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

Service Features

Digital Forensics and Incident Response (DFIR)

Trustwave will provide Client with an emergency contact number and email address to connect Client with a DFIR-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 ("**Incident**"), Trustwave will triage the 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 compromise (cause, source, and extent) determination
- Computer forensics (laptop, desktop, servers, and disk imaging)
- Network forensics
- Active network monitoring
- Malware analysis
- Keyword searching, data culling, and electronic discovery
- Ransomware support
- Remediation consulting

Security Colony Subscription

The Service includes access to Security Colony. Security Colony is available at https://www.securitycolony.com/. Client's subscription type will depend on the retainer option Client has purchased:

- Essentials Retainer: Security Colony STARTUP
- Advance Retainer: Security Colony STARTUP
- Premium Retainer: Security Colony CORE

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Malware Reversing

Client may also 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 & Acknowledgements

For Trustwave to provide the Service, Client will

- clearly describe the nature of the Incident and provide ongoing updates as facts change;
- 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 requested information, data, logs, code, artefacts, or telemetry relating to or needed to further the Service;
- provide Trustwave with all relevant documents that are required to conduct the investigation;
- provide Trustwave with any available and applicable decryption keys or passwords required to access the data if encryption is used within the environment under investigation; 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 providing 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

Subject to Client fulfilling its obligations, 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;
- assign an investigator and respond to the Incident request within one (1) hour of receiving such a request. The assigned investigator will rely on Client-supplied email addresses or phone numbers in responding to the Incident;
- 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 incident response management team (IRMT) which are identified to Trustwave in writing;
- summarize the nature of Trustwave's recommended response and its containment efforts;
- 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.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Retainer Options

Essentials Retainer

Trustwave will provide up to forty (40) hours of the Service during the Term of the applicable SOW or Order Form. Under the Essentials Retainer, Client may choose to assign any of the forty (40) hours towards Group A, B, or C proactive services (see tables below) at any point during the Retainer Year. A "**Retainer Year**" is the successive twelve (12) month increments for which the Service is sold during the Term of the applicable SOW or Order Form.

Unused Hours

Client may not use all forty (40) hours of the Service during the Term of the applicable SOW or Order Form. Unused hours may be used in the three (3) months immediately following the Retainer Year for any proactive service in Group A, B, or C below provided that: (a) any hours to be consumed are used within those three (3) months and b) Client has purchased a subsequent twelve (12) months of the Service immediately following the Retainer Year. Unused hours will be subject to the terms of the Order Form or SOW for the subsequent year of the Service and any additional scoping document agreed in writing between Trustwave and Client. Client may not reallocate unused 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 Form. Under the Advanced Retainer, Client will select a Group A proactive service and may assign any of the eighty (80) hours towards Group A, B, or C proactive services at any point during the Retainer Year.

Unused Hours

Client may not use all eighty (80) hours of the Service during the Term of the applicable SOW or Order Form. Up to forty (40) unused hours may be used in the three (3) months immediately following the Retainer Year for any proactive service in Group A, B, or C below provided that: a) any hours to be consumed are used within those three (3) months and b) Client has purchased a subsequent twelve (12) months of the Service immediately following the Retainer Year. Unused hours will be subject to the terms of the Order Form or SOW for the subsequent year of the Service and any additional scoping document agreed in writing between Trustwave and Client. Client may not reallocate hours to alternate Trustwave services.

Premium Retainer

Trustwave will provide up to one hundred sixty (160) hours of the Service during the Term of the applicable SOW or Order Form. Under the Premium Retainer, Client will select two (2) proactive services from Group A or one (1) proactive service from Group B and may choose to assign any of the one hundred sixty (160) hours towards Group A, B, or C proactive services at any point during the Retainer Year.

Unused Hours

Client may not use all one hundred sixty (160) hours of the Service during the Term of the applicable SOW or Order Form. Up to forty (40) unused hours may be used in the three (3) months immediately following the Retainer Year for any proactive service in Group A, B, or C below provided that: a) any hours to be consumed are used within those three (3) months and b) Client has purchased a

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

subsequent twelve (12) months of the Service immediately following the Retainer Year. Unused hours will be subject to the terms of the Order Form or SOW for the subsequent year of the Service and any additional scoping document agreed in writing between Trustwave and Client. Client may not reallocate hours to alternate Trustwave services.

Premium Plus Retainer

Where Client has purchased the Premium Retainer, Client may purchase additional hours at the same rate as the first one hundred and sixty (160) hours at any time during the Retainer Year (subject to an additional written agreement between the parties).

