SERVICE DESCRIPTION

Security & Compliance Monitoring

Service Description Overview

Trustwave's Security and Compliance Monitoring services enable the Client to submit Log Data from supported Log Source devices to the Trustwave Platform for collection, correlation, storage, analysis, investigation and reporting. The Security and Compliance Monitoring service consists of:

Service Provisioning – the performance of remote activities required to establish the service to a steady state; deploy and connection of the Collector(s) to transport Log Data the Trustwave Platform; the collection and assessment of the Provisioning Questionnaire and the initial configuration and baselining of the Collector(s); Portal account provisioning and user orientation.

Collector Device Management – the ongoing configuration, management and maintenance of Collector(s) and implementation of Security Updates and Product Updates. The Trustwave Security Operations Center (SOC) teams provide these services through globally located facilities.

Reporting and Exploration – access to interactive functionality via the TrustKeeper Client Portal.

There are **four** monitoring, analysis and detection service options available:

- **Cloud Log Monitoring** – collection and storage of Log Data in the Trustwave platform, access to data via the Trustkeeper Portal.
- **Managed Compliance Monitoring** – collection and storage of Log Data plus periodic human analyst review from a compliance perspective; includes a Daily Report indicating completion of compliance review and Client access to the Trustkeeper Portal
- **Periodic Threat Review** – collection and storage of Log Data plus automated Use Cases and other analysis producing Threat Findings and periodic human analyst review of collected Logs and generated Findings, at least once every 24 hour period. Includes a Daily Report indicating the results of the daily review and Client access to the Trustkeeper Portal
- **Managed Threat Detection** – collection and storage of Log Data plus automated Use Cases and other analysis producing Threat Findings and 24X7 real-time human analyst review of collected Logs and generated Findings. Analyst review includes investigation, notification and where applicable remediation advice. Includes Client access to the Trustkeeper Portal.

Service | Feature	Acquisition from ~600 log sources	Storage in Trustwave Platform	Self-service access via Trustkeeper Portal	Daily Log Collection Report	Automated Analysis	Analyst Review – periodic high level	Analyst Review – real time and ongoing
Cloud Log Monitoring	X	X	X	X			
Managed Compliance Monitoring	X	X	X	X			
Periodic Threat Review	X	X	X	X	X	X	
Managed Threat Detection	X	X	X	X	X		X

Pricing Model

The **Cloud Log Monitoring and Managed Compliance Monitoring** services will be billed per log source, grouped and priced by class of source; Workstation, Server, Network or Policy.

The **Periodic Threat Review and Managed Threat Detection** services will be billed in a tiered system; banded pricing defined by multiple metrics – Count of Log Sources, Volume of Data Storage, Events per Day. In the case of extreme variance in the relationship of the 3 metrics, EPD shall be considered the primary measure.

For all metrics, an average is measured and recorded over a given Quarter (3-month period). There will be a yearly review on or around the contract anniversary date and if frequent overages of 25% or more on any of the metrics have been observed in the Quarterly measurements Trustwave may require the customer to move to a more appropriate price tier for the next year or reconfigure their Log Sources to reduce the source volume, events collected or the storage used. If consistent under-utilization is noted, the customer will be informed that more log sources may be on-boarded to the service or a move to a lower tier may be considered for the next year.

The Client will be notified by Trustwave that an adjustment is required within 45 days. A contract addendum will be executed to note the new tier.

Reports on current metrics are available upon request from the Trustwave SOC; Submit requests using the TrustKeeper Client Portal or email Trustwave support team.

