Security Testing Services

Penetration testing. Vulnerability assessment. Security code review. Infrastructure security audit. Compliance testing
ScienceSoft is an IBM Silver Business Partner that has been working in the Security Intelligence area since 2003.

- **18** years in information security
- **700** employees
- **150+** projects in security consulting
Our Customers in Security
Security Testing Services We Provide

- **Penetration testing**
  to check the protection of the entire IT infrastructure or applications by finding and exploiting security vulnerabilities

- **Vulnerability assessment**
  to detect and prioritize security weaknesses in the IT infrastructure and provide recommendations on their mitigation

- **Infrastructure security audit**
  to find vulnerabilities in security policies and procedures, security monitoring tools, physical access control, etc.

- **Compliance testing**
  to ensure the compliance with PCI DSS, HIPAA, and other regulatory standards

- **Security code review**
  to identify encryption, buffer overflow, XSS vulnerabilities, and other security weaknesses possibly overlooked in the development phase
Penetration testing aims to identify security vulnerabilities and determine whether they are genuine and what damage they may inflict. For that, we exploit vulnerabilities to simulate an attack on the system. We carry out OWASP TOP 10-based penetration testing of:

- Web applications
- Mobile apps
- Network services
- Remote access
- IoT devices
- Employee behavior (Social engineering testing)
Types of Penetration Testing We Provide

1. **Black box model**
   - We work in life-like conditions having strictly limited knowledge of your network and no information on the security policies, network structure, software and network protection used.

2. **Gray box model**
   - We examine your system having some information on your network, such as user login details, architecture diagrams or the network's overview.

3. **White box model**
   - We identify potential points of weakness by using admin rights and access to server configuration files, database encryption principles, source code or architecture documentation.
Vulnerability assessment intends to identify, quantify and rank vulnerabilities, as well as provide customers with recommendations to help eliminate security risks. We perform automated and manual evaluation to detect security weaknesses in:

**IT infrastructure**
- Network
- Email services

**Applications**
- Web apps
- Mobile apps
- Desktop apps
We check the infrastructure to identify vulnerabilities in the following areas:

- Security policies and procedures
- Security monitoring tools
- Physical access control
- Configuration management
- Version control
Compliance Testing

We perform automated scanning and manual analysis to:

Ensure a customer’s **compliance** with PCI DSS, HIPAA and other regulatory standards.

Further **provide** a customer with an **attestation letter** on the basis of testing results.
Security Code Review

We examine an application source code to find errors overlooked in the development phase, e.g.:

- Encryption errors
- SQL injection vulnerabilities
- Buffer overflows
- XSS vulnerabilities

```python
txtUserId = get_request_string("UserId");
txtSQL = "SELECT * FROM Users WHERE UserID = " + txtUserId;
```
Elimination of Detected Vulnerabilities

We have the necessary skills to eliminate vulnerabilities and errors using our own resources, i.e. by engaging:

- Developers
- DevOps engineers
- Cybersecurity team
Cooperation Models

One-time services

- Gathering all the details about the object of assessment
- Impartial security assessment
- Security evaluation without vendor lock-in

Managed services

- Conducting security assessment on a regular basis
- Spending less time and money to implement projects
- Constant awareness of occurring security vulnerabilities
Success Story

Vulnerability Assessment for a US Reporting Services Provider

Customer

A US mobile credit monitoring and reporting services provider

Solution

ScienceSoft assessed the security level of the Customer’s network, revealed critical security issues and prepared the Customer for passing PCI DSS validation

Tools & Methodologies

Nessus, OpenVAS, Nmap, ARP-scan
Penetration Testing for a Fintech Company

Customer: A UK financial technology company providing a supply chain finance portal

Solution: ScienceSoft conducted black box penetration testing of the Customer’s supply chain management portal and complementing mobile apps, and defined corrective measures to mitigate identified vulnerabilities.

Tools & Methodologies: Metasploit, Nmap, SQLMap, Nikto, DIRB, BurpSuite, Nessus, Zmap
Success Story

Code Review and Penetration Testing of a Cloud App

Customer

An award-winning European IT company

Solution

ScienceSoft performed automated and manual source code reviews and penetration testing of a cloud-based application for tax return, allowing to reveal and mitigate vulnerabilities critical to the security of sensitive data

Tools & Methodologies

Metasploit, Wireshark, OpenVAS, Nessus, BurpSuite, w3af
Success Story

API Penetration Testing for a Bank

Customer

A European bank with $400+ million in assets

Solution

ScienceSoft carried out manual and automated penetration testing using both black box and white box models and provided a detailed report on how to improve the current API security and to ensure the safety of sensitive data

Tools & Methodologies

Nessus, IBM AppScan, IBM Application Security on Cloud, Acunetix, BurpSuite Pro, Sqlmap