Trustwave®

SERVICE DESCRIPTION

Threat Monitoring

Overview

Trustwave's Threat Monitoring service ("**Service**") provides monitoring, correlation, analysis, and investigation capabilities for log data from specific Client log sources. 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:

24x7 Threat Analysis and Investigation

Trustwave will use its proprietary threat analysis engine to help identify potential indicators of attack and external efforts to compromise Client's environment. The Service includes both (i) automatic, globally deployed, threat-focused detection capabilities and (ii) human-led threat monitoring.

Threat Analysis and Investigation

The Trustwave Fusion platform ingests event data from Client's supported log sources and processes such data through threat intelligence and threat-focused detection. Any potential threat findings from this process ("**Threat Findings**") are either (i) initially reviewed by Trustwave representatives and then escalated as needed or (ii) automatically escalated according to Trustwave algorithms.

Escalated Threat Findings are deemed "**Actionable Threat Findings**" and the Trustwave Fusion platform 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 escalated are deemed "**Non-Actionable Threat Findings**" and no Incident is created. Client may review Trustwave's Incident 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).

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

- review Threat Findings, Incidents, 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.
- work with Trustwave to resolve each Incident by providing relevant personnel and ensuring support and engagement 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.
- request changes in accordance with Trustwave's change management process.

Trustwave Obligations

For this feature and upon Client reaching Steady State (see Onboarding feature below), Trustwave will

- collect and monitor log data from agreed log sources via the Trustwave Fusion platform.
- maintain availability of events and Threat Findings in the Trustwave Fusion platform according to Trustwave's data retention procedures.
- investigate and analyze log source data and notify Client of Threat Findings according to the above procedures.
- maintain updated status of Incidents in the Trustwave Fusion platform and record all communications between Client and Trustwave pertaining to such Incidents.

Core Trustwave Features

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

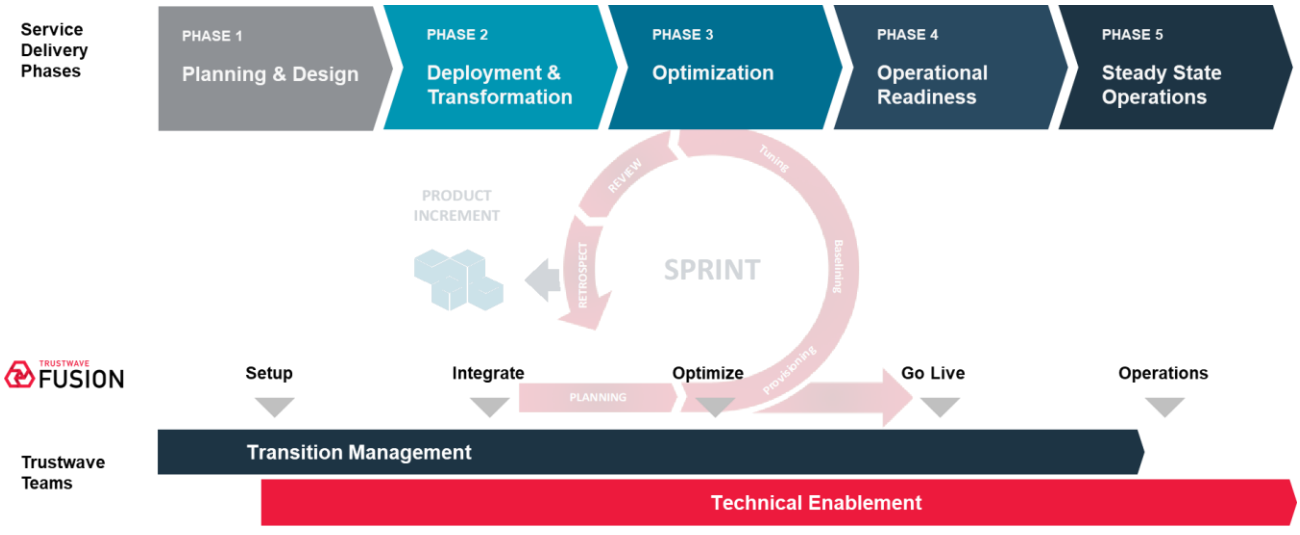
The Service includes transition management to facilitate the integration of Client's security solution(s) with the Trustwave Fusion platform.

Trustwave will assign a transition manager and additional technical enablement resources, as needed, to work directly with Client in onboarding Client to the Service and the Trustwave Fusion platform.

Trustwave will advise Client through its five (5) phases of transition management. Client is deemed fully transitioned and at steady-state (beginning of the Service) following Trustwave's conclusion of the fifth (5th) phase ("**Steady State**"). Trustwave and Client may agree to additional scoping terms in an Order Confirmation or SOW for this onboarding feature to accommodate varying complexity, size, and project governance requirements for Client's security solution(s).

Transition Management Phases

THE FOLLOWING CHART SUMMARIZES THE FIVE (5) PHASES OF TRANSITION MANAGEMENT IN THIS FEATURE:



Trustwave Obligations

As a part of the onboarding feature of the Service, Trustwave will

- schedule and host a kick-off meeting with Client;

- provide new-user orientation materials and training;
- coordinate Trustwave technical delivery resources for
    - collection, review, and assessment of event data for the Service;
    - deployment of connectivity elements for the Trustwave Fusion platform;
    - initial configuration and baselining of data flow, quality, and analysis;
    - contextualization of threat detection coverage for Client;
    - contextualization of threat detection coverage for Client's security solution(s) and provide guidance or recommendation(s) to improve possible detections and Threat Findings;
    - definition of authorized contacts for the Notification Procedures listed above; and
    - conducting final operational readiness assessment in preparation for steady-state status of the Service; and
- keep Client informed and up to date on transition progress and report on risks and issues relating to transition management.

Client Obligations

- Client will configure all its log sources (except for any Trustwave-managed log sources).

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 signed between Client and Trustwave.

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 or (ii) to set up event data so it is sent to Trustwave.

Direct Connectivity to the Trustwave Fusion platform

For certain supported cloud solutions, the Trustwave Fusion platform supports 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. Client may have access to self-service options for onboarding Client's security solutions.

Trustwave Endpoint

Client may also select Trustwave-provided, dedicated endpoint solution ("**Trustwave Endpoint**") to support log collection of Windows security events. Trustwave Endpoint is provided and distributed through the Trustwave Fusion platform and prepared by Trustwave with the applicable configuration set for Client's environment.

If utilized, Trustwave will be responsible keeping Trustwave Endpoint up-to-date and applying configuration changes according to any Trustwave change management procedures.

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

Log Source Support Policy

Trustwave may deliver the Service by acquiring, parsing, or normalizing log data collected from commercially-available off the shelf products. Trustwave maintains support for a defined list of log sources supported under the Service. Any changes to monitoring and parsing activities are at Trustwave's sole discretion.

Correlation & Use Case Management

Trustwave maintains proprietary global processes to model high-fidelity attack scenarios and event sequences within the Trustwave Fusion platform 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's global correlation and use cases aim to reliably detect high-fidelity threats applicable to all Trustwave's subscribed clients. Trustwave retains sole discretion in determining if conditions are added, modified, or removed to the use case catalog.

Event Consumption Overages

The Service is provided with a set data volume capacity (as set forth in the applicable SOW or Order Confirmation between Client and Trustwave) ("**Data Volume Cap**"). Trustwave may, from time to time, review the volume of data and events processed for Client in relation to the Service and recommend changes.

Where Client's data and event volumes are found to exceed the Data Volume Cap 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; or
- 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.