Spirent **SecurityLabs**

Comprehensive security testing and monitoring services

Leverage Our Expertise to Identify and Mitigate Vulnerabilities

Testing and analyzing the security and compliance of your networks, apps, and devices is critical. But in-house security testing does not necessarily require internal staff.

Spirent SecurityLabs provides a variety of comprehensive managed testing services, delivered by certified, seasoned professionals. Our security consultants act as an extension of your in-house security team, proactively identifying vulnerabilities and mitigating risks.

Augmenting your teams with SecurityLabs experts can help you optimize staffing, supplement your internal expertise, and facilitate compliance through independent third-party testing and reporting. Our testing professionals can assist you with:

- **Manual penetration testing** of your network infrastructure, web and mobile applications, embedded devices, and source code
- **Automated scanning and reporting** via a unique, unified SaaS platform that offers continuous visibility of your security posture by scanning, analyzing and monitoring your organization's IT infrastructure
- **Continuous compliance** through independent, customized, automated, on-demand testing
- **Sector-specific vulnerability testing** covering every industry and geography
- **Consulting services** ranging from implementation of best-practice testing methodologies to risk analysis of potential attack scenarios to remediation strategies.

What Makes SecurityLabs Unique

We are at the cutting edge of cybersecurity

SecurityLabs consultants live and breathe cybersecurity and constantly expand the depth and breadth of their expertise. We implement and experiment in advanced methodologies; we explore emerging areas such as IoT and cryptocurrencies; and we have experience in multiple industry sectors, including automotive, health care, industrial systems (ICS/SCADA) and more.

We do not work for you; we work with you

Improving security requires active collaboration between your in-house team and our consultants. We proactively share our knowledge and experience with your team.

Our services are used by governments

SecurityLabs has been engaged to test the security of many government systems, including elements of critical national infrastructure such as telecommunication, energy and utilities, and transportation, and we have the security clearances needed for testing classified and military systems.

We run a test lab for CTIA IoT Authorized Cybersecurity Certification

We are trusted to formally test and certify the security design and capabilities of cellular-connected Internet of Things (IoT) devices.

Spirent SecurityLabs Certifications

Customized Engagements Delivered by Certified Experts

We begin each engagement by thoroughly understanding your unique requirements and objectives. Then we recommend a tailored testing solution specifically for your needs. We fine-tune the scope of the test, required scan depth and frequency to fulfill your requirements.

SecurityLabs gives you access to testing professionals who are experienced and independent; experienced with companies of your type, size, and industry sector; and certified as required to meet your specific needs.

Our smart and comprehensive testing product suite includes:

- Best-of-breed scanning tools coupled with manual validation and penetration testing
- Custom scanning profiles to fit customer budget and testing needs
- Compliance testing (PCI, GDPR, GLBA, HIPPA, SOX, etc.) and CTIA IoT Cybersecurity Certification Testing
- Customized reports with actionable remediation recommendations and risk prioritization
- Key Performance Indicators (KPIs), reflecting the security posture of your organization
- Vulnerability lifecycle management; the ability to track vulnerabilities through remediation via sequential tests

Automate and Consolidate with Our Unified Platform

SecurityLabs enables you to automate scanning and consolidate your resources—so you can streamline your testing processes and unburden your staff while improving your security posture.

To accomplish this, we combine our consulting expertise with a unified **SaaS-based platform**. Our platform automates vulnerability scans on applications, networks, devices and source code and presents the results graphically in a unified view. The platform provides secure, on-demand access to actionable insights, including comprehensive information about all your existing and past tests, and helps you prioritize risk and remediation efforts. This provides a cost-effective, easy-to-use, robust vulnerability assessment option.

