SERVICE DESCRIPTION

MXDR for Microsoft

Overview

Trustwave's Managed Extended Detection & Response (MXDR) for Microsoft service ("**Service**") provides 24x7x365 threat detection, threat hunts, and threat response for Microsoft Defender XDR and for cybersecurity alerts generated in the Trustwave Fusion platform ("**Fusion Alerts**"). The Service includes managed SIEM service which Trustwave operates in conjunction with Client to monitor the Client-owned Microsoft Sentinel (SIEM). The following description sets out the parameters of the Service.

Core Features

The Service includes threat-based prevention, managed detection, investigation, and response for the following Client owned Microsoft Security products ("**Managed Technology**"):

- Microsoft Sentinel
- Microsoft Defender XDR, including
  - Microsoft Defender for Endpoint
  - Microsoft Defender for Identity
  - Microsoft Defender for Cloud Apps
  - Microsoft Defender for Office

The Service may include additional Microsoft-supported data sources for enrichment, as indicated in the applicable SOW or Order Form. The Service includes coverage for one (1) instance of Microsoft Defender XDR with one (1) Microsoft Sentinel (SIEM). Client may elect to include additional instance(s) for an additional fee, as indicated in the applicable SOW or Order Form. Client is responsible for procuring and maintaining all applicable Microsoft licenses as well as any associated data ingestion and consumption fees. The Service does not include support for Microsoft features denoted as "Public Preview" or "Private Preview."

The Service includes the following core features:

Trustwave Fusion Platform & Fusion Mobile App

The Trustwave Fusion platform is Trustwave's proprietary cloud-based security operations platform. Client and Trustwave will cooperate to add the Managed Technology to one Client account in the Trustwave Fusion platform as part of the Onboarding feature (see below). Client will have access to the following capabilities and related documentation on the Trustwave Fusion platform via web or mobile application:

- Information on XDR Incidents, Fusion Alerts, and Security Incidents (as defined in this description)
- Health and availability incident tickets

- Client’s reports and dashboards
- Request methods for change support and management
- Methods of communication including tickets and chats

Such capabilities are available to Client in the Trustwave Fusion platform, including allowing for ticketing integration. Client is responsible for any further connectivity, access, health, and advanced ticketing integrations between Client infrastructure, software, the Managed Technology, and the Trustwave Fusion platform. Any changes to connectivity, services, and documentation for the Trustwave Fusion platform advanced integrations are at Trustwave’s sole discretion.

Ingestion & Log Source Support

Trustwave will collect supported cybersecurity alerts and incidents generated by Microsoft Defender XDR and Microsoft Sentinel (“**XDR Incidents**”) into the Trustwave Fusion platform. The applicable SOW or Order Form between Trustwave and Client will indicate the monthly allowance of XDR Incidents Client has purchased for the Term.

The Service may include data sources for which Microsoft Sentinel includes an existing connector and which Trustwave supports, as indicated in the applicable SOW or Order Form. For data sources that are not native to Microsoft or any data sources which Trustwave does not currently support, Client may be required to purchase additional consulting services to onboard such data sources.

Any changes to XDR Incidents ingestion, parsing, analysis, detection, automation, monitoring, and reporting are at Trustwave’s sole discretion.

If Trustwave gives Client the option to select the region in which it wants its Trustwave Fusion platform account to be hosted then Client understands it must select the region in its sole discretion. Client is responsible for all appropriate analysis to verify Client selects the region appropriate for its Trustwave Fusion platform account (including any legal or regulatory analysis). Client may only select one region for all Trustwave services it procures. The SOW or Order Form between Trustwave and Client will indicate which region Client selects. The country where Trustwave Fusion platform accounts are hosted for each region is as follows:

Region	Hosting Country
AMS | TGS	United States
EMEA	Germany
APAC	Australia

Consumption Overages

The Service is provided and priced according to monthly XDR Incidents maximums, as set forth in the applicable SOW or Order Form. Trustwave will periodically review the volume of XDR Incidents processed for Client in relation to the Service. Client will regularly review its XDR Incidents volume in the Trustwave Fusion platform and work with Trustwave to tune its configurations to stay within purchased volumes. Where Client’s XDR Incidents volumes spike and are found to signal that Client will or has exceeded the agreed threshold for the current month, Trustwave may

- evaluate excess XDR Incidents and determine if increased volume is (i) a signal of an attack and related alert information that can be consolidated under a single Security Incident, or (ii) a configuration error documented in a ticket that requires Client to take corrective action within 24 hours; or
- suppress, filter, throttle, consolidate, or send notification of excess XDR Incidents from Client's systems at Trustwave's discretion.

Where Client's XDR Incidents volumes are found to exceed the agreed threshold persistently by five percent (5%) or more on average over a thirty (30) day period, Trustwave may either

- charge Client for the excess data and event volumes at current list price; or
- suppress, throttle, or filter excessive data and events from the Managed Technology.

