

Professional Security Services



EXPOSING SECURITY ISSUES

The SANS Institute reports tens of millions of scans per day on a single server for known vulnerabilities. If your organization is susceptible to any of these a typical server will be compromised within about 20 minutes of being accessible from the Internet.

Whether you are launching a new production service, upgrading existing services, or expanding them, Terremark will provide the Professional Security Services needed to clarify the overall security posture of your organization.

Thorough analysis is ensured by covering the IT infrastructure from the ground up: networking equipment, servers and desktops, applications, and human issues such as policies and procedures and the reality as practiced inside the organization. The end results are a deep understanding of your security position and remediation recommendations that fit within the context of your business requirements.

A FULL LINE OF PROFESSIONAL SECURITY SERVICES

Terremark currently offers a full line of security-related professional services, such as Penetration Tests, Incident Response, Incident Preparation, and customized services to

help our customers identify, understand, and effectively deal with security issues.

VULNERABILITY ASSESSMENTS AND PENETRATION TESTS

Vulnerability Assessments and Penetration Tests are related but serve different purposes. Vulnerability Assessments evaluate systems, applications, and processes for known vulnerabilities using a combination of automated and manual tools and techniques. Penetration Tests often follow a Vulnerability Assessment, attempting to use any identified vulnerabilities to compromise a system or network; essentially proof that a vulnerability can actually be used to breach your organization's security.

Benefits

- Provide fresh set of eyes for your own IT or security groups
- Expert view of your current security environment (i.e. want to find the holes before the bad guys do)
- Security policy or framework requirements (ISO 17799 or COSO, for example)
- Prepare for a regulatory audit such as Sarbanes, GLBA, or PCI.

INCIDENT PREPARATION AND RESPONSE

Most of the best-practices controls and security frameworks require an incident response capability and plan to be in place, and given that all of the new controls and security-oriented regulations such as Sarbanes Oxley, Gramm-Leach-Bliley and HIPAA require that such a framework be chosen, this means that all regulated organizations must have this capability in place.

Too often, security practitioners and incident responders are at odds because neither group is well versed in the other's requirements, techniques, and constraints. For example, the security practitioners want to clean up the aftermath of an incident as quickly as possible and get the organization back to normal operations. While the incident responder needs to gather data and evidence in an investigational and forensically sound manner to be able to perform a root cause analysis that may have to hold up in court or satisfy regulators.

Terremark's team has expertise and real-world experience in both areas and has built methodologies, tools and techniques to support both group's needs and get the organization back to business quickly while still preserving the integrity of the investigation. For existing Terremark customers with systems residing in one of our facilities, our familiarity with your systems plus the immediate accessibility of those systems means an incident can be dealt with very rapidly, much more so than in a traditional enterprise environment.



DIGITAL FORENSIC SERVICES

Companies maintain critical and confidential data in computer systems, and whether they are stored in a computer server, desktop, tapes or laptop there is the possibility of loss of data

MIAMI - DALLAS - WASHINGTON D.C. - SILICON VALLEY - LONDON



MADRID - BRUSSELS - AMSTERDAM - SÃO PAULO - SANTO DOMINGO - BOGOTA

ADDITIONAL PROFESSIONAL SECURITY SERVICES

- Secure Information Systems Design and Implementation
- Information Security Policy and Procedure Development and Review
- Regulatory Compliance Information Systems Pre-Audit and Remediation
- Business Dependency and IT Organizational Review Methodology
- NSA Infosec Assessment Methodology (IAM) Project
- Security Event Logging Best Practices Review
- External Network Vulnerability Assessment
- Application Vulnerability Assessment

integrity and or confidentiality. In the event of a data breach, the need to determine how this data was compromised often requires a Digital Forensics Investigation. Terremark's forensic experts can help answer questions such as "What actions took place before a specific computer event occurred?" and "What is the extent of the Breach?" Terremark adheres to strict rules of evidentiary preservation, forensic industry standards and custody chain processes to ensure that the evidence collection, analysis and secure maintenance is accepted in courts of law.

Terremark's offers a complete selection of services in the forensics field such as Data Acquisition, Forensic Analysis, Correlation Analysis, Network Forensics, and Email Forensics.

A RECOGNIZED LEADER

Terremark Worldwide, Inc. (NASDAQ:TMRK) is a leading global provider of IT infrastructure services delivered on the industry's most robust and advanced operations platform, leveraging data centers in the United States, Europe and Latin America and access to massive and diverse network connectivity. Terremark delivers government and enterprise customers a comprehensive suite of managed solutions including hosting, colocation, connectivity and security services.