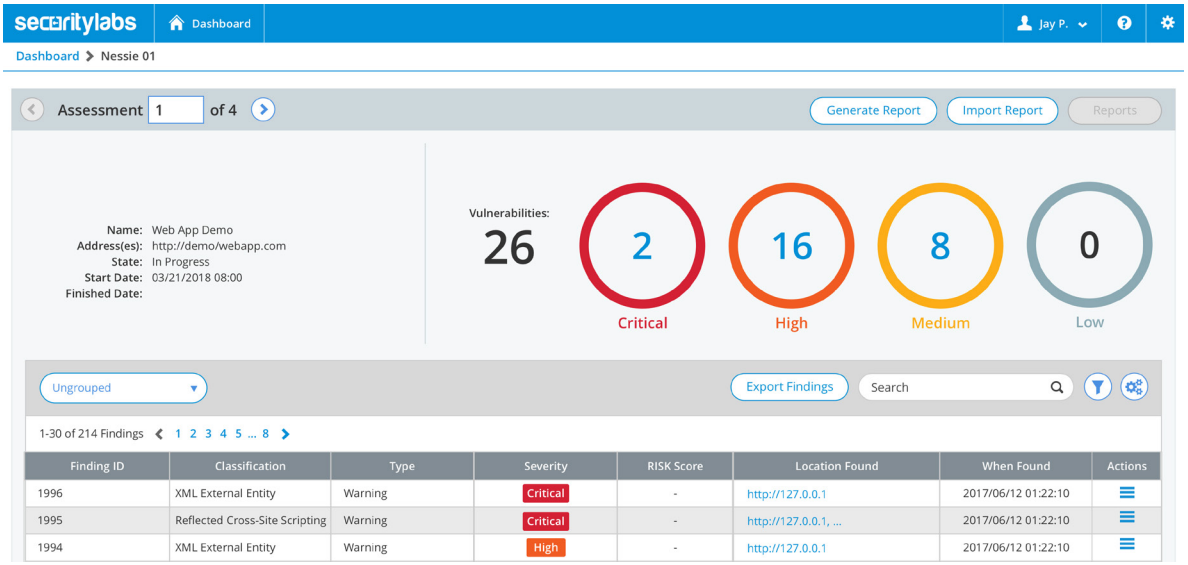

Figure 1: The SecurityLabs web-platform offers automated, deep and dynamic scanning that provides quick insights into potential vulnerabilities without the physical presence of a security expert.

The broad capabilities of the platform enable you to consolidate the tools and technologies you're currently using for security testing, monitoring, and reporting. In addition, the reports provided by the platform help you see which elements of your infrastructure are ineffective or redundant in addressing high-priority risks, enabling you to save CapEx while also reducing the need to manage and maintain superfluous or unsecure infrastructure.

The platform also gives you access to sophisticated analytics that drill down into trends and vulnerabilities and allow you to prioritize the necessary corrective actions. The analytics can even provide insights about the level of security specific development teams or infrastructure elements are delivering—so you can make informed decisions about where improvements are needed and the level of urgency.

CUSTOMER REFERENCES/USE CASES

Large Regional Hospital

Penetration testing of medical devices, applications, external and internal network

- Network penetration testing on large IP ranges/ infrastructure (Class B-sized networks, several thousand users)
- Followed appropriate precautions with internal coordination to avoid impacting live clinical systems and patient safety
- Server-side and client-side vulnerability testing
- Performed penetration testing, embedded medical device testing, and mobile application pen-testing to help identify vulnerabilities and suggested remediations

International Railway Company

Red team engagement

- Identified random internal domain names using a thorough recon process
- Breached external network and gained access to the internal network remotely without triggering any IDS/ IPS/firewall/AV/SIEM alert
- Breached physical security to obtain company-sensitive assets
- Bypassed various security controls and compromised the internal network to gain access to mission-critical data and systems