Trustwave will notify Client of the overage and will select the method that is expected to limit impact to the Service.

Systems Management

Trustwave will manage and monitor the security configuration of those Client security applications running on the Managed Technology which are included in the Service, as indicated in the applicable SOW or Order Form ("**Managed Technology Security Applications**") according to the following sections. For the avoidance of doubt, Trustwave will solely provide the Systems Management aspect of the Service for the Managed Technology Security Applications (unless otherwise agreed between Client and Trustwave in writing).

Security Policy and Change Management

Client and Trustwave will collaborate on the initial configuration of security policies and settings and work together during the Term to maintain that configuration. This must be completed to achieve Steady State (defined below).

When the Managed Technology Security Applications have no existing security policies, Trustwave will assist the Client in developing and applying a base policy.

Trustwave may modify these security policies and settings further at any time during the Term with the aim of protecting against threats to Client.

The following are change-control and security policy management procedures for standard change requests during the Term whether initiated by Client or by Trustwave:

Change Request Type	Description
Emergency Change	A change which Trustwave views as necessary to mitigate immediate and material security risk(s) identified by Trustwave or Client (and communicated to Trustwave); provided that such request involves only security policy settings and is not a major software patch update for the Managed Technology Security Applications.
Standard Change	Repetitive, typically low risk changes. It has repeatable implementation steps and predictable outcomes.
Complex Change	A change which meets the following criteria:

	• may cause technical system impact and could have significant outage effects or affects multiple business units or environments • may impact security controls • does not have repeatable implementation steps
Project	A change which meets the following criteria: • due to its scope of work, cannot be considered as standard or complex change and specifications require Trustwave to consult Client • due to its volume, cannot be completed within SLAs agreed for Emergency, Standard, or Complex Changes • Trustwave determines such a change may alter the architectural design of the Managed Technology • may require proof of concept to be completed before executing • due to use case complexity and scope beyond tactical development, such as in response to an immediate threat requiring rapid detection, as determined by Trustwave *Note*: Projects may require Client to agree to additional services and Fees to complete this request. Classifying a change as a Project Change is at Trustwave’s sole discretion.

Client-Initiated Change Management

Trustwave will assess and implement change requests submitted by Client through Trustwave approved communication methods. Trustwave evaluates such requests against industry best practices and the change’s potential cybersecurity impact on Client’s security environment. Trustwave will propose a schedule and notify Client of changes Trustwave expects (in its sole discretion) may disrupt Client’s environment, and Client will approve or deny these scheduled change windows. Client acknowledges that denying a scheduled change window may impact Trustwave’s ability to provide the Service and service level agreements (SLAs) may not apply until Trustwave is able to implement the change.

Trustwave will also notify Client if a change request is (i) so significant in scope that it would require a separate engagement between Trustwave and Client or (ii) outside the scope of the Service and, therefore, will only be performed at Trustwave’s discretion.

Client acknowledges that any configuration change management requests for Managed Technology Security Applications or Client environment that are categorized as a complex change may, in Trustwave’s sole discretion, be deemed a project and would require a written addendum between the Parties.

Trustwave-Initiated Change Management

Trustwave will implement Trustwave-initiated changes through the Trustwave Fusion platform. Trustwave determines the applicability of such changes against industry best practices and the change’s potential impact on Client’s environment. Client may review each proposed change.

Trustwave will perform the change according to the change window schedule agreed between Client and Trustwave.

Trustwave-Initiated Maintenance and Management

Trustwave, at its discretion, may recommend version updates for the Managed Technology Security Applications. Client will be responsible for implementing such updates and understands failure to implement may result in Trustwave's inability to provide the Service.

Trustwave will monitor the Managed Technology Security Applications that is connected to the Trustwave Fusion platform to ensure the health and availability of the connectivity.

Connectivity

Client and Trustwave will work together to connect the Trustwave Fusion platform and the Managed Technology using direct connectivity, which is a direct connection between the Managed Technology and the Trustwave Fusion platform using an API connection.

Health Monitoring

If Trustwave detects an API connection which is unresponsive or fails to transmit data, Trustwave will inform Client and may assist, upon request, in diagnosing the issue.

Client remains solely responsible for managing and monitoring the health and availability of Client's endpoints connected to the Managed Technology that are not within the scope of this Service.

Trustwave will not be responsible for the design, implementation, effect, or any damages, direct or indirect, of any Client changes made to the Managed Technology or Client-managed systems the Service relies upon.

Security Colony Subscription

The Service includes limited access to Trustwave's Security Colony service. To access this feature of the Service, Client must enroll at https://www.securitycolony.com/.

Service Features

The Service includes the following features:

Onboarding

The Onboarding includes two (2) components: Client-side implementation and MSS Transition.

Client-side Implementation

Client will take the necessary steps to connect Client's systems which generate XDR Incidents to the Trustwave Fusion platform and the Managed Technology (including endpoints to management stations and sensor agents on each endpoint in scope) as agreed between Trustwave and Client in the applicable SOW or Order Form. Client will ensure the Managed Technology is prepared and continues to provide appropriate and consistent information about Client's environment in a manner that allows Trustwave to provide the Service. Trustwave may assist Client during this phase.

