ScienceSoft

Security Testing Services

Protecting businesses from cyber threats for 22 years

Key Facts

ScienceSoft is an IT security testing and software development company headquartered in McKinney, TX, with offices in Europe and the Middle East.

22

years in information security

Certified

specialists on board, including Certified Ethical Hackers

Vast portfolio

of security projects

FT FINANCIAL TIMES statista THE AMERICAS' FASTEST GROWING COMPANIES 2025

4 YEAR CHAMPION
RECOGNIZED EVERY YEAR SINCE 2022

AMERICA'S MOST RELIABLE COMPANIES 2025 Newsweek statista

aws PARTNER Select Tier Services

Microsoft Solutions Partner

ORACLE | Partner

Software Testing Help
Top 10 Penetration Testing Companies

Software Testing Help
Top 30 Cybersecurity Companies

ISO 9001
LL-C (Certification)

ISO 27001
LL-C (Certification)

What Makes ScienceSoft Different

We Find Vulnerabilities Others Miss

We go beyond formal, surface-level security assessments that are all too common in the market. By fully exploring all possible threat vectors and simulating non-obvious attack scenarios, we identify previously overlooked security gaps and deliver strategies to mitigate them.

Our Clients in Security

IBM®
rh Robert Half
NASA JPL
M&T Bank
بنك الإسكان للتجارة والتمويل
The Housing Bank for Trade & Finance
RBC
RBC Royal Bank
Eurasian Bank
tieto
REALTIME
CLINICAL TRIAL MANAGEMENT SYSTEMS
APIFONICA
Carrefour
TELEKOM AUSTRIA GROUP

Industries We Serve

BFSI

Fintech

Healthcare

Logistics

Retail, Wholesale

Oil & Gas

Manufacturing

Professional services

Software product companies

MSSPs

Security Testing Services and Beyond

- **Offensive security services**
  by simulating attacks across your IT infrastructure and apps to find and exploit security vulnerabilities.

- **Defensive security services**
  to assess the viability of your security policies and procedures, security monitoring tools, physical access control, etc.

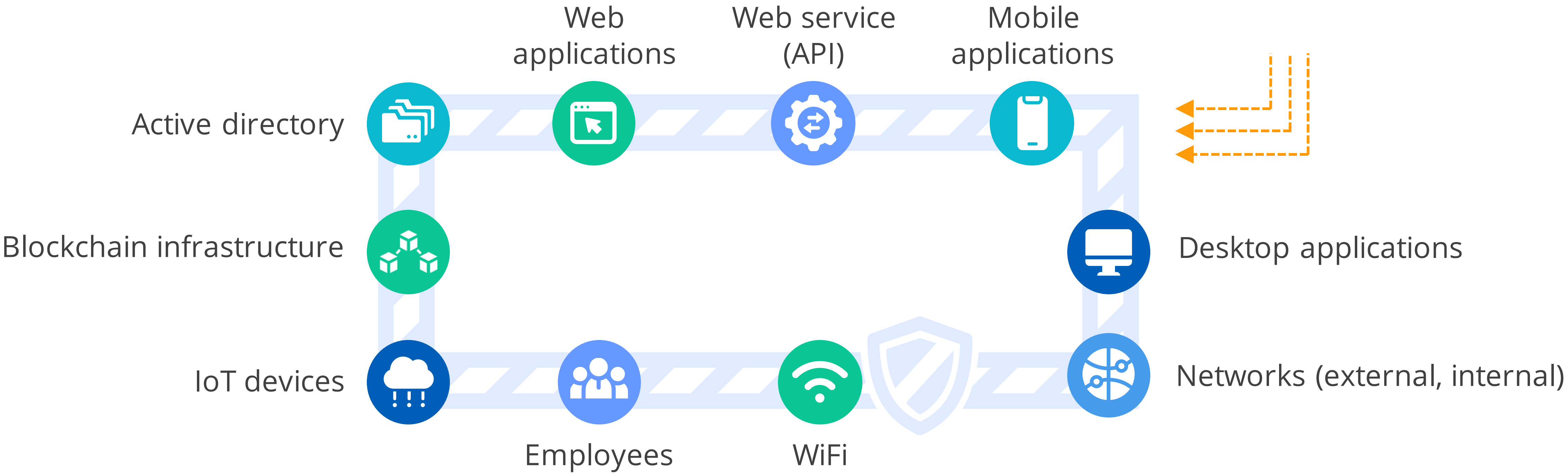
- **Stress and performance testing**
  to examine the responsiveness, stability, scalability, reliability, speed, and resource usage of your software and infrastructure.

