Trustwave SpiderLabs

CROSS-DISCIPLINE CYBER SECURITY EXPERTISE
FOR SUPERIOR PROTECTION

Trustwave®
SpiderLabs®

Few if any enterprises have in-house all the expertise it takes to provide sound, holistic cyber security defenses day in and day out. Even if you did, given the demand for people with security experience, it'd be exceedingly difficult and expensive to keep them.

Indeed, providing cyber security is a complex endeavor that requires expertise in a number of disciplines, including:

- Security research, to identify and keep track of the latest threats
- Vulnerability Scanning, penetration and red team testing, to find holes in your security armor
- Incident response, to identify the source of a breach and its impact, and secure evidence
- Threat hunting, to find and eliminate active threats lurking in your environment

While all of these functions are necessary, they are not likely what you're in business to provide.

At Trustwave, on the other hand, cyber security is all we do. We've developed the technical tools and expertise it takes to address the security challenges an enterprise confronts. They're provided to you by four distinct groups, each with its own area of expertise, but all wrapped under our SpiderLabs umbrella.

Trustwave SpiderLabs: A team approach

Each individual SpiderLabs team is world-class in its own right; taken together they add up to a formidable force.

At the center is the Research Team, which houses an extensive database of known threats while keeping a constant eye out for emerging threats.

SpiderLabs teams also engage each other as needs and your requirements dictate. On the pages that follow, we'll provide examples and take a deep dive on each team to demonstrate their depth, breadth and value.

Security Research Team

The SpiderLabs Security Research Team consists of more than 50 cyber security experts. They maintain the Trustwave Global Threat Database, which holds billions of records about cyber threats, malware and vulnerabilities from around the world, including malicious URLs, IP addresses, file hashes and the like.

The Research Team collects cyber intelligence through a constantly expanding network of feeds and partnerships, and shares its knowledge through various global projects.

To keep abreast of what adversaries are up to, our Research Team also monitors the dark web. Researchers actually infiltrate closed forums used by cyber criminals, to monitor their activity and identify emerging threats early on.

They routinely publish important findings in the SpiderLabs Blog, with detailed explanations that often gain global attention from top-tier news organizations. A few examples include:

- BlackByte Ransomware, which Trustwave discovered during an incident response. Our October 2021 blog post included detailed technical analysis and, in part 2, a code obfuscation analysis. The topic was picked up by several technical publications, including Ars Technica, Engadget, TechCrunch and TechRadar.
- Our blog post in Feb. 2021 detailed three severe vulnerabilities in several SolarWinds products, including one that allowed remote code execution with high privileges. It was timely in that the industry was dealing with a widespread attack with SolarWinds at the root. The piece prompted some 120 global media mentions, including from the likes of NBC, The Washington Post, Forbes, Dark Reading and ZDNet.
- Amid the 2020 U.S. presidential election, Trustwave researchers found a massive database for sale on several hacker forums containing data on millions of U.S. voters. "The information found in the voter database can be used to conduct effective social engineering scams and spread disinformation to potentially impact the elections, particularly in swing states," our blog post warned. That post was publicized by The New York Times, DailyMail UK, Business Insider US/AU, MSN, NBC, Next Gov, FOX News, Dark Reading, and other news outlets.

Additionally, vulnerabilities that are found in third-party products are responsibly reported to vendors. SpiderLabs assists the vendor in test fixes and collaboratively issues advisories/patch bulletins. All security advisories are published online.

Deep learning and a global view

In an effort to constantly improve its research capabilities, the Spider Labs Research Team also works to develop machine learning and deep learning algorithms to detect malware. In addition to furthering its research efforts, the fruits of this labor can end up in products. Machine learning models that are currently in use for inspecting web content and in the Trustwave MailMarshall product to identify malicious email threats was developed by the Research Team, for example.

Most importantly, though, its various efforts give the Spider Labs Research Team a broad and deep understanding of cyber-crime, covering a range of threats to databases, networks, email, servers and more. That's crucial to identify threats that span multiple attack vectors, as many do. An intrusion that begins with a social engineering attack, where a user downloads malicious code, may end up leaving traces across numerous other servers and applications. It takes a researcher with deep experience in how attackers think to identify all the tell-tale signs.

