Spirent **SecurityLabs**

Solutions

Security testing and monitoring consulting services that complement Spirent core solutions for test & measurement. Gives customers ability to do testing in-house and leverage our expertise for third party security testing, analysis and compliance.

Team of experienced security specialists providing comprehensive managed services for networks, web and mobile applications, embedded devices and source code analysis.

Complete range of security services with in-house vulnerability scanning, pen-testing and vulnerability research team.

Service Levels of Managed Security Testing

- **Standard–**Basic compliance level scan (OWASP Top 10, SANS 20, PCI (6.5, 6.6)
- **Premium–**All tests in Standard level with the addition of Best Practices

Manual Penetration Testing

- **Web application–**Thorough penetration of a web application and any related hosts in critical areas such as input validation, injection, phishing, authentication mechanisms, session security, encryption usage, policy compliance, and many others.
- **Mobile application–**Penetration testing of mobile applications' binary code, related web services and http(s) communication for dynamic analysis and device end security to uncover security vulnerabilities related to sensitive data stored in cache, unencrypted data storage on the device, log files, crash logs, SQL injection, Unrestricted file upload session security, encryption usage, supported cyphers, MITM etc.
- **Embedded device (POS/ATM/Automotive)–**The penetration test will assess the device firmware, binary code, related web services and http(s) communication for exploitable vulnerabilities, discover and exploit underlying web application for security weaknesses such as authentication bypass, authorization boundary, CSRF & XSS in Embedded Web Application Servers, and many others.
- **Network and wireless–**In depth scanning and penetration testing of the network/wireless to uncover exploitable vulnerabilities regarding Insecure Server Configuration, Default System Passwords, Unpatched Servers with Known Vulnerabilities, Rogue access points, War Driving, Eavesdropping, Insecure Firewall Configuration, Insecure Communications, Information Leakage and Improper Error Handling.
- **Static code analysis–**Code Review Service, also known as White-Box testing, used to highlight possible vulnerabilities such as buffer overflows, SQL Injection Flaws, backdoors, authentication bypass and authorization boundary etc., within "static" (non-running) source code by using techniques such as Taint Analysis and Data Flow Analysis.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information visit: www.spirent.com

AMERICAS 1-800-SPIRENT
+1-800-774-7368
sales@spirent.com

US Government & Defense
info@spirentfederal.com
spirentfederal.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979
emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539
salesasia@spirent.com

Technology

Our smart and comprehensive testing product suite, coupled with industry experts includes:

- Best of breed scanning tools coupled with manual validation and pentesting
- Custom scanning profiles to fit customer budget and testing needs
- Compliance scanning (PCI, GLBA, HIPPA, SOX, etc.)
- Customized reports with actionable remediation recommendations and risk prioritization
- Report findings can be used to configure WAFs
- Vulnerability lifecycle management; track found vulnerabilities until remediation via sequential tests

Solution

Our full-service consulting practice includes:

- Seasoned security pen-testers with extensive experience working with companies ranging in size from Global 100 to SMBs
- Flexible solutions tailored to fit customer needs based on scan depth and frequency
- Security consultants act as an extension of your in-house security team proactively identifying vulnerabilities and assist with mitigating risks
- Available as a one-time test which includes a single scan + 1 retest within 60 days, or an annual subscription which includes quarterly tests, 4 total tests in the year, within 1 year from subscription activation date

Testing Methodology

Our SecurityLabs services follow testing methodology that are structured to deliver consistent, high impact results with minimal impact on the client organization. The project proceeds in three distinct phases:

- **Project planning**
  Spirent consultants identify key characteristics of the customer's asset and construct guidelines for remote or onsite assessment
- **Assessment and analysis**
  Using Spirent's proprietary testing solutions and manual penetration testing techniques; Consultants will identify critical vulnerabilities that could lead to a potential compromise, misuse of the functionality and create a potential security risk
- **Presentation and final report review**
  Spirent Consultants will present the final report that summarizes the assessment process, identified vulnerabilities, risk analysis, potential attack scenario(s) and suggested remediation

Rev B | 08/18