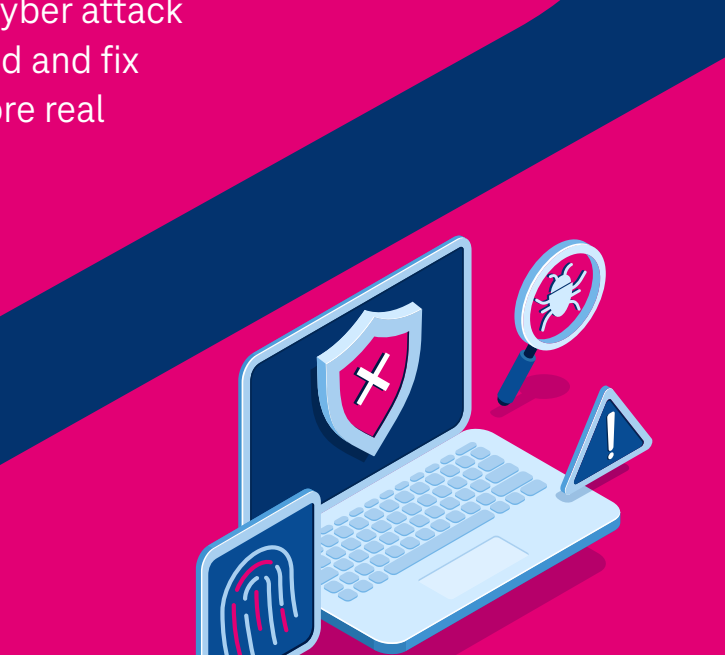
T Systems

Automated penetration testing under a minute

What is penetration testing in security?

It's a simulated cyber attack on systems to find and fix weaknesses before real attackers do.



Why?

It helps organizations assess how well their defenses hold up under real-world attack scenarios.

What is automated penetration testing?

It's a type of penetration testing that uses advanced software tools to perform the same tasks a human ethical hacker would, but much faster and continuously.

Automated pentesting in action

1 Target discovery

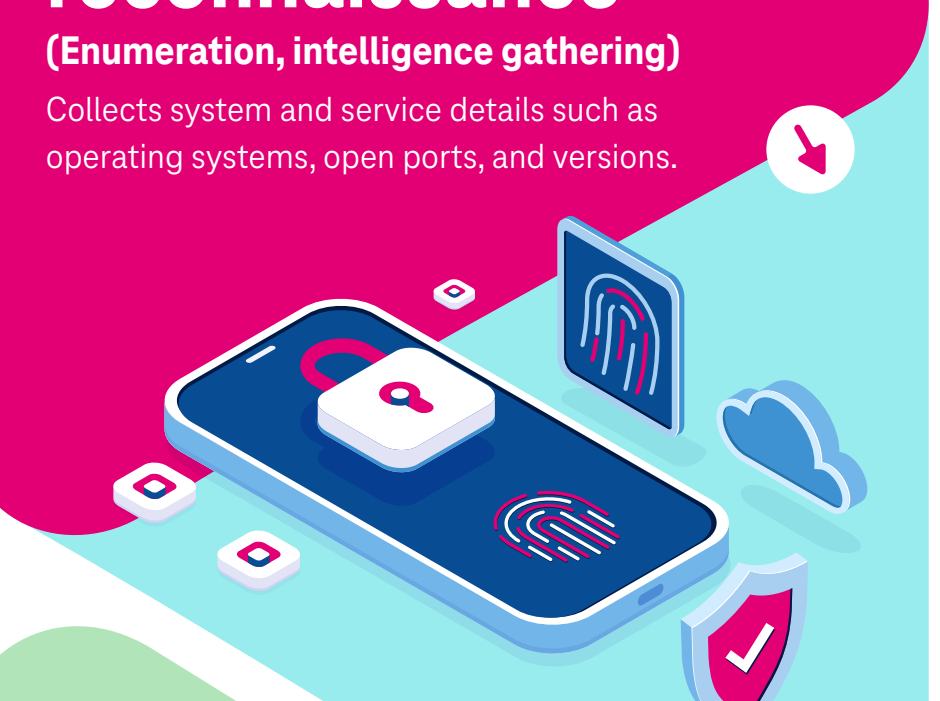
(Asset discovery, network mapping)

Finds systems, applications, or services on a network to identify what's available for testing.

