SERVICE DESCRIPTION

Co-Managed SOC

Overview

Trustwave's Co-Managed SOC service ("**Service**") offers Client threat detection services operating in conjunction with Client's own identified and agreed upon security information and event management (SIEM) technology ("**SIEM Technology**"). The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Service Features

The Service includes the following features:

SIEM Jumpstart

The SIEM Jumpstart feature is an onboarding service for the SIEM Technology. It is available in two different service tiers: Essentials and Premium. Trustwave will work with Client to onboard the SIEM Technology to the Service and refine its configuration. Trustwave will provide architecture documentation identifying the points of connection between the SIEM Technology, Client's environment, and Trustwave's environment. Trustwave will work directly with Client in onboarding Client to the Service and the Trustwave Fusion platform.

Service Tiers

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

Jumpstart Essentials: This service tier includes the following:

- Trustwave will coordinate all Client and Trustwave responsibilities, tasks, and status reports related to delivery of the feature.
- Trustwave will guide and assist Client in the transition to co-management of the SIEM Technology.
- Trustwave will review SIEM use cases applicable to the SIEM Technology to tune the alert volumes relative to Client's purchased capacity and licensing restrictions associated with the SIEM Technology of which Trustwave is made aware.
- Trustwave will provide standard (non-custom) use cases and refine alerting and reporting.

Jumpstart Premium: This service tier includes the above items from the Essentials service tier and the following:

- Trustwave will created customized SIEM use cases tailored to Client's environment (however, this is restricted to event sources supported by the SIEM Technology and the capacity Client has subscribed to).

- Trustwave will onboard new SIEM data sources for identified deployed products.
- Trustwave will draft and provide a security operations center (SOC) people, process, and technology gap assessment report.

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

Use Case Accelerator

(Optional SIEM Jumpstart Extension)

The Use Case Accelerator feature extends SIEM Jumpstart to the duration of the Term of the Service. The applicable SOW or Order Confirmation will indicate if Client has purchased this feature.

During the Use Case Accelerator feature, Trustwave will continue the work of the SIEM Jumpstart feature by conducting quarterly use case analysis workshops.

Trustwave will provide the following on a quarterly basis for the Term of the feature:

- Use case updates and further refinement to existing rules
- Trustwave may assist Client in connecting additional devices to the SIEM Technology
- Threat detection and response maturity report
- Use case library, pipeline, and technology implementation roadmap updates
- SOC processes and playbook manual updates
- People and technology capacity modelling updates

Client Obligations for SIEM Jumpstart and Use Case Accelerator

For Trustwave to provide these features of the Service, 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, provide Trustwave with evidence of internal approval for change orders;
- update Client's contracts providing the SIEM Technology so as to license Trustwave with necessary access and user rights; and
- onboard log sources which are required for the SIEM Technology.

Trustwave Obligations for SIEM Jumpstart and Use Case Accelerator

For these features, Trustwave will

- assign a project manager who will be a single point of contact for and first point of escalation throughout the duration of each feature;
- maintain a project plan; and
- schedule and coordinate technical calls and use case workshops, as appropriate.

24x7 SIEM Threat Analysis and Investigation

The Trustwave Fusion platform ingests SIEM alerts from the SIEM Technology and processes such data through threat intelligence and threat-focused detectors.

Trustwave will display escalated SIEM alerts in the Trustwave Fusion platform ("**Threat Findings**"). Trustwave analysts will review the Threat Findings and will access the SIEM Technology to conduct investigation with the aim of gaining more context from collected events and activity trends.

For Threat Findings that are deemed "**Actionable Threat Findings**" and after the above investigation process, Trustwave will generate an incident ticket in the system ("**Incident**"). Client will receive notifications according to the Incident's assigned priority (see below).

Threat Findings which are not deemed actionable are "**Non-Actionable Threat Findings**" and no Incident is created. Client may review Trustwave's closure notes relating to Non-Actionable Threat Findings in the Trustwave Fusion platform. These closure notes may document (i) implemented or recommended service tuning or (ii) managed or unmanaged security technology policy updates (each provided at Trustwave's discretion).

