eSENTIRE

Managed Detection and Response Services (MDR) with Microsoft Defender for Identity and Cloud Apps

The Service name was updated by eSentire from "eSentire MDR with Microsoft Defender for Identity and Cloud Apps", to "Managed, Detection and Response Services - Microsoft Defender for Identity and Cloud Apps". All other content remains the same.

Definitions

"Alert" means an event that eSentire will escalate to the Client.
"Business Impact" means any quantification of the reputational, operational, compliance or financial impact to the Client's business.
"Configuration Worksheet" filled out by the Client during deployment that gives eSentire more context into Client environment.
"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).
"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.
"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.
"Litigation Support" means support, including but not limited to expert and fact witness testimony.
"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.

Service Description

MDR with Microsoft Defender for Identity and Cloud Apps (the "MDICA Service") provides Client with user identity, application control, and visibility to support threat prevention, detection, investigation, and response. The Service enables the eSentire Security Operations Center ("SOC") to prevent, detect and respond to threats based on detection via the Microsoft Defender for Identity ("MDI") sensor, and Defender for Cloud Apps ("MDCA") platform. MDI (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages Clients on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at Clients organization. MDCA (formerly Microsoft Cloud App Security) provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all Clients Microsoft and third-party cloud services. Together, both services help protect against risky behavior across data, users, and – SaaS – applications, and help gain visibility of deployed cloud apps, discover shadow IT, and protect Clients sensitive information. eSentire supports analyzing suspicious identity and cloud application 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 and tuning support on MDI and MDCA, to harden overall security posture and ensure service functionality.
- Knowledge transfer and walkthrough of MDCA portal.
- 24x7x365 Investigation and response into identity/app-based threats.
- Dedicated platform designed for identity/app-based threat investigations.
- Direct API integration for disabling user accounts and revoking refresh/session tokens based on risky identity/app behavior.
- Extended visibility across business-critical SaaS applications and adds user-level threat detection and containment capabilities.

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 MDICA Service:

- Revoke refresh/session token of a user (for M365 apps)
- User / Identity isolation of compromised user
- Force password reset

The native response capabilities for the MDICA Service are available for all non-privileged users within the Client environment. For any user that has elevated permissions (such as Global Administrator, Security Operator, etc.) within Clients Active Directory environment, eSentire will require that Client assign the Global Administrator role to our Enterprise Application (Service Principal) during deployment. Without providing the Global Administrator role to eSentire's Enterprise Application, Client will be forfeiting the ability for eSentire to leverage the available response actions for all privileged users in Client's environment.

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 Client. All Alerts are available within the eSentire Insight Portal (the "Portal") for Client's review. All reporting is delivered through the Portal..

Deployment

1. Access. eSentire will provide the Client with a detailed deployment document (Onboarding Guide) 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 Client environment to operationalize the eSentire MDICA Service. Client will also need to provide eSentire Client's Cloud APPS API token as well as Cloud APPS URL specific to their organization.
2. Configuration. eSentire will assign a consultant, and provide guidance to Client, for implementation of fundamental configurations and various security components within Clients MDCA portal. The eSentire consultant will have up to 4 hours allocated to provide guidance to Client for implementation of the main features and functionality that are identified below.
    a. Azure Identity Protection:
        i. Configure risky user policy for automated response actions through Microsoft
        ii. Configure sign-in risk policy for automated response actions through Microsoft
    b. Defender for Cloud Apps:
        i. MDCA portal walkthrough and knowledge transfer
        ii. Enable Shadow IT Discovery via MDCA for Endpoint
        iii. Discover and assess cloud apps and app discovery policies
        iv. Connect Office 365 app – establishing actionable governance for Office 365, SharePoint, OneDrive, Teams, Power BI, etc.
        v. Essential practice configurations
3. Tuning. eSentire will monitor 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 Client. Once the protection and detection capabilities are enabled, eSentire will work with Client to ensure the security platform is in a healthy state and security posture before transitioning to production monitoring.
4. Reporting and Data Access. eSentire delivers all SOC led investigation reporting through the eSentire Portal. The Client has direct access to the MDICA platform which includes both the raw data and access to custom reporting which natively includes cloud discovery dashboard, app risk levels, app categories and discovered apps, top entities (most active within your network), etc. Client, as the Microsoft license holder, will have the rights 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 MDICA Service 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 for Identity and Cloud Apps API setup	R	I
System – Azure AD Account provisioning setup	R	I
System – Data ingest tuning	I	RA
System – Defender for Identity and Cloud Apps knowledge transfer session	I	RA
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.

1. The Client is responsible for:
    a. Working with eSentire staff to implement the proper security protections to limit the attack exposure of their email footprint.
    b. Ensuring changes to API and/or access into the environment is communicated to eSentire
    c. 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 Identity and Cloud Apps
    d. 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 MDICA 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

Exclusions

The MDR service does not provide Emergency Incident Response (as defined above) including but not limited to deep Forensic Investigation, recovery support, Litigation Support, Disaster Recovery and Business Continuity Planning, and/or the quantification of the Business Impact, with respect to all customer assets, whether currently under Embedded Incident Response or not.

The Service does not include any Microsoft licensing.