2 Fingerprinting and reconnaissance

(Enumeration, intelligence gathering)

Collects system and service details such as operating systems, open ports, and versions.



3 Vulnerability scanning

(Security scanning, vulnerability assessment)

Scans for known flaws such as outdated software, misconfigurations, or weak passwords.

4 Exploitation

(Attack simulation, payload execution)

Attempts to exploit found vulnerabilities to gain unauthorized access.

5 Privilege escalation

(Root access attempts, local exploits)

Tries to gain higher-level access such as admin or root privileges after an initial breach.

6 Lateral movement

(Pivoting, network propagation)

Moves from one compromised system to the other within the network to reach more critical systems.

7 Persistence simulation

(Backdoor creation, access retention)

Simulates how an attacker would stay inside a system by installing backdoors or scheduled tasks.

8 Risk prioritization

(Threat ranking, risk scoring)

Ranks vulnerabilities based on how dangerous they are and how likely they are to be exploited.

9 Reporting and evidence

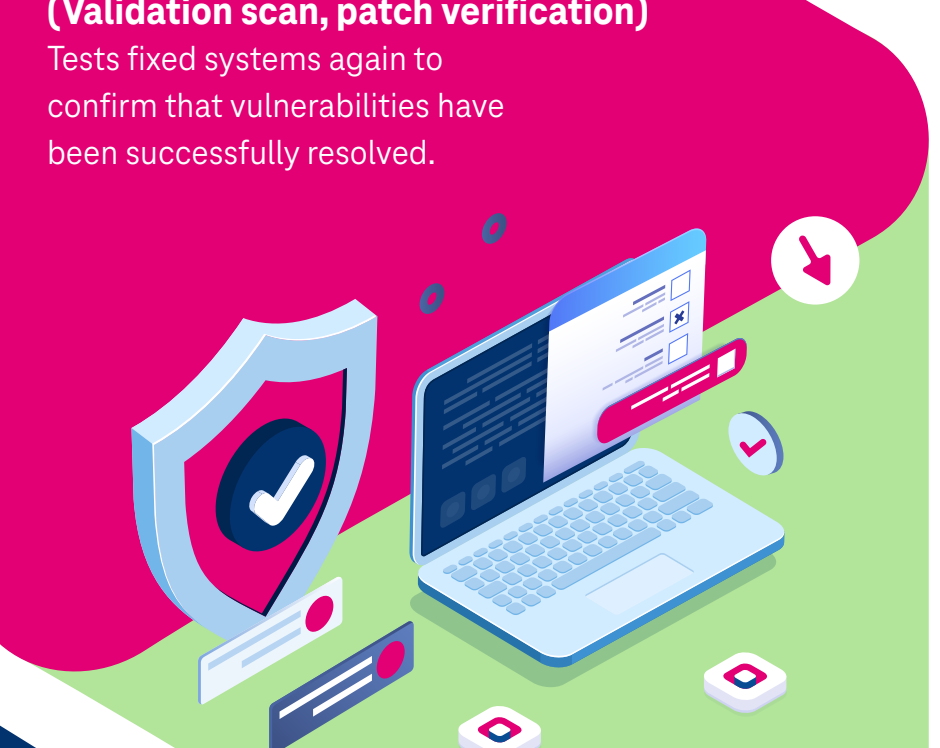
(Proof of exploit, executive summary)

Provides proof of attack details and methods, including screenshots, or captured data.

10 Retesting

(Validation scan, patch verification)

Tests fixed systems again to confirm that vulnerabilities have been successfully resolved.



AI + Automation packs a punch in pentesting

Autonomous testing
Scans networks, finds vulnerabilities, and runs real exploits, automatically.

Smart decisions
AI prioritizes risks, chains attacks, and adapts strategy like a real hacker.

Zero touch
No human input needed for execution or retesting.

Clear reporting
Generates detailed, evidence-based reports and verifies fixes.