If necessary for the Managed Technology to work with the Service, Client will create access groups, individual Trustwave-users, and Trustwave-service accounts in the Client environment that allow such users to deliver services. Client is responsible for providing initial and ongoing Trustwave user and system remote access to the Managed Technology to accommodate Trustwave's threat analysis and investigation.

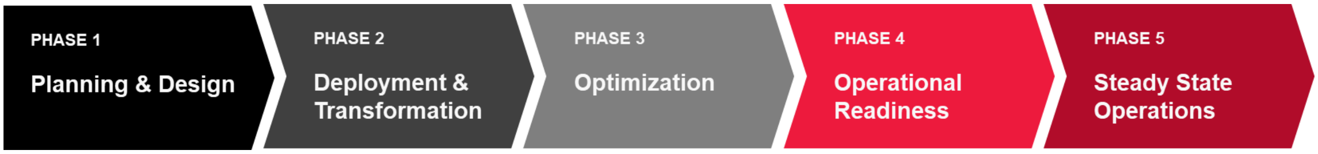
Trustwave will provide Client with an initial list of users during Onboarding. After Onboarding (during Steady State as defined below), Trustwave will provide Client with ongoing user access, update requests, and use change management tickets to maintain updated user access to the Client's Managed Technology. If Client fails to perform changes and maintain Client-side implementation responsibilities for Trustwave user access to Managed Technology, then Trustwave has no responsibility for providing the Service and Trustwave will not continue with this feature of the Service until Trustwave has the necessary access to the Managed Technology.

MSS Transition

MSS Transition is designed to facilitate the integration of the Managed Technology with the Trustwave Fusion platform. Trustwave will assign a Transition Manager and additional technical enablement resources (at Trustwave's discretion) to work with Client on onboarding the Service. Trustwave will advise Client through five (5) phases of transition management. Client is deemed fully transitioned and at steady-state operations (beginning of the Service features other than Onboarding) following Trustwave's conclusion of the fifth (5th) phase ("**Steady State**").

Transition Management Phases

The following chart summarizes the five (5) phases of transition management in this feature:



PHASE 1
Planning & Design

PHASE 2
Deployment & Transformation

PHASE 3
Optimization

PHASE 4
Operational Readiness

PHASE 5
Steady State Operations

Client Obligations

For Trustwave to provide Onboarding, Client will:

- be responsible for deploying the software necessary for Trustwave to provide the Service for the Managed Technology or related telemetry, unless otherwise specified at Trustwave's sole discretion, and any additional Client deployment activities will be described in the applicable SOW or Order Form;
- configure initial and ongoing network connectivity from Client systems to Managed Technology utilizing the Trustwave address ranges and domains that allow Trustwave to provide the Service;
- configure initial and ongoing supported Trustwave Fusion platform ingestion architecture in the Managed Technology, utilizing Trustwave-defined standards and conventions which allow Trustwave to provide the Service;
- upon Trustwave's request, confirm to Trustwave that Client systems are reporting to the Managed Technology in order to support log and alert collection;
- if agreed by Trustwave, provide its domain to be whitelisted for Microsoft Teams, which would be used as an optional communications channel during incident investigations;
- provide Trustwave the appropriate permissions and access required to deliver the Service, including enabling granular delegated administrative privileges (GDAP) and granting the 'security administrator' role to Trustwave for permissions to manage security-related features in the Managed Technology;
- define initial Response Authorization Protocol and authorized actions (see details below); and

- ensure Managed Technology has appropriate licensing and support contracts with third parties during the Term.

Trustwave Obligations

As a part of Onboarding, Trustwave will:

- schedule and host a kick-off meeting with Client;
- provide new-user orientation materials and training regarding the Service (as available);
- if agreed by Trustwave, whitelist Client’s domain for Microsoft Teams as an optional communications channel to be used during incident investigations;
- keep Client informed of transition progress; and
- coordinate Trustwave technical delivery resources to
  - enroll Client and Client’s indicated authorized user(s) in the Trustwave Fusion platform;
  - collect, review, and assess event data for tuning;
  - validate network connectivity from Client systems to Managed Technology utilizing the Trustwave address ranges and domains that allow Trustwave to provide the Service;
  - review data flow, quality, and analysis subject to the scope agreed between Trustwave and Client in the applicable SOW or Order Form;
  - review initial Client Response Authorization Protocol and authorized actions (see details below);
  - validate Client has added authorized contacts to groups for the Notification Procedures listed for Security Incident Priority Levels table below; and
  - conduct an operational readiness assessment to determine if Client has reached Steady State.

