Offensive Security & Assurance Testing

Proactively Identify and Mitigate Cybersecurity Weaknesses

"Organizations that perform regular penetration testing reduce breach risks by up to 70%." ~ Cybersecurity Ventures

Product Overview

Cyber attackers constantly exploit weaknesses in infrastructure, applications, and human behavior. Traditional defenses alone are not enough, organizations must validate their security posture through simulated attacks and deep technical testing.
stc Bahrain delivers Offensive Security & Assurance Testing Services to uncover vulnerabilities, validate defenses, and provide actionable remediation guidance.

Our services cover five key areas:

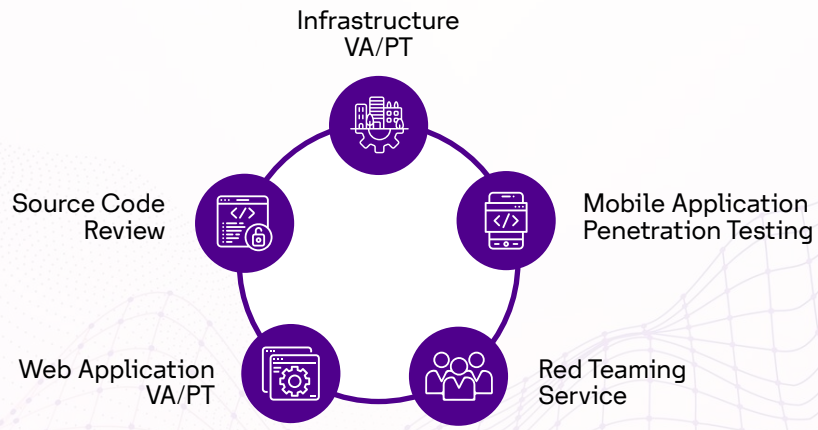
- **Infrastructure Vulnerability Assessment & Penetration Testing (VA/PT)**
- **Web Application VA/PT**
- **Mobile Application Penetration Testing**
- **Source Code Review**
- **Red Teaming Services**

Customer Challenges

- Undetected vulnerabilities in infrastructure and networks
- Web and mobile applications exposed to real-world exploitation risks
- Lack of assurance in secure coding practices
- Unpreparedness for advanced, persistent attacker techniques
- Difficulty demonstrating security assurance to regulators and customers
- Resource gaps in executing continuous penetration testing

Our Solution

- **Infrastructure VA/PT:** Identify exploitable weaknesses in systems and networks before attackers do.
- **Web Application VA/PT:** Detect OWASP Top 10 and business-logic flaws in web applications.
- **Mobile Application Penetration Testing:** Test resilience against reverse engineering, insecure storage, and runtime attacks.
- **Source Code Review:** Analyze application code to find hidden flaws like hardcoded passwords and input validation issues.
- **Red Teaming Services:** Simulate real-world, multi-vector attacks to test defenses and incident response.



Key Features

- **Comprehensive Testing Coverage** – Infrastructure, web, mobile, and code-level vulnerabilities.
- **Red Team Simulations** – Realistic, scenario-based attack simulations.
- **Actionable Reporting** – Executive summaries with risk ratings and remediation guidance.
- **Expert Advisory** – Certified ethical hackers and security testers with proven expertise.

Business Benefits

- **Reduced Breach Likelihood** – Fix weaknesses before exploitation.
- **Regulatory & Audit Confidence** – Evidence of testing for ISO, PCI DSS, GDPR, PDPL, and others.
- **Cost Efficiency** – Address flaws early, reducing expensive post-breach recovery.
- **Operational Resilience** – Test real-world readiness of defenses and incident response.
- **Customer Assurance** – Demonstrate commitment to proactive security.

Service Snapshot

Category	Details
Delivery Model	Vulnerability assessments, penetration testing, code reviews, red team exercises.
Support	Optional integration with stc's Cyber Defense Center (CDC) for continuous monitoring and validation.
Coverage	From infrastructure and applications to advanced attacker simulations.
SLA	99% availability for scheduled VA/PT and red teaming engagements.
Industries Served	Banking, finance, healthcare, government, enterprises, and critical infrastructure.

stc Edge

- **Local Presence, Global Standards** – Delivered by stc Bahrain
- **Ethical Hacking Expertise** – Certified penetration testers and red team specialists
- **Trusted by Enterprises** – Supporting compliance, resilience, and customer confidence
- **Proactive Security Posture** – Shifting organizations from reactive to preventive defense

Take the Next Step

Don't wait for compliance failures or cyber risks to disrupt your business.

Contact stc Bahrain Cybersecurity Team today to schedule a consultation and strengthen your governance and compliance posture.

BusinessSupport@stc.com.bh +973 33 128 128 business.stc.com.bh