Available tiers

i. 5M events/day, 2GB/day, 10 data sources (MTD only)
ii. 10M events/day, 5GB/day, 20 data sources
iii. 25M events/day, 12GB/day, 50 data sources
iv. 50M events/day, 23GB/day, 95 data sources
v. 75M events/day, 35GB/day, 145 data sources
vi. 100M events/day, 47GB/day, 195 data sources
vii. 175M events/day, 81GB/day, 340 data sources
viii. 250M events/day, 116GB/day, 480 data sources
ix. 325M events/day, 151GB/day, 625 data sources

x. 500M events/day, 233GB/day, 965 data sources

BASE FEATURES OF SERVICES

The Security and Compliance Monitoring services include the following basic service features:

- TrustKeeper Client Portal providing access to:
  - Tracking of provisioning progress;
  - 24x7 Event and Finding reporting and exploration;
  - downloadable software applicable to the Security and Compliance Monitoring services; and
  - Incident, change and support requests creation and management;
- Supply and delivery of Collector(s);
- Initial policy configuration, baseline and tuning of the Collector(s),
- 24x7 technical assistance email support;
- Management and maintenance of Collector(s), including related Product Updates and Data Module Updates;
- Subscription to one of Cloud Log Monitoring, Managed Compliance Monitoring, Periodic Threat Review or Managed Threat Detection.

Collector device options

Depending on the complexity of the Client's Log Source devices and / or Log Data, one or more of the following Collector device(s) will be required:

- Trustwave Log Collector (LCA) is a physical, virtual or public-cloud device for collection of Log Data via syslog, SNMP; flat files via FTP and SCP; DB connections via JDBC, and via the following proprietary application programming interfaces; Windows, OPSEC LEA (Checkpoint), Cisco Sourcefire, Cisco SDEE and REST API. Deployed and managed by Trustwave. Hosted by the Client or their designated cloud, virtualization or data centre provider.
- Trustwave SIEM (Enterprise): Available in cases where requirements warrant the Hybrid Managed Threat Detection Service. See Managed SIEM Service Description.

Collector deployment models

The following Collector deployment models are available for the Security and Compliance Monitoring service:

- Physical Appliances: The Collector model for deployment in the Client's environment is based on the size and scope of the Log Data for collection (refer https://www.trustwave.com/en-us/resources/library/documents/trustwave-siem-appliances/)
- Virtual Appliances: the Collector is available as VMWare, Amazon Web Services, Microsoft Hyper-V and Azure virtual images.

CLOUD LOG MONITORING – OPTION

Overview

Cloud Log Monitoring is a base service feature option, which may be selected by the Client and includes the following features:

- Collection of selected Log Data on the Trustwave Platform;
- Normalization of Log Data to Events;
- 24x7 access to charts, reports and interactive search functionality through the TrustKeeper Client Portal;
- 1-year storage of Log Data

Trustwave Responsibilities

- Collect Log Data via the Trustwave Platform via automated processes;
- Maintain availability of Events in the TrustKeeper Client Portal.

Client Responsibilities

- Review Events in the TrustKeeper Client Portal as required.
- Notify Trustwave if Events are not available in the TrustKeeper Client Portal as expected.

MANAGED COMPLIANCE MONITORING – OPTION

Overview

Managed Compliance Monitoring is a base service feature option, which may be selected by the Client and includes the following features:

- Collection of selected Log Data on the Trustwave Platform;
- Normalization of Log Data to Events;
- 24x7 access to charts, reports and interactive search functionality through the TrustKeeper Client Portal;
- 1-year storage of Log Data;
- Trustwave analyst review of Log Data and Events for compliance-related activity on a daily basis. Trustwave's Security Operations Center (SOC) will review on a periodic basis and at least one time per day notify Client to any concerns as per the agreed escalation procedures, generally via an Incident in the Trustkeeper Client Portal;
- 24X7 access to email support;
- Daily, Monthly and Quarterly Reports.

Trustwave Responsibilities

- Collect and Monitor Log Data via the Trustwave Platform via automated processes;
- Review Events and help in identification of Findings via automated processes and via periodic review by human analysis;

- Create Incidents and notify Client when compliance and security concerns are detected during periodic review.
- Maintain availability of Events and Findings in the TrustKeeper Client Portal. Generate and publish the relevant reports to the TrustKeeper Client Portal.

Client Responsibilities

- Review Event and Finding activity in the TrustKeeper Client Portal. Review reports published to the TrustKeeper Client Portal.
- Notify Trustwave if Events, Findings or relevant reports are not available in the TrustKeeper Client Portal, as expected.

