

SERVICE DESCRIPTION

Cyber Advisory – vCISO / vTeam

Overview

Trustwave's Cyber Advisory - vCISO / vTeam (the “**Service**”) provides a flexible engagement model through which Clients gain access to all of Trustwave's Consulting & Professional Services (CPS) team members, through a single point of contact (the “**vCISO**”), to assist Client in developing, reviewing, implementing, or optimizing elements of their cyber security program.

The following description sets out the parameters of the Service, as may be further modified by an applicable SOW between Trustwave and Client.

Service Features

The Service includes the following standard features:

- **vCISO / vTeam Lead** – A consultant who provides guidance, project oversight, and quality assurance for any reports and serves as Client's point of contact for escalations.
- **Security Colony 'Core' Subscription** – For the duration of the vCISO / vTeam engagement, Client will be provided with a 'Core' level subscription to our Security Colony platform, subject to Security Colony's Terms & Conditions located at <https://portal.securitycolony.com/terms-and-conditions>.
- **Incident Response (IR) Hotline Access** – Trustwave will provide Client with an emergency contact number and email address to connect Client with an IR-trained Trustwave representative, available 24 hours a day, 7 days a week, 365 days a year.
- **Quarterly Executive Briefings** – Briefings delivered by a Trustwave CPS team member to Client on a quarterly basis.
- **Access to Trustwave's CPS team** – When specialist consulting skills are required to deliver part of the Service, the vCISO / vTeam Lead can allocate such tasks to other members of Trustwave's CPS team.

Delivery & Implementation

Project Initiation

Hand-picked members of Trustwave's CPS team deliver the Service. The Service begins by scheduling and then conducting a kickoff meeting (held remotely, unless otherwise agreed between Client and Trustwave) to define and agree to a high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables, resource requirements, and escalation procedures.

Work Allocation & Hours Usage

This kickoff meeting will include discussion and agreement as to the approvals required for the vCISO / vTeam Lead to allocate work to other Trustwave CPS team members, using the pre-committed hours budgeted for the Service.

If not specified in the high-level project plan, the approval process will be:

- vCISO / vTeam Lead sends an email to the Client, with the following details:
 - High level description of the task requiring specialist support;
 - Details of the nominated Trustwave CPS team member(s) (“**Specialist(s)**”) to complete the task;
 - An estimate of the number of hours required for the task to be completed;
 - A proposed approach to ‘funding’ this task, which could be either:
 - The vCISO / vTeam Lead works less hours themselves over a specific period of time, to balance out with the additional hours worked by the Specialist; or
 - The vCISO / vTeam Lead works the same number of hours as normal, and the specialist hours are consumed from the overall vCISO / vTeam budget of hours in addition.
- Note that if no funding model is specified in the email, option #2 will be assumed to be chosen.
- Client responds to the email and indicates acceptance or rejection of the Specialist request. No work will commence without an acceptance from Client Project Manager except for Incident Response projects as discussed below.

If Client places a call (or its email equivalent) to the IR Hotline requesting support for an actual or suspected cybersecurity incident, Trustwave’s Digital Forensics & Incident Response team will respond as soon as possible, with an initial twenty (20) hours of Client pre-approved effort. These hours will be consumed from the overall vCISO / vTeam budget, and in the event the remaining project budget is insufficient to cover this expense, Trustwave will raise an invoice at the prevailing vCISO / vTeam hourly rate for any additional time required.

Consulting Delivery

The Service can be delivered from any group of members within Trustwave’s CPS team.

These services are described within their individual Service Descriptions, as follows:

Cyber Advisory, Cyber Architecture & Integration Engagement

- See General Consulting Service Description - <https://www.trustwave.com/media/18440/cps-general-consulting-cyber-advisory-and-cyber-architecture-and-integration-service-description-02-february-2022.pdf>

SpiderLabs Penetration Testing Engagement

- See Managed Security Testing Service Description - <https://www.trustwave.com/media/18248/security-testing-managed-security-testing-service-description-13-october-2021.pdf>

Digital Forensics & Incident Response Engagement

- See Breach Response Consulting Service Description - <https://www.trustwave.com/media/18225/dfir-breach-response-consulting-service-description-13-august-2021.pdf>

Project Closeout

Following completion of the Service, Trustwave will conduct a closeout meeting with Client.

Client Obligations

For Trustwave to provide this Service, Client will:

- Establish contact and remain available for communications from Trustwave.
- Establish communication and escalation plans.
- Review, provide feedback, and agree to the high-level project plan for delivery.
- Where necessary, provide contact details of and access to key stakeholders within Client's organization.
- Where necessary, provide logistics support for booking meetings, coordinating workshops, and arranging access to required documentation or personnel.
- Provide the necessary documentation and interview access so as to support off-site delivery of the Service by Trustwave CPS team members who may be based in the same or different countries to the Client.
- Make available resources needed for the Service.
- Participate in and understand materials explained during calls, meetings, interviews, workshops, discussions, facilities inspection, and controls analysis.
- Provide responses to vCISO / vTeam messages proposing the allocation of tasks to Specialists

Client acknowledges:

- The Service may consist of onsite and remote consulting activities;
- The specific services delivered within the Service can include any of Trustwave's consulting and professional services offerings, subject to mutual agreement between Client and Trustwave;
- Trustwave will perform the Service in the English language;
- Trustwave will not offer any legal guidance or counseling; and
- The quality and accuracy of the Service is dependent on Client's provision of accurate information to Trustwave.

Client is responsible for:

- Making its own assessments and judgements regarding the configuration and suitability of its security solutions, including where Client obtains advice and consultancy from Trustwave;
- Making its own business decisions about technology security;
- Assessing its risks and deciding the most appropriate security solution;
- Having personnel who have the ability to assess the advice received from third parties as it relates to Client and its business;
- Its own security and access management;
- Its data backup, retention, and deletion;
- Its data recovery, disaster recovery and business continuity management;
- Making decisions on location of data and transferring data, particularly in relation to personal information; and
- Its redundancy of networks / systems and support obligations.

Trustwave Obligations

For this Service, Trustwave will:

- Allocate Trustwave's CPS team as necessary to deliver the Service;
- Establish contact and remain available for communications from Client;
- Establish communication and escalation plans;
- Define a high-level project management plan including milestone dates, key steps, estimates for duration, change management process, key contact details, and resource requirements;
- Schedule and conduct kickoff, periodic status, and closeout meetings, as appropriate.
- Interview and collect information from applicable Client personnel;
- Deliver the Service and, if included in the scope, document the findings of the Service in a report; and
- Confirm Service completion.

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.