SERVICE DESCRIPTION

Threat Detection & Response – Managed Detection

Service Description Overview

Trustwave's Threat Detection & Response services (the "Services") enable the Client to submit data from supported Log Sources to the Trustwave Fusion Platform for collection, correlation, storage, analysis, investigation and reporting. The Services consist of:

Service Provisioning – the performance of remote activities required to establish the Service to a steady state; deployment and connection of Collector(s) to transport data to the Trustwave Fusion Platform ; the collection and assessment of the Provisioning Questionnaire; the initial configuration and baselining of the Collector(s) data flow and analysis; Trustwave Fusion Platform account provisioning and user orientation.

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

Exploration, Reporting and service interaction – access to interactive functionality via the Trustwave Fusion Platform.

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

- **Managed Detection Essential** – collection and storage of Log Data, automated use cases and other analysis producing Threat Findings with Analyst Review of such data at least once every 24 hours. Includes a daily report indicating the results of such daily review and Client access to the Trustwave Fusion Platform.
- **Managed Detection Complete** – collection and storage of Log Data, automated use cases and other analysis producing Threat Findings and 24X7 real-time human analyst review of such data. Includes Client access to the Trustwave Fusion Platform.

BASE FEATURES OF SERVICES

The Services include the following basic features:

- Trustwave Fusion Platform providing access to:
  - Tracking of provisioning progress;
  - 24x7 log, Event and Threat Finding reporting and exploration;
  - downloadable software applicable to the services; and
  - Incidents, 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 Managed Detection Essential or Managed Detection Complete.

Data Collection Options

Trustwave Log Collector ("LCA") resides on the Trustwave Connect Device. LCA facilitates collection of Log Data via syslog, 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 selected REST APIs. Deployed and managed by Trustwave. Hosted by the Client or its designated cloud, virtualization or data centre or by Trustwave in Trustwave data centres or cloud as the deployment warrants.

Collector Deployment Models

The following Collector deployment models are available for the Services:

- Physical Appliances
- Virtual Appliances: Trustwave cloud, VMWare, Amazon Web Services, Microsoft Hyper-V and Azure virtual images.

Trustwave Fusion Platform

Trustwave Managed Security Services provide the Client with comprehensive security operations delivered by Trustwave's Threat Prevention (SOC), Global Threat Operations (GTO) and SpiderLabs teams working out of Trustwave's worldwide ASOCs. These teams deliver services using Trustwave Fusion Platform (or "Fusion"), a cloud-based cybersecurity platform that serves as the foundation for the Trustwave managed security services, products and other cybersecurity offerings. Trustwave Fusion Platform is deployed in secure public cloud and physical data centers worldwide.

Trustwave Fusion Platform provides clients with access to the expertise of the SOC and GTO staff and the security information and analysis provided by the supporting Trustwave managed services infrastructure.

- Trustwave Fusion Platform provides a method for the Client to securely communicate with Trustwave MSS Provisioning, SOC and GTO Personnel.
- Allows Client to review current Events and Threat Findings of Client's Trustwave-monitored service, as well as historical data; and

- Create and track change tickets and support.
- Provides 1 year of events and Threat Findings;
- Allows Export of search results;
    - For exports of in excess of 1 million records contact support. Trustwave will perform the export and work with the Client to arrange transport of storage media if online delivery is not efficient. Client assumes cost and risk of transport.

For clients who require country specific operational resources, Trustwave is able to offer service delivery resourcing for SOC and GTO based services. These services will include delivery exclusively utilizing Fusion deployed in Trustwave data centers in the specified country and staffed by country specified employees. Data will be collected, processed and stored in the specified country's data center instance of Fusion.

Service defaults delivery and resource staffing:

- Country base for SOC resources: worldwide
- Country base for GTO resources: worldwide
- Country base for Fusion: worldwide

Provisioning and Implementation

Provisioning of the Services, the deployment of Collector(s) where required and Trustwave Fusion Platform accounts will be handled under standard Trustwave delivery procedures.

Configuration of logging from log sources to the Collector(s) is the responsibility of the Client except in cases where the Log Source is managed by Trustwave.

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 Services include security-focused use cases and are augmented by the GTO team of security analysts. The Services share a base set of rules, with Managed Detection Complete 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 Fusion Platform by the Collector(s). Based on threat intelligence, use cases, behavioural analytics, machine learning and correlation rules within the Trustwave analytics engine, Threat Findings are created, classified and a level of importance is allocated to each;
- Analyst manual review and hunting may also result in Threat Findings;
- Sources subscribed to Managed Detection Essential will be subject to periodic review by the GTO team of security analysts, monitoring for significant potential security concerns. Threat Findings will be escalated to the Client via Incidents in the Trustwave Fusion Platform.
- Sources subscribed to Managed Detection Complete receive real-time monitoring and analysis by the GTO team of security analysts. Threat Findings will be escalated to the Client via Incidents in the Trustwave Fusion Platform as they are detected.