PERIODIC THREAT REVIEW – OPTION

Overview

Periodic Threat Review is a base service feature option, which may be selected by the Client and includes the following features:

- Collection of selected Log Data on the Trustwave Platform;
- Normalization of Log Data to Events;
- 24x7 access to reports and interactive search functionality for Events through the TrustKeeper Client Portal;
- 1-year storage of Log Data;
- Automated Use Cases, Correlation and other analysis for identification of Threats, indicated by the creation of Findings.
- Trustwave analyst review of Log Data, Events and Findings. Trustwave's Security Operations Center (SOC) will review on a periodic basis, at least one time per day and notify Client to significant Threats as per the agreed escalation procedures, generally via an Incident in the Trustkeeper Client Portal;
- Daily, Monthly and Quarterly Reports.

Trustwave Responsibilities

- Collect Log Data via the Trustwave Platform via automated processes;
- Maintain availability of Events in the TrustKeeper Client Portal. Generate and publish the relevant reports to the TrustKeeper Client Portal.
- Perform automated analysis of collected Events in the Trustwave analytics platform;
- Review, at least once in each 24 hour period, the collected events and generated Findings, notifying the Client that the review was performed via a daily summary.

Client Responsibilities

- Review Event activity in the TrustKeeper Client Portal. Review reports published to the TrustKeeper Client Portal.

- Notify Trustwave if Events or relevant reports are not available in the TrustKeeper Client Portal, as expected.
- Review the daily review summary

MANAGED THREAT DETECTION – OPTION

Overview

Managed Threat Detection is a base service feature option, which may be selected by the Client and includes the following features:

- Collection of selected Log Data on the Trustwave Platform;
- Normalization of Log Data to Events;
- 24x7 access to reports and interactive search functionality for Events through the TrustKeeper Client Portal;
- 1-year storage of Log Data;
- Automated Use Cases, Behavioral Analytics, Correlation and other analysis for identification of Threats, indicated by the creation of Findings.
- 24X7 Trustwave analyst review of Log Data, Events and Findings. Trustwave's Security Operations Center (SOC) will monitor threat Findings and notify Client to actionable Threats as per the agreed escalation procedures, generally via an Incident in the Trustkeeper Client Portal;
- 24X7 access to telephone support;
- Daily, Monthly and Quarterly Reports.

Trustwave Responsibilities

- Collect and Monitor Log Data via the Trustwave Platform via automated processes; Review Events and help in identification of threat Findings via automated and manual review processes;
- Maintain availability of Events and Findings in the TrustKeeper Client Portal. Generate and publish the relevant reports to the TrustKeeper Client Portal.
- Generate notifications of Findings via the TrustKeeper Client Portal.

Client Responsibilities

- Review Event and Findings activity in the TrustKeeper Client Portal.
- Review reports published to the TrustKeeper Client Portal. Notify Trustwave if Events or relevant reports are not available in the TrustKeeper Client Portal, as expected.

Reporting and data access

The Security and Compliance Monitoring services include the following available self-service reporting features accessed through the TrustKeeper Client Portal:

- Interactive Dashboard;
- Pre-defined reports;
- Interactive searches for Events, Findings, Log Data and Assets;
- Incident management;
- 1 year of Events and Findings;
- Export of search results up to a predefined record limit;
- For large exports of up to 12 months of Log Data, Events or Findings, which can accessed securely through the TrustKeeper Client Portal, contact Support.

Threat Detection

Overview

Trustwave's proprietary threat analysis engine considers client log data plus Trustwave and client security and infrastructure information to help identify potential indicators of attacks and attempts to compromise a Client's network environment. The Periodic Threat Review and Managed Threat Detection services include security-focused use cases and is augmented by the Global Threat Operations (GTO) team of Security Analysts. PTR and MTD share a base set of rules, with MTD also including extended and advanced detection utilizing a more complex set of rules, behavioral analytics and machine learning.

