Trustwave®

SERVICE DESCRIPTION

Managed Detection & Response (U.S. Government)

Overview

Trustwave's Managed Detection & Response service (U.S. Government) ("**Service**") provides 24x7x365 threat detection for cybersecurity alerts generated in the Trustwave Fusion platform ("**Fusion Alerts**"), emerging threat hunting, and threat response. Trustwave uses analytics, systematic enrichment, automation, reporting, visualizations, and workflow to conduct investigations and search for threats within those Client security solutions which are included in the Service as indicated in the applicable SOW or Order Form ("**Managed Technology**"). The following description sets out the parameters of the Service.

Core Features

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:

- Security Event information, Fusion Alerts, and Security Incidents (each as defined below)
- Device 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.

Security Events Ingestion & Log Source Support

The Trustwave Fusion platform will ingest from only a set list of log-based event sources outlined in the Data Source Ingestion Value available on the Trustwave Contract Documents webpage. Trustwave

maintains a defined list of log-based event sources supported by the Trustwave Fusion platform and the Service ("**Security Events**").

The Service includes unlimited collection of Security Events only for the total quantity of contracted, active endpoints in the endpoint detection and response (EDR) Managed Technology specifically set forth in the applicable SOW or Order Form between Client and Trustwave.

The Trustwave Fusion platform tracks its ingestion of Security Events from non-EDR Managed Technology. Ingestion is measured in millions of Security Events per day (MEPD) and offered at different amounts based on the non-EDR Managed Technology type and Client's purchased service tier. Client's service tier will be indicated in the applicable SOW or Order Form for the Service. The MEPDs allotted to each service tier per Managed Technology type are listed in SOW or Order Form and subject to change during the Term at Trustwave's sole discretion. Client may purchase additional MEPD allotments, and any such additional allotments will be indicated on the Order Form or SOW executed between Trustwave and Client. Client is responsible for monitoring its MEPD usage and maintaining it within the permitted allotment of its service tier. Client will take actions (including tuning and configuration changes) to maintain volumes within the service tier.

The Service is provided with a set data volume capacity (as set forth in the applicable SOW or Order Form between Client and Trustwave) ("**Data Volume Cap**"). Where Client's data and event volumes are found to exceed the Data Volume Cap, 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 reserves the right to tune, suppress, throttle or stop ingestion of data sources to maximize fidelity, align to security best practices, protect platform health, meet licensed levels, or other reasons as needed. Trustwave may bill Client for excessive alerts upon Client refusal to allow Trustwave to tune excessive alerts.

Trustwave does not support the ingestion and processing of all event-based log data as it requires evaluation of Trustwave's capability to detect specific threats, alert acquisition methods, and parsed log formats that change over time. Any changes to the Data Source Ingestion Value and Trustwave's ingestion, parsing, analysis, detection, automation, monitoring, and reporting on Security Events are at Trustwave's sole discretion.

The Service includes ingestion of Security Events solely from Managed Security Applications as outlined in the applicable SOW or Order Form between Trustwave and Client. Trustwave will classify any other EDR or SIEM products that were not included in the SOW or Order Form as TDR Value /Type C as outlined in the Data Source Ingestion Value and they will be treated as raw logs with no expectation of threat detection outcomes. Clients desiring to expand the Service to include additional Managed Security Applications will work with Trustwave on a Service change request.

Trustwave Fusion platform accounts are hosted in the United States.

Historical Log Access & Retrieval

Client will have access to collected Security Events for a rolling retention period of the most recent sixty (60) consecutive days during the Term of the applicable SOW or Order Form, beginning on the first day of such Term. Client may access such Security Events via the self-service feature in the Trustwave Fusion platform.

To access Security Events beyond the most recent sixty (60) consecutive days, Client may submit a ticket in the Trustwave Fusion platform requesting access ("**Access Request**"). Any Access Requests

(i) requesting a download of two (2) gigabytes or more, or (ii) totaling more than one (1) per calendar month are subject to additional Fees and are available only at Trustwave's sole discretion.

Correlation & Use Case Management

Trustwave maintains proprietary global processes for correlation and use case catalog management. This includes proprietary detection of high-fidelity attack scenarios and event sequences within the Trustwave Fusion platform using Trustwave intelligence and collected Security Events. Trustwave's proprietary global analytics and use cases are leveraged across all clients. Trustwave does not create custom or client-specific use cases. Trustwave may share its use case catalog with Client and retains sole discretion in determining when use cases are shared with Client, added, modified, or removed from 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 Security Application**") according to the following sections. For the avoidance of doubt, Trustwave will solely provide the Service for Managed Security Applications running on Managed Technology (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 for the Managed Security Application and work together during the Term to maintain that configuration. This must be completed to achieve Steady State (defined below).