MXDR Jumpstart

The MXDR Jumpstart (“**Jumpstart**”) feature is an implementation service for the Managed Technology and contributes towards Client reaching Steady State (defined above). Trustwave will gather information and facilitate Client workshops to review the Managed Technology and related data environments supporting threat monitoring and response operations. The Service is available in two different service tiers: Essentials and Premium. Trustwave will work with Client to onboard the Managed Technology to the Service and refine its configuration. Trustwave will also create a use case catalog in which Trustwave may document and manage use cases. Trustwave also offers a “renewal” version of Jumpstart if Client has previously onboarded the Managed Technology with Trustwave under a different service which will conclude as this Service commences. This “renewal” Jumpstart will incorporate the MXDR Jumpstart Essential components described below.

Service Tiers

The applicable service tier will be indicated in Client’s SOW or Order Form.

MXDR Jumpstart Essentials:

This service tier includes the following:

- Trustwave will coordinate Client and Trustwave interactions, Jumpstart tasks, and status reports.
- Trustwave will guide and assist Client in the transition to co-management of Microsoft Sentinel.
- Trustwave will review Microsoft Sentinel use cases to tune the alert volumes relative to Client’s purchased capacity and licensing restrictions to the extent Client provides such information to Trustwave.

- Trustwave will provide standard (non-custom) use cases and refine alerting and reporting. Client and Trustwave together will review requirements for all standard Microsoft Sentinel use cases, such as investigation details and response guidelines.
- Client and Trustwave will collaborate on the initial configuration of a policy and the settings of the Managed Technology for the Service and work together during the Term to maintain that configuration. This must be completed to achieve Steady State.
- Trustwave will assist Client and may provide recommendations for the deployment of Microsoft Defender XDR sensor/agent software.
- Trustwave will assist in providing recommendations for the configuration and policy set in Microsoft Defender XDR console.

MXDR Jumpstart Premium:

This service tier includes the above Jumpstart Essentials items and the following.

- Trustwave will create customized Microsoft Sentinel use cases tailored to Client’s environment (this is restricted to data sources currently contributing to Microsoft Sentinel, event sources supported by Microsoft Sentinel, and the monthly XDR Incidents Client has purchased for the Service).
- Trustwave will assist Client in onboarding supported data sources from the supported Microsoft Security products identified in SOW or Order Form.
- Trustwave may provide recommendations to Client in its efforts to connect Microsoft Sentinel to data sources not otherwise supported by Microsoft.

Additional activities may be available subject to Trustwave’s discretion. Any additional activities will be set out in the applicable SOW or Order Form.

Client Obligations

For Trustwave to provide Jumpstart, Client will

- assign a project manager to be single point of contact on behalf of Client’s business teams, technical team, and vendor group throughout the Service;
- to the extent required by Trustwave, provide evidence of internal approval for change orders;
- provide initial and ongoing Trustwave user and system remote access to the Managed Technology;
- be responsible for all Microsoft licensing and Azure consumption requirements;
- onboard log sources which are required to generate the XDR Incidents; and
- collaborate with Trustwave where Trustwave has identified persistent alerting issues during initial configuration of a policy and settings and work together to resolve configuration items prior to Steady State.

Trustwave Obligations

For Jumpstart, Trustwave will:

- maintain a project plan;
- schedule and coordinate technical calls and use case workshops, as appropriate;
- schedule and host a kick-off meeting with Client;
- provide new-user orientation materials and training regarding the Trustwave Fusion platform;
- keep Client informed and up to date on transition progress and report on risks and issues relating to transition management; and

- coordinate Trustwave technical delivery resources for
  - enrollment of Client and Client's indicated authorized user(s) to the Trustwave Fusion platform;
  - Connectivity (as described below);
  - monitoring of the volume of findings promoted in the Trustwave Fusion platform are within Client's purchased XDR Incidents volume;
  - completion of final operational readiness assessment to determine if Steady State has been reached.

Customized SIEM Optimization Program (Optional Add-On)

The Trustwave Customized SIEM Optimization Program ("**CSOP**") is an optional add-on service that can be purchased at any time during the Term. CSOP provides Client with enhanced SIEM environment support through custom use case development and implementation, as well as threat monitoring advisory. Specifically, CSOP extends the capabilities of the Service by providing structured, ongoing enhancement of SIEM threat monitoring analytics through tailored use case development and implementation.

While the ISA can develop tactical use cases, such as in response to an immediate threat requiring rapid detection, CSOP is a proactive approach to threat monitoring customization. CSOP can be purchased for an additional fee, as reflected in the applicable SOW or Order Form between Trustwave and Client.

24x7 Threat Analysis, Investigation, and Response

Trustwave will use Client's high-fidelity XDR Incidents, SpiderLabs threat intelligence, and the Trustwave Fusion platform to identify potential indicators of attack, or compromise, in Client's environment. The Service includes system-led and human-led (i) threat-focused detection analytics; (ii) threat investigation; and (iii) graphic summaries and reporting in the Trustwave Fusion platform.

