Trustwave®

SERVICE DESCRIPTION

Managed SIEM for Microsoft Sentinel

Overview

Trustwave's Managed SIEM for Microsoft Sentinel Service ("**Service**") offers Client threat detection services, operating in conjunction with Client, to monitor the Client-licensed or Client-owned Microsoft Sentinel security information and event management (SIEM) technology indicated in the applicable SOW or Order Form ("**Managed Technology**"). The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Form between Trustwave and Client.

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 on the Trustwave Fusion platform via web or mobile application:

- SIEM Alert information, Fusion Alerts, and Security Incidents (each as defined below)
- Health and availability incident tickets
- Reports and dashboards related to the Service
- Request methods for change support and management
- Methods of communication including tickets and chats

Such capabilities and related documentation 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.

SIEM Alert Ingestion & Log Source Support

Trustwave will collect cybersecurity alerts generated by the Managed Technology ("**SIEM Alert**") in the Trustwave Fusion platform. The Service includes ingestion of SIEM Alerts solely from the Managed Technology. The applicable SOW or Order Form between Trustwave and Client will indicate the monthly allowance of SIEM Alerts Client has purchased for the Term.

The Service solely includes ingestion of SIEM Alerts from the following Microsoft data sources into the Managed Technology ("**Microsoft Data Sources**").

Microsoft Data Sources	
Microsoft Entra ID	Microsoft Defender 0365
Microsoft Defender for Identity	Microsoft Defender for Cloud Apps
Microsoft Azure Activity	Microsoft Defender for Endpoint

Client may review currently supported SIEM Alerts in the Fusion Data Source Ingestion guidelines. Any changes to SIEM Alert 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	United States
EMEA	Germany
PAC	Australia

Historical Log Access & Retrieval

Client will have access to collected Fusion Alerts for a rolling retention period of the most recent ninety (90) consecutive days during the Term of the applicable SOW or Order Form, beginning on the first day of such Term. Client may access such SIEM Alert via the self-service feature in the Trustwave Fusion platform.

To access such collected Fusion Alerts beyond the most recent ninety (90) 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) totalling more than one (1) per calendar month are subject to additional Fees and are available only at Trustwave's sole discretion.

Fusion Alert Consumption Overages

The Service is provided and priced according to monthly SIEM Alert maximums, asset forth in the applicable SOW or Order Form. Trustwave will periodically review the volume of SIEM Alerts processed for Client in relation to the Service.

Where Client's SIEM alert volumes spike and are found to signal that Client will or has exceeded the agreed threshold for the current month, Trustwave may

- evaluate excess SIEM Alerts 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 SIEM Alerts from Client's systems at Trustwave's discretion;

Client will regularly review its SIEM Alert volume in the Trustwave Fusion platform and Trustwave may tune the Managed Technology configuration to stay within the purchased volume of SIEM Alerts. Moreover, where Client's SIEM Alert volumes are found to exceed the agreed threshold persistently by five percent (5%) or more on average over seven (7) 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 SIEM Application**") according to the following sections. For the avoidance of doubt, Trustwave will solely provide the Service for Managed SIEM 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 SIEM Application and work together during the Term to maintain that configuration. This must be completed to achieve Steady State (defined below).

When the Managed SIEM 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 SIEM 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 SIEM 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 SIEM Management

Trustwave, at its discretion, may recommend version updates for the Managed SIEM 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 Managed SIEM Application that is connected to the Trustwave Fusion platform to ensuring the receipt of alerts. The health and availability of the Client on-premise appliance(s), whether virtual or physical, and endpoints that connect to the Managed SIEM 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 a direct connection between the Managed Technology and the Trustwave Fusion platform via an API connection.

Change Management

Trustwave may provide Client with read-only access permissions to the Managed SIEM Application so that Client can monitor Managed SIEM Application, but not directly alter configuration, policy, access, or version without contacting Trustwave.

Client is responsible for its Microsoft Azure environment and to the extent Microsoft Azure management provides Client with access to the Managed SIEM Application, Client agrees to the following shared change and change audit process:

- Restrictions: Client will not implement any changes including configuration, content ingestion, or use case changes to the Managed SIEM Application. Instead, Client will create a change ticket in the Trustwave Fusion platform, identifying which policies and configuration settings the Client requests to change and of any other planned effects. Upon receiving the ticket, Trustwave may review the requested changes made by Client and may make recommendations or deny requested changes. Client acknowledges change request decisions are at the sole discretion of Trustwave.
- Client acknowledges if it gains additional access permissions, such permissions 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 SIEM 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 SIEM 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 access to the Managed SIEM Application will be responsible for attaining reasonable competency and training in cybersecurity to make standard changes to the Managed SIEM 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 SIEM Application;
- monitor and maintain patches, health, and connectivity of Client's non-Trustwave managed systems, software, and endpoint agents to any Managed SIEM 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;
- provide Trustwave with access to the Managed SIEM Application; and
- maintain read-only access for existing users and new Client users.