Trustwave may suppress SIEM alerts without prior Client approval due to conversion rate, volume, and persistence.

Incident Priority Levels

Trustwave will assign a priority level (P1 – P4) to each Incident. Subject to any notification procedures separately agreed in a SOW or Order Confirmation, Trustwave will notify up to five (5) Client-designated point(s)-of-contact for each Incident and according to the notification procedure and its assigned priority.

Priority	Notification Procedure	Priority Description
Critical (P1)	Phone call & Email	Incidents at this level are actionable, potentially pose a 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 Incident.
High (P2)	Phone call & Email	Incidents at this level are actionable, 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 Incident.
Medium (P3)	Email	Incidents at this level are actionable, 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	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.

Client may request that Trustwave follow additional or different notification policy standards as a set of guidelines. Such guidelines have no binding effect on Trustwave.

Client Obligations

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

- provide access to the SIEM Technology for Trustwave analysts to perform triage and investigation;
- review Threat Findings, Incidents, and reports as made available in the Trustwave Fusion platform;
- work with Trustwave to resolve each Incident by providing relevant personnel and ensuring support of third parties, as reasonably required by Trustwave. Client acknowledges that Client retains exclusive responsibility for mitigating actual and potential threats to its environment;
- 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; and
- work with Trustwave to focus alert use cases on urgent threat conditions requiring monitoring with a reasonable level of conversion rate.

Trustwave Obligations

For this feature Trustwave will

- collect and monitor SIEM alert data via the Trustwave Fusion platform for use cases meeting agreed upon conversion, volumetric, and process standards;
- maintain availability of Threat Findings in the Trustwave Fusion platform according to Trustwave's data retention procedures;
- investigate and analyze Threat Findings and notify Client of Threat Findings according to the above procedures; and
- maintain updated status of Incidents in the Trustwave Fusion platform and record relevant communications between Client and Trustwave pertaining to such Incidents.

Security Technology Management

The Service is provided as a co-managed model where both Client and Trustwave assume the role of administrator and manage the SIEM Technology according to its system design. This feature is offered for both on-premises and cloud native types of SIEM Technology. The aspects of this feature apply to each type of SIEM Technology according to the following table.

Service Type	On Premises	Cloud Native
Change Management	X	X
Product and Security Updates	X	
Health Monitoring	X	
Backup and Restore	X	X

Change Management

Trustwave will manage and monitor the configuration of the SIEM Technology according to the following terms:

Client-Initiated Change Management

Trustwave will assess and implement change requests submitted by Client through the Trustwave Fusion platform. Trustwave evaluates such requests against industry best practices and the change's potential impact on Client's security environment. Trustwave will schedule and notify Client of changes Trustwave expects may disrupt Client's environment, and Client will approve or deny these scheduled change windows. Trustwave will also notify Client if a change request is outside the scope of the Service and, therefore, will only be performed at Trustwave's discretion.

Trustwave will categorize changes requested by Client according to the following types:

Change Request Type	Description
Emergency Change Request	A change which is 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 SIEM Technology.
Standard Change Request	A change which is • non-scheduled; • is proactive in nature; • does not alter architectural design or functions (such as new features or functionality) of the SIEM Technology; • does not require a re-install or redesign; or • does not require SIEM consultant resources to complete the update or upgrade.
Complex Change Request	Large changes that are planned and scheduled in advance because such changes • could significantly impact the functions of the SIEM Technology; • could alter the architectural design of the SIEM Technology; • could require proof of concept to be completed prior to scheduling; • errors during this change could have significant outage consequences; • add a new feature or functionality of the SIEM Technology; • require a re-install, reconfiguration, or replacement or requires SIEM consultant resources; or • will take longer than the 24 hours to complete and therefore cannot be completed under existing change time agreement or objectives.

Trustwave may deny performing any Complex Change Request and require Client to purchase additional services for such change request.

Client acknowledges that denial of a scheduled change window may impact Trustwave's ability to provide the Service.

