eSENTIRE

Managed Detection and Response Services (MDR) with Microsoft Defender for Office 365

The Service name was updated by eSentire from “eSentire MDR with Microsoft Defender for Office 365”, to “Managed, Detection and Response Services - Microsoft Defender for Office 365”. All other content remains the same.

Definitions

Alert means an event that eSentire will escalate to the Client.

Sender Policy Framework (SPF) – helps receiving servers confirm mail sent from your domain is from your organization.

Domain Keys Identified Mail (DKIM) – confirms received email was sent/authorized by the owner of that domain.

Domain-based Message Authentication, Reporting and Conformance (DMARC) – Uses SPF and DKIM to determine the authenticity of an email message.

Service Description

eSentire MDR with Microsoft Defender for Office 365 provides Client with email-level visibility and control to support threat prevention, detection, investigation, and response. The service enables the SOC to prevent, detect and respond to threats based on detection via the Microsoft Defender for Office 365 platform. Microsoft Defender for Office 365 (formerly Office 365 Advanced Threat Protection) helps protect organizations against sophisticated attacks such as phishing and zero-day malware. Microsoft Defender for Office 365 also provides actionable insights by correlating signals from a broad range of data to help identify, prioritize, and provide recommendations on how to address potential threats. eSentire supports analyzing suspicious O365 security events and uncovering additional context in multi-signal MDR investigations depending on supported services. The service is supported by eSentire’s SOC on a 24x7x365 basis.

Key Benefits

- Configuration hardening to prevent social engineering, malware, and other email-based threats.
- Implementation of security configuration for SharePoint, OneDrive, and Microsoft Teams.
- 24x7x365 Investigation and response into email-based threats.
- Dedicated platform designed for email-based threat investigations.
- User-escalated suspected phishing emails for investigation and response.
- Direct API integrations for blocking and removing identified malicious content.

Service Features / Service Capabilities

Investigation and Analysis

eSentire is responsible for threat detection, analysis, investigation, escalation, and response. In addition, eSentire is responsible for security event analysis and investigation to determine if a security event is considered a legitimate threat and warrants an escalation to the Client and potential response action. If an event is deemed as actionable, due to its behavior and the type of detection, it will be escalated to the Client as an Alert. The SOC will perform event triage, assign criticality, and include all supporting information within the Alert and, if necessary, initiate escalation to the Client. Malicious activity will be identified and resolved immediately utilizing response playbooks by eSentire.

eSentire is responsible for providing guidance on implementing configuration changes to support prevention at the Microsoft Defender for O365 email gateway. This includes email authentication, email protection and detection capabilities via policies.

eSentire will investigate all security events identified through the eSentire MDR with Microsoft Defender for Office 365 Services and escalate actionable alerts as appropriate in accordance with the Service Level Objectives (SLOs). eSentire holds all rights to filter traffic based on volume to optimize service delivery. User escalated phishing emails are considered security events. Once investigated, events are classified, alerted, and escalated to the Client if there is an action required. eSentire will utilize the escalation process, agreed upon during the on-boarding process, to contact and relay information to the Client. The defined escalation process is a mutually agreed upon process between the Client and eSentire.

Response Actions for Identified Threats

eSentire has the below native capabilities within the eSentire MDR with Microsoft Defender for Office 365:

- Deletion / quarantine of malicious email
- Blocklist of bad IPs/domain/email sender
- User / Identity isolation of compromised user

If Client is subscribed to multiple eSentire Services, additional response actions can be utilized based on the most effective response action. This can include endpoint, network, identity, and cloud response.

Incident Alerts and Reporting

eSentire sends Alerts via email for Medium, High, and Critical severity events followed by escalation(s) for High and Critical severity events, as necessary, based on agreed upon escalation procedure in the configuration worksheet. A member of the eSentire customer success team will be assigned to review the overall Alerts with the Client. All Alerts are available within the eSentire Portal for Client's review. All reporting is delivered through the eSentire Portal.

Deployment

Access

eSentire will provide the Client with a detailed deployment document outlining the access required and configuration that is necessary for eSentire to connect to the Client. This is a requirement for eSentire resources to securely access the customer environment to operationalize the eSentire MDR with Microsoft Defender for Office 365 Service.

Configuration

eSentire will assign a consultant and provide guidance for implementation of email authentication security components and various email security policies which are the main ways to filter out potentially malicious content. The eSentire consultant will have 4 hours allocated to provide guidance for implementation of the main features and functionality that are identified below.

Email Authentication:

- SPF
- DKIM
- DMARC

Protection and detection capabilities:

- Anti-malware Policy
- Anti-spam policy
- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams
- Anti-phishing protection in Defender for Office 365
- Real-time detections
- External Email Warning

Tuning

eSentire will monitor all preventions and detections that are triggered within the platform and make the necessary changes to allow legitimate emails to reach the Client's infrastructure during the tuning phase. During the tuning phase, an assessment will be made on whether minor policy changes are needed depending on the specific requirements of the Client. Once the email authentication, protection and detection capabilities are enabled eSentire will work with the Client to ensure the email security platform is in a healthy state before transitioning to production monitoring.

Reporting and Data Access

eSentire delivers all SOC led investigation reporting through the eSentire Portal. The Client has direct access to the Microsoft Defender for O365 platform which includes both the raw data and access to custom reporting which natively includes URL Protection Report, Compromised User Report, Spam Detection Report, Safe Attachment Report, etc. Client has the right to use the Microsoft software which allows them full visibility and access into the data.

Maintenance and Support

eSentire will provide support to the Client for both security and system issues related to the eSentire MDR with Microsoft Defender for Office 365 as defined below.

Responsibilities

Function	Client	eSentire
Threat Detection – deploy content	I	RA
Threat Detection – content tuning	A	R
Threat Detection – custom use cases	RA	I
Threat Detection – submit new use cases to eSentire content teams	I	RA
Threat Detection – Alert monitoring, analysis	I	RA
Threat Detection – Notification	I	RA
Threat Detection – Resolution	RA	RA
System – Microsoft Defender O365 API setup	R	I
System – Azure AD Account provisioning setup	R	I
System – Data ingest tuning	I	RA

Function	Client	eSentire
System – MDO365 knowledge transfer session	I	RA
System – Email allow listing for non-security events	RA	I
System – User account management	RA	RA
Health – Data ingestion uptime monitoring	I	RA
Health – General troubleshooting	RA	C
Data – Resolving collection issues	RA	C
Data – Monitoring collection (in scope data)	I	RA
Data – Notification of lack of collection	A	R

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.

The Client is responsible for:

- Working with eSentire staff to implement the proper security protections to limit the attack exposure of their email footprint.
- Ensuring changes to API and/or access into the environment is communicated to eSentire
- Designating a project coordinator to work directly with and serve as the primary Client contact with eSentire for the term of the eSentire MDR with Microsoft Defender for O365 Services
- Providing the necessary resources, information, documentation and access to personnel, equipment, and systems, as reasonably required by eSentire, to allow eSentire to perform the Services.

In the event Client fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption set out herein with respect to the eSentire MDR with Microsoft Defender for Office 365 Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

Service Level Objectives

Severity/Priority	Description	Notification/Escalation
Low P4	Informational / Minor activity recorded but not alerted.	None
Medium P3	Unusual alerts – alert to client for additional context	Alert (via email) within 60 minutes of the determination of a security event followed by phone call to the Client per defined escalation procedures
Critical and High Security Alerts (P1 and P2)	Threats identified from Microsoft Defender for O365 events	Alert (via email) within 40 minutes of the determination of a security event followed by phone call to the Client per defined escalation procedures