Trustwave Obligations

- For this feature and upon Client reaching Steady State (see Onboarding feature below), Trustwave will provide assistance with issues resulting from updates and changes to the Managed Technology and Managed SIEM Application;
- provide Service-related remote assistance, support, and configuration within the Managed SIEM Application;
- attempt to resolve connectivity issues identified by Trustwave pertaining to the Managed Technology and Managed SIEM Application to return it to a steady state of operation;
- 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 SIEM Application, Managed Technology, or Client-managed systems the Service relies upon.

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 SIEM Alerts 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 SIEM 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 SIEM 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 SIEM 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 (5^{th}) 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 SIEM Application or related telemetry;
- upon Trustwave's request, confirm to Trustwave that Client systems are reporting to the Managed Technology and Managed SIEM Application in order to support log and alert collection; and

- ensure Managed Technology and Managed SIEM 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;
    - review data flow, quality, and analysis subject to the scope agreed between Trustwave and Client in the applicable SOW or Order Form;
    - 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.

Microsoft Sentinel Jumpstart

The Microsoft Sentinel Jumpstart feature is an onboarding service for the Managed Technology and contributes towards Client reaching Steady State (defined below). Trustwave will gather information and review the Managed Technology and related data environments supporting threat monitoring operations. Trustwave will work with Client to onboard the Managed Technology to the Service and refine its configuration.

This feature includes the following:

- Trustwave will coordinate Client and Trustwave interactions, Microsoft Sentiinel Jumpstart tasks, and status reports.
- Trustwave will guide and assist Client in the transition to Trustwave's management of Microsoft Sentinel.
- Trustwave will provide standard (non-custom) use cases and refine alerting and reporting. At Trustwave's discretion, Trustwave may update the standard use case repository.

Client Obligations

For Trustwave to provide SIEM Jumpstart, Client will

- assign a 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 access to the Managed Technology
- be responsible for purchasing and abiding by license requirements of the vendor of the Managed Technology;
- onboard the Microsoft Data Sources which are required for the Managed Technology to generate the SIEM Alerts; and
- collaborate with Trustwave where Trustwave has identified persistent alerting issues during initial configuration of a policy and settings of the Managed Technology for the Service and work together to resolve configuration items prior Steady State.

Trustwave Obligations

For Microsoft Sentinel Jumpstart, Trustwave will

- maintain a deployment plan;
- schedule and coordinate technical calls, 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 deployment progress; and
- coordinate Trustwave technical delivery 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 SIEM Alerts volume;
    - completion of final operational readiness assessment to determine if Steady State has been reached.

24x7 Threat Analysis, Investigation, and Response

Trustwave will use Client's high-fidelity SIEM Alerts, 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) graphic summaries and reporting in the Trustwave Fusion platform.

Threat Analysis and Investigation

The Trustwave Fusion platform ingests SIEM Alerts, 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 SIEM Alert as suspicious, Trustwave will generate an alert with an associated priority level in the Trustwave Fusion platform ("**Fusion Alert**"). For the avoidance of doubt, Trustwave will perform human-led threat investigation of Fusion Alerts only within the Trustwave Fusion platform and the Managed Technology.

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 SIEM Alerts. A description of each priority level follows:

Fusion Alert 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 SIEM Alerts, 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 SIEM Alerts, 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:

i. 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;
ii. manually add the Fusion Alert a new or existing investigation or Security Incident with details on Trustwave's examination, determination, and recommendation; or
iii. 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 SIEM Alerts. Trustwave will send Client notifications according to the Security Incident's assigned priority (see below). Security Incidents may include any of the following information:

- Summary of the 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 SIEM Alerts 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 developed 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. SIEM Alerts 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 SIEM Alerts;
- 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; or
- recommendations for tuning unmanaged security technology configuration or policy updates.

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 incident management and incident response;
- regularly update 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 SIEM Alerts and allow timely threat detection;
- provide initial and ongoing Trustwave user and system remote access to the Managed Technology to accommodate Trustwave's remote analysis as defined by this service description;
- 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 SIEM Alerts 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;
- identify Client personnel authorized to request Security Incident or Change Tickets, or request additional information; and
- agree to maintain existing users, and create new user accounts, with 'read-only' access.

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 SIEM Alerts into Fusion Alerts;
- analyze and raise Security Incidents, Fusion Alerts, investigations, and reports identified by Trustwave from SIEM Alerts in Client's environment;
- 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 Priority Levels

Client 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 assigns 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 SIEM Alerts 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.

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.

Tuning and Content Management

This feature offers Client the following services:

- SIEM Content Management – Trustwave will manage and add additional SIEM content (at Trustwave discretion). This may include the following activities:
  - New use case version management;
  - Interactive dashboard support;
  - Maintenance of threat feeds which Trustwave may have agreed to include in the Service; and
  - Creation and maintenance of Trustwave approved watchlists.
- Tuning – Trustwave will perform tuning changes to the Managed Technology. At Trustwave's discretion, Trustwave may modify the conditions of existing use cases or suppress the intake of findings in the Trustwave Fusion platform to the extent such findings reach a volume that could impair the Service. Client remains responsible for monitoring threat intake volumes so as to not impair the Service.

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; and
- collaborate with Trustwave as required in a timely manner;
- provide information and documentation to Trustwave as required to perform the Service; 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 Statement of Work or Order Form between Trustwave and Client.