TAM serves as a trusted partner in the client's security journey — providing ongoing visibility into their security posture, staying ahead of emerging threats, and ensuring their environment is continuously optimized. Through regular reviews and proactive guidance, the TAM translates complex security insights into clear, actionable recommendations tailored to the client's business. Their goal is simple: to ensure every client feels supported, informed, and confident in their security program.
- You can expect the following from your TAM:
- Onboarding Support: Your named Technical Account Manager will be by your side from day 1 and throughout the lifetime of your partnership with eSentire.

- Business Risk Reviews deliver outcomes such as security posture analysis, notable events, a threat landscape review, and detection capability assessment.
-
- Executive Security Briefing covers current trends, an industry threat analysis, peer analysis, security recommendations, a security maturity assessment, and compliance status reporting.
- Architecture Assessment conducting a comprehensive security audit, review of threat hunting results, analysis of current security tool effectiveness, as well as gap analysis and recommendations.
- Where applicable, coordinate incident response updates and escalation management
- Automated Reporting: Automated reports available via the Atlas UI providing visibility into security operations and threat activity.

License Requirements

Endpoint Services are provided in a 'Bring Your Own License' capacity. Client is responsible for procuring and maintaining the required E5/E7 licensing directly with Microsoft during the entire Term and coordinating proper licensing permissions to allow eSentire API access and credentials into Client's licensed environment.

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 wall 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.

Service Level Agreement

For more information on our Service Level Agreement, please refer to the SLA description in the Legal Catalogue

Available Add-Ons

For details on all available package add-ons, please refer to the corresponding Add-On Service Description.