infocom
TRUSTED SECURITY

JE Infocom
8, Volodymyrska str.
Kyiv, 01001, Ukraine
tel.: +380 (44) 230 52 00
infocom@infocom.ua
infocom.ua

infoScan

Independent Infrastructure Security Assessment

infocom.ua

2024

infoScan

Web Page

INDEPENDENT INFRASTRUCTURE SECURITY ASSESSMENT

