SERVICE DESCRIPTION

Advanced Threat Hunting

Overview

Trustwave's Advanced Threat Hunting (ATH) service ("**Service**") offers Trustwave's threat hunting capabilities specifically aimed at identifying and responding to undetected threat actors that may be in Client's environment. Trustwave uses behavioral indicator collection, analytics, and systematic enrichment to identify threats within Client's endpoint detection and response (EDR) security solutions which are included in the Service and indicated in the applicable SOW or Order Form ("**Client Technology**"). The following description sets out the parameters of the Service.

Core Trustwave Features

Trustwave Fusion Platform & Fusion Mobile App

The Trustwave Fusion platform is Trustwave's proprietary cloud-based security operations platform. Client will have access to the following capabilities on the Trustwave Fusion platform via web or mobile application:

- Security Incident (as defined below)
- Methods of communication including tickets

Such capabilities and related documentation are available to Client in the Trustwave Fusion platform, including allowing for ticketing integration.

Onboarding

Trustwave and Client will work together to onboard Client and prepare for Service commencement.

Client Obligations

Client will:

- procure and maintain all applicable Client Technology license(s);
- provide Trustwave with a list of Client's authorized user(s) for access to the Trustwave Fusion Platform;
- provide Trustwave with the necessary permissions for Trustwave to connect to the Client Technology;
- work with Trustwave to troubleshoot access to the Client Technology if necessary; and
- provide Trustwave's authorized users (as may be updated from time to time) with access to the Client Technology.

Trustwave Obligations

Trustwave will:

- schedule and host a welcome meeting with Client;
- enroll Client's authorized user(s) in the Trustwave Fusion Platform;
- provide new-user support materials and guidance for to the Trustwave Fusion Platform; and
- connect directly to the Client Technology via the Client-provided API.

Hunt Development

Trustwave will analyze Client's current threat landscape using open-source and other intelligence sources, and SpiderLabs proprietary threat intelligence. Then, Trustwave will build a profile of targeted threat actors' common tactics, techniques, and procedures (TTPs) and design custom, hypothesis-based hunts with the assumption a breach has already occurred on Client's network.

Threat Hunts

Trustwave will perform one of the threat hunts designed above by leveraging Client Technology and, when the Service is purchased in conjunction with Trustwave's Managed Detection & Response services, Trustwave may use other telemetry inside Client's environment as Trustwave deems appropriate. Trustwave may use the following threat modeling variables and processes to perform such threat hunts:

- **Threat Actors** - Trustwave tracks active threat actor groups operating around the world, including nation-state sponsored threat groups, hacktivists, and cybercrime syndicates.

- **Industry Historical Breach Analysis** - Trustwave examines historical data breaches from Client's industry to identify previously successful TTPs.

- **Data Leakage & Credential Compromise** - Trustwave reviews intelligence sources and credential harvesting sites to identify leaked corporate data, employee personally identifiable information (as determined by provided username and domain name credentials from Client), or user credentials. This may help identify potential previous compromises and existing corporate vulnerabilities.

Methodology

To perform the hunts, Trustwave will use a proprietary library of hunt queries designed to identify behaviors exhibited by threat groups, actors, and malware campaigns. This library contains queries curated and routinely updated to map to the MITRE ATT&CK matrix. Trustwave will investigate identified and suspicious behaviors that fit into one of the MITRE ATT&CK tactics categories below:

- **Reconnaissance –** Adversary is trying to gather information for future operations.
- **Resource Development –** Adversary is trying to establish resources to support operations.
- **Initial Access –** Adversary is trying to get a foothold in the environment.
- **Execution –** Adversary is trying to run malicious code.
- **Persistence** – Adversary is trying to maintain foothold.
- **Privilege Escalation** – Adversary is trying to gain higher-level permissions.
- **Defense Evasion** – Adversary is trying to avoid detection.
- **Credential Access** – Adversary is trying to steal usernames / passwords.
- **Discovery** – Adversary is trying to conduct reconnaissance internally in the environment.
- **Lateral Movement** – Adversary is moving throughout the environment.
- **Collection** – Adversary is aggregating targeted data.
- **Command and Control** – Adversary is communicating to compromised systems internally or externally.

- **Exfiltration** – Adversary is exporting stolen data.
- **Impact** – Adversary is trying to manipulate, interrupt or destroy, systems, operations and data.

Service Tiers

The Service is available in two service tiers. The applicable service tier will be indicated in Client's SOW or Order Form.

Advanced Continual Threat Hunting

- Trustwave will perform ongoing hunt development analysis and threat hunts up to ten to twelve (10-12) hunts per year. The actual quantity and timing of hunts will vary based on changes to threat intelligence, findings of prior hunts, variability in the scope of each hunt, and other factors, each to be determined in Trustwave's reasonable discretion.

Advanced Threat Hunting

- Trustwave will perform four (4) hunts per year. The timing of hunts will vary based on changes to threat intelligence, findings of prior hunts, variability in the scope of each hunt, and other factors, each to be determined in Trustwave's reasonable discretion.

Triage

Trustwave will review the data resulting from each hunt for false positives and isolate suspicious elements for deeper human-led investigation.