When the Managed Security Application has 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 to the Managed Security Application 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.
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 *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 Security Application 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 Endpoint Management

Trustwave, at its discretion, may recommend version updates for the Managed Security Application. 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 health and availability of the alert and event data from Managed Security Application that is connected to the Trustwave Fusion platform. For on-premise applications, Trustwave will monitor the alert and event data ingestion using Trustwave Connect. The health and availability of the Client on-premise appliance(s), whether virtual or physical, and endpoints that connect to the Managed Security Application that are not directly connected to the Trustwave Fusion platform, are Client's sole responsibility to manage and monitor.

Connectivity

Client and Trustwave will work together to connect the Trustwave Fusion platform and the Managed Technology using one or more of the following connection methods (subject to the applicable SOW or Order Form between Client and Trustwave).

- **Trustwave Connect**: A virtual appliance jump box hosted in Client's environment that allows Trustwave to remotely connect the Trustwave Fusion platform to the Managed Technology. Trustwave will deploy Trustwave Connect based on the model of the Managed Technology indicated in the applicable SOW or Order Form.

- **Direct Connectivity**: A direct connection between the Managed Technology and the Trustwave Fusion platform using either:
    - Trustwave-hosted managed console;
    - Client-hosted managed console; or
    - API connection to the Trustwave Fusion platform (available only with cloud-based Managed Technology via API)

Additional Information

Where Trustwave Connect is used, Trustwave will provide Client the applicable Trustwave Connect deployment model and the necessary perimeter network access configurations for the Service.

Where a Client-hosted managed console is used to connect the Managed Technology to the Trustwave Fusion platform, Client is responsible for implementation and creating Trustwave-user accounts as requested by Trustwave. This connection method is only available to the extent explicitly agreed to by Trustwave in the applicable SOW or Order Form. Client acknowledges certain access methods may require increases in the applicable Fees.

Where a beta version of a Managed Security Application's API must be used, Trustwave provides no warranties regarding its availability, uninterrupted operation, or error-free performance.

Co-Managed Access Change Management

Trustwave may administer access to the Managed Security Application and may provide Client with access permissions to the Managed Security Application when Client requires co-management of the Managed Security Application's feature sets. Such additional access permissions may include:

- **Read Only**: Default option. Trustwave fully manages the Managed Security Application. Client can monitor Managed Security Application, but not directly alter configuration, policy, access, or version without contacting Trustwave.
- **Role Based**: Co-managed option (as permitted by Trustwave). Trustwave grants Client partial access to manage the Managed Security Application. See below for related restrictions.
- **Full Admin**: Co-managed option (as permitted by Trustwave). Trustwave grants Client full access to manage the Managed Security Application. See below for related restrictions.
- **Client Managed**: Client managed option. Client grants Trustwave full access to manage the Managed Security Application as designated by the Trustwave role-based access requirements.

If granted Role Based or Full Admin access permissions, Client agrees to the following shared change and change audit process:

- Restrictions: Before implementing any change to the Managed Security Application, Client will create a change ticket in the Trustwave Fusion platform, identifying which policies and configuration settings will change and of any other planned effects. Upon receiving the ticket, Trustwave may review changes made by Client and make recommendations.
- Client acknowledges this co-managed structure may result in increased risk of security incidents or Service outages. Client will work in good faith with Trustwave to remediate any such security incident and Client will perform a review of any Managed Security Application failure. If Trustwave reasonably determines that the security incident or outage was caused by a change or activity performed by Client on the Managed Security Application, Managed Technology, or Client-managed systems, Client will be solely responsible for the effects of the change and for completing and producing the root cause analysis.
- Client representatives with co-managed access to the Managed Security Application will be responsible for attaining reasonable competency and training in cybersecurity to make standard changes to the Managed Security Application's rules and configurations. Client is responsible for validating such competency and training.
- Client will address all Trustwave-initiated changes for access in a timely manner that allows Trustwave to maintain access and compliance with prescribed Service terms. Failure to respond to these requests will negatively impact the response time outlined in the Service description.

Client Obligations

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

- procure and maintain valid vendor software licenses and maintenance contracts applicable to the Managed Security Application;
- monitor and maintain patches, health, and connectivity of Client's non-Trustwave managed systems, software, and EDR agents to any Managed Security Application, including security application on-premise appliance(s) and networking equipment and applications.
- provide, when requested by Trustwave, prompt and legally permitted access to third-party vendor portals to allow for software and license downloads and provide necessary authorizations for Trustwave to act on behalf of the Client for management and maintenance purposes;
- submit Change Ticket requests, respond to tickets, and confirm scheduled change windows via the Trustwave Fusion platform;
- consider risk factors related to change requests and promptly provide requested information to Trustwave;
- review and assess Trustwave-initiated changes and promptly provide Trustwave with approval or rejection of such proposals;
- at Trustwave's reasonable request, provide pre-determined change control windows during which change management functions can be executed without ad hoc approval;
- inform Trustwave of all maintenance activities and changes in Client's environment that may impact Trustwave's ability to provide the Service; and
- provide Trustwave with access to the Managed Security Application.

