Trustwave®

SERVICE DESCRIPTION

Rapid Action Program

Overview

Trustwave's Rapid Action Program ("**Service**") offers Client a set of combined Trustwave services aimed at reducing Client's exposure to external cybersecurity threats. Rapid Action Program include the following features:

- Security Colony Core Subscription
- Facilitated Security Colony Maturity Assessment
- Pre-Attack Vulnerability Assessment
- Tabletop Exercise
- Roadmap
- 80 Additional consulting hours – to address issues identified in the assessment phases

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:

Security Colony Core Subscription

The Service includes a 12-month subscription to Security Colony's Core tier. In using the Security Colony feature, Client will agree to the terms of use at https://portal.securitycolony.com/terms-and-conditions.

Facilitated Security Colony Maturity Assessment

A Trustwave consultant will assist Client in completing a Maturity Assessment, hosted within the Security Colony platform. The Maturity Assessment tool is a multiple-choice assessment based on the NIST Cybersecurity Framework.

Client Obligations

For Trustwave to provide this feature of the Service, Client will

- make available relevant personnel to respond to the questions included in the Maturity Assessment tool at a time agreed between Trustwave and Client
- provide accurate responses to the questions included in the Maturity Assessment tool.

Trustwave Obligations

For this Feature, a Trustwave Consultant will

Copyright © 2021 Trustwave Holdings, Inc. All rights reserved.

- attend a virtual (via Microsoft Teams) meeting, in which the Consultant will facilitate the completion of the Security Colony Maturity Assessment tool.
- provide additional detail and context to the questions posed in the tool, challenge the proposed responses from Client, and seek to ensure the best answer is chosen for each question.

Pre-Attack Vulnerability Assessment

Trustwave will investigate to define Client's attack surface from an external perspective, mimicking potential initial reconnaissance activities that may precede a cyber-attack or breach. Trustwave will focus on data and vulnerability exposure from this external perspective. Trustwave will deliver a report with findings and recommendations on ways Client may make the identified attack surface less attractive to threat actors.

Client Obligations

For Trustwave to provide this feature of the Service, Client will

- provide all scoping information required by Trustwave to deliver the Service; and
- provide a timely response to information requests from Trustwave.

Trustwave Obligations

For this feature, Trustwave will

- conduct a Pre Attack Vulnerability Assessment remotely

Tabletop Exercise (TTX)

Trustwave will develop and execute with Client a scenario-based exercise, based on real SpiderLabs investigations, to help review Client's incident response capability. This feature evaluates and aims to improve Client's incident response plan without any significant disruption to operations. The scenario will be designed and agreed upon between Client and Trustwave to test and validate various components of Client's incident response capabilities and raise awareness of any deficiencies in the response and investigation process.

Client Obligations

For Trustwave to provide this feature of the Service, Client will:

- Provide documentation required by Trustwave and be available for interview sessions to gather the required information. Trustwave will deliver a live session and findings report at the conclusion of the Service.
- Identify all relevant stakeholders to be included in the exercise including their names, position, and roles in the incident response activity.
- Support the logistics of booking in the tabletop exercise.

Trustwave Obligations

For this Feature, a Trustwave Consultant 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 cybersecurity incident.
- Deliver and facilitate the tabletop exercise remotely at a date and time agreed between Trustwave and Client.
- Develop a report giving details of the assessment, the outcomes, and highlighting any areas of the response, including observations regarding the incident response plan and/or playbooks, that may need addressing.

Roadmap

Trustwave will develop a combined report (the Roadmap) with recommended actions by integrating findings from the Security Colony Maturity Assessment, Tabletop Exercise, and Pre-Attack Vulnerability Assessment.

Client Obligations

For Trustwave to provide this feature of the Service, Client will indicate which remedial actions suggested by the Security Colony Maturity Assessment, Tabletop Exercise, and Pre-Attack Vulnerability Assessment Client agrees to implement.

Trustwave Obligations

For this feature, Trustwave will develop and deliver (remotely) the Roadmap.

Additional Consulting Hours

The Service includes eighty (80) consulting hours in addition to the features described above. Client may apply these hours towards services in Trustwave's Cyber Advisory practice, Cyber Architecture & Integration practice, or Digital Forensics and Incident Response (DFIR) practice.

These eighty (80) additional consulting hours are subject to the General Consulting & Professional Services Service Description available at (https://www.trustwave.com/media/19024/cps-general-consulting-professional-services-12-september-2022.pdf).

Client Obligations

For Trustwave to provide this feature of the Service, Client will

- apply the hours to tasks identified within the Roadmap (or other tasks as may be agreed between Client and Trustwave)
- support the delivery of the chosen tasks as required by the relevant Service Description.

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.

Copyright © 2021 Trustwave Holdings, Inc. All rights reserved.