The SpiderLabs Research Team also benefits from having a global view. Trustwave has clients literally around the world, in various vertical industries. That provides our researchers with visibility into threats no matter where they originate – and puts them in position to sound the alert.

Penetration Testing / Red Team

The SpiderLabs Penetration Testing team includes some 120 cyber security professionals who are focused on helping clients find vulnerabilities in their infrastructure. They help clients continually refine their defenses to raise their level of cyber security maturity.

The main avenues for accomplishing that include regular vulnerability assessments, penetration testing and red/purple team exercises.

Vulnerability management

Vulnerability management involves regular scans to check for known vulnerabilities. Any vulnerabilities found must then be assessed to find those that truly present risk, vs. others that are mitigated by other security measures.

With regular vulnerability scans, you can stay on top of the vulnerabilities your organization faces and identify gaps in your security programs and technologies, such as holes in applications, software flaws, configuration issues and patching problems. Trustwave will provide mitigation guidance for any issues it finds.

Penetration testing

Penetration testing provides the next step up from vulnerability management. Rather than just find vulnerabilities that may present cyber security issues, penetration testing involves experienced "white hat" hackers who attempt to infiltrate your cyber defenses, to expose any weaknesses by proving they can be exploited.

Deep experience, CREST-certified

While many companies offer penetration testing, few have the deep experience of Trustwave. Our penetration testing team, established some 15 years ago, last year conducted over 100,000 hours of pen testing. In that time we found 30,000 vulnerabilities, 900 of which were deemed "critical," meaning a real breach would have potentially devastating consequences.

All of these findings were fed back into our Global Threat Database and the cloud-based Fusion Platform, which serves as the foundation for all Trustwave security offerings. Given that, the findings end up benefiting all Trustwave clients.

Trustwave was also the first global member of CREST, the Council for Registered Ethical Security Testers. CREST membership gives clients a level of trust that there's a methodology and rigor to pen testing procedures, and that all testers have been properly screened.

What to expect from a pen test

In terms of what to expect from a penetration test, given they last a finite amount of time, the tests typically target a specific area. A given pen test may target web applications, network infrastructure, servers, mobile applications, or APIs, for example. Trustwave can also target specialty areas, notably Internet of Things (IoT) devices and applications that are proliferating throughout many enterprises – and presenting new attack surfaces.

Trustwave pen tests also come in different varieties that relate to degree of difficulty. With a "white box" test, the pen tester has access to significant information on what's being tested while with a "black box" test the tester gets no information. A grey box test sits somewhere in between.

No matter the type, Trustwave shares the results of each test, including the exact steps the tester took and, if any defenses were breached, how that was accomplished. Clients can then use that information to shore up defenses, to continually improve their security posture. Reporting is provided for both technical and executive audiences.

Red team, purple team exercises

As your security defenses mature, you may be interested in a red team or purple team exercise.

Red team exercises involve a simulated attack with far fewer constraints than a penetration test, giving your security team a chance to practice and hone its defensive policies and procedures. The assessment will often include aspects of penetration testing combined with social engineering and physical security testing. You'll provide Trustwave with an exercise objective, such as a target to breach. Our red team will attempt to reach that objective without being detected, with the goal being to expose any flaws in your blue team – the security people, processes and technology that defend your enterprise.

A purple team exercise involves your blue team of defenders working in conjunction with Trustwave to defend against a red team attack. Such an exercise typically focuses on a scenario you select, based on your immediate risk concerns.

We'll collaborate with your team throughout the attack, guiding them through advanced defense tactics, techniques and procedures (TTPs). After the engagement, we'll continue to collaborate on remediation advice for any issues uncovered during the exercise.

Global Digital Forensics and Incident Response (DFIR)

In the event of an actual security incident, you can call on the SpiderLabs Global Digital Forensics and Incident Response (DFIR) team.