Trustwave Obligations

- For this feature and upon Client reaching Steady State (see Onboarding feature below), Trustwave will provide product and security update recommendations and assistance with issues resulting from upgrades;
- provide Service-related remote assistance, support, and configuration within the Managed Technology and Managed Security Application. For the avoidance of doubt assistance for on-premise appliances will be limited to the Managed Security Application software operating on the appliance;
- attempt to resolve connectivity or application issues identified regarding the Managed Security Application to return it to a steady state of operation. Assistance for on-premises appliances will be provided after the Client has provided sufficient evidence of no existing environmental issues or self-initiated changes to the infrastructure that may negatively impact the steady-state operation of the appliance;
- perform assessment of a change request based on Trustwave's risk level and change categories and determine whether a change request is in-scope for the Service;
- Trustwave may notify Client if a change request is outside the scope of the Service or if additional charges will apply to a change request;
- perform change management activities only in compliance with Trustwave policies;
- Trustwave may audit any Client-directed change and confirm whether there are any errors or consequences resulting from the change. If Trustwave determines no additional action is required, Trustwave may close the relevant change ticket. If Trustwave's review raises any questions or concerns, Trustwave may communicate such questions or concerns to Client and Client will work with Trustwave to resolution.
- Trustwave will not be responsible for the design, implementation, effect, or any damages, direct or indirect, of any Client changes made to the Managed Security Application, 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 components: Client-side implementation and MSS Transition.

Client-side Implementation

Client will take the necessary steps to connect Client's systems which generate Security Events 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 and individual Trustwave-users 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 and Managed Security Application to accommodate Trustwave's remote system management and threat analysis and investigation.

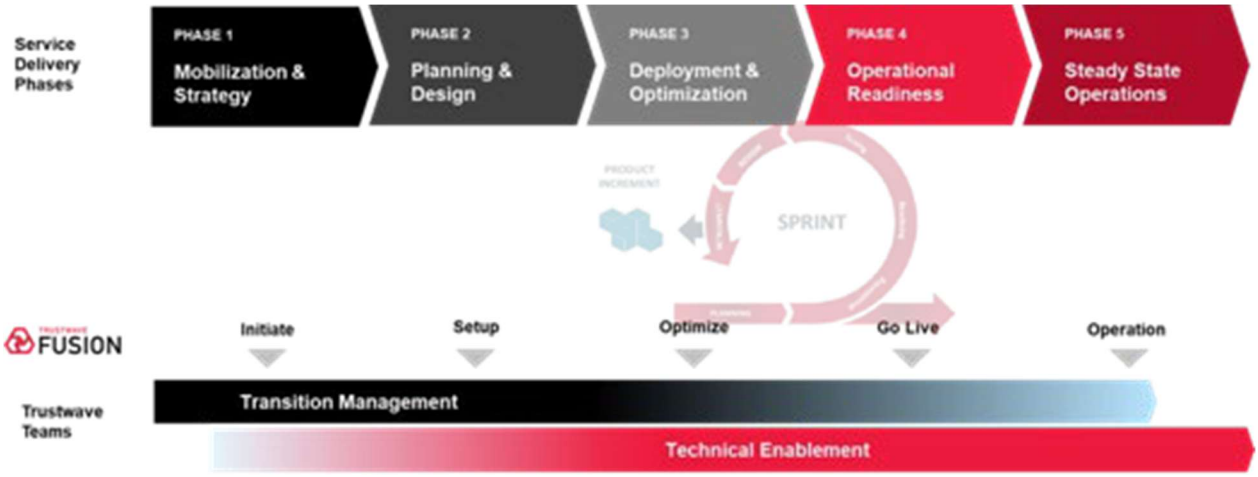
Trustwave will provide Client with an initial list of users during Onboarding. After Onboarding (during Steady State as defined below), Trustwave will provide Client with ongoing user access, update requests, and use change management tickets to maintain updated user access to the Client's Managed Technology and Managed Security Application. Client agrees to abide by the Systems Management section above and must use the Trustwave Fusion platform to document user updates. 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 and Managed Security Application.

