

Infrastructure Security

Find and close the gaps in your networks

Every application, user and service in your organisation runs on your network. Servers, workstations, firewalls, VPN gateways, switches and wireless networks change every week as teams add assets, open ports and grant access. Each change can leave behind a misconfiguration, an unpatched service or a weak credential.

One exposed service on the perimeter, or one compromised laptop on the internal network, is often all an attacker needs to reach domain admin and the data behind it.

SentryArk's infrastructure penetration testing looks at your network the way an attacker would, from the internet and from inside, and shows which weaknesses can actually be chained into a breach.

EXTERNAL AND INTERNAL TESTING

External testing maps everything you expose to the internet, including forgotten hosts, VPN portals, mail servers and remote access services, and tests whether any of it gives an outsider a way in. Internal testing starts from the position of a malicious insider or an attacker who has compromised one workstation, and measures how far they can get.

- | | | |
|-----------------------------|---------------------------|---------------------------|
| ■ External network VAPT | ■ Internal network VAPT | ■ Active Directory review |
| ■ Wireless security testing | ■ Firewall and VPN review | ■ Server and OS hardening |

BEYOND THE SCANNER REPORT

Vulnerability scanners produce long lists of CVEs ranked by score, many of them false positives or unreachable in practice. We validate each result manually, remove the noise and focus on the attack paths that matter: Active Directory misconfigurations, credential reuse, insecure protocols such as LLMNR and SMBv1, and trust between systems.

Every finding is proven with evidence, so your team spends its time fixing real risk. Testing windows and exclusions are agreed in advance, and we coordinate with your operations team so production keeps running.

ASSESSMENT DETAILS AND METHODOLOGY

Our infrastructure methodology combines automated scanning with manual testing by certified engineers. It follows established standards such as PTES, NIST SP 800-115 and the CIS Benchmarks, and is adapted to your environment, whether on-premises, hybrid or segmented across sites.

Planning and scoping	01	IP ranges, testing windows, exclusions and points of contact are agreed in writing, so testing never disrupts production.
Discovery and enumeration	02	Host discovery, port and service enumeration, OS fingerprinting and Active Directory enumeration build a complete map of the in-scope network.
Vulnerability analysis	03	Scanner output is combined with manual checks for misconfigurations, default credentials, missing patches and weak protocols, and every result is validated.
Exploitation and lateral movement	04	We safely exploit confirmed weaknesses, then chain them through credential harvesting, privilege escalation and lateral movement to show the real business impact.
Reporting and retest	05	A clear report with risk ratings, proof and fix steps for every finding, and a free retest once you've patched.

The assessment includes

- Executive summary
- Identified vulnerabilities and CVSS ratings
- Hosts and data compromised during testing
- Network attack paths and chained findings
- Detailed remediation and hardening steps
- Retest report confirming fixes

ABOUT SENTRYARK

SentryArk is a team of security engineers and offensive security specialists. Our consultants hold OSCE, CRYPTO and CEH certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Our focus is offensive security that shows the real-world risk to your business.