Trustwave®

SERVICE DESCRIPTION

Incident Response Readiness Assessment and Planning

Overview

Trustwave's Incident Response Readiness Assessment and Planning Review service ("**Service**") offers Client develop and understanding of their preparedness to respond to a security incident, and to evolve their planning in preparation for an incident should it occur.

The Service is available to Client as a proactive service under the Advanced or Premium Digital Forensics Incident Response Retainers or as an a la carte service. The following descriptions 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

Trustwave will provide one or both of the following versions of the Service (as indicated in the applicable SOW or Order Confirmation between Trustwave and Client):

- Incident Response Readiness Assessment (IRRA)
- Computer Security Incident Response Plan (CSIRP)

Incident Response Readiness Assessment

Trustwave will assess Client's ability to respond to cybersecurity incidents based on the following metrics:

- Personnel to be engaged in incident handling (e.g. management, technical teams, HR, legal, 3rd parties)
- High-level incident response (IR) plan review
- Incident identification and escalation process
- Ticketing and case management
- Alerting technologies available (including any perceived gaps)
- Investigation technologies available (including any perceived gaps)
- Logging and audit facilities that are available or active
- Third party engagements
    - IR providers
    - IT services
    - Other – Legal, HR etc.

Trustwave will provide a report detailing the results of the assessment.

Trustwave Responsibilities

Trustwave will provide the Service either onsite at Client's place of business or remotely, as agreed between Trustwave and the Client. As directed by Trustwave, Client will distribute materials and information to Client personnel and provide requested documentation and information to Trustwave.

Client Obligations

Client will make Client personnel available for remote interviews as reasonably requested by Trustwave (such as IR team managers and IT administrators). Client acknowledges that Trustwave cannot perform the Service unless such personnel are made available.

Client will provide Trustwave with the following documentation:

- Client's computer security incident response plan
- Client's high-level network diagram
- Asset list and locations

Computer Security Incident Response Plan Review

Client and Trustwave will review Client's existing incident response plan (IRP) together. Client and Trustwave will work together to build on and further develop the IRP to reflect operational processes. Client and Trustwave will work together to outline playbooks.

Trustwave will provide a report detailing suggested additions, amendments, and other improvements to the Client's IRP. Client will remain solely responsible for implementing any changes and ensuring the efficacy of the IRP.

Trustwave Responsibilities

Trustwave will provide the Service either onsite at Client's place of business or remotely, as agreed between Trustwave and the Client. As directed by Trustwave, Client will distribute materials and information to Client personnel and provide requested documentation and information to Trustwave.

Client Obligations

Client will make Client personnel available for remote interviews as reasonably requested by Trustwave (such as IR team managers and IT administrators). Client acknowledges that Trustwave cannot perform the Service unless such personnel are made available.

Client will provide Trustwave with the following documentation:

- Client's existing IRP
- Details of network and endpoint monitoring processes and technologies including SOC/SIEM implementation and operation in Client's environment
- Details of key stakeholders during incident response processes
- Details of any technologies deployed within Client's environment that may aid IR investigation (e.g. EDR toolsets, AV, full network packet capture capability, forensic software/staffing, file transfer capability (where data for analysis needs to be extracted from the environment for local analysis by Trustwave – for example SFTP servers)).

Retainer Hours Consumption

If Trustwave provides the Service as a proactive service under the Advanced or Premium Digital Forensics Incident Response Retainer, the Service consumes forty (40) retainer hours.

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 Confirmation between Trustwave and Client.