SERVICE DESCRIPTION

Standard 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 and 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's 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 ensure a premium and consistent client experience.
- Clarity on 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 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 Standard DFIR Retainer (the "**Services**"). The Services are designed for organizations primarily seeking 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 or a one-off data exposure investigation. 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 Agreement.

Included in the Standard DFIR Retainer Services

1. A data exposure investigation (the "**Investigation**")
2. 80 available hours of DFIR reactive services

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.

Further details can be found in the service description for Data Exposure and Investigation available here.

Digital Forensics and Incident Response

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 a 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. These can 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; and/or malware reverse engineering needed to address the incident reported in the Support Request.

Typical DFIR engagements 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
- E-mail and lost or erased data recovery
- Network activity monitoring

As a part of the 80 hours included in 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 use to identify other instances of malware within Client's environment.

Service Level Agreements

An experience 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 that initial Response Call, the investigator will triage the incident and work with Client to determine the most appropriate next steps. If remote assistance is required, such assistance will begin immediately after the Response Call. For illustrative purposes, approximately 70% of all Support Requests are handled remotely. If onsite assistance is required, investigators will use reasonable efforts to commence travel to the Client site by the next business day after the Response Call.

Unused hours

If Client does not use 40 hours or more of the 80 available hours during the contract period, Client may choose to take advantage two of the following services during the final three months of the contract period:

	Service	**Service Description**
1.	Readiness and Detection Assessment	Link
2.	First Responder Training	Link
3.	Plan and Policy Development	Link
4.	Tabletop Exercises	Link