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 will review, assess, and notify Trustwave of approval or non-approval of each proposed change. Trustwave will perform the change according to the change schedule agreed between Client and Trustwave.

Co-Managed Access Change Management

Trustwave will provide Client with access to the SIEM Technology. While receiving the Service with such co-managed access, Client agrees to the following shared change and change audit process:

- Before implementing any changes to the SIEM Technology, Client will create a 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 perform a root cause analysis. If Trustwave reasonably determines that the security incident or outage was caused by a change or activity performed by Client, Client will be solely responsible for the effects of the change and for completing and producing the full root cause analysis.
- Client representatives with co-managed access to the SIEM Technology will be responsible for attaining reasonable competency and training in cybersecurity to make standard changes to the SIEM Technology's rules and configurations. Client is responsible for validating such competency and training.

Product and Security Updates

The Service includes the application of security updates, product updates, and patches. Client's failure to implement required security updates, product updates, and patches as required by Trustwave may adversely impact the operation and functionality of the SIEM Technology or the Service.

Trustwave will monitor the availability of security updates, product updates, and patches and apply such updates to the SIEM Technology according to the following:

- Updates or security patches that include bug and vulnerability fixes will be reviewed by Trustwave and applied to the SIEM Technology only when the update applies to any active subscriptions or feature set.
- Trustwave will schedule product updates and security updates available under the relevant SIEM Technology application license or maintenance contract with Client prior to implementation.
- Trustwave will use reasonable efforts to accommodate Client's preferred maintenance window to minimize disruptions. Trustwave will implement the relevant product updates and security updates according to its assessment of priority.
- Trustwave is not responsible for maintaining or upgrading the SIEM Technology's operating system or any hardware.

Update types include:

- **Security Content Updates**: New content for protection engines, initiated by the vendor of such protection engines, to address latest threats. Such updates typically do not interfere with proper function of the SIEM Technology.
- **Patches or Hotfixes**: Updates to address immediate and specific product issues initiated by the vendor for such products. Client acknowledges such patches or hotfixes may inhibit proper function of the SIEM Technology.
- **Product Feature Updates**: Feature updates provided by the vendor of the applicable product. These updates will typically cause brief downtime or restart of the SIEM Technology. Application of these updates requires a pre-defined change control window coordinated with Client. Trustwave will assess such updates on a case-by-case basis as to whether the update would be treated as a standard change request or a complex change request (see table above).

Health Status Monitoring

For on-premises SIEM Technology, the Service includes health and availability monitoring. Trustwave will seek to assess the cause of any detected issue and then remediate the issue if able. If remediation steps available to Trustwave are not successful and if a certain outage type, Trustwave will notify Client and provide subsequent updates to Client.

If Trustwave identifies a health issue with the SIEM Technology, Trustwave will file an incident ticket and provide Client with details related to the outage. Trustwave may include in the incident report recommended mitigation strategies to bring the SIEM Technology back to production performance and necessary changes to its configuration to recommence the Service.

Health monitoring metrics supported by Trustwave will vary according to the SIEM Technology included in the Service. Health monitoring metrics may include:

- **Network Availability**: Determines if the SIEM Technology shows as available via the network interface.
- **CPU Utilization**: Provides measurement of CPU utilization and warns of overutilized CPU that could threaten the SIEM Technology's functions.
- **Disk Space**: Provides advanced warning of full disk/volume/filesystem utilization.
- **Heat Indicators**: Alerts Client if the SIEM Technology reaches extreme temperature (only applies to physical appliances and not for VM implementations).
- **Component Connectivity**: Monitors system components for their uptime activity, their connections, their availability of data, etc.
- **Data Management**: Monitors for license quota or queue thresholds and abnormal thresholds of data flow (low data, high data).
- **System Errors**: Tracks logs and errors of system functions to monitor stability of the SIEM Technology.

Backup and Restore

Trustwave will back up the SIEM Technology configuration and policy using regular polling and will help ensure the latest version of the configuration is saved if a recovery is required. Backups are kept for ninety (90) days from initial back up action.