Unused Hours

Unused additional hours may be used towards proactive services under the same conditions as the Premium Retainer above.

Proactive Services

Client may not roll over or extend unused retainer hours beyond the Term of the applicable SOW or Order Form except under the Advanced and Premium Retainers and subject to the following conditions:

- The quantity of roll over hours is limited to forty (40) hours
- The hours must be used within the first three (3) months of the immediately succeeding Retainer Year (if no such subsequent Retainer Year is purchased, the unused hours are not available for use)

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

- Client cannot use retainer hours for proactive services until at least three (3) months into the Retainer Year.
- 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 the Retainer Year.
- Retainer hours cannot be repurposed for any other services other than the proactive services listed below.
- If Trustwave cannot fully provide a proactive service within the usual retainer hours cost of twenty (20) or 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 (excluding the Premium Plus Retainer if such proactive services are used in the Retainer Year).

The following comprise proactive services. Please refer to Exhibits A – C for the applicable description of each proactive service.

Service Group A	**Usual Retainer Hours Cost** **hours to be agreed via email between parties*
1. Data Exposure Investigation	20
2. Incident Response Plan Review	20
3. Playbook Development	20

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Service Group B	Usual Retainer Hours Cost **hours to be agreed via email between parties*
1. Pre-Attack Vulnerability Assessment	40
2. Incident Response Plan Development	40
3. Detection and Readiness Assessment	40
4. Tabletop Exercise (Executive or Technical)	40
5. Training	40

Service Group C	Usual Retainer Hours Cost* **hours to be agreed via email between parties*
1. Cyber Advisory Services	Custom
2. Penetration Testing & Red Team Services	Custom
3. Purple Team Exercises	Custom

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 Form between Trustwave and Client.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

EXHIBIT A

Group A Services

Data Exposure Investigation

Trustwave will search the dark web and public sources for exposed Client data. Trustwave will perform analysis to determine if data from Client environment has been compromised. The investigation can be performed with key terms Client specifies surrounding areas of sensitivity (domains, executive employees, key products/projects, etc.) or with open-source intelligence. If key terms are to be used, Client will provide those terms for Trustwave to research against. Trustwave will deliver a findings report at the conclusion of the investigation.

Incident Response Plan Review

Trustwave will review the breach response aspects of Client's incident response plan. Client must have existing incident response plans that undergo annual or semi-annual review to keep current with industry and environmental changes. Client will provide documentation required by Trustwave and be available for interview sessions to gather the required information. Trustwave will deliver a report outlining suggested changes to the incident response plan at the conclusion of the review.

Playbook Development

Trustwave will review or develop up to five (5) playbooks for use in the Client's incident response process. Client will provide documentation required by Trustwave and be available for interview sessions to gather the required information. Trustwave will deliver the agreed upon playbooks at the conclusion of the Services.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

EXHIBIT B

Group B Services

Pre-Attack Vulnerability Assessment

Trustwave will investigate a wide attack surface, from a perspective external to Client, which mimics 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 findings report with recommendations for improvement at the conclusion of the Service.

Incident Response Plan Development

Trustwave will develop an incident response plan for breach response. This Service best serves Client where Client has no existing incident response plan or one that needs significant updates to be current with industry and environmental changes. Client will provide documentation required by Trustwave and be available for interview sessions to gather the required information. Trustwave will deliver an incident response plan at the conclusion of the Service.

Detection and Readiness Assessment

Trustwave will assess the current state of Client's incident response readiness and its roadmap for development towards incident response maturity. This Service evaluates Client's ability to detect and respond to incidents via technical and process controls. Client will provide documentation required by Trustwave and be available for interview sessions to gather the required information. Trustwave will deliver a findings report with recommendations that include security gap analysis and action plans at the conclusion of the Service.

Tabletop Exercise (Executive or Technical)

Trustwave will develop and execute with Client a scenario-based exercise, based on real SpiderLabs investigations, to help review incident response capability. This Service evaluates and aims to improve Client's incident response plan without any significant disruption to operations. 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.

Training

Trustwave will provide a virtual training session that offers incident response training such as fundamentals of incident response, anatomy of a compromise, evidence acquisition, response management, digital forensics, and response analysis for consumption by Client representatives. Client will provide documentation required by Trustwave and be available for interview sessions to gather the required information. Trustwave will deliver a live session covering the training objectives.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

EXHIBIT C

Group C Services

Please refer to our General Consulting & Professional Services description available on our website at https://www.trustwave.com/en-us/legal-documents/contract-documents/

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.