Our DFIR team provides 24×7 on-call response services for retainer-based clients and in emergency situations for any company. In either case, our DFIR team strives to quickly identify the source of the breach and the extent of the damage.

We'll get to the bottom of the origin of the breach, how it spread, its consequences in terms of compromised resources, and steps to control and remediate. Throughout the engagement, we'll help with forensics and protect the chain of evidence in case of any future litigation involving the incident.

Importantly, our DFIR services are technology agnostic. We're not tied to or affiliated with any specific endpoint detection and response (EDR) tool; rather, we'll adapt our approach to the security defenses you have in place.

Retainer clients

As a Trustwave retainer client, you can rest assured that you won't be seeing us for the first time when an incident occurs. We'll get to know your environment ahead of time, including your main points of contact, so we're not starting from ground zero.

You'll also have access to a direct number you can call for an immediate response in case of emergency. Our service level agreement says you'll get a response in less than 2 hours; in 2021, the actual figure was less than 10 minutes. Once engaged, our DFIR team acts as a technology lead on the incident investigation.

Consulting services

Should you be fortunate enough not to have to engage our DFIR team during your retainer period, Standard and Advanced tier retainer clients can use some of the unused hours towards other Trustwave consulting services. These proactive services, which help you to prepare to deal with an attack, include:

- Gap analysis, to identify holes in your security maturity
- Developing an incident response playbook
- Conducting training, including tabletop exercises to walk your team through an effective incident response
- Penetration testing

DFIR within SpiderLabs

Within SpiderLabs the DFIR team works with the Security Research Team to understand new and emerging threats. The Research Team also helps to reverse-engineer any new malware the DFIR Team finds, to create new indicators of compromise (IOCs) that all teams can benefit from going forward.

The DFIR team also acts as an escalation point for Trustwave Managed Detection and Response (MDR) service teams and penetration testers. When they identify a breach and can't immediately identify the source, they can come to the DFIR team for further investigation.

Global Threat Hunting

The SpiderLabs Global Threat Hunting team conducts the deepest level of threat investigations. Its mission is to identify active adversaries in your environment using threat intelligence, threat actor TTPs, and cyber kill chain acumen to guide hypothesis-based hunts.

Similar to the DFIR team, our threat hunters also respond to security incidents on behalf of clients as an escalation point for the Global Threat Operations team. But where the DFIR team responds to incidents when there's clear evidence of a breach, the Global Threat Hunting team may be called in on only the suspicion of a breach. Given that, the team has no timeframe to go by in conducting the investigation, making the job more difficult.

Another way to look at the work the Global Threat Hunting team does is to ponder the question, "How do you know you're not breached right now?" Unless you're actively threat-hunting, you don't.

Trustwave threat hunters pick up where automated tools leave off, because such tools are often not enough to catch active threats. Our threat hunters look for what tools don't or can't find. That requires expertise to understand not just IOCs, but anomalous behaviors that suggest malicious intent.

The SpiderLabs Global Threat Hunters take on three main roles:

- Continual threat hunts involves up-front research to understand the client environment, including any threats specific to your vertical industry. A threat hunter is assigned and rotated yearly, while threat hunts are conducted on a quarterly basis.
- Escalation point for global threat hunts in our security operations center (SOC). The Global Threat Hunt team is part of the tier-3 SOC escalation point.
- Proactive threat hunts. Trustwave can also perform custom threat hunts for clients. These may follow a merger/acquisition or post-breach remediation, for example, where you want to check out the threat environment of the company.

Our threat hunters do more than merely identify anomalous behavior. In some instance, there may be no evidence of anomalous behavior, but the team nonetheless identifies multiple vulnerabilities that could have been exploited. In such cases, we'll point them out and provide advice on how to address them.

As with our DFIR team, Trustwave threat hunters work with a variety of best-in-breed EDR tools, including Carbon Black Cloud, Carbon Black Response, Cybereason, Cortex XDR, and Microsoft Defender for Endpoints.