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 SIEM Technology;

- provide Trustwave with access to vendor support sites to allow for software and license downloads and provide necessary authorizations for Trustwave to act on behalf of Client for management and maintenance purposes (all as relates to the SIEM Technology);
- inform Trustwave of all maintenance activity in Client's environment and changes that may impact Trustwave's ability to provide the Service;
- access the Trustwave Fusion platform to submit change request, respond to tickets, and confirm the scheduled change windows;
- work in collaboration with Trustwave regarding relevant risk factors related to a given change request as part of change risk classifications and provide requested information in a reasonable timeframe; and
- if required by Trustwave, provide pre-determined change control windows for change management functions.

Trustwave Responsibilities

For this feature Trustwave will

- attempt to resolve connectivity or system issues identified to return the SIEM Technology to a steady state of operation;
- provide remote assistance, support, and configuration, in respect of any repaired or replaced SIEM Technology to restore it to a steady state of operation; and
- perform change management activities when requested and in compliance with Trustwave policies and inform Client of implemented changes.

Information Security Advisor (ISA)

This feature offers Client access to a Trustwave representative with security expertise to customize and enhance the Service.

Single Point-of-Contact

An ISA serves as Client's single point-of-contact for obtaining analytical support and escalating technical and security-related activities. Trustwave will assign a primary Trustwave representative (an ISA) to Client during the Term of the Service. Trustwave reserves the right to change the individual representative at any time provided it does not materially disrupt the Service. The ISA will be available to Client to advise on a variety of security- and threat-related topics according to the service tier indicated in the SOW or Order Confirmation. The ISA will host regular meetings with Client on topics which may include security status, tuning opportunities, incident reviews, and service updates.

Monitoring & Reviews

During the Term of the Service, Trustwave will perform the following monitoring tasks and topical reviews:

- **Dark Web Monitoring** – Trustwave will continuously monitor the dark web resources, noting any findings it deems relevant to Client.
- **Fusion Data Review** – Trustwave will perform a regular human-led investigation of Client specific data in the Trustwave Fusion platform data lake.
- **Architecture Review** – Following initial onboarding to the Service or following a significant change to Client's security environment, Trustwave will review any provided materials relating to Client's network topology diagrams, policies, processes, and procedures to both familiarize Trustwave with Client's environment and to provide recommendations for security improvements (at Trustwave's discretion).

- **Industry Monitoring** – Trustwave will conduct ongoing monitoring of information security activities and trends which may affect Client's industry (as indicated by Client and agreed with Trustwave).
- **Emerging Threat Monitoring** – Trustwave will conduct ongoing monitoring of various cybersecurity intelligence sources with regard to emerging cybersecurity threats.

Client-Specific Customization

This feature also helps to tailor the Service to Client's specific environment. This may include:

- **Customized Reporting** – Trustwave reviews Client's Trustwave Fusion data lake to produce Client-specific reports focusing on information agreed upon between Trustwave and Client.
- **Educate and Update Delivery Teams** – Trustwave reviews Client's security environment to provide delivery teams for concurrent Trustwave services with additional context into Client's security environment.
- **Tuning** – Trustwave will review use cases and perform tuning exercises at Trustwave's discretion. This will vary depending on the SIEM Technology. This includes the following activities:
    - Data source volume expansion support
    - Existing rule creation and tuning (around data sources onboarded to the SIEM Technology)
    - Active log collection
    - Disk and data storage availability and capacity

Trustwave will not add, remove, or change rules in the SIEM Technology without approval from Client. Client may request Trustwave create additional rule content. Trustwave may supply rule recommendations on available SIEM integrated data sources. Trustwave will not add or integrate new data types and technologies, design, or updated SIEM content to integrate that data source in the ISA feature.

Executive Sponsor

In addition to the assigned ISA, Trustwave will assign an executive- or management-level representative to Client ("**Executive Sponsor**"). The Executive Sponsor will be available to participate in meetings with Client's executives (as agreed between Client and Trustwave). Client may request Trustwave to facilitate an executive business review (EBR) where Trustwave hosts a formalized meeting to cover operational topics and present metrics and updates to Client's senior leadership.

