SERVICE DESCRIPTION

Comprehensive IR Retainer
SpiderLabs DFIR

Trustwave SpiderLabs is an industry leader in responding to and providing incident response to customers who have suffered data compromises or security breaches involving credit card fraud, unauthorized access, data theft, insider threat, malware outbreaks or other security incidents.

Alone, most organizations are not adequately protected and are poorly prepared to detect, respond to and investigate such security incidents. Together, Trustwave SpiderLabs and Client can better prepare Client’s systems to prevent and respond to such security incidents.

Trustwave SpiderLabs provide Client with Digital Forensics and Incident Response (“DFIR”) consulting services based on the following engagement principles:

- Work product that is built on the foundation of Trustwave’s leading industry expertise.
- A well-defined engagement model that helps to ensure a premium and consistent client experience.
- Clarity in communications to improve Client’s understanding of complex technical findings.
- A rigorous quality assurance process to standardize deliverables on a global scale.
- Prompt notification procedures for alerting Client to any material, high, or critical risk issues affecting Client’s environment.
- Continual innovation based on people, process, and technology.

Overview

This service description outlines the services provided under the Comprehensive DFIR Retainer (the “Services”). The Services are designed for organizations seeking to improve their overall cyber security incident response capability and to have rapid access to a team of experts capable of assisting in the event of a cyber security incident. Trustwave SpiderLabs provides experienced investigators on-call 24x7x365 all over the world. The Services include an agreed allotment of hours that Client may use when requesting Trustwave SpiderLabs to respond to an incident of any size. Client acknowledges that additional hours may be needed to ensure a complete response by Trustwave SpiderLabs. Trustwave SpiderLabs offers Client additional hours at a discounted hourly rate during the term of the Services.

Comprehensive DFIR Retainer Services

Services Included

- A Readiness and Detection Assessment (the “Assessment”)
- 130 available hours of DFIR reactive consulting services
Option to assign minimum 40-hour increments of the available 130 hours to DFIR proactive consulting services

Readiness and Detection Assessment

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

For further details, please refer to the Readiness and Detection Assessment service description available at [here](#).

Digital Forensics and Incident Response Reactive Services

Trustwave SpiderLabs provides Client with an emergency contact number and email address that will connect Client with an experienced investigator able to provide prompt guidance and assistance 24 hours a day, 7 days a week, 365 days a year. Using a global team of forensic investigators, Trustwave SpiderLabs adheres to the follow-the-sun model. In this way, Trustwave SpiderLabs avoids the need to direct customer calls to an answering service or to a less experienced help-desk operator.

Once Client calls the emergency contact number (a “Support Request”), the on-call investigator will triage the Support Request and related incident to determine the appropriate next steps. Such steps range from remote support using remote agents and remote analysis of data supplied by Client, to deploying members of Trustwave SpiderLabs’ global team to multiple onsite locations (to be determined solely by Trustwave). The triage process will determine the most appropriate combination of technical investigative techniques, digital forensic imaging and analysis, or malware reverse engineering needed to address the Support Request.

Typical DFIR reactive services may include the following services, (depending upon what is legally permitted within the relevant jurisdiction(s) or what is applicable to Client):

- 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

As a the Services, Client may choose to 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 SpiderLabs for analysis. Depending on the outcome of such analysis, Trustwave SpiderLabs may provide an analysis report in as little as half a day. Such an analysis report will identify the malware’s capabilities and threat intelligence information that Client may then use to identify other instances of malware within Client’s environment.

Any hours Client elects to use toward reactive DFIR consulting will be deducted from the 130-hour total of consulting service provided with the Services.
Service Level Agreements

All retainer services and SLAs are for remote delivery only. Trustwave and Client will separately agree to any onsite assistance as deemed necessary by Trustwave.

An experienced investigator from Trustwave SpiderLabs will respond to a Support Request within 2 hours of receiving such Support Request (the “Response Call”). Such investigator will rely on Client-supplied email addresses or phone numbers in responding to the Support Request.

During the Response Call, the investigator will triage the incident and work with Client to determine the most appropriate next steps to investigate the matter at hand.

Trustwave DFIR Consultants – Roles and Responsibilities

The role of Trustwave DFIR Consultants is to work with, and advise, Client’s incident response management team (IRMT) in the following ways:

- Lead the technical response to the the Support Request based on the requirements of Client’s IRMT
- Advise on the security incident and recommendations for containing it
- Capture and analyze relevant data related to:
  - nature of the incident
  - root cause of the incident
  - impact and extent of the incident
- Recommend, and advise on deployment of, methodologies and technologies to assist in the investigation
- Advise on remediation activities
- Produce a final report summarizing the incident, response steps taken, and the outcome of the technical investigation

Proactive DFIR Services and Unused Retainer Hours

Unused hours cannot be rolled over or extended beyond the end of the term of the Services.

If Client does not use 40 hours or more of the hours purchased as part of the Services during the term, Client has the option to take advantage the following proactive incident response services (“Proactive Services”). Each service specified below is delivered at a minimum cost of 40 hours to the retainer and is subject to following conditions:

- Client cannot schedule retainer hours for Proactive Services until at least 3 months of the term have elapsed and Client will notify Trustwave, in writing, of the desire to use retainer hours at least 3 months before the end of the term.
- Retainer hours cannot under any circumstances be repurposed for any other services beyond the DFIR Services specified in the table below.
- If a Proactive Service cannot be supplied within the minimum of 40 retainer hours, Trustwave will draw down any extra hours required from the Client’s balance of hours.
- Client may not ‘top up’ the Services for use on Proactive services.
The Proactive Services that may be called upon using unused hours are listed below:

<table>
<thead>
<tr>
<th>DFIR Services</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Readiness and Detection Assessment</td>
<td>[Link]</td>
</tr>
<tr>
<td>2. First Responder Training</td>
<td>[Link]</td>
</tr>
<tr>
<td>3. Incident Response Plan and Policy Development</td>
<td>[Link]</td>
</tr>
<tr>
<td>4. Incident Response Tabletop Exercises</td>
<td>[Link]</td>
</tr>
</tbody>
</table>