Threat hunters also complement the DFIR team. DFIR is on the forefront of emerging threats on a global basis. As such, they can feed intelligence to our threat hunters, helping to make them more effective. The threat hunt team can also engage DFIR as necessary, such as for incident response and digital forensics.

The threat hunt team engages with the Security Research Team when necessary, as well, such as to reverse-engineer a potentially malicious binary to determine whether it's truly a threat and, if so, come up with an IOC.

Powered by elite security experts

All four SpiderLabs focus areas depend on one common element for their success: experienced people. As is hopefully clear by now, it takes more than the latest tools to ensure proper security; you need expertise to understand what the tools are telling you – and to look for what the tools don't find.

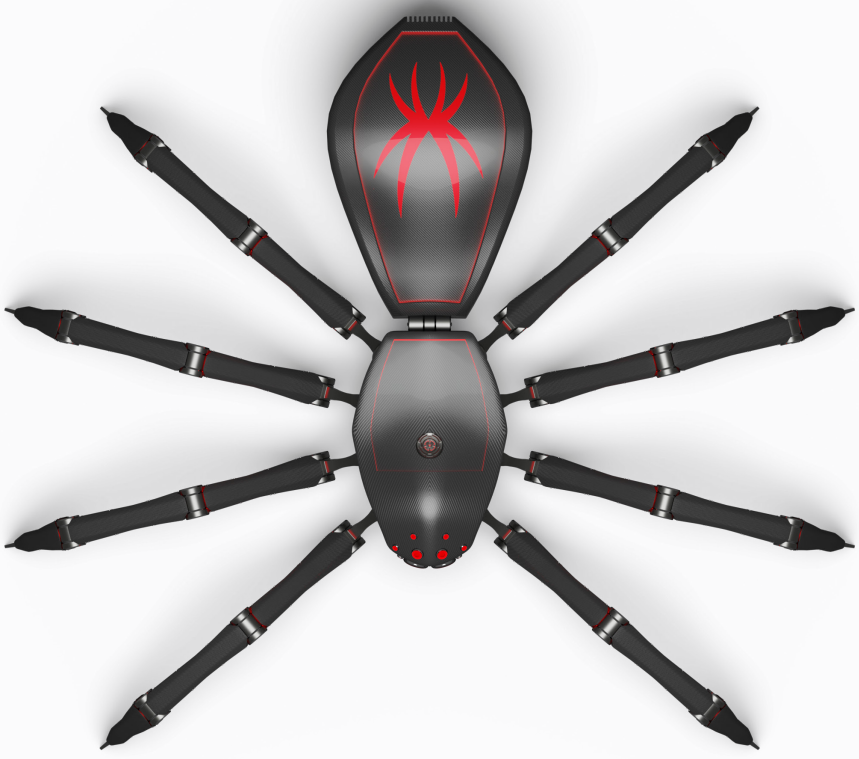
In an environment where security expertise is at a premium, such expertise is not easy to come by. That's why Trustwave focuses on not only hiring the best available security experts, but developing from within and retaining our best and brightest.

As a global company, we source security talent from around the world. We also focus on finding people with experience at organizations that we know focus heavily on security, including the military, telecommunications companies and managed security service providers.

Our employees are not "9 to 5'ers." They are flexible, able to adapt to situations as they arise, communicate effectively, and generally do what it takes to win the cyber security battle.

In return, Trustwave invests in its staff, devoting both time and budget each year to all SpiderLabs employees to help them further their training and enhance their skills.

We also develop our own tools to help automate routine tasks, so our security professionals aren't mired in mundane, tedious tasks and processes. Rather, we challenge them with interesting projects that help them put to use what they've learned and further refine their skills – for their benefit and yours. Additionally, the SpiderLabs team engages with the cyber security industry by releasing tools (Responder, SocialMapper, CrackQ, etc.) and contributing to the MITRE and ATT&CK frameworks.



Engage with Trustwave SpiderLabs

Learn more about how Trustwave and its SpiderLabs experts can improve your security posture.

www.trustwave.com

Trustwave®