SERVICE DESCRIPTION

# Proactive Threat Hunting

## Overview

Trustwave’s Proactive Threat Hunting service (“**Service**”) offers Trustwave’s threat hunting capabilities as a one-time, non-subscription service specifically aimed at identifying and responding to undetected threat actors currently in Client’s environment and focused on providing deep insight into Client’s security gaps, risks, and exposures. The Service assumes a security breach has already occurred and searches for any indications of such attacks, their root cause, and present threats to Client’s environment.  The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Form between Trustwave and Client.

## Requirements

The Service requires that a supported endpoint detection and response (“**EDR**”) technology is deployed on Client’s in-scope systems. The EDR agents can be existing client-managed technology or be agent software provided by Trustwave for the duration of the Service. If the EDR technology used for the Service is provided by Trustwave, Client must deploy the endpoint agent to the in-scope systems.

Operating systems that are not supported by the EDR technology fall outside of the scope of the Service. Client must review Trustwave’s current supported EDR technology (Cybereason, Carbon Black, Cortex XDR, SentinelOne, and Microsoft Defender for Endpoint) to determine if Client’s specific operating systems are supported.  Client and Trustwave will work together to establish a connection between Trustwave and the Client’s in-scope systems.  Where a Client-hosted managed console is used, Client is responsible for implementing and creating Trustwave user accounts as requested by Trustwave.

Client is responsible for evaluating the capacity of the in-scope systems to run the EDR technology and for the operational health of the in-scope systems.  If the EDR technology used for the Service is provided by Trustwave, Client may purchase the EDR technology by an applicable SOW or Order Form between Trustwave and Client or remove the endpoint agent to the in-scope systems at the end of the Service.

## Service Features

The Service includes the following features:

### Hunt Development

Trustwave will analyze Client’s current threat landscape using open-source intelligence, dark-web intelligence, and Trustwave’s proprietary threat intelligence. Based on this analysis, Trustwave will build a profile of targeted threat actors’ common tactics, techniques, and procedures (“**TTPs**”), and design custom, hypothesis-based hunts with the assumption that a breach has already occurred on Client's network.

## Threat Hunts

Trustwave will perform the hunt leveraging the EDR technology. When the Service is purchased in conjunction with Trustwave 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 process 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 Service, 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.

## Triage

Trustwave will review the data resulting from each hunt for false positives and separate out suspicious elements for a 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 threat or 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 to Client information and support for ongoing security events related to any such incident response engagement during the Term of the Service.

## Reporting

Where Trustwave identifies malicious findings, vulnerabilities, and network infrastructure deficiencies, Trustwave may generate a security incident communication to Client. Trustwave will communicate the security incident to Client's designated point-of-contact. In addition, Trustwave will coordinate a weekly call cadence to report on the status of the hunt, blockers, findings, and recommendations, as well as to gather any relevant feedback from Client. Trustwave will provide a Threat Hunt Investigation Report, which may include an executive summary, evidence, findings, recommendations, and actions taken as part of the Service.

### *Client Obligations*

For Trustwave to provide this Service, Client will

- provide access to the Client-managed EDR application program interface (API) (e.g., Microsoft Defender) when requested by Trustwave;
- deploy EDR endpoint agents provided by Trustwave as necessary;
- provide a point-of-contact;
- provide timely responses to email or ticket communications from Trustwave;
- provide network documentation promptly upon Trustwave's request; and
- provide additional telemetry as required by Trustwave.

### *Trustwave Obligations*

For this Service, Trustwave will

- provide recommendations aimed to improve Client's overall security posture if the hunt yields actionable findings;
- conduct further analysis on binaries that are suspicious or that require reversing to validate malicious intent and gather additional indicators of compromise;
- provide weekly update calls; and
- provide a final report and a walkthrough of the findings.

# 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 SOW or Order Form between Trustwave and Client.