Trustwave®

SERVICE DESCRIPTION

Incident Response Retainer

Overview

Trustwave's Digital Forensics Incident Response Retainer ("**Service**") consists of an allotment of hours Client may apply towards assistance from Trustwave in the event of a cybersecurity incident. Trustwave is available to provide such assistance 24x7x365 (subject to any posted service level agreements). 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

Digital Forensics and Incident Response (IR)

Trustwave will provide Client with an emergency contact number and email address to connect Client with a IR-trained Trustwave representative, available 24 hours a day, 7 days a week, 365 days a year.

Upon receiving a Client request to use retainer hours (a "**Support Request**"), Trustwave will triage the Support Request and related incident to determine the appropriate next steps. Next steps may include:

- Use of remote agents and remote analysis of data supplied by Client
- Deployment of Trustwave representatives to onsite locations (to be determined solely by Trustwave)
- Electronic break-in cause determination
- Electronic break-in source determination
- Laptop forensics
- Desktop forensics
- Server forensics
- Disk imaging
- Malware analysis
- Keyword searches
- Network activity monitoring

Malware Reversing

Client also may request support from Trustwave's malware reversing team. If Client identifies malware in Client's environment, Client should upload the malware to a platform identified by Trustwave for analysis. Depending on the outcome of such analysis, Trustwave may provide an analysis report identifying the malware's capabilities and threat intelligence information that Client may then use to identify other instances of malware within Client's environment.

Client Obligations & Acknowledgments

For Trustwave to provide the Service, Client will:

- provide Trustwave with access to its systems as necessary to perform the Service;
- remain in communication with Trustwave through the duration of the incident and investigation;
- deliver to Trustwave any data, logs, artefacts, or telemetry requested to further the Service; and
- keep Trustwave informed of any developments in the investigation including progress reports, problems encountered, changes in the aims, or closure of the investigation.

Client acknowledges that Trustwave only commits to provide the Service through remote delivery. Trustwave may recommend onsite delivery at its sole discretion. Any such onsite delivery will be agreed upon between Trustwave and Client.

Client acknowledges that additional hours may be needed to ensure a complete response by Trustwave.

Trustwave Responsibilities

Trustwave will

- provide Client with a red phone, unlisted telephone number, and an email address that may be used to initiate incident response escalations to Trustwave;
- try to respond to Support Requests within two (2) hours of receipt using Client-supplied email addresses or phone numbers;
- triage the incident and work with Client to determine the most appropriate next steps to investigate the incident
- lead the technical response to the incident in line with the requirements of Client's IR management team (IRMT) which are identified to Trustwave in writing;
- capture and analyze relevant data in order to work towards providing Client's IRMT with an understanding of:
    - nature of the incident
    - root cause of the incident
    - impact and extent of the incident
- advise Client's IRMT on methodologies and technologies to assist in the investigation, and their deployment;
- advise Client's IRMT on remediation activities; and
- produce a final report detailing the background, conduct, and outcomes of the Service.

Retainer Options

Essentials Retainer

Trustwave will provide up to forty (40) hours of the Service during the Term of the applicable SOW or Order Confirmation.

Unused Hours

Client may not use all forty (40) hours of the Service during the Term of the applicable SOW or Order Confirmation. Unused hours cannot be rolled over or extended beyond the Term. Client may not reallocate hours to alternate Trustwave services.

Advanced Retainer

Trustwave will provide up to eighty (80) hours of the Service during the Term of the applicable SOW or Order Confirmation. Under the Advanced Retainer, the Service also includes a data exposure investigation (the "**Investigation**") and the option to assign forty (40) of the available eight (80) hours to one proactive service (see next section).

Data Exposure Investigation

The Investigation aims to identify unauthorized exposure of Client data on the internet. The Investigation covers underground (also referred to as darknet or darkweb) sources including TOR websites, forums, and IRC (internet relay channels) deep web, and high-interest sites on the surface web.

Premium Retainer

Trustwave will provide up to one hundred and thirty (130) hours of the Service during the Term of the applicable SOW or Order Confirmation. Under the Premium Retainer, the Service also includes a Readiness and Detection Assessment (the "**Assessment**") and the option to assign a maximum of eighty (80) of the available one hundred and thirty (130) hours to proactive services (divided among two forty (40) hour proactive services or for one eighty (80) hour proactive service).

Readiness and Detection Assessment

The Assessment evaluates Client's ability to detect, investigate, and contain an information technology security breach. Trustwave will assess Client's people, processes, and technology against the five (5) stages of the incident response lifecycle for detection, evidence collection, analysis, and containment. During the Assessment, Trustwave will use interviews, documentation review, and limited testing to collect data.

Proactive Services

Client may not roll over or extend unused retainer hours beyond the Term of the applicable SOW or Order Confirmation.

Under the Advanced or Premium Retainers, Client may apply unused hours to proactive incident response services, subject to conditions outlined above and the following:

- Client cannot use retainer hours for proactive services until at least three (3) months of the Term.

- Client will notify Trustwave, in writing, of the desire to use retainer hours for proactive services at least three (3) months before the end of Retainer Year. A "**Retainer Year**" is the successive twelve (12) month increments during the Term of the applicable SOW or Order Confirmation.
- Retainer hours cannot under any circumstances be repurposed for any other services other than the proactive services listed below.
- If Trustwave cannot fully provide a proactive service within forty (40) hours, Trustwave will draw down any extra hours required from the Client's balance of hours if necessary.
- Client cannot top-up retainer hours to use the proactive services.

The following comprise the proactive services. Please refer to the applicable a la carte Service Description for each service. Trustwave will provide the proactive service in accordance with such Service Descriptions and Client will abide by any obligations under the same.

	Service	Usual Retainer Hours Cost
1.	Readiness and Detection Assessment	40
2.	First Responder Training	40
3.	Incident Response Plan and Policy Development	40
4.	Incident Response Tabletop Exercises	40
5.	Tactical Compromise Assessment	Maximum 80 hours (based on size of data)

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.