Trustwave®

DATA SHEET

Trustwave SpiderLabs® Proactive Threat Hunting

HUNT DOWN THREATS HIDING IN YOUR NETWORK

Benefits

- Combines renown SpiderLabs threat intelligence and incident response security expertise with customized tactics to aggressively hunt cyber-threats on your network
- Identifies advanced threats as well as minor threats, potential vulnerabilities, and poor network/software configurations
- Delivers a security roadmap designed from intimate knowledge of every single network callout and binary on every endpoint in your network

A credit card number. A common password used on five other websites. Your address, your social security number and your mother's maiden name. Billions of pieces of personal -and valuable- information like this are stolen every year. One day you may find your own secrets posted online for the world to see, or worse: data from millions of your customers. Companies, careers, and lives have been shattered because sophisticated cyber criminals constantly pursue your data and will stop at nothing to acquire it. Don't find yourself regretting a breach after it happens. Identify and eliminate the threat before it gets to that point.

Trustwave SpiderLabs Proactive Threat Hunting

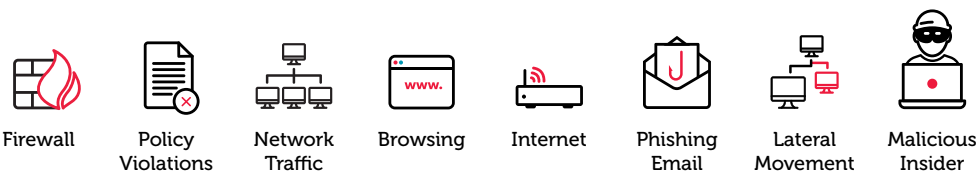
The Trustwave Global Security Report states average attacker dwell time (elapsed time from intrusion to detection) is 83 days but can last several years when dealing with professional and covert Advanced Persistent Threats (APT) attackers. How do you know if APT attackers currently dwell in your network? A Trustwave Proactive Threat Hunt finds and kills these threats. We have a proven history of identifying well-hidden compromises and eradicating advanced attackers.

While finding and eliminating threats is the primary goal of a threat hunt, there are other benefits. The hunt provides visibility into previously unknown weaknesses in your environment, such as outdated and vulnerable software, violations to policy, insider threats, and unprotected databases.

A proactive threat hunt will produce a prioritized security roadmap with clear action items to reduce corporate risk. Every bit of data matters when the hunt begins. Even the most mundane events or simple transactions can cause major breaches.

Nothing in a Network is Overlooked

When you partner with Trustwave SpiderLabs for a proactive threat hunt, our expert hunters will employ our proprietary Threat Hunting Platform, combined with industry-leading EDR and powerful SpiderLabs cyber threat intelligence to find threats and weaknesses within your network infrastructure.



SpiderLabs EDR agents and proactive threat hunting toolkits enable the Trustwave threat hunting team to quickly and consistently deliver the highest level of service. Their mission is to detect, contain, and eliminate threat actors, and to reduce the overall security risk of an organization by identifying gaps in the client's network.

Trustwave SpiderLabs Threat Hunters

Threat hunters at Trustwave use and develop threat detection and identification methods with their **decades of deep experience** in computer forensics, cyber threat intelligence, and malware analysis. Our methods reduce the time and resources needed for thorough identification of threats and vulnerabilities.

Our Comprehensive Approach

Starting with a broad foundation and systematically targeting in on the world's most dangerous APTs, our **Threat Hunting Pyramid** defines each essential building block of our approach to a proactive threat hunt.

Following the Threat Hunting Pyramid, our hunters locate and identify multiple types of threats, including:

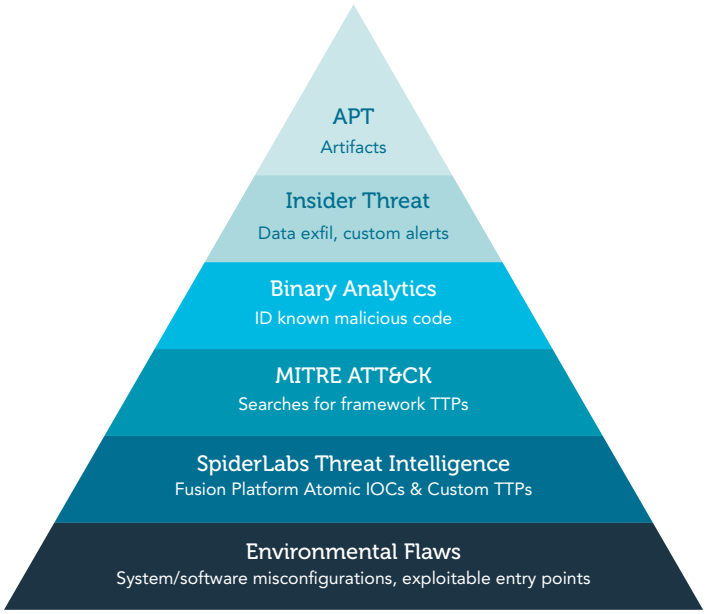
- Advanced Persistent Threats
- Out-of-place Files / Objects
- Risky Software / Apps
- Binary Threat Scores
- System Admin Tools
- Outdated Software
- Malware / Adware
- Criminal Threats
- Business Threats
- Insider Threats
- Vulnerabilities

This approach ensures a comprehensive threat hunt is conducted efficiently and effectively.

Adversary Tactics and Techniques

APT methods vary by threat actor, individual campaign, and target environment. The Trustwave SpiderLabs Proactive Threat Hunting team has developed detection use cases derived from every technique outlined in MITRE's ATT&CK Framework, ensuring comprehensive coverage.

With an initial baseline of the threat landscape that is relevant to your organization, the Proactive Threat Hunting platform, MITRE framework, SpiderLabs threat intel, and the best hunters in the world behind the wheel, each threat hunt is a comprehensive exercise that will put you at ease about your security posture.



Threat Hunting Pyramid

Trustwave® | sure.business