Deep Analysis

Once filtered, Trustwave will hunt through the newly discovered TTPs throughout Client's network to determine the severity of the associated incident. If Trustwave discovers a significant ongoing data breach or widespread infection, Trustwave may recommend Client escalate the incident to a digital forensics and incident response (DFIR) provider. Trustwave will provide information and support for ongoing security events within the Trustwave Fusion platform and the Client Technology related to any such incident response engagement during the Term of the Service.

Security Incident Escalations

Trustwave will create and store the output of deep analysis where Trustwave identifies malicious findings, vulnerabilities, and network infrastructure deficiencies in Client's environment using security incident tickets within the Trustwave Fusion platform ("**Security Incident**"). Trustwave will send Client notifications according to the Security Incident's assigned priority (see below). Security Incidents may include any of the following information:

- Summary of the incident
- Analysis
- Recommendations
- List of Trustwave actions taken
- Requests for Client to perform recommended actions

In addition, at its sole discretion, Trustwave may request Client collect and submit binary files and suspected malware within the Security Incident for SpiderLabs Malware Reverse Engineering. In such cases, Trustwave may add any further observations, findings, or recommendations developed by this process to the applicable Security Incident.

Client Obligations

For Trustwave to provide this feature, Client will

- retain exclusive responsibility for mitigating actual and potential threats to its environment;
- lead and execute Client processes for incident management and incident response;
- regularly update incident contacts and their respective accesses and information in the Trustwave Fusion platform including contact email, phone numbers, and contact order;
- utilize the Trustwave Fusion platform and mobile app to generate secure communications, notifications, and Service feedback;
- collaborate with Trustwave on security detection and response best practices, including Client deployed configurations, and policy definitions;
- provide initial and ongoing Trustwave user and system remote access to the Client Technology to accommodate Trustwave's remote analysis as defined by this service description;
- review Security Incidents, notifications, and reports as made available in the Trustwave Fusion platform;
- notify Trustwave if Security Incidents, events or reports are not available in the Trustwave Fusion platform as reasonably expected;
- resolve each Security Incident by providing Security Incident feedback, relevant personnel, and ensuring support, and engagement of third parties, as reasonably required by Trustwave;
- provide Trustwave with requested information and confirmations in a timely manner. Client acknowledges failure to do so may inhibit Trustwave's ability to provide the Service;
- provide network documentation promptly upon request; and
- provide additional telemetry as required.

Trustwave Obligations

For this feature, Trustwave will

- allow authorized Client personnel (authorized by Client) access to the Trustwave Fusion platform to interact with Trustwave personnel and to monitor the Service and as a repository for Client communications for Security Incidents;
- create tickets within the Trustwave Fusion platform to notify of hunt iteration, findings, and required actions;
- collect and process events from the Client Technology;
- analyze and raise Security Incidents, investigations, and reports identified by Trustwave from events collected from Client's environment;
- provide recommendations aimed to improve Client's overall security posture if a hunt yields actionable findings in Trustwave's sole discretion;
- periodically update the status of Security Incidents in the Trustwave Fusion platform and record communications between Client and Trustwave pertaining to such Security Incidents;
- review Client feedback; and
- conduct further analysis on binaries that are suspicious or require reversing to validate malicious intent and gather additional indicators of compromise.

Security Incident Priority Levels

Client incident contacts defined in the Trustwave Fusion platform will receive communications from Trustwave for Security Incidents via the Trustwave Fusion platform, the Fusion mobile app, email, or phone. Clients should continuously update notification groups in the Trustwave Fusion platform.

Trustwave assigns priority levels to Security Incidents based on factors from Trustwave's investigation, including attack classification, SpiderLabs threat intelligence, security outcome, derived risk, impact, and properties of the events related to the Security Incident. Trustwave will send Client notifications according to the Security Incident's assigned priority and using Trustwave integrated phone, app, and email systems (see table below). Client will document all communications, questions, clarifications, and feedback for the Security Incident in the Trustwave Fusion platform or Fusion mobile app.

Priority	Notification Procedure	Priority Description
Critical (P1)	Phone, App, Email	Security Incidents at this level potentially pose an immediate and high security risk to Client's environment, and signal an active compromise, extensive damage, or total disruption of operations to high value assets in Client's environment. Investigations that result in this priority require the Client to take immediate containment, response, or recovery actions to contain the Security Incident.
High (P2)	Phone, App, Email	Security Incidents at this level potentially pose a high security risk to Client's environment, and signal a potential compromise, severe damage, or disruption of operations to high value assets in Client's environment. Investigations that result in this priority require Client to take nearly immediate defensive actions to contain the Security Incident.
Medium (P3)	Email	Security Incidents at this level potentially pose medium-level security risk and signal the potential for limited damage or disruption to standard assets in Client's environment. Investigations that result in this priority require Client to take timely, but not necessarily immediate, action to contain the Incident.
Low (P4)	Email	Security Incidents at this level are not immediately actionable and may require further investigation by Client to determine possible actions. Investigations that result in this priority require additional context or may signal known risks and deviations from security best practices.

Problem Management

A problem is a cause or potential cause of one or more incidents impacting the health of the Service. Client agrees to report problems through the Trustwave Fusion platform. Client and Trustwave agree to collaborate on problem resolution subject to Trustwave policy.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable Statement of Work or Order Form between Trustwave and Client.