SERVICE DESCRIPTION

SpiderLabs Proactive Threat Hunting Service

Service Scope

Trustwave SpiderLabs is an industry leader in responding to providing incident response to customers who have suffered data compromises or security breaches involving credit card fraud, unauthorized access, data theft, insider threat, and malware outbreaks. Incident Response and Digital Forensic engagements reveal a common theme; many organizations were not adequately protected with the use of regular signature-based and some behavioral-based controls, resulting in greater exposure to security risk. Client Systems are often compromised for years prior to detection and containment of the attacker. The goal of the SpiderLabs Proactive Threat Hunt service is to help identify undetected threat actors currently on the network and to provide increase integrity of Client's environment.

The strategy of a Proactive Threat Hunt assumes a breach has already occurred and searches for any indication of an attack and its root cause. Proactive Threat Hunts have quickly become best practice for organizations with low risk tolerance as well as recommended for situations including in advance of merger and acquisition activity and following confirmed data breaches. A Proactive Threat Hunt initially defines the current threat landscape facing Client and its individual industry by examining specific threat actors motivated to target the organization as well as the TTPs (Tactics, Techniques, and Procedures) that these identified threat actors are known to utilize. Threat modeling focuses on the following elements:

- **Corporate and industry analysis**

  Trustwave SpiderLabs Intel Fusion Team actively tracks 60+ active threat actor groups operating throughout the globe. In addition to tracking nation-state sponsored threat group (such as significantly active organizations in China and Russia), the Intel Fusion Team also tracks global hacktivists and cybercrime syndicates currently actively in cyber-crime hot spots such as Brazil, the Middle East, USA, Canada, and North Korea. Reports provides comprehensive threat actor analysis and their TTPs.

- **Industry historical breach analysis**

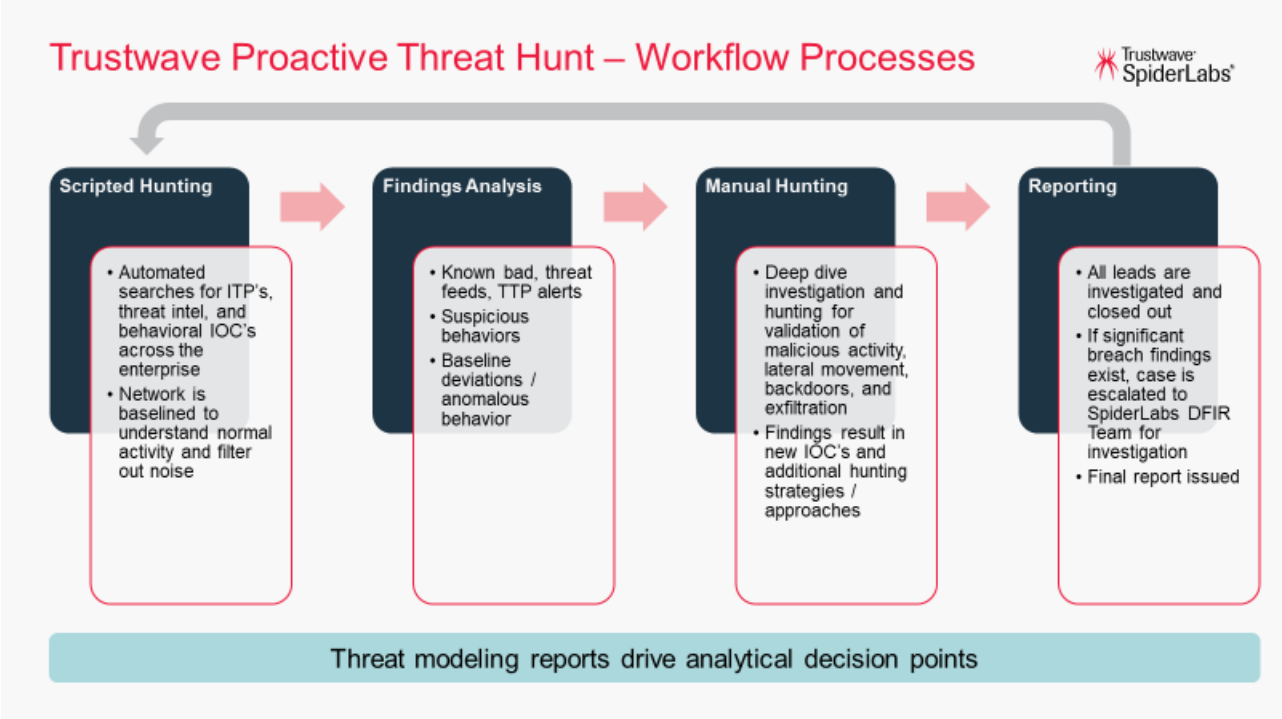
  Trustwave SpiderLabs will examine historical data breaches from the same industry to identify previously successful TTPs. These will be one of the first data sets examined as the hunt is launched.