- Automated analytics are applied to the Events sent to the Trustwave Platform by the Collector(s). Based on threat intelligence, use cases, behavioral analytics, machine learning and correlation rules within the Trustwave analytics engine. A Finding is created and a level of importance is allocated to each;
- Analyst manual review and hunting may also result in Findings (MTD service only);
- Sources subscribed to Periodic Threat Review will be subject to periodic review by the Trustwave Global Threat Operations team of security analysts, monitoring for significant potential security concerns. Discovered threats will be escalated to the customer via Incidents in the Trustkeeper Portal.
- Sources subscribed to Managed Threat Detection receive real-time monitoring and analysis by the Trustwave Global Threat Operations team of security analysts. Discovered threats will be escalated to the customer via Incidents in the Trustkeeper Portal as they are detected.

Automated Threat Detection and Standard correlation rules

Periodic Threat Review and Managed Threat Detection include an evolving set of automated analysis use cases for Threat Detection. Use cases may include but are not limited to:

- account lockouts
- failed administrator authentications

- audit trails cleared
- account privileges modified
- time sync errors
- network traffic anomalies
- anomalous login behavior
- audit system errors
- brute force authentication attempts
- configuration changes
- security audit trails cleared
- escalation of high priority Intrusion Detection and Endpoint Protection events
- multiple suspected attacks from same source
- multiple suspected attacks to same target
- failed login (same user) on many hosts
- recurring operational errors
- source-specific escalations by event ID (critical events as defined by the log source)
- source or target is in Known Bad Actor watchlist

Trustwave's Threat Detection rules are managed by an internal Content Team and are under continuous improvement and integration. Rules may vary by service level. The above list is a subset and example set. Actual rules in production are subject to change.

Analytics and Use Case Workshop

Log Sources subscribed to Managed Threat Detection are subject to analysis via the standard base use cases described above and plus additional automated and human analysis selected for maximum effectiveness based on a Use Case Workshop review. The Use Case Workshop is a one-time 2 to 4-hour session at service inception between Trustwave MSS-SIEM, GTO and Content Teams and the Client. The goal of this session is to select from the Trustwave Use Case Library an effective set of use cases and procedures based on the Client's subscribed data sources, environment, security maturity and capabilities. The output of the Use Case Workshop will be a defined set of Use Cases, Configurations, Runbooks and escalation procedures. The Use Case Workshop process is initiated independently and after completion of service provisioning described below.

Trustwave Responsibilities

- Meet with Client's designated representative for information gathering and ongoing discussion regarding threat detection for their environment within the capabilities of the Trustwave platform using configurations available in the Use Case Library;

- Define and implement the Client's set of Use Cases;
- Define the Client's escalation procedures for threat Findings if this differs from the standard escalation procedures established in the standard provisioning processes defined below.

Client Responsibilities

- Designate representative to meet with Trustwave to discuss threat detection;
- Review and approve selected Use Cases and Runbooks developed as a result of the Use Case Workshop.

Global Threat Operations monitoring and threat analysis

The Trustwave Global Threat Operations (GTO) team is located in globally disparate facilities and performs additional human analysis and investigation of Events and Findings for subscribers to the Daily Threat Review and Managed Threat Detection service.

Security threat investigation and incident identification

The GTO team has established incident investigation processes that provide for a consistent methodology of investigation across the globally distributed GTO teams. This process includes the advice and guidance from Trustwave Spider Labs malware research, threat intelligence and incident response teams. The GTO team will evaluate the available information it has to the point of helping to identify a potential attack attempts or Security Incidents. Where the investigation identifies a Security Incident, the GTO team will notify the Client of the results. Where the investigation does not result in a Security Incident, the GTO team will record the investigation without Client notification. The Client may access the history of investigations performed by the GTO via the TrustKeeper Client Portal.

- Security Alerts are analysed by the GTO team on a 24 / 7 / 365 basis
- GTO analysts leverage all available Client information and intelligence associated with the Security Alert to determine the severity of the Security Alert.
- Where warranted, the GTO analyst will escalate a Finding being investigated, to a Security Incident and assign a priority. The priority level defines the response actions to be taken by the GTO and the Client.
- The GTO analyst categorizes the Security Incident based on the descriptions specified in Table 2 below.