- **Compliance assessment**
  to ensure compliance with PCI DSS, HIPAA, ISO 27001, SOC T1/T2, and other regulatory standards.

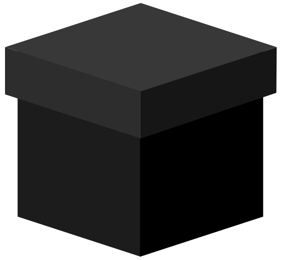
- **Post-testing services: security risk management**
  to eliminate the discovered vulnerabilities and help implement the most suitable security mechanisms to minimize future risks.

Penetration Testing

Penetration testing aims to identify security vulnerabilities and determine what damage they may cause if exploited by malicious actors. Our experts go beyond standard checklists, examining all possible threat vectors based on your industry, business, and technology specifics. Through meticulous planning and the use of controlled testing environments, we ensure no damage or disruption occurs while simulating real-life attacks targeting:

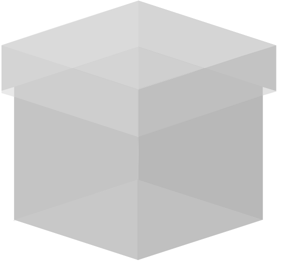


Types of Penetration Testing We Provide



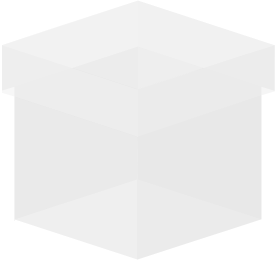
Black box model

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 in use.



Gray box model

We examine your system having some information about your network, such as user login details, architecture diagrams, or network overview.



White box model

We identify potential weak points by gaining admin rights and full access to server configuration files, database encryption principles, source code, or architecture documentation.

Vulnerability Assessment

Vulnerability assessment is needed to identify, quantify, and prioritize vulnerabilities, as well as to provide recommendations to help eliminate security risks. We combine automated scanning and manual validation to ensure there are no false positives or missed threats in:

IT infrastructure

- Networks
- Email services

+

Applications

- Web apps
- Mobile apps
- Desktop apps

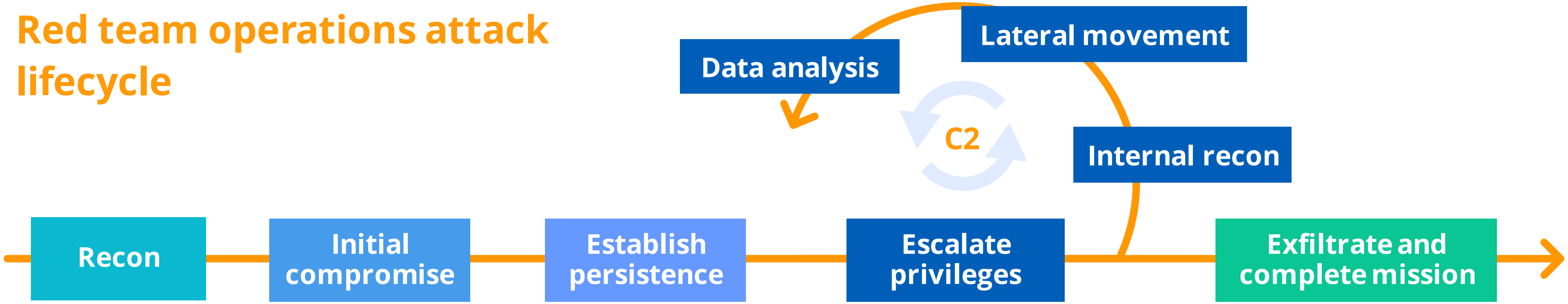
Red Team Assessment

Red team assessment is a multi-layered attack campaign that mimics the tactics and techniques of real-world attackers. It may involve OSINT, vulnerability scanning, application and network pentesting, and social engineering testing.

