SERVICE DESCRIPTION

DFIR Proactive Services

SpiderLabs DFIR

The Trustwave SpiderLabs Incident Response Readiness Program ("**IRRP**") is a multi-faceted program built to help improve an organization's resilience and ability to detect and respond to data security breaches.

Trustwave SpiderLabs is an industry leader in responding to and providing incident response services to customers who have suffered data compromises or security breaches involving credit card fraud, unauthorized access, data theft, insider threat, malware outbreaks and 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 has created a comprehensive program that blends its knowledge and experience in incident response, proactive security testing, and first responder training. Trustwave customizes this program to meet the needs of Client. The first step is a readiness assessment which identifies gaps in Client's incident response capability. Trustwave then tests a mix of development and business as usual (BAU) tasks to achieve and maintain the desired level of readiness.

Trustwave SpiderLabs provides 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 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 material, high, or critical risk issues affecting Client's environment.
- Continual innovation based on people, process, and technology.

Overview

IRRP is comprised of various proactive DFIR consulting services designed to improve Client's threat readiness before, during, and after incidents. Trustwave's structured and holistic approach to incident management helps Client raise its security awareness and establish a proactive mindset. Trustwave customizes such improvements based on Client's needs. Client benefits from Trustwave's historical knowledge cultivated over many years of testing and strengthening client systems. Trustwave SpiderLabs will provide key insights for addressing the most common security threats and vulnerabilities that lead to a data compromise.

Thanks to the range of offerings under IRRP, hours not allocated to DFIR reactive consulting requests may be reallocated to any of the available options in the following table (dependent upon the details of Client's retainer services):

Service	Description	Deliverables Link	
Readiness and Detection Assessment	Evaluation of Client's ability to detect incidents and identify gaps providing recommendations for improvement.	Assessment report Gap analysis and action plan for all findings	Link
Computer Security Incident Response Plan (CSIRP) Development	Development and documentation of a process for incident response (IR). Development includes interactive sessions that will result into baseline documents (to include in playbooks) addressing each incident class from the readiness and detection review.	CSIRP review and/or development IR Templates and Playbooks	Link
Training courses	A range of Digital Forensic and Incident Response training courses.	Onsite training and training materials	Link
Data Exposure Investigation	Identification of unauthorized exposure of Client data on the Internet and darkweb sources.	A full report on findings and recommendations based on the information discovered.	Link
Tabletop Exercises	A series of Tabletop Exercises to evaluate and improve CSIRPs without any significant disruption of operations.	Tabletop Exercises simulating various scenarios	Link

Individual Service Summaries

Readiness and Detection Assessment

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

For further details, please refer to the Readiness and Detection Assessment service description available at Link.

Computer Security Incident Response Plan (CSIRP) Development

Through CSIRP, Trustwave SpiderLabs develops and documents an appropriate incident response ("**IR**") process for Client to include in playbooks, IR templates, and IR/Security Training. Trustwave SpiderLabs

holds interactive sessions with Client to prepare a baseline document that Client may customize and expand over time.

Separate response plans will be developed for each of the incident classes identified and reviewed by the Assessment.

Trustwave SpiderLabs will assist Client in developing incident response playbooks specific to Client's environment and develop business processes specific to applicable industry best practice guidelines (such as NIST (SP-800)). Incident response playbooks complement existing CSIRP by providing Client with environment-specific technical guidance for in-house incident response teams on preparing, identifying, containing, remediating, and recovering from computer security incidents.

For further details, please refer to the Computer Security Incident Response Plan (CSIRP) Development service description available at Link.

DFIR Training

Seasoned Trustwave SpiderLabs security professionals deliver pre-defined or custom incident response, computer forensics, and malware analysis courses to meet the targeted needs of Client's security team (as agreed between Client and Trustwave). Typically, at least half of each course is spent conducting hands-on exercises. The following are examples of the types of training available:

- **Fundamentals of Incident Response (FIRE)** – 2 days onsite – Trustwave SpiderLabs prepares and delivers onsite training to prepare Client's cyber incident response team to be the first on the scene, while preserving the confidentiality and integrity of the systems in question. Through this training, Client's CIRT is shown the tools and techniques necessary to properly gather volatile data while leaving the smallest digital footprint possible on the affected systems. (**Hours used: 40 hours**)
- **Incident Management and Investigation** – 2 days remote – This course teaches Client representatives about the proactive, reactive and reflective activities that may be relied on before, during and after security incidents. The target audience before this course includes anyone involved with security incidents (not only security staff). (**Hours used: 40 hours**).

Note: Due to the high demand for our Trustwave SpiderLabs trainers, Client may need to book these courses several months in advance.

Further details can be found in the service descriptions for Fundamentals of Incident Response (FIRE) training available at Link and Incident Management and Investigation training at Link.

Data Exposure Investigation

The Trustwave SpiderLabs Data Exposure Investigation service aims to identify unauthorized exposure of Client data on the Internet. Data Exposure 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 at Link.

Tabletop Exercises

During Tabletop Exercises, Trustwave SpiderLabs evaluates and improves Client's CSIRP without any significant disruption to its operation (Trustwave SpiderLabs leverages Tabletop Exercises for both the Assessment and DFIR training). The exercises include various realistic scenarios which Trustwave has encountered during investigations. These scenarios cultivate the skills and mindset which enhance Client's security response capabilities.

Further details can be found in the service description for Tabletop Exercises available at Link.