Threat Analysis and Investigation

The Trustwave Fusion platform ingests XDR Incidents, evaluates these against SpiderLabs threat intelligence, and applies threat-focused detection analytics to seek out suspicious patterns. To the extent this results in Trustwave identifying an XDR Incidents as suspicious, Trustwave will generate Fusion Alerts with an associated priority level in the Trustwave Fusion platform.

Trustwave will indicate a Fusion Alert's priority level in the Trustwave Fusion platform. Priority levels are based the applicable Trustwave use-case, including classification, historical reliability, and confidence across all Trustwave clients, SpiderLabs threat intelligence, and attributes of the related XDR Incidents.

A description of each priority level follows:

Fusion Alert Priorities	
Priority	**Priority Description**
Critical	Fusion Alerts at this level potentially pose an immediate and high security risk to Client's environment, and can signal an active compromise, extensive damage, or total disruption of operations to high value assets in Client's environment. The underlying XDR Incidents, intelligence, confidence, and historical performance of the use case signal what might be immediate threats

	to Client systems. Fusion Alerts in this priority level are routed to the top of the global queue in the Trustwave Fusion platform for triage and analysis.
High	Fusion Alerts at this level potentially pose a high security risk to Client's environment, and can signal a potential compromise, severe damage, or disruption of operations to high value assets in Client's environment. The underlying XDR Incidents, intelligence, confidence, and historical performance of the use case signal what might be a high threat to Client systems. Fusion Alerts at this priority level are second to critical Fusion Alerts for triage and analysis within the queue in the Trustwave Fusion platform.
Medium	Fusion Alerts at this level potentially pose medium-level security risk and signal the potential for limited damage or disruption to standard assets in Client's environment. Fusion Alerts at this priority level are second to high Fusion Alerts for triage and analysis within the queue in the Trustwave Fusion platform.
Low	Fusion Alerts at this level are not immediately actionable and may require further investigation by Client to determine possible actions. Alerts that result in this priority require additional context, may signal known risks and deviations from security best practices, or may signal alerts where the Client security tools delivered the expected outcome and protected systems. Fusion Alerts at this priority level are displayed to Clients in the Trustwave Fusion platform for further investigation.
Informational	Fusion Alerts at this level are not immediately actionable and may require further inspection by Client to determine when there are possible actions. Alerts that result in this priority require additional context from Clients and may signal potential policy-based deviations. Fusion Alerts at this priority are displayed to Clients in the Trustwave Fusion platform for further investigation.

Then, Trustwave may:

- automatically add the Fusion Alert to a new or existing investigation, visualization, report, or security incident ticket ("**Security Incident**"). Trustwave may recommend next steps and tasks for Client action, in Trustwave's sole discretion;
- manually add the Fusion Alert to a new or existing investigation or Security Incident with details on Trustwave's examination, determination, and recommendation; or
- deem the Fusion Alert non-threatening by additional system or human-led analysis.

Trustwave creates and stores Security Incidents in the Trustwave Fusion platform. Security Incidents will reference any related Fusion Alerts and XDR Incidents. Trustwave will send Client notifications according to the Security Incident's assigned priority (see "Security Incident Escalations" below).

Security Incidents may include any of the following information:

- Summary of the Security Incident
- Analysis
- Recommendations
- List of Trustwave actions taken

- Requests for Client to perform recommended actions

In addition, at its sole discretion, Trustwave may:

- add additional Fusion Alerts and XDR Incidents to an existing investigation and Security Incident for related follow-up activity; and
- request Client collect and submit binary files and suspected malware within the Security Incident for SpiderLabs Malware Reverse Engineering. In such cases, Trustwave may add any further observations, Fusion Alerts, or recommendations identified by this process to the applicable Security Incident.

Client understands that not all Fusion Alerts may be deemed actionable. Non-actionable Fusion Alerts are not added to a Security Incident. XDR Incidents that are not classified as Fusion Alerts and Fusion Alerts that are not added as Security Incidents are still available for review by Client via the Trustwave Fusion platform either (i) in Event Explorer or (ii) as low and informational priority Fusion Alerts.

For any Fusion Alerts of a medium priority or higher but deemed non-actionable, Client may be able to review Trustwave's related investigation closure notes in the Trustwave Fusion platform. This means Trustwave has reviewed associated threat indicators and determined such indicators to be non-threatening due to context, threat intelligence, or other factors lessening the confidence that a threat has been identified. Trustwave provides such closure notes at its sole discretion. Such closure notes may include:

- intelligence resources reviewed;
- details available within XDR Incidents;
- factors that appeared as a threat but that can be attributed to testing, problem management, or change management processes;
- items that can be implemented or recommended as tuning measures for the Service or policy updates for Managed Technology and Managed Security Application; or
- recommendations for tuning unmanaged security technology configuration or policy updates.

Client understands that Trustwave may not investigate or may cease an investigation if Client takes assignment or ownership of an incident from any Microsoft portal, including Microsoft Sentinel and Microsoft Defender.