The key areas ScienceSoft will assess:

- ✓ Protective security policies and technology
- ✓ Employees’ security awareness
- ✓ Threat detection techniques and tools
- ✓ Incident response processes

Red team operations attack lifecycle



Social Engineering Simulations

Testing the security awareness and behavior of your employees in case of phishing, vishing, and other social engineering attacks. It is an important testing step as insider threats are harder to predict and prevent.

Social engineering attacks ScienceSoft simulates:

Phishing

Malicious emails sent to multiple employees

Spear phishing

Emails sent to a specific employee(s) responsible for high-level decisions

Whaling

Email attacks targeting the C-suite

Vishing

Manipulative phone calls

Open Source Intelligence (OSINT) Services

Passive information gathering

No contact with the target and its IT infrastructure, using only publicly available sources.

What we can find: the company's partners, privacy policies, employees' names and email addresses, leaked credentials, public IP addresses, domain names, DNS records, etc.

Semi-passive information gathering

Mimicking normal Internet traffic and behavior.

What we can find: general info about web servers, metadata from published documents and files, etc.

Active information gathering

Direct interaction with the target and its IT infrastructure: network mapping, OS fingerprinting, port scanning, DNS enumeration, web server scanning, phishing / vishing, etc.

What we can find: network topology, technologies used, software versions, open ports, API keys, etc.

OSINT helps:

- ✓ Determine possible threat vectors
- ✓ Reduce a company's attack surface
- ✓ Investigate past cyber incidents
- ✓ Detect data leaks

Application Security Testing

Analyzing applications from different angles, we detect weaknesses in the app’s architecture, code, logic, and configuration that may enable unauthorized access to the app’s data and functionality.

What we check:

- Web applications and APIs
- Mobile applications
- Desktop applications

Security testing techniques we apply:

- ✓ Automated code review
- ✓ Manual code review
- ✓ Application pentesting
- ✓ Compliance testing