- **Data leakage and email credential compromise review**

  Trustwave SpiderLabs will review dark web and credential harvesting sites to identify leaked corporate data, employee PII, and/or lost credentials. These data sources will reveal potential previous compromises and existing corporate vulnerabilities.

Trustwave's SpiderLabs methodology, as demonstrated by the Threat Modeling Report, enable our cyber-threat hunters to narrow the scope of their investigation and focus on actionable intelligence and TTPs, resulting in effective and efficient threat hunt services with reduced time to completion and cost.

The general hunt process is outlined in the graphic below:



- **Scripted Hunting:** The SpiderLabs Threat Fusion Team has developed a library of hunt scripts designed to identify suspect behavior exhibited by APT and cybercrime groups monitored within the SpiderLabs Intel Fusion Platform (IFP). This library is constantly updated to match the current threat landscape. Suspect behavior that will be identified and analyzed includes:
    - **Unsigned / unauthorized persistence –** Processes that start automatically on reboot.
    - **Privilege Escalation –** Processes / users that have elevated privilege to SYSTEM / ADMIN.
    - **Lateral Movement –** Processes / users that have moved throughout the network in an unusual manner or have conducted unusual network reconnaissance activities.
    - **Data Theft –** Processes / users transmitting unusually high volumes of data.
    - **Suspect Process Execution** – Hidden or obfuscated file execution, execution from TEMP or suspect directories, downloaded file execution, Powershell and PSEXEC execution, etc.
    - **Fileless Malware memory injection** – Processes injected into other process' memory space.
    - **System / Protected File Modifications** – Unauthorized changes to protected files.
    - **Remote Admin** – RDP and other remote administrative tool usage.
    - **SpiderLabs IFP Threat Intelligence IOC Search** – Millions of contextualized IOCs attributed to known threat actors will be automatically identified.

    ***Note: this is only a small sample of the suspect behavior that will be reviewed in the Proactive Threat Hunt and is not a comprehensive list.*

- **Findings Analysis:** The scripted hunt will produce voluminous results requiring extensive expert analysis. False positives are dismissed and suspicious elements are separated for manual analysis.
- **Manual Analysis:** The Threat Fusion Team is composed of computer forensic and security experts who reverse engineer suspected malware. If true malicious behavior is identified, the newly discovered TTPs will again be hunted throughout the network. ***In the event of significant ongoing data breach or widespread infection, hours will be added to the SOW to enable the investigation and the SpiderLabs Digital Forensic & Incident Response (DFIR) may be engaged.*
- **Reporting:** Weekly reporting and ad hoc communications will occur throughout the course of the Proactive Threat Hunt. The final report will include positive malicious findings, identified vulnerabilities and network infrastructure deficiencies that could lead to a future breach, as well as any other relevant findings generated throughout the course of the Proactive Threat Hunt.

The Trustwave SpiderLabs Threat Hunt is designed to identify potential malicious activity within Client's environment. It leverages multiple data sources to enable correlation of events providing deep insight into user behavior.

OVERVIEW AND DATA SOURCES

Each industry has different needs and security infrastructure, with each environment having different requirements. Tto accommodate these variations Trustwave's Threat Hunts are customized to the customer's needs, including available sources of evidence, budget and desired level of confidence in the outcome.

Trustwave SpiderLabs Proactive Threat Hunts require deployment of an Endpoint Detection and Response (EDR) agent to all systems within the scope of the hunt. The EDR agent (also known as a sensor) is a small, light-weight executable that can be deployed easily and in an automated method. These agents cause minimal network and system impact and are usually not noticed by users or system administrators. Currently, Trustwave partners with industry leading EDR providers Cybereason and Carbon Black to conduct Proactive Threat Hunting.

In addition to the EDR agent, Trustwave SpiderLabs will request access to network traffic data, if available. This may include SIEM access, application of a custom-built Sysmon/ELK Event monitor hunting tool, PCAP data, or any other relevant network-specific data source that may assist our hunters. However, while additional data points are helpful and may improve the efficiency and efficacy of the hunt, the only required element is the EDR agent.

DELIVERABLES

- If malicious activity is identified during the engagement the client will be notified and assistance in engaging appropriate incident response provided.
- Upon Client request after the threat hunt is completed, Client will be provided with a report detailing the methods of analysis and any findings of malicious activity and remedy actions that have occurred.