Threat Response

As part of Onboarding and during the Term, Trustwave and Client will agree to one of the following client-level response authorization protocols. These response authorization protocols are actions Trustwave may take on the Managed Technology natively or in the Trustwave Fusion platform. Such pre-authorizations comprise Client's "Response Authorization Protocol."

The following describes the two (2) Client options for Response Authorization Protocol.

- **Response Authorization Protocol – Green**: Trustwave has explicit permission from Client to initiate response actions native to the Managed Technology and/or Trustwave Fusion platform to contain a direct threat to any Client entity (which may include, and subject to change, users, devices, applications, identities) by any means without separate authorization from Client, at Trustwave's sole discretion.
- **Response Authorization Protocol – Red**: Trustwave will not initiate any response actions and will notify Client by creating a security incident, noting Trustwave recommended response actions. From there, Client is responsible and may implement Trustwave-recommended response actions.

Client understands that any recommended response actions, as described above, may include 1) response actions which were determined by Trustwave in the course of its threat analysis and investigation, 2) recommendations which may be provided by Client's integration of Microsoft Copilot for Security for which Client has explicitly authorized Trustwave to use in the course of threat analysis, investigation, or response, or 3) any Microsoft feature designed to provide response recommendations or automated attack disruption that's integrated with the Managed Technology.

Notwithstanding anything in this section, Trustwave and Client agree to the following:

- **Response Authorization Protocol – Green**: Trustwave may deploy automated responses and document such actions in the Trustwave Fusion platform. Trustwave may, in its reasonable discretion, decide not to act and instead discuss with Client.
- **Response Authorization Protocol – Red**: Unless otherwise defined, Trustwave will not implement manual or automated containment actions, unless Client requests actions or policy updates through the Trustwave change management process.
- **Policy and Non-Asset Basis Responses** – Client understands that any Response Authorization Protocol designations may be temporarily superseded where Trustwave deems emergency action is necessary to respond to time sensitive, emerging threats in Client's environment. To the extent such protocols conflict with the Response Protocol, Trustwave will instead act according to the Change Management protocol agreed between Client and Trustwave or as Trustwave reasonably sees fit.
- **Changes** – any changes to the Response Authorization Protocol by Client must be submitted by an authorized representative of Client within the Trustwave Fusion platform. Trustwave does not guarantee such updates will have immediate effect but will take reasonable steps to incorporate changes into Trustwave's ongoing response actions.

Client understands that Trustwave is not responsible for managing any existing or yet to be released Microsoft product feature designed to provide automated attack disruption or automated response action configured by the Client or Client's third-party vendor.

Client has the option to include and contract Trustwave to provide emergency response services for digital forensics and incident response (DFIR) actions.

Client Obligations

For Trustwave to provide this feature of the Service, Client will:

- retain exclusive responsibility for mitigating actual and potential threats to its environment;
- lead and execute Client processes for Security Incident management and incident response;
- regularly update Security Incident contacts and their respective accesses and information in the Trustwave Fusion platform including contact email, phone numbers, and contact order;
- utilize the Trustwave Fusion platform and mobile app to generate secure communications, notifications, and Service feedback;
- collaborate with Trustwave on security detection and response best practices, including Client deployed configurations, policy definitions, and settings that enable high fidelity XDR Incidents and allow timely threat detection;
- provide initial and ongoing Trustwave user and system remote access to the Managed Technology and Managed Security Application to accommodate Trustwave's remote analysis as defined by this service description;
- review and update Response Protocol and authorized actions;

- review Fusion Alerts, Security Incidents, notifications, and reports as made available in the Trustwave Fusion platform;
- notify Trustwave if events or reports are not available in the Trustwave Fusion platform as reasonably expected;
- resolve each Security Incident by providing Security Incident feedback, relevant personnel, and ensuring support and engagement of third parties, as reasonably required by Trustwave;
- provide Trustwave with requested information and confirmations in a timely manner. Client acknowledges failure to do so may inhibit Trustwave's ability to provide the Service;
- when requesting tuning configuration modifications, use change tickets in the Trustwave Fusion platform ("**Change Tickets**"). Such requests may include:
  - tuning of Fusion Alerts from recurring XDR Incidents which Client is unable to resolve using Client change processes; or
  - tuning of Security Incidents with exception conditions which Client does not find actionable and is unable to resolve using Client change processes; and
- identify Client personnel authorized to request Security Incident or Change Tickets, or request additional information.

Trustwave Obligations

For this feature and upon Client reaching Steady State, Trustwave will:

- allow authorized Client personnel (authorized by Client) access to the Trustwave Fusion platform to interact with Trustwave personnel and to monitor the Service and as a repository for Client communications for Security Incidents and tuning Change Tickets;
- collect and process XDR Incidents into Fusion Alerts;
- analyze and raise Security Incidents, Fusion Alerts, investigations, and reports identified by Trustwave from XDR Incidents in Client's environment;
- perform Response Authorization Protocol actions;
- periodically update the status of Security Incidents in the Trustwave Fusion platform and record communications between Client and Trustwave pertaining to such Security Incidents;
- review Client feedback;
- confirm that tuning and filtering Change Tickets are submitted by authorized Client contacts and notify Client when unauthorized requests are received;
- assess the potential risk that may result from implementation of a change request and advise Client on such assessment; and
- confirm Client approval to implement such a change request after reviewing risk assessment results with Client.

