Trustwave®

SERVICE DESCRIPTION

General Consulting & Professional Services

Overview

Trustwave's General Consulting & Professional Services ("Service") is designed to assist organizations in developing, reviewing, implementing, or optimizing elements of their cybersecurity program. This Service includes Trustwave's Cyber Advisory practice, Cyber Architecture & Integration practice, Digital Forensics and Incident Response (DFIR) practice, and SpiderLabs Penetration Testing (PSO).

The Cyber Advisory practice delivers strategic advice, planning, and consulting around aspects of cyber security governance, risk, compliance, policy, and awareness.

The Cyber Architecture & Integration practice delivers consulting in relation to technical controls (and the people and processes supporting and operating them), including designing, building, and optimizing solutions to mitigate threats in the cloud and the enterprise.

The DFIR practice delivers consulting and preparatory training exercises in relation to incident response (IR) readiness, including IR plan review or development, technical tabletop exercises, exposure investigations, and training programs.

SpiderLabs Penetration Testing (PSO) delivers technical testing engagements using tools and techniques that replicate real-world attacks Client may face for many types of environments whether on premises, cloud based, or hybrid.

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 standard features:

- **Security Consultant** – A security consultant is the primary resource for the fulfilment of the Service and is responsible for scheduling and conducting the consulting activities. Security consultants range in levels of seniority and experience.
- **Managing Consultant (MC)** or **Lead Security Principal (LSP)** – An MC or LSP provides guidance, project oversight, and quality assurance for any reports and serves as Client's point of contact for escalations.

Project Types

Trustwave will perform the Service based on one of the following engagement styles (please refer to the relevant SOW or Order Confirmation to determine which style applies):

- **Time and Materials** – The Service is based on a defined outcome and a potentially open-ended number of hours available to deliver that outcome. The Service is charged based on time used in delivery. Where a cap is applied to the number of hours available under a given SOW, the Service will be treated as Time Boxed (see below).
- **Fixed Price** – The Service is based on a defined outcome and may include an estimate of the hours required to deliver this outcome. In such a case, the Service is complete when the outcome is reached (as defined by the SOW, or if not defined, as reasonably determined by Trustwave). The Service is charged based on the fixed price amount. When a Fixed Price Service is Time Boxed, a second defined outcome will be the completion of the specified number of hours in the given SOW. In such a case, completion of either defined outcome will constitute full delivery of the Service.

Both Time and Materials and Fixed Price Services may also be Time Boxed as follows:

- **Time Boxed** – The Service is allotted a defined number of hours for delivery. In such a case, the scope of the Service is limited to the work Trustwave can deliver within the agreed number of hours.

If a SOW or Order Confirmation does not specify which of the above engagement styles is applicable, the default is Fixed Price and Time Boxed.

Delivery & Implementation

Project Initiation

Hand-picked members of the Trustwave Consulting & Professional Services team deliver the Service.

For services other than SpiderLabs Penetration Testing (PSO), 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.

For SpiderLabs Penetration Testing (PSO) services, Trustwave and Client will agree on a start date for commencing the Service and cooperate in the collection of any information required to begin and complete the Service.

Consulting Engagement

Trustwave and Client will review and examine Client's information security protection requirements within the scope of the Service.

For Cyber Advisory and Cyber Architecture and Integration services, the Service may include, but is not limited to the following:

- Information gathering via documentation review and interviews;
- Review of security control status and evidence of operational effectiveness;
- Assessment of obtained information to identify threats, risks, process maturity or compliance gaps;
- Development of security artifacts (including strategies, policies, procedures, plans, standards, guidelines and awareness resources) to support organizations in addressing identified gaps;
- Assisting in the evaluation of emerging technologies, service providers, tools, platforms and applications that are best suited to the specific needs of a given organization;
- Implementation of and optimization efforts for security controls; and
- Providing recommendations for remediation of compliance and security issues.

For SpiderLabs Penetration Testing (PSO) services, the Service may include one or more of the following tests (exact testing to be agreed between Trustwave and Client in an applicable SOW):

- **Application Penetration Test** – Trustwave will look for vulnerabilities and exploitable and unexploitable weaknesses in the agreed application to be tested;
- **Network Penetration Tests** (internal and external) – Trustwave will look for vulnerabilities and exploitable and unexploitable weaknesses in Client's network infrastructure;
- **Wireless Penetration Test** – Trustwave will gauge the resilience of Client's in-scope wireless networks against various classes of attacks (launched from radio side and wired side) This includes an examination of further attacks that could be leveraged against internal wired resources should a malicious individual gain unauthorized access to Client's wireless networks;
- **Active Directory Review** – Trustwave will review Client's active directory structure based on number of users, trusts, and forests;
- **AWS or Azure Configuration Review** - Trustwave will test the configuration of Client's cloud environment.
- **Red Team** – Trustwave will conduct an adversary simulation exercise aimed at Client's organization. Trustwave will provide this as either an assumed breach, remote, remote plus physical, or custom scoped engagement model;
- **Purple Team** – Trustwave will work cooperatively with Client's defensive team to fine tune an agreed upon area of improvement with respect to its people, processes, or technology;
- **Physical Security Assessment** – Client will identify its primary physical security control objectives, and Trustwave will review Client's in-scope facilities against such objectives. This will include: a site survey, identification and assessment of physical security controls weaknesses and failures, and a networked physical access control system review.

The applicable SOW or Order Form between Trustwave and Client will set out the specific methodology and in-scope applications or networks for the relevant penetration tests listed above. Trustwave and Client may agree to a penetration test or other technical test other than what is listed above. In such cases, the parameters of the Services will be listed in the SOW or Order Form between Client and Trustwave.

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 (not applicable for SpiderLabs Penetration Testing (PSO)).
- 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 consultants 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.

Client acknowledges:

- The Service may consist of onsite and remote consulting activities;
- The Service does not include in-depth testing or review of system settings, configurations, or observation of implemented processes and procedures (unless specifically stated otherwise in the SOW or Order Form between Trustwave and Client);
- The Service does not include visits to third parties or direct engagement with third parties. All information will be obtained directly from Client;
- Trustwave may request evidence from Client's systems and processes as required to prove compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner;
- Trustwave will perform the Service in the English language;
- Trustwave will not create or modify Client documentation as part of the Service;
- Trustwave will not provide remediation services as part of the Service;
- 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;
- Providing necessary network and system access, user accounts, and credentials as required by Trustwave;
- 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 consultants 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 (not applicable for SpiderLabs Penetration Testing (PSO));
- Schedule and conduct kickoff, periodic status, and closeout meetings, as appropriate.
- Interview and collect information from applicable Client personnel (if required);
- 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.