Table 1: Criticality of Incident

Priority	Analyst Response	Recommended client Response	Priority Description
Critical (Sev1)	Phone call & Email	Immediate	Security incidents at this level are actionable, high risk events which are actively compromising or damaging the client environment. Investigations that result in this priority require immediate action to contain the threat.
High (Sev2)	Phone call & Email	One to four hours	Security incidents at this level are actionable, high risk events that have the potential to cause severe damage to client environments. Investigations that result in priority require clients to take nearly immediate defensive actions.
Medium (Sev3)	Email	Twelve to twenty four hours	Security incidents at this level are actionable, medium-risk events that have the potential to cause limited damage to client environments. Investigations that result in priority require clients to take timely, but not necessarily immediate action.
Low (Sev4)	Email	Informational Only	Security incidents at this level are not immediately actionable, and may require further investigation by the client to determine possible actions.

Table 2: Category of Incident

Category Number	Security Incident Category	Category Description
CAT-0	Security Assessments (Network Defense Testing)	This category encompasses approved penetration testing and vulnerability scanning (both internal and external).
CAT-1	Unauthorized Access	In this category, an individual gains access without permission to a network, a system, an application, data, or other resource. This includes attack vectors such as privilege escalation, command injections, and brute force login attempts.
CAT-2	Denial of Service (Dos/DDoS)	This category is comprised of any attempt that successfully prevents or impairs normal authorized functionality of a network, system or application.
CAT-3	Malicious Code	The successful installation of any malicious software which compromises the security or functionality of a system or application. (e.g. virus, worm, trojan, adware, keylogger)
CAT-4	Improper Usage	This category is used to classify a situation in which an individual or individuals violate the client organization's acceptable use policies (e.g. peer-to-peer file sharing where there is a policy against such activity).
CAT-5	Reconnaissance Activity (Scans/Probes/Attempted Access)	This category identifies unauthorized attempts to obtain information about systems, networks and applications (e.g. port scans, operating system fingerprinting, service identification). Anomalous activity that is deemed to warrant further investigation by the client, but which cannot immediately be

		determined as malicious falls into this category.
CAT-6	Trend Analysis	Anomalous activity that is deemed to warrant further investigation by the client, but which cannot immediately be determined as malicious falls into this category.

Trustwave Responsibilities

- Investigate and analyze Findings, help identify false positives and notify Client in the case of a suspected actual or potential threat.
- Help identify and prioritize Security Incidents and notify designated Client personnel based on the priority of the incident and the appropriate response identified. Classify Security Incidents according to the categories defined.
- If needed, escalate the Incident based on its priority and according to the service level agreement ("SLA").
- Create an exception rule or turn off the relevant rule, for identified false positives;
- Maintain updated status of Security Incidents on the TrustKeeper Client Portal. Record all communications in the Ticketing system.

Client Responsibilities

- Validate the prioritization of a Security Incident according to its business impact and notify Trustwave of priority classification errors.
- Work with Trustwave to resolve each Security Incident by providing relevant personnel and ensuring support and engagement of third parties as required.
- Provide Trustwave with requested information and confirmations in a timely manner.
- Maintain access to the Client TrustKeeper Portal to confirm updated status of Security Incidents.
- Request changes in accordance with the Trustwave change management process and use and access the TrustKeeper Client Portal to log tickets, receive notifications, view, download and track the status of and respond to, Security Alerts and Security Incidents.

Provisioning and Implementation

Provisioning and implementation

The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with the Client to provision and implement the Collector(s) into the Client's environment so that the Collector(s) can be handed over to the SOC for on-going management, maintenance and support. Please see the Trustwave Provisioning Guide for additional details on the service implementation.

Device and environment assessment

- Trustwave provisioning engineers work with the Client to help ensure optimal configuration, including Log Source device(s) to ensure they are Supported Device(s);

Collector and Log Source configuration

- Trustwave provisioning will work with the Client to verify that:
- The Collector(s) have been supplied and delivered to the Client's premises or where applicable that the Collector software and image files are available for download from the TrustKeeper Client Portal;
- The Collector(s) are configured and able to communicate with Trustwave Platform for Log Data collection and device management and access control;
- The Log Source devices are configured to send data to the Collector(s);

Device Baselining

- During baselining the GTO analysts monitor the Collector(s) and work with the Client to tune the devices into an approved state for Trustwave standard operations.
- Collector(s) are monitored to identify inconsistencies or errors with the Trustwave Platform requirements, such as Log Data level and signature sets and recommendations are made for tuning the Collector(s) and Log Source(s);
- Once the Collector(s) are optimally configured, the baselining period ends, and the Collector(s) are transitioned to the SOC operations for monitoring and management.