Security Incident Escalations

Client Security Incident contacts, defined in the Trustwave Fusion platform, will receive communications from Trustwave for Security Incidents via the Trustwave Fusion platform, the Fusion mobile app, email, phone, or Microsoft Teams chat. Client should promptly update notification groups in the Trustwave Fusion platform as needed.

Trustwave will assign priority levels to Security Incidents based on factors from Trustwave's investigation, which may include attack classification, SpiderLabs threat intelligence, security outcome, derived risk, impact, and properties of the XDR Incidents related to the Security Incident.

Trustwave will send Client notifications according to the Security Incident's assigned priority and using Trustwave integrated phone, Fusion mobile app, and email systems (see table below) and may include

Microsoft Teams chat. Client will document all communications, questions, clarifications, and feedback for the Security Incident in the Trustwave Fusion platform or Fusion mobile app.

Security Incident Priorities		
Priority	**Notification Procedure**	**Priority Description**
Critical (P1)	Phone, App, Email	Security Incidents at this level potentially pose an immediate and high security risk to Client's environment, and signal an active compromise, extensive damage, or total disruption of operations to high value assets in Client's environment. Investigations that result in this priority require Client to take immediate containment, response, or recovery actions to contain the Security Incident.
High (P2)	Phone, App, Email	Security Incidents at this level potentially pose a high security risk to Client's environment, and signal a potential compromise, severe damage, or disruption of operations to high value assets in Client's environment. Investigations that result in this priority require Client to take nearly immediate defensive actions to contain the Security Incident.
Medium (P3)	Email	Security Incidents at this level potentially pose medium-level security risk and signal the potential for limited damage or disruption to standard assets in Client's environment. Investigations that result in this priority require Client to take timely, but not necessarily immediate, action to contain the Incident.
Low (P4)	Email	Security Incidents at this level are not immediately actionable and may require further investigation by Client to determine possible actions. Investigations that result in this priority require additional context or may signal known risks and deviations from security best practices.

Microsoft Teams chat notification may only be initiated by Trustwave under the following circumstances and at Trustwave's sole discretion:

- For Security Incident priority level: Critical (P1);
- For Clients with Response Authorization Protocol: Green, whereby Trustwave deems immediate communication with Client may be necessary before a response action; and
- After all other notification procedures listed in the table above have failed to reach Client.

Microsoft Teams chat sessions are limited to Client's five (5) incident contacts listed in the Trustwave Fusion platform call tree. Trustwave reserves sole discretion to end the Microsoft Teams chat session immediately following security incident notification as described in this section. Trustwave will not accept incoming Microsoft Teams chat requests.

The Service may include the following Microsoft Security products or features as additional enrichment sources and as indicated in the applicable SOW or Order Form.

- Microsoft Copilot for Security (MCS): Trustwave may use this feature to facilitate Trustwave's investigation, response, and reporting. Client must give Trustwave explicit approval to use MCS. Trustwave's use of this feature is available on Client's MCS deployment only. Client is responsible for all fees that may be billed by Microsoft.
- Microsoft Defender Vulnerability Management (MDVM): Trustwave may use MDVM data to provide analysts with more context during an investigation. Trustwave will not perform any type of vulnerability management function, including patching or resolution.

Threat Hunts (TH)

As part of the Service, Trustwave will perform ad hoc threat hunts for indicators of compromise (IoC) using the Managed Technology.

Trustwave will solely:

- determine the scope of each TH, including the threats, indicators, and TTPs;
- assess the impact of any discovered and material threats relevant to Client's environment;
- inform Client of potentially impactful threats (as determined by Trustwave in its sole discretion) via a Security Incident ticket in the Trustwave Fusion platform;
- perform threat response actions in accordance with the above "Threat Response" section; and
- reasonably coordinate with and provide Security Incident-related information with Client's lead DFIR investigator or Client's approved delegate for incident management activities.