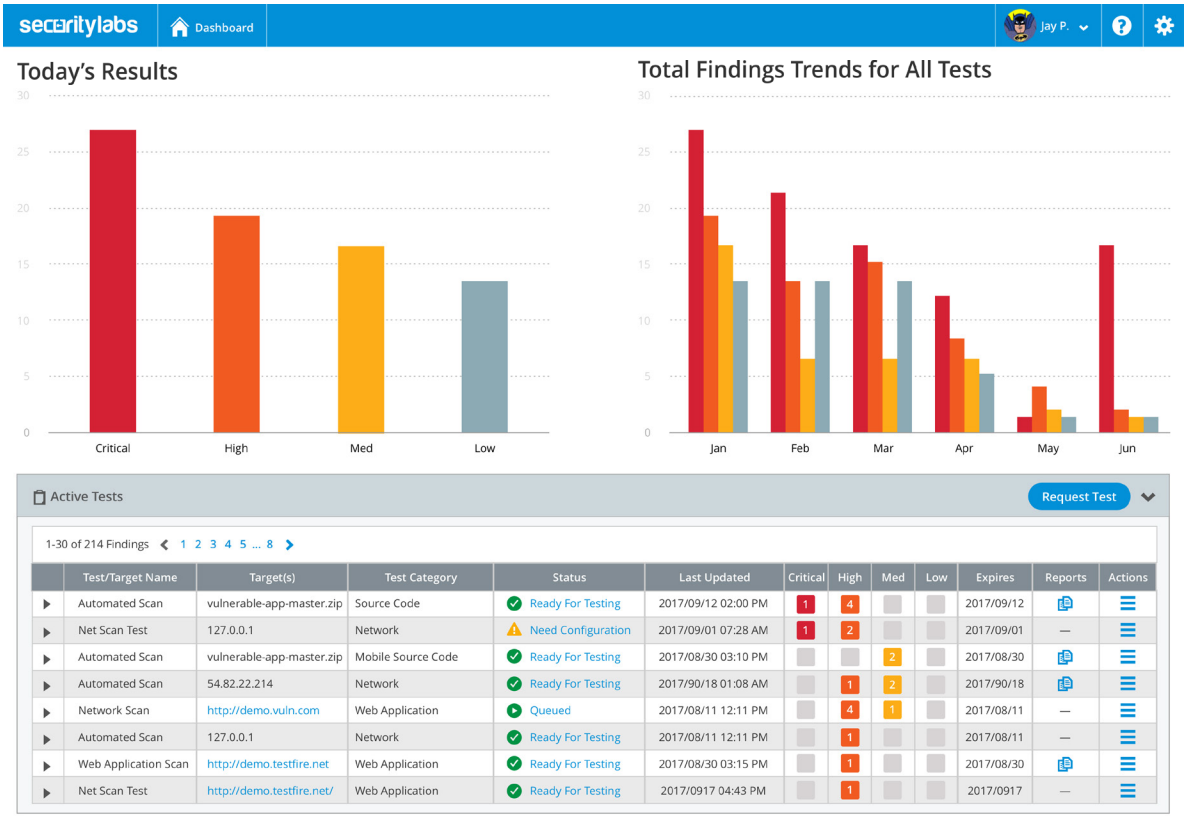

Figure 2:
The unified, web-based dashboard provides a high-level overview to manage application, network, and device security throughout the organization at a glance.

The net result of our unique platform? You can:

- standardize your vulnerability and compliance results
- bring consistency to your testing processes across organizations
- unburden your internal security teams so they can pursue other high-value activities
- keep the things you like about your current testing processes while taking advantage of our expertise and unified platform.

CUSTOMER REFERENCES/USE CASES

Government Entity

External penetration test, internal penetration test, wireless assessment

- External network penetration testing and vulnerability scanning for primary and secondary data centers
- Internal penetration testing covering network, server, and client systems and vulnerabilities
- Wireless network security assessment and rogue access point detection/mapping

Financial Services Firm

Penetration testing

- External network penetration testing on large IP ranges/infrastructure
- Followed appropriate precautions with internal coordination to avoid impacting live systems
- Performed unauthenticated and authenticated web application penetration testing to help identify vulnerabilities and suggested remediation

Manual Penetrating Testing Capabilities

Web application–Thorough penetration of a web application and any related hosts in all 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.

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 is a part of White-Box testing, used to identify difficult-to-find vulnerabilities such as buffer overflows, SQL Injection Flaws, backdoors, authentication bypass and authorization boundary, etc. We check for those vulnerabilities within "static" (non-running) source code by using techniques such as Taint Analysis and Data Flow Analysis.

Advanced Testing Capabilities

Red Teaming–We can assess the security of the whole organization by challenging its policies, processes, and IT systems while introducing an adversarial approach. Red Teaming is always objective-driven and simulates a real-world scenario, e.g. copying sensitive information, accessing protected perimeter, etc. Red Teaming uses various physical, electronic, and social engineering techniques to try to exploit your personnel and any physical weaknesses in order to gain access to the premises.

IoT and embedded device (POS/ATM/Automotive)–The penetration test of embedded devices includes device hardware assessment, firmware extraction and reverse-engineering, communication analysis (wired and wireless), cryptographic analysis, analysis of any associated web services, and device management application for exploitable vulnerabilities such as authentication bypass, authorization boundary, injection attacks, and many others.

The SecurityLabs Advantage

Experience of our team, over many combined decades, enables us to deliver a comprehensive vulnerability assessment

Certifications covering the full spectrum of relevant industry and regulatory associations

Objectivity in testing and assessing your security vulnerabilities

Automation of scanning for cost-effective, easy-to-use and robust vulnerability assessment

Consolidation of tools, vendors, technologies and results: one platform, one partner

Standardization of processes and methodologies for efficiency and consistency

Visualization of test results, vulnerability assessments, security KPIs, and trends on a single pane of glass

Analytics to determine the most effective teams/processes in identifying and mitigating risks

Testing Methodology

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

Flexible Pricing and Service Level Options

SecurityLabs can create a custom testing solution for your specific needs. Penetration testing is 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.

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

Talk to us.

We encourage organizations of all types and sizes to get accurate, objective, automated testing of their security vulnerabilities to strengthen security and guide business decisions.

Contact us at securitylabs@spirent.com to discuss your specific questions or requirements.

For additional information about Spirent and Spirent SecurityLabs, visit our YouTube Channel

CUSTOMER REFERENCES/USE CASES

Global Hospitality Chain

Web and mobile app scanning and penetration testing

- SecurityLabs dashboard being used to manage the entire web and mobile application security program and remediation process for the organization worldwide
- SecurityLabs platform integrated with the client's application development lifecycle to perform security assessments on the pre-production and production environments
- The organization uses the platform to monitor the overall security status of the organization, utilizes the APIs, alerts and notifications for prioritizing risk and remediation efforts

Large Enterprise

Web application and external network penetration testing

- Performed a penetration test against publicly exposed infrastructure such as servers, devices, applications, and services
- Open source intelligence (OSINT) led to the discovery of critical data such as IP ranges, employee details, domain and sub-domain names, administrative interfaces, remote-access services, etc.
- Carefully crafted stealth attack based on the information gathered enabled Spirent to breach the external perimeter and gain access to the internal network
- Compromised the primary internal domain and achieved the highest level of access, making it possible to gain unauthorized administrative access to all the critical resources from the internet without setting off any alarms

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

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

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev A | 09/19