You should also know

48% of apps contain critical risks[1]

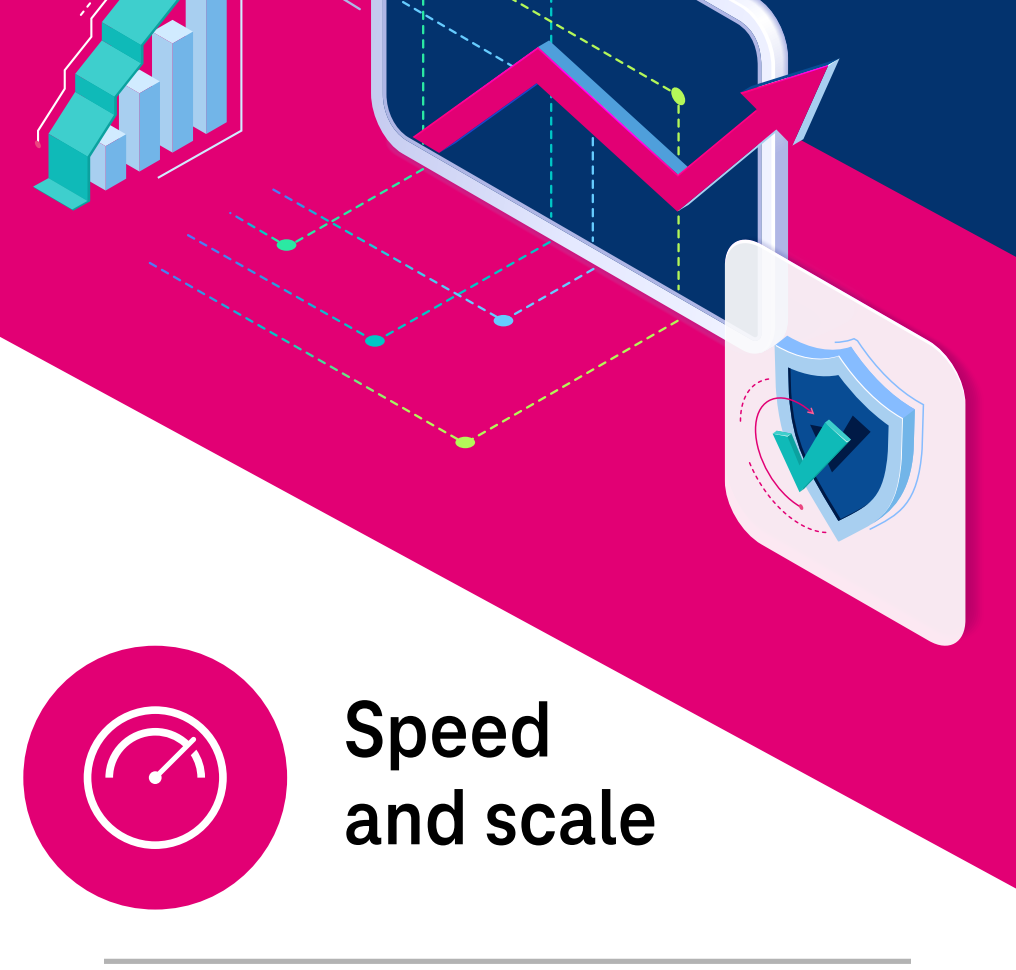
5 million shortfall in cyber security personnel[2]

180% increase in exploitation of vulnerabilities in 2024[3]

Average cost of data breach in 2025
$4.8 million[4]

The window to act on vulnerabilities is shrinking from
74 days (2014) to just
5 days (2025)[5]

Business benefits



- Speed and scale
- Cost-efficiency and savings
- Real-world simulation
- Continuous security
- Better risk management?
- Audit-ready reports
- Compliance
- Visibility

Sources

- Veracode State of Software Security report 2025
- ISC2 Cyber Security Workforce Study 2024
- Verizon 2024 Data Breach Investigation report
- Statista 2025
- CyberMindr Report

Act before attackers do. Find the gaps and fix them.

Contact us today

Andreas Pecka
Head of International Expert Sales & Pre-Sales
cybersecuritysales@t-systems.com
a.pecka@t-systems.com