SERVICE OVERVIEW

Incident Response & Digital Forensics

powered by Terra Verde

Now organizations of all sizes can better arm themselves against cyber-attacks with expert resources and defense programs.

Organizations of all sizes across the globe are being targeted and attacked. Whether by nation states, individual hackers, 'hacktivist' organizations, cyber criminals, or cyber terrorists—multiple studies show that small and mid-sized organizations are easy targets for cyber attacks. Why? Because they are typically less likely to have the programs, policies, technologies and resources to defend against such attacks.

Many companies also lack the resources or capital to recover from financial theft or a massive data breach that may result in millions of dollars in fines. That's when security should be an even bigger priority.

With a growing shortage of security experts, an increasing number of attacks and threats, and constantly changing technology, how can organizations internally build a sustainable answer to the problem?

In 2015, 62% of breaches were driven by malicious outsiders and 60% of breaches occurred in businesses with less than 1,000 employees.

Introducing Incident Response & Digital Forensics Solutions

cStor has partnered with the security experts at Terra Verde to offer a comprehensive suite of security, risk and compliance solutions and services, pulling together the core elements required to make the unsustainable task of building and operating a security, risk and compliance program, sustainable.

cStor and Terra Verde collaborate with clients to implement a pragmatic, customized, effective and sustainable method of responding to cyber-security incidents. Upon discovery of a cyber-security incident, our specialists evaluate the situation and deploy the most appropriate actions to enable recovery and prevent reoccurrence.

Incident Response Services

- Defining the term "cyber-security incident" and what it means to your company.
- Establishing incident severity levels and types.
- Developing sustainable response processes and services and deploying resources.
- Implementing program governance and response monitoring and management systems and resources to ensure remediation activities are completed.

cStor
We look beyond IT

IRDFSOV010516

Incident Response & Digital Forensics

SERVICE OVERVIEW

With a growing shortage of security experts, an increasing number of attacks and threats, and constantly changing technology, how can organizations internally build a sustainable answer to the problem?

Digital Forensics

Dealing with a sophisticated cyber-security incident or attack is a time consuming, complex task, even for experienced teams. cStor provides specialized response capabilities such as technical or forensic investigation services that are customized to address each customer's unique situation and business.

Using a proven methodology and approach, we assist clients in a variety of forensic situations including intellectual property theft, financial embezzlement, corporate espionage, and improper employee behavior.

Tools & Techniques Used in Forensic Engagements:

- Memory (RAM) capture and analysis
- Network device log analysis, DHCP, firewall, wireless, and syslog review
- Basic and advanced web browser and email forensics
- Social media and instant messaging forensics
- Mobile device forensics
- Basic and advanced registry analysis
- Scan and print temporary files, including .mdi, .tif,.spl files, Windows system, application, security and firewall log analysis
- Windows prefetch analysis
- Basic and advanced file carving, including unallocated space, page and hibernation files, and restore points
- Data exfiltration analysis, i.e. USB, webmail, email, CD/DVD burning history

Digital Forensics Services Include:

- eDiscovery
- Computer & Mobile Forensics
- Social Media & Open Source Intelligence
- Cloud Forensics
- Memory Forensics & Malware Analysis
- Incident Response & Data Breach Support

eDiscovery

cStor provides a dedicated project manager to oversee the eDiscovery process and to shepherd the flow of information and case data. As the data is loaded into our early case assessment tool, it can be clustered based upon file type, size and date range—either globally or by custodian.

After indexing the data, our tool can present the litigation team with a dynamic search and subsequently cluster the hit results across custodian or date range. This pre-processing aids our clients in determining which custodians and date ranges to focus on, and where to begin the actual processing of the collected data set for ultimate review.

We can deliver any file standard for your own review platform, or load the data into Terra Verde's proprietary Relativity platform.

Incident Response & Digital Forensics

SERVICE OVERVIEW

Our experts collaborate with clients to implement a pragmatic, customized, effective and sustainable method of responding to cyber-security incidents. At discovery, we evaluate the situation and deploy the most appropriate actions to enable recovery and prevent reoccurrence.

Computer & Mobile Forensics

Preserving data is critical to any investigation or litigation matter. Data collected by well meaning but unqualified technology staff is often incomplete, causes changes to the information's metadata, and can lead to incorrect interpretations or loss of information.

Our experts employ forensically sound collection methods to acquire digital evidence; thereby preserving all available data and maintaining a defensible chain of custody.

Once acquired, evidence is analyzed together to draw connections between the subject's activity on his/her mobile device, computer, and online activity.

This process and service helps provide evidence of that can be utilized within legal proceedings.

Social Media & Open Source Intelligence

Our investigations often find critical pieces of evidence through its use of open source intelligence methods and social media. Valuable information such as conflicting statements by witnesses, purloined data posted on public sites, proof of intent through social media posts, and reverse video and image searches for bullying or extortion cases are often instrumental. As our team uncovers this information, it is collected via our cloud forensics tools in order to maintain the evidence's authenticity and chain of custody.

The Federal Government suffered a staggering 61,000 cyber-security breaches in 2014 alone.*

Cloud Forensics

With pervasive usage of cloud services and web based access, new challenges present themselves to acquiring forensically sound data from third-party providers; including correct identification of where data is stored (logically and geographically), authority to collect the data, involvement of additional stakeholders, limited access to third party systems, slower network connections to acquire the data, perishability of logs, recovery of deleted data, and timestamp synchronization.

Our team actively monitors the rapid changes in this field and utilizes a number of investigative methods and forensic tools to manage the challenges of cloud forensics and to deliver our clients with accurate datasets and analysis.

Memory Forensics & Malware Analysis

Sometimes simply removing a compromised machine from the network does not satisfy internal or regulatory requirements. Rather the compromise must be understood more deeply so that actions can be taken to implement additional technical controls, deliver employee education, or provide customer notification.

Using forensic investigative techniques combined with static and dynamic malware analysis, we distill the inner workings of the malware into high level actionable intelligence. This approach enables us to help make critical business and technical decisions and define the appropriate resolution plan.

*Source: "These 5 Facts Explain the Threat of Cyber Warfare", TIME (June 2015)

The Terra Verde solutions have helped advance the security and risk management operations of State Collection Service. Selecting them was an easy decision.

The cStor & Terra Verde Sustainable Value

The cStor and Terra Verde solutions leverage certified, experienced security personnel, best practice processes, and modern technologies to provide comprehensive and sustainable security, risk and compliance programs for your organization.

- Our services and solutions are often utilized by organizations and executives looking to:
- Reduce overall security and compliance risk
- Reduce or eliminate capital expenditures on security technology and personnel
- Deploy a new, or optimize an existing Security Operations Center or Incident Response Program
- Gain deeper visibility and understanding of cyber security vulnerabilities and risks
- Deploy a repeatable, scalable set of standards, practices and a "program" for security alert monitoring, management and remediation

Let's Get Started

Learn more about how cStor and Terra Verde can work with your team to design a smart, comprehensive cyber-security solution that helps protect your business from evolving threats. Contact cStor to schedule a consultation today.

About cStor

cStor helps companies strategize, create, and implement video surveillance, data center and cloud solutions that address the business needs and demands of today's successful enterprise.

cStor
We look beyond IT

Powered By TERRA VERDE

info@cStor.com
www.cStor.com
1.877.CSTOR.81
(1.877.278.6781)