Trustwave Managed Security Portal

- The Trustwave Managed Security portal provides clients with access to the expertise of the SOC staff and the security information and analysis provided by the supporting Trustwave managed Services infrastructure.
- The Trustwave Portal provides a method for the Client to Securely communicate with Trustwave MSS Provisioning and SOC Personnel to upload documentation and security policies and and includes Designated client contact information.
- Allows client to review current security events and Security Alerts of Client's Trustwave-monitored service, as well as historical data; and
- Create and track Change tickets and support.

Trustwave Responsibilities

- Supply and deliver the Collector(s).
- Assist the Client to configure the Log Source device(s) based on information provided by Client so that collectors are functioning according to the service delivery design and collecting, storing and correlating log data.

Client Responsibilities

- Provide remote access to on-premise infrastructure to accommodate installation and configuration of Collector(s). Make available an onsite resource capable of installing of the Collector(s) and troubleshooting the Client environment.
- Provide appropriate credentialed access to Trustwave, to the Log Source device(s). where applicable.

- Provide and maintain a secure connection between the Collector(s) and the Trustwave Platform, that is compatible with available Trustwave connection standards.
- The Client is responsible for the initial and ongoing configuration of the Log Source(s) to send the relevant Log Data to the Collector(s).

Collector Device Management

Device management overview

- The Security and Compliance Monitoring service includes the configuration, 24 x7 health monitoring and provision of Product Updates and Data Module Updates to the Collector(s). These management features ensure that the Collector(s) are performing their function within the Client environment as designed.
- The Trustwave SOC manage the Collector(s) to ensure that the Collector(s) are active; Track the version of firmware or software that is active on the Collector(s); Apply Product Updates and Data Module Updates to the Collector(s).

Health status

- The health status monitors the network availability of the Collector(s) to ensure they are visible to the Trustwave Platform.
- The Collector(s) are monitored to help detect when these devices are no longer showing as active within the Trustwave Platform. This includes Initial steps taken to assess the cause of the offline status of the relevant device and remediate the issue if possible;
- The SOC analysts will contact the Client's technical contact or other designated contact to notify the Client if remediation steps available to Trustwave are not successful;
- The notifications sent to the Client regarding the device status will be provided within the time requirements specified in the SLA.
- The SOC analyst will activate an RMA process and provide remote assistance; support and configuration, in respect of any repaired or replaced Collector(s).

Product Updates and Data Module Updates

The Trustwave SOC will monitor the availability of Product Updates and Data Module Updates and apply those updates to the Collector(s).

- When a Product Update or Data Module Updates becomes available, a Ticket will be created and assigned to the Client by the Trustwave SOC;
- Product Updates and Data Module Updates available will be scheduled with the Client for implementation;
- While the Trustwave SOC will give consideration to accommodate the Client's preferred maintenance window and apply any features with the least disruption to the Collector(s), as possible the Trustwave SOC will implement the relevant Product Updates and Data Module Updates within timeframes required depending on priority, to ensure that the Collector(s) are operating, and the Security and Compliance Management service is provided, as designed.
- Security and Product Updates-All Data Module Updates and Product Updates for Collector(s) software and underlining Collector OS will be completed during version upgrades and Bug fixes will be applied as Product Updates to the Collector(s) only when applicable to that device.

Trustwave Responsibilities

- Maintain management connection to the Collector(s). Monitor the Collector(s) to ensure their active online status and that they are available.
- Notify Client within SLA timeframe if management connection is unavailable and cannot be restored by Trustwave.
- Identify available Product Updates and provide remote assistance, support and configuration, in respect of any repaired or replaced Collector(s).
- Apply Data Module Updates and Product Updates as they are made available within timeframe required depending on the relevant update's priority.
- Create a Security and Compliance Monitoring service Ticket and schedule the Product Update and / or Data Module Update with the Client.
- Attempt to resolve any connectivity or system issues identified in order to return the device to a steady state of operation.

