Trustwave®

SERVICE DESCRIPTION

Threat Intelligence as a Service

Overview

Trustwave Threat Intelligence as a Service (TIaaS) (**"Service"**) provides timely, contextualized, and prioritized threat intelligence based on factors relevant to Client's operations, enabling Client to make risk-based and threat-informed decisions which benefit its organization.

The Service is delivered using Trustwave's SpiderLabs Intelligence Led Knowledgebase (SILK) Methodology, a human-led approach that combines expert analysis with advanced threat intelligence tooling to produce validated, high-value intelligence.

The following description sets out the parameters of the Service, as may be further modified by an applicable Statement of Work or Order Form between Trustwave and Client.

Service Features

The Service is a 12-month engagement between Trustwave and Client. The Service includes the following features:

- **Initial Threat Assessment Workshop:** A collaborative workshop to identify Client's concerns, posture, context, technologies, and services Client is dependent on.
- **Attack Surface Analysis:** Analysis of Client's attack surface, including domains, subdomains, and external-facing assets, seeking to identify insecure services and detect data exposure via, for example, cloud services or code repositories.
- **Intelligence Analysis:** Continuous gathering and analysis of information and insights on Client, enabling threat intelligence to be contextualized and specific to Client's operations. This includes analysis of global incidents, vulnerabilities, and advisories, creating an early warning system of actionable risk-based intelligence, alongside base recommendations.
- **Dark Web & Public Internet Monitoring:** Dark web and public internet monitoring for evidence of data or credential breaches, and to identify evidence indicative of an increased threat likelihood, or information likely to impact brand or reputation.
- **Threat Knowledgebase:** Maintenance of a knowledgebase of relevant threat groups and actors, attack methods, trends, target industries, Tactics, Techniques, and Procedures (TTPs), Indicators of Compromise (IOCs), and advice on remedial activities and security controls.
- **Tabletop Exercise:** An incident response tabletop exercise to test and enhance the efficacy of Client's incident response processes.
- **Threat Intelligence Reporting:** Strategic, tactical, and ad hoc threat intelligence reporting, including details on threats and trends based on Client's industry, geography, technology, and operating environment.

Delivery & Implementation

Trustwave will work with Client throughout the threat intelligence journey to provide Client with curated and actionable threat intelligence.

Initial Threat Assessment Workshop

Trustwave will conduct a collaborative workshop to identify Client's concerns, posture, context, technologies, and services Client is dependent on.

Client Obligations

For Trustwave to provide the Service, Client will:

- Provide contact details for and access to Client stakeholders and escalation points and remain available for communication from Trustwave.
- Provide logistics support for booking meetings, coordinating workshops, and arranging access to required personnel.
- Provide access to systems with appropriate credentials, as reasonably requested by Trustwave.
- Provide any documentation Trustwave may reasonably request to perform the Service, which may include:
  - IT and security strategy
  - Sample reports from existing systems
  - Risk Management Framework (RMF)
  - Incident Response Plan (IRP)

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Establish engagement roles and responsibilities for stakeholders.
- Review current state information and documentation provided by Client.
- Deliver and facilitate the initial workshop at a date and time agreed between Trustwave and Client.
- Develop a report giving details on the workshop and outcomes.

Intelligence Analysis

Trustwave will gather and analyze information and insights on Client, as well as perform attack surface analysis and monitoring. Threat intelligence is gathered from a wide range of sources, including commercial and custom-built tooling, open-source research, and technical research, including technical data obtained from Trustwave's global cybersecurity teams and capabilities.

Client Obligations

For Trustwave to provide the Service, Client will:

- Provide details on technical assets and networked environment.
- Provide context and information regarding Client's most critical assets, services, personnel, and operations.
- Provide details on any existent threat intelligence solutions or capabilities in use.
- Provide input on Trustwave findings, as requested by Trustwave.

- Participate in and understand materials explained during calls, meetings, interviews, discussions, inspections, and controls analysis.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Set up Client within the threat intelligence platform (which only Trustwave will access and manage).
- Configure keywords within the threat intelligence platform to facilitate monitoring and alerting.
- Analyze Client's attack surface, including domains, subdomains, and external-facing assets, seeking to identify insecure services and detect data exposure via, for example, cloud services or code repositories.
- Analyze global incidents, vulnerabilities, and advisories, in the context of Client's operations.
- Perform dark web and public internet searching, monitoring, and analysis for indications of data or credential breaches or threats to people/brand.
- Maintain a knowledgebase of relevant threat groups and actors, attack methods, trends, target industries, TTPs, IOCs, and advice on remedial activities and security controls.

Tabletop Exercise

Trustwave will conduct an incident response tabletop exercise to test and enhance the efficacy of Client's incident response processes. The scenario is based on real-world investigations and will be designed and agreed between Trustwave and Client.

Client Obligations

For Trustwave to provide the Service, Client will:

- Provide documentation required by Trustwave and be available for interview sessions to gather the required information.
- Identify all relevant stakeholders to be included in the exercise, including names, positions, and roles in incident response activities.
- Support the logistics of scheduling the exercise.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Engage with Client to determine the most relevant scenario for the industry, threat profile, and maturity level.
- Tailor the scenario presentation and 'injects' to focus on communication, critical decisions, notifications, tooling, technology, and processes necessary to respond to the chosen incident.
- Deliver and facilitate the exercise at a date and time agreed between Trustwave and Client.
- Develop a report giving details on the exercise and outcomes and highlight any areas of the response, including observations regarding the incident response plan and/or playbooks, that may need addressing.

Threat Intelligence Reporting

Trustwave will provide Client with curated strategic and tactical reporting, as well as ad hoc threat alerting to inform Client's decision making.

Client Obligations

For Trustwave to provide the Service, Client will:

- Review Trustwave's reports and attend review sessions conducted by Trustwave.
- Support the identification of appropriate owners for Trustwave's findings and recommendations.
- Action 'imminent threat' alerts, as required.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Deliver an initial baseline report to form a baseline view of Client's environment.
- Deliver monthly tactical reporting to help inform the short- to mid-term direction of Client's security initiatives.
- Deliver quarterly strategic reporting (or other agreed cadence) to help underpin Client's security program and help define Client's security maturity and focus.
- Deliver 'imminent threat' alerting to notify Client of findings assessed as presenting an elevated risk to Client's organization, and which may require Client action.

Additional Information

Trustwave can be Client's threat intelligence team or augment Client's existing team, depending on the maturity of Client and whether Client has an existing threat intelligence program in place:

- **Client Does not Have a Threat Intelligence Team in Place:** Trustwave forms the threat intelligence team, ensuring Client has a program in place to inform decision making.
- **Client Does Have a Threat Intelligence Team in Place:** Trustwave augments Client's threat intelligence team, enriching Client's threat intelligence and acting as a subject matter expert.

Trustwave will provide Client with a threat intelligence point of contact throughout the Service. This allows Trustwave to build up knowledge and expertise about Client's organization, refining and tailoring the threat intelligence to the needs of Client.

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.