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 (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:



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 and Managed Security Application or related telemetry;
- 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;

- upon Trustwave's request, confirm to Trustwave that Client systems are reporting to the Managed Technology and Managed Security Application in order to support log and alert collection;
- define initial Response Protocol and authorized actions (see details below); and
- ensure Managed Technology and Managed Security Application 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);
- 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 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.

24x7 Threat Analysis, Investigation, and Response

Trustwave will use Client's high-fidelity Security Events, SpiderLabs threat intelligence, and the Trustwave Fusion platform to identify potential indicators of attack in, or compromise of, Client's environment. The Service includes system-led and human-led (i) threat-focused detection analytics; (ii) threat investigation; and (iii) emerging threat hunting; (iv) threat response containment guided by Client's pre-approved Response Protocol; and (v) graphic summaries and reporting in the Trustwave Fusion platform.

Threat Analysis and Investigation

The Trustwave Fusion platform ingests Security Events, 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 a Security Event as suspicious, Trustwave will generate a Fusion Alert.

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

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 Security Events, 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 Security Events, 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 third to critical 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 Security Events. 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 Security Events 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, findings, 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. Security Events 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, Clients 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 Security Events;
- 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.

Threat Response

Trustwave and Client will co-develop pre-authorizations for response actions Trustwave may take on the Managed Technology within the Trustwave Fusion platform. Such pre-authorizations comprise Client's "Response Protocol" and are listed on the basis of individual-endpoints and groups of endpoints.

The following describes the TLP color designations that Client may assign to each individual-endpoint or group of endpoints included in the Response Protocol:

- **Green**: Trustwave may contain a direct threat to a Client endpoint or group of endpoints by any means without separate authorization from Client ("**TLP Green**");

- **Yellow**: Trustwave may contain a direct threat to a Client endpoint or group of endpoints by a pre-agreed set of actions using the Trustwave Fusion platform without separate authorization from Client ("**TLP Yellow**");
- **Red**: Trustwave will not act and will notify Client if Trustwave recommends a response action to a Client endpoint or group of endpoints. From there, Client may select and explicitly approve Trustwave-recommended response actions via the Trustwave Fusion platform ("**TLP Red**").

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

- **TLP Green and TLP Yellow Endpoints** – where an individual-endpoint or group of endpoints of the Managed Technology are designated as TLP Green or TLP Yellow, Trustwave may deploy automated responses and document such actions in the Trustwave Fusion platform. Trustwave may in its reasonable discretion decide not to take action for a TLP Green or TLP Yellow endpoint or discuss with Client instead.
- **Undefined Endpoints or TLP Red Endpoints** – for endpoints (i) not included in the Response Protocol or (ii) defined as TLP Red (including default assignment to TLP Red), Trustwave will not take action, unless Client provides separate and specific approval of the automated response using the Trustwave Fusion platform in acknowledgement to Trustwave's notification and recommendation.
- **Policy and Non-Asset Basis Responses** – Client understands that TLP 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 during Onboarding or as Trustwave reasonably sees fit.
- **Changes** – any changes to the Response 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.

Upon request by Client, the Service includes access to Trustwave's Dynamic List feature in the Trustwave Fusion platform, a resource that allows Client to subscribe the Managed Technology or Client-managed systems to receive automated IP, domain, and URL threat intelligence updates. Notwithstanding the Order Form or SOW, such access is on an as-is basis and without any warranties. Trustwave will publish and update the Dynamic List at its sole discretion. Client is responsible for determining what intelligence lists within the Dynamic List to access, what systems to enroll, and what policy actions to take from the lists. Client may subscribe the Managed Technology to Dynamic Lists and, if so, must agree to applicable Change Management protocols with Trustwave. Client understands that the Dynamic List feature may result in changes to Client assets that supersede the Response Protocol associated with such assets.

Trustwave will take threat response actions for the Managed Technology solely from the Trustwave Fusion platform. This Service is not a threat or incident response service. Client may contract Trustwave or a third-party to provide threat response services for further digital forensics and incident response 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 Security Events 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 Security Events 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 Security Events into Fusion Alerts;
- analyze and raise Security Incidents, Fusion Alerts, investigations, and reports identified by Trustwave from Security Events in Client's environment;
- perform Response Protocol authorized 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, or phone. Clients 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, including attack classification, SpiderLabs threat intelligence, security outcome, derived risk, impact, and properties of the Security Events related to the Security Incident. Trustwave will send Client notifications according to the Security Incident's assigned priority and using Trustwave integrated phone, app, and email systems (see table below). 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 the 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.

Emerging Threat Hunts (ETH)

As part of the Service, Trustwave will perform ETHs for indicators of compromise (IoC) using Client's Security Events and Fusion Alerts.

For an ETH, Trustwave will:

- determine the scope of each ETH, 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.

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 Statement of Work or Order Form between Trustwave and Client.