Blockchain Security Testing

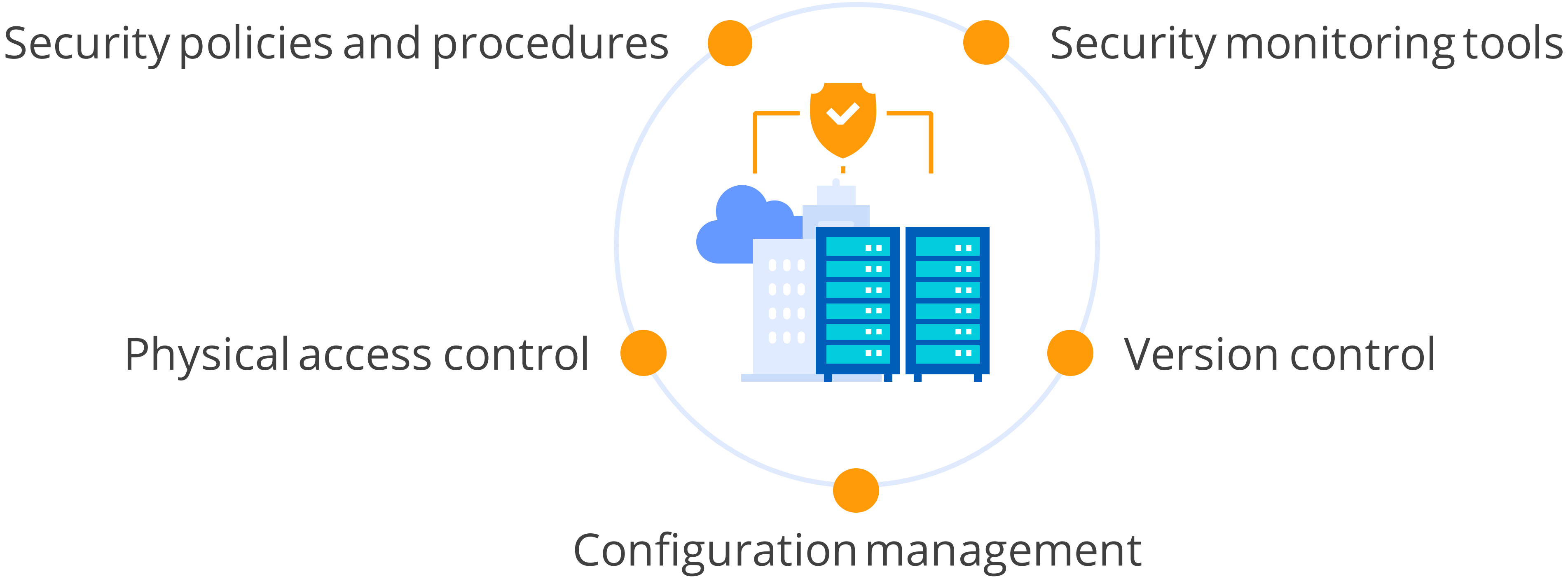
We analyze the security of blockchain-based solutions at all levels, including architecture, code, APIs, user-facing components, and infrastructure.

What we check:

- Blockchain networks
- Smart contracts
- Cryptocurrencies
- Wallets
- DApps
- Asset tokenization platforms
- Initial coin offering (ICO) and security token offering (STO) platforms
- Blockchain-based market platforms: e.g., NFT marketplaces, DeFi lending platforms, crypto exchange platforms
- Decentralized autonomous organizations (DAO)

Infrastructure Security Audit

We check the infrastructure to identify vulnerabilities in the following areas:



Security policies and procedures

Security monitoring tools

Physical access control

Version control

Configuration management

Cloud Security Assessment

We detect weaknesses, vulnerabilities, and misconfigurations that may enable unauthorized access your data, apps and IT infrastructure components in cloud.

Security controls we check

Identity and access management

- Authentication mechanisms
- Authorization mechanisms

Logging and threat detection

- Security alerts
- Log ingestion
- Log querying
- Log archiving

Data protection

- Server-side data encryption
- Client-side data encryption

Network-level protection

- Network architecture
- Security tools

All-around cloud security configuration

aws Microsoft Azure Google Cloud Digital Ocean rackspace.

Stress and Performance Testing

Our testing team examines the responsiveness, stability, scalability, reliability, speed, and resource usage of your software and infrastructure.

Testing types we perform:

- Load testing
- Volume testing
- Stress testing
- Stability testing
- Scalability testing

APACHE JMeter™

Visual Studio

hp Loadrunner

Compliance Assessment

Standards we work with

ISO 9001 LL-C (Certification)
ISO 27001 LL-C (Certification)
ISO 13485 LL-C (Certification)
HIPAA COMPLIANT
PCI DSS COMPLIANT
PCI Software Security Framework
GDPR
NIST Security Framework
Cybersecurity Regulation
AICPA SOC 2

Compliance assessment scope

- Review of security and/or quality assurance **policies and procedures** in place.
- Security testing of **the software and/or IT infrastructure.**
- Checking **employees' security awareness** and knowledge of applicable standards and regulations.
- Actionable **remediation guidance or practical aid** to close the detected compliance gaps.

Our compliance assessment team

- Tech-savvy security testing engineers.
- Certified Ethical Hackers.
- A certified internal auditor for ISO 27001, ISO 9001, and ISO 13485.

Cybersecurity Consulting

Our cybersecurity consulting services cover the three key levels:

Strategic level

Security strategy definition, creating a roadmap to its implementation or improvement.