Client Responsibilities

- Inform Trustwave of all Client environment maintenance activity and changes that may impact on Trustwave's ability to provide the Security and Compliance Monitoring service, as designed. Inform Trustwave about any planned or unplanned changes to Log Source device(s).
- If Client receives notification from Trustwave that the output of the Log Source device(s) is exceeding the Collector(s) capacity levels; Approve provisioning of additional Collector(s) if Log Data volumes are not reduced;
- Provide and provision the infrastructure required to host additional Collector(s) pursuant to specifications provided by Trustwave. Maintain the required connectivity from the Collector(s) to the Trustwave Platform.
- Access the TrustKeeper Client Portal, respond to Tickets and confirm scheduled implementation of Product Updates and Data Module Updates.
- When requested by Trustwave, provide onsite support, for the Collector(s), to resolve connectivity or support issues.
- In relation to the RMA Process-Confirm delivery of an RMA Device; Perform the physical installation of an RMA Device; Contact the SOC to arrange for Trustwave remote support and configuration of an RMA Device.
- Procure and maintain valid vendor software and hardware licenses and maintenance contracts for Log Source device(s) that are not owned or managed by Trustwave.
- The Client acknowledges that the implementation of necessary Product Updates and Data Module Update is not an optional feature of the Security and Compliance Management service and failure to implement a required Product Update or Data Module Update as required, may adversely impact the operation and functionality of the Collector(s).

Change Management

Overview

- Trustwave maintains an overall change control and configuration management procedure for its support infrastructure and associated managed services. Changes that could affect the operation of Client systems are coordinated with appropriate Client IT staff. Trustwave establishes an email

address for each Client contact that is used to support communication with the Client and its service contractors responsible for administration of its networks.

- The SOC will assesses and implements change requests submitted by the Client or SOC through the TrustKeeper Client Portal. All requests are evaluated to help ensure that they are aligned with the features included with the service and will not detrimentally impact the security of the Client environment. Typical change request for the Security and Compliance Monitoring service are:
- Configuration changes to the Collector(s) as requested by authorized Client contact or a GTO analyst.
- Change reversals as requested by an authorized Client contact.

Trustwave Responsibilities

- Perform change management activities when requested and in compliance with Trustwave policies.
- Validate that the request was submitted by an authorized Client contact, and notify Client if validation is not successful.
- Determine whether the request is in-scope with the terms of the Service. Source additional information as necessary to support the implementation of the change request.
- Assess the potential risk that will result from implementation of the change request and advise Client of the outcome. Confirm Client approval to implement the change request after reviewing risk assessment results with Client. Confirm Client acceptance of implemented changes.
- When authorized Client personnel request that Trustwave roll back or reverse a change request:
- Confirm receipt of Client's request for a change reversal. Confirm completion of the change rollback upon successful execution of change reversal activities.
- Execute joint testing with Client to validate the rollback is aligned to Client's request, and gain Client confirmation of the same.
- Update the change request with information on rollback changes.
- Notify Client a change request is outside the scope of the Service and or if additional charges will apply to a change request.

Client Responsibilities

- Submit change requests using the TrustKeeper Client Portal. Provide Trustwave with requested information in a reasonable timeframe.
- Provide resources to review the risk assessment relating to requested changes.
- Review, assess and notify Trustwave of approval or non-approval to a proposed change request.
- When required, authorized Client personnel may request that Trustwave roll back or reverse a change request; Submit reversal requests using the TrustKeeper Client Portal, emailing or phoning the Trustwave support team.
- Provide resources to execute joint testing and confirm the change reversal is aligned with the Client-submitted request. Confirm completion of the change rollback request.
- The Client acknowledges that Change requests that exceed two (2) man days of effort is deemed a project and is subject to acceptance by the Client of separately quoted additional charges.