Correlation & Use Case Management

Trustwave maintains proprietary global processes to model high fidelity attack scenarios and sequences of events within Fusion from normalized, high utility logs that may represent known or suspicious threats that need to be classified, analyzed, and actioned to minimize or to mitigate organizational risks.

Trustwave is the sole decision maker for conditions added to the use case catalog in Fusion. Correlation and use cases are global and must reliably detect high fidelity threats across all customers subscribed to the service.

Trustwave use cases are constant and each is applied consistently to all customer logs that match the key value pairs of key fields mapped in the normalization and taxonomization processes performed in log collection & enrichment.

Use Case Customization

Use case customization is available only in a limited number of instances:

- Dedicated solution architectures that include a correlation system parallel to Fusion (from Trustwave or supported third-party) that is part of the security architecture within the scope of the services agreement.
- Emergence of high-fidelity controls and logging outputs that can be repeatably, globally executed by Trustwave when integrated to Fusion through change management processes within the terms of the services agreement.

Global Threat Operations Monitoring and Threat Analysis

The GTO team is in globally disparate facilities and performs Analyst Reviews and investigations of Events and Threat Findings for subscribers to the Managed Detection Essential and Complete services.

Security Threat Investigation and Incident Identification

The GTO team has established an Incident investigation process that provide for a consistent methodology of investigation across the GTO. This process includes the advice and guidance from Trustwave SpiderLabs malware research, threat intelligence and Incident response teams. Where the investigation identifies an Incident, the GTO team will notify the Client. Where the investigation does not result in an 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 Trustwave Fusion Platform .

- Findings are analysed by the GTO team on a 24 / 7 / 365 basis (Managed Detection Complete)
- Findings are analysed in aggregate at least once every 24 hours (Managed Detection Essential)
- GTO analysts leverage all available Client information and intelligence associated with the Threat Findings to determine the severity of the Incident.
- Where warranted, the GTO analyst will escalate a Threat Finding being investigated to an Incident and assign a priority, and is detailed as follows:

-

Priority	Analyst Response	Priority Description
Critical (P1)	Phone call & Email	Incidents at this level are actionable, pose high risk, and signal active compromise, damage, or disruption of operations to high value assets in the Client environment. Investigations that result in this priority require immediate action to contain the threat or response and recovery actions to mitigate the bypass of multiple security controls.
High (P2)	Phone call & Email	Incidents at this level are actionable, pose high risk, and signal the potential compromise, severe damage, or disruption of operations to high value assets in the Client environment. Investigations that result in this priority require clients to take nearly immediate defensive actions to contain the threat.
Medium (P3)	Email	Incidents at this level are actionable, pose medium-risk, and signal the potential of limited damage or disruption to standard assets in the Client environment. Investigations that result in this priority require clients to take timely, yet not necessarily immediate action to contain a threat.
Low (P4)	Email	Incidents at this level are not immediately actionable and may require further investigation by the client to determine possible actions. Investigations that result in this priority require additional context or may signal known risks and deviations from security best practice

Trustwave Responsibilities

- Investigate and analyze Threat Findings, help identify false positives and notify Client in the case of a suspected actual or potential threat;
- Help identify and prioritize Incidents and notify designated Client personnel based on the priority of the incident and the appropriate response identified. Classify 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 Incidents in the Trustwave Fusion Platform; and
- Record all communications.

Client Responsibilities

- Validate the prioritization of an Incident according to its business impact and notify Trustwave of priority classification errors.
- Work with Trustwave to resolve each 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 Trustwave Fusion Platform to confirm updated status of Incidents.
- Request changes in accordance with the Trustwave change management process and use and access the Trustwave Fusion Platform to log tickets, receive notifications, view, download and track the status of and respond to, Threat Findings and Incidents.

MANAGED DETECTION ESSENTIAL – OPTION

Overview

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

- Collection of selected data on the Trustwave Fusion Platform ;
- Normalization of data to Events;
- 24x7 access to reports and interactive search functionality for Events through the Trustwave Fusion Platform
- Automated use cases, correlation, machine learning and other analysis for identification of threats, indicated by the creation of Threat Findings;
- 1-year storage of Events and Threat Findings;
- Trustwave analyst review of data, Events and Threat Findings. Trustwave's Global Threat Operations ("GTO") will review on a periodic basis, at least one time per day and notify Client of significant Threats per the agreed escalation procedures, generally via an Incident in the Trustwave Fusion Platform ;
- Daily Threat review summary report.