Operational level

Analyzing the existing policies and processes and improving them. Designing and implementing new security policies and processes.

Technical level

Designing secure app/network architecture, recommending the optimal app security features/ network security tools, and more.

Security Controls Implementation

We don’t limit ourselves to assessment and consulting. Our developers, DevSecOps and IT security engineers, and compliance consultants are ready to eliminate any security and compliance gaps in your IT environment.

We offer:

- Secure network segmentation
- Setting up and configuring preventive and detective security tools
- Implementing security features required for your app
- Fixing bugs in the source code
- Conducting security awareness training for your employees

Cooperation Models

One-time services

- Gathering all the details about the assessment targets
- An impartial security assessment

Fixed price

▼

Security evaluation without vendor lock-in

Managed services

- Conducting security assessment on a regular basis
- Spending less time and resources on each project

Fixed price

T&M

▼

Constant security awareness and timely remediation of vulnerabilities

Vulnerability Assessment for a US Credit Monitoring Services Provider

Client

A US mobile services provider that gives its users instant access to their credit reports and scores.

Solution

ScienceSoft assessed the security level of the Client's network, revealed over 300 security issues, including critical ones, and prepared the Client for PCI DSS validation.

Tools & Technologies

Nessus, OpenVAS, Nmap, ARP-scan

Project details →

Penetration Testing of a Hospital IT Infrastructure

Client

A large US public health system with over 20 outpatient clinics and a teaching hospital.

Solution

We conducted gray box pentesting of the hospital network's internal IT infrastructure and provided a report describing the detected vulnerabilities and actionable remediation guidelines.

Tools & Technologies

Nessus, OWASP Zed Attack Proxy (ZAP), SSLScan, Metasploit, Burp Suite, Nmap, dirb, DBeaver

Project details →

Security Assessment to Ensure HIPAA Compliance of a Patient Portal

Client

A US healthcare provider with multiple offices across different states.

Solution

As a result of pentesting, vulnerability scanning, and code review, we found acute security issues. We advised on the necessary fixes and helped improve the portal's protection and meet HIPAA requirements.

Tools & Technologies

Static Analyzer Security Scanner, PHP Mess Detector, PHP Inspections, PHP Code Sniffer, PHP Copy/Paste Detector

Project details →

ISO 27001 Pre-Audit for a Fintech Company

Client

An international B2C financial technology company with offices in the US and Europe.

Solution

To help the client prepare for an ISO 27001 audit, we provided a gap analysis report on the inconsistencies in its information security documentation and recommended how to address the discovered issues.

Tools & Technologies

Q&A sessions, analysis of documents.

Project details →

IT Infrastructure Security Testing for an Asian Bank

Client

A large Asian retail bank with over 550 branches and more than 2.5 million clients.

Solution

A vulnerability assessment and pentesting of 60 external IP addresses and the bank's internal network; a security risk assessment of the bank's digital channels; a simulation of social engineering attacks.

Tools & Technologies

Nmap, Nessus, Burp Suite, Gophish, Metasploit, Netcat, DIRB, Nikto, SSLScan, Firefox Developer Tools.

Project details →

Let’s Make Your Project a Success!

Atlanta, Georgia
+1 972 454 4730
contact@scnsoft.com

Headquarters
McKinney, Texas
+1 214 306 68 37
contact@scnsoft.com

Mexico City, Mexico
+52 55 6952 0374
contact@scnsoft.com

Riga, Latvia
+371 66 011 905
eu@scnsoft.com

Vilnius, Lithuania
+370 52 07 97 07
eu@scnsoft.com

Warsaw, Poland
+48 22 162 18 13
eu@scnsoft.com

Vantaa, Finland
+358 94 272 63 77
nordics@scnsoft.com

Fujairah, the UAE
+971 600 57 59 69
gulf@scnsoft.com

Riyadh, the KSA
+966 800 880 3035
ksa@scnsoft.com