Microsoft Security Advisory (MSA)

This feature offers Client access to a set of Microsoft security and cybersecurity experts who act as the initial point of contact for Service-related security matters once the Service has reached Steady State. To this end, MSAs may provide the following activities:

Managed Technology	Activity	Activity Scope
All	Client Meeting	Included (upon request)
	Trustwave enriched customized reporting leveraging data from the Managed Technologies based on out-of-the-box templates and Trustwave best practices (as agreed by Trustwave and Client).	Included (upon request)
	Complex or bulk changes— limited to the scope of this Service	Included (upon request)
	Implementation of auto-notification or batch reporting of non-monitored alerts as requested by client and where technically supported.	Included

Microsoft Sentinel	Standard automations and playbooks—continuously updated from Trustwave’s catalog	Included
	Creation and maintenance of custom automation and playbooks	Included (upon request)
	Standard threat correlations – continuously updated from Trustwave’s catalog	Included
	Client requested security threat correlation or analytics	Included (upon request)
	Proactive addition of Trustwave vetted high-confidence emerging threat indicator(s) to Sentinel	Included
	Standard workbooks – continuously updated from Trustwave’s catalog	Included
	Custom workbooks – create or edit custom workbook	Included (upon request)
	Standard proactive tuning—Trustwave initiated tuning to improve alert fidelity and reduce noise in order to improve service performance.	Included
	Client requested Indicator of Compromise hunts.	Included (upon request)
Defender for Endpoint	Update Defender for Endpoints detections with Trustwave SpiderLabs Threat Intelligence – signature, behavioral, and reputation data	Included
	Trustwave initiated customized default detections for Defender for Endpoint	Included
	Custom requested Defender for Endpoints detections	Included (upon request)
	Microsoft Secure Score review and prioritization of recommendations	Included (upon request)
	Microsoft Exposure Score review and prioritization of recommendations	Included (upon request)
	Attack surface reduction –analysis of current attack surface rules and recommended improvements to meet best practices	Included (upon request)

	Ongoing review of Defender for Endpoint configuration and provide recommendations in line with Trustwave and vendor best practices when applicable	Included
Defender for Office	Ongoing review of Defender for Office configuration and provide recommendations in line with Trustwave and vendor best practices when applicable.	Included
	Standard proactive tuning—Trustwave initiated tuning to improve alert fidelity and reduce noise in order to improve service performance.	Included
	Email and collaboration reporting – Investigate the source, destination, and path of messages within the client environment, and create custom reports using available features within Defender for Office	Included (upon request)
Defender for Identity	Standard proactive tuning—Trustwave initiated tuning to improve alert fidelity and reduce noise in order to improve service performance.	Included
	Ongoing review of Defender for Identity configuration and provide recommendations inline with Trustwave and vendor best practices when applicable.	Included
Defender for Cloud Apps	Standard proactive tuning—Trustwave initiated tuning to improve alert fidelity and reduce noise in order to improve service performance.	Included
	Ongoing review of Defender for Cloud Apps configuration and provide recommendations in line with Trustwave and vendor best practices when applicable.	Included
	High investigation score users – notify Client of new users within Client’s environment that have an elevated investigation score	Included
	Trustwave will assist client with categorization and tagging of applications as sanctioned/unsanctioned within Defender for Cloud Apps.	Included (upon request)
	Review of current conditional access policies and recommendations for improvement based on best practices	Included (upon request)
	Changes to Defender for Cloud Apps policy configurations	Included (upon request)

The activities in the table above listed as “Included” are proactive and may be automated. Client does not have to take any action to start an included activity.

For an activity listed in the table above as “Included (upon request)”, Client must submit an MSA activity request ticket in the Trustwave Fusion platform to request such activity. Should Trustwave determine a request is out of the scope of this Service, additional Trustwave billable consulting services may be required. Trustwave will work with Client to scope any additional billable services.

Additionally, for activities listed as “Included (upon request)” in the table above, Trustwave will perform no more than one requested activity at a time. Client may request Trustwave to consider and scope at most one “Included (upon request)” activity per week.

The Service, including MSA activity, MSA activity service requests, and change requests are subject to the limitations (e.g., technical, availability, licensing, feature changes) imposed by the Managed Technology vendor (i.e., Microsoft). Trustwave reserves the right to modify the list of activities based on these limitations.

Tuning

Trustwave will perform tuning changes to the Managed Technology. At Trustwave’s sole discretion, Trustwave may modify the conditions of existing use cases, suppress the intake of XDR Incidents, or automate Fusion Alert notifications in the Trustwave Fusion platform to the extent such XDR Incidents reach a volume that could impair the Service. Client remains responsible for monitoring threat intake volumes so as not to impair the Service. Tuning will vary depending on the Managed Technology.

MSA Availability

The MSA will be available during normal business hours in the MSA’s location unless otherwise indicated. Trustwave may change the individual representative at any time.

Client Obligations

For Trustwave to provide this feature, Client will:

- establish and maintain communication with Trustwave;
- provide and maintain access for Trustwave to the Managed Technology as required by Trustwave to deliver the Service;
- collaborate with Trustwave as required in a timely manner;
- use the Trustwave Fusion platform to start an activity request or change request;
- provide information and documentation to Trustwave as required to perform the Service or activity; and
- participate in tuning and Service optimization activities as required by Trustwave.

Problem Management

A problem is a cause or potential cause of one or more incidents impacting the health of the Service. Client agrees to report problems through the Trustwave Fusion platform. Client and Trustwave agree to collaborate on problem resolution subject to Trustwave policy.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave’s Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable SOW or Order Form between Trustwave and Client.