Trustwave Responsibilities

- Collect data on the Trustwave Fusion Platform ;
- Maintain availability of Events. Generate and publish the relevant reports.
- 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 Threat Findings, creating Incidents where appropriate, notifying the Client that the review was performed via a daily summary.

Client Responsibilities

- Review Event and Reports activity as made available in the Trustwave Fusion Platform .
- Notify Trustwave if Events or relevant reports are not available as expected.

- Review the daily review summary.

MANAGED DETECTION COMPLETE – OPTION

Overview

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

- Collection of selected Log Data on the Trustwave Fusion Platform ;
- Normalization of Log Data to Events;
- 24x7 access to reports and interactive search functionality for Events through the Trustwave Fusion Platform
- Automated use cases, machine learning, correlation and other analysis for identification of threats, indicated by the creation of Threat Findings.
- 1-year storage of Events and Threat Findings;
- 24X7 Analyst Review of Log Data, Events and Threat Findings. GTO will monitor Threat Findings and notify Client to actionable threats as per the agreed escalation procedures, generally via an Incident in the Trustwave Fusion Platform ;
- 24X7 access to telephone support;

Trustwave Responsibilities

- Collect and monitor Log Data via the Trustwave Fusion Platform via automated processes.
- Review Events and help in identification of Threat Findings via automated and manual review processes.
- Maintain availability of Events and Threat Findings Trustwave Fusion Platform ;
- Generate and publish the relevant reports Trustwave Fusion Platform ;
- Generate notifications of Threat Findings.

Client Responsibilities

- Review Threat Findings and reports as made available in the Trustwave Fusion Platform.
- Notify Trustwave if Events or relevant reports are not available in the Trustwave Fusion Platform , as expected.
- Respond to escalated Incidents;

Pricing Model

The Services will be billed in a tiered system; banded pricing defined by multiple metrics such as number of Log Sources, volume of data storage, Events per day. In the case of extreme variance in the relationship of the 3 metrics, Events per day 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 review on or around the contract anniversary date or if frequent overages of 25% or more on any

of the metrics have been observed in the quarterly measurements, Trustwave may require the Client to move to a more appropriate price tier or reconfigure their Log Sources to reduce the source volume, events collected or the storage used. If consistent under-utilization is noted, the Client 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. Any changes considered will be negotiated with the Client.

A contract addendum will be executed to note the new tier.

Reports on current metrics are available in Fusion or on request from the Trustwave SOC; Submit requests using Fusion.

Available tiers

i. 5M events/day, 2GB/day, 10 data sources
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

Trustwave Services Scope

Supported Sources

For all supported devices, Trustwave will create work orders for the purpose of implementing collection from these devices during the installation timeframe defined in the applicable Statement of Work.

Enter log source – vendor, product name, version and interface method (if known), and service tier

Supported Device, Application, or OS to be monitored:	**Version / Model:**	**Interface Method (syslog, DB, file, API, etc):**	**Quantity:**	**Service Tier:**
Vendor, Product/App Name	Version	Syslog OR Database OR Flat file OR API		Managed Detection Essential OR Managed Detection Complete

Unsupported Sources

For all unsupported devices requested, Trustwave will create work orders for the purpose of determining if support is possible based on the product, interface method, and service tier requested. No billing will take place relating to the unsupported device list until it is determined that support is possible, and that support has been implemented.

Unsupported Device, Application, or OS requested:	Version / Model:	Interface Method:	Quantity:	Service Tier:

Definitions

Analyst Review means a review by a Trustwave human analyst, including investigation, notification and, where applicable, recommendations for remediation services.

Collector means a Trustwave device that automates the collection, storage, and management of Log Data.

Event is a normalized record of Log Data, detailing a message, record, alert or audit from a Log Source.

Incident means a notification to the Client to a detected threat.

Log Data means a record received from a Log Source.

Log Source means a Supported Device for the service that generates Log Data.

Provisioning Questionnaire is the tracking document used to detail and track the fulfillment of the Service.

Product Updates are software patches to Trustwave managed systems deploying new features, updates and enhancements.

Report is static document with the results of queries for information collected and generated in the Service.

Security Updates are software patches to Trustwave managed systems which fix security vulnerabilities.

Threat Findings are potential security concerns detected by Trustwave systems and Analysts.

Trustwave Connect Device is a physical, virtual, public-cloud or Trustwave-hosted device used to house certain features of the Service.

Trustwave Fusion Platform means the Trustwave managed security service infrastructure utilized in providing the Service.

Trustwave Use Case Library is a continuously evolving set of automated detection algorithms designed to analyze collected Events and generate Threat Findings.

Use Case Review is a one-time 2 to 4- hour session at service inception between Trustwave MSS-SIEM, GTO, content teams and the Client.