Trustwave®

Trustwave Incident Readiness Program

PREPARE FOR AND MITIGATE THE INEVITABLE

Detecting intrusions and containing them quickly can prevent a minor incident from becoming a ruinous, large-scale data compromise. Clients choose the Trustwave Incident Readiness Program to prepare for, recognize and immediately deploy expert Trustwave SpiderLabs incident responders to a compromise before it's too late.

Many organizations simply haven't developed or tested their incident response program, and too many depend upon a dusty plan stored in a desk drawer. In 81 percent of compromises investigated by Trustwave last year, victims failed to detect a breach themselves. Trustwave Incident Readiness Program customers know how to detect an incident and respond quickly to reduce its impact. As a complete package, the Trustwave Incident Readiness Program will give you the capability to investigate any threat ranging from advanced-persistent-threat-style attacks to a recently terminated administrator logging into your network remotely. Trustwave Incident Readiness Program customers enter into a retained services agreement that includes discounted pricing and immediate escalation to the top of the Trustwave incident response work queue. Throughout the year, customers can spend funds on emergency response services, or choose from items available as part of four classes of services: Preparedness Services, Risk Management Services, Incident Response Services or Insider Threat Services. Any incident response engagement draws down your pre-purchased credits, and if you ever need more, adding credits is simple and quick.

Unmatched Expertise

Trustwave SpiderLabs has responded to thousands of data security incidents and conducted thousands of penetration tests. In addition, the team's research division is a go-to resource for the latest developments in data security threats. This experience gives Trustwave SpiderLabs unique insight into indicators of compromise (IoCs) and attackers' patterns of behavior. Because of its flexible retained services agreement, customers enjoy direct access to some of the best incident responders in the industry at discounted cost and with prioritized service. Custom fit to your organization's needs, the program can include preparedness services, risk management services, on-call incident response at a moment's notice and insider threat or HR services.

Why Trustwave?

Clients choose the Trustwave Incident Readiness Program for the following reasons:

1. **Speed** Completing paperwork ahead of time eliminates deployment delays that could spell the difference between an incident and a crippling, headline-grabbing data breach.
2. **Priority** No matter the demands on Trustwave SpiderLabs' time, program participants receive priority over any other work.
3. **Lower cost** The program's structure allows us to significantly discount our rates.
4. **Fully customizable** A Trustwave SpiderLabs incident response expert will serve as your trusted advisor and ensure you get and pay for only the services you need.

The four classes of services available as part of the Trustwave Incident Readiness Program

Preparedness Services

Trustwave SpiderLabs has responded to and investigated thousands of data breaches, and responds to hundreds more each year. Our experts apply lessons learned from each of these compromises to help customers identify and address the latest threats and vulnerabilities that lead to compromise. The following table describes preparedness services available as part of the Trustwave SpiderLabs Incident Readiness Program:

Service	Description	Deliverables
Readiness and Detection Review	Trustwave SpiderLabs will evaluate the client's ability to detect five classes of incidents (additional classes can be added in subsequent years), and identify gaps along with recommendations for improvement.	• Detection review report • Gap analysis assessment and action plan
Computer Security Incident Response Plan (CSIRP) Development	Trustwave SpiderLabs will work with the client to develop and document a clearly defined procedure for incident response. Development includes interactive sessions that will result in a baseline document addressing each incident class from the readiness and detection review.	• CSIRP review • CSIRP development
Computer Incident Response Team (CIRT) Development	Trustwave SpiderLabs will provide a team framework and help the client appoint leaders and CIRT team members. As part of CIRT development, Trustwave SpiderLabs can create and deliver first responder training on site to teach staff how to use tools and techniques to gather volatile data while preserving the confidentiality and integrity of affected systems.	• CIRT roles and responsibilities review • CIRT roles and responsibilities development • CIRT first responder training
Attack Simulation Exercises	Trustwave SpiderLabs will work with the client to arrange half- or full-day tabletop exercises to evaluate and improve CSIRPs without any significant disruption of operations. Trustwave SpiderLabs also orchestrates real-time attack scenarios including custom malware and system modification to evaluate the client's ability to respond to a real incident.	• Half- or full-day tabletop exercises (blue team services) • Targeted attack scenario simulations for CSIRP rehearsal (red team services)
Scheduled Onsite Debrief	Trustwave SpiderLabs experts can present bi-annual onsite briefings covering the latest threats and trends observed in forensic investigations or annual, onsite reviews of clients' CSIRP and incident readiness maturity.	• Bi-annual onsite briefing • Annual review of CSIRP and readiness maturity

Risk Management Services

Mitigating risk is a challenge when so many employees need open access to your corporate data to fulfill their duties. As a result, you need to address risky employee termination and turnover situations, such as a software developer resigning and potentially taking your intellectual property to a competitor or a terminated and disgruntled system administrator remotely destroying your databases.

Risk management services may include, but are not limited to, the following:

- **Resignation response** Determine whether former employees are exposing intellectual property
- **Termination response** Shut down former administrators' access points to prevent them from remotely damaging your network or exposing data
- **Breach assessment**If you suspect a breach, but don't have evidence to support or eliminate your suspicions, we can confirm or rule out a compromise

Incident Response Services

The Trustwave Incident Readiness Program will give you a team of expert incident responders on-call whenever you need them. With prioritized status, forensics investigators can immediately deploy wherever you need them to investigate a potential breach. As a result, you'll minimize the impact of a breach and understand how the attacker gained access to your network and how to contain and remediate the threat. An incident response engagement includes digital evidence acquisition and deep-dive intrusion, volatile memory and malware analysis, as well as, real-time recommendations for the quick remediation of associated network vulnerabilities. The investigation and analysis will locate active malware on your network, remove it, evaluate the possibility of any lateral attacks and determine what data was exposed and exfiltrated culminating in a formal report and, if desired, expert witness testimony.

Insider Threat and HR Assistance Services

If you're concerned about an employee betraying your organization, Trustwave SpiderLabs will help you determine whether an employee has gone rogue, who they might be communicating with and how they may be damaging your company or exposing your intellectual property. Insider threats range from corporate espionage to simple employee misconduct, and as part of the program, we will help you gather evidence and information to develop an appropriate, informed response.

Trustwave®

For more information: https://www.trustwave.com