Service Management

Trustwave will provide guidance regarding additional Trustwave technologies and services that Client may benefit from in improving their security maturity. Trustwave will monitor Client's data usage thresholds with regard to any limitations established in the applicable SOW or Order Confirmation to inform Client of possible room for expansion of such services.

Client Obligations

For Trustwave to provide this Service, Client will

- establish and maintain communication with Trustwave;
- collaborate with Trustwave as required;
- configure Client's systems as required to enable the Service and any other service purchased by Client from Trustwave;
- provide information and documentation to Trustwave as required to perform the Service;
- where Client has purchased Managed Detection and Response (MDR) services, respond in a

timely manner to Trustwave regarding Incidents (see service descriptions) logged in the Trustwave Fusion platform;
- participate in tuning and service optimization activities as required;
- resolve deviations from any agreed project plan in a timely manner; and
- reimburse Trustwave's travel and expenses when incurred from activities requested by Client.

Trustwave Obligations

For this Service, Trustwave will

- review relevant documents with Client to coordinate and manage technical activities;
- work with Client to maintain communication throughout the Term;
- coordinate, manage, or execute technical and advisory tasks as may be agreed between Trustwave and Client;
- provide reports at Trustwave's discretion; and
- help resolve Service issues, escalating with Client or within Trustwave, as applicable.

Core Trustwave Features

The Service includes the following core features which are standard to many of Trustwave services:

Trustwave Fusion Platform

The Trustwave Fusion platform is Trustwave's proprietary cloud-based cybersecurity platform. Client will be automatically enrolled in the Trustwave Fusion platform as a part of the Service. Client will have access to the following on the Trustwave Fusion platform:

- Event information, Threat Findings, and Incident tickets
- Client's reports and dashboards
- Request methods for change support and management
- Multiple methods for Client to securely communicate with Trustwave and the ability to upload documentation, security policies, and more

Trustwave Connectivity

The Service includes the following options to connect Client's log sources with the Trustwave Fusion platform. Trustwave will provide one or more of the following options in accordance with the SOW or Order Confirmation.

Trustwave Connect

Trustwave Connect collects log data from Client's security solution(s). Trustwave Connect facilitates collection of log data via syslog, REST APIs, and other supported methods. It is hosted by Client or its designated cloud, virtualization, or data center.

The following deployment models are available for Trustwave Connect:

- Virtual Appliances (included in the Service): VMWare, Amazon Web Services, Microsoft Hyper-V, and Azure
- Physical appliances (additional fee)

Client may be required (i) to install a Trustwave Connect solution within its environment and establish the necessary network access for the Service and (ii) to set up event data so it is sent to Trustwave.

Direct Connectivity to the Trustwave Fusion platform

For certain SIEM Technology, the Trustwave Fusion platform may permit direct connectivity from Client's environment for log collections via an API. Trustwave and Client will work together to set up direct connectivity, as applicable and as agreed in the applicable SOW or Order Confirmation. Client may have access to self-service options for onboarding Client's security solutions.

Problem Management

Trustwave will perform service failure analysis and suggest solutions designed to address the suspected causes of one or more Service interruptions in the form of an Incident post-mortem document. Trustwave will provide an Incident post-mortem document for P1 and P2 severity Incidents and Client may request similar reports for P3 and P4 severity Incidents and Trustwave will provide at its discretion.

Additional Information

Consumption Overages

The Service is provided and priced according to SIEM alerting volume thresholds set forth in the applicable SOW or Order Confirmation. Trustwave may, from time to time, review the volume of data and events processed for Client in relation to the Service.

Where Client's data and event volumes are found to exceed the agreed threshold (as indicated in a SOW or Order Confirmation) by twenty-five percent (25%) or more on average over any three (3) month-period, Trustwave may either

- request that Client agree to amend the current Order Confirmation or SOW to accommodate a higher threshold of data and event volumes and corresponding price change.
- suppress, throttle, or filter excessive data and events from Client's systems.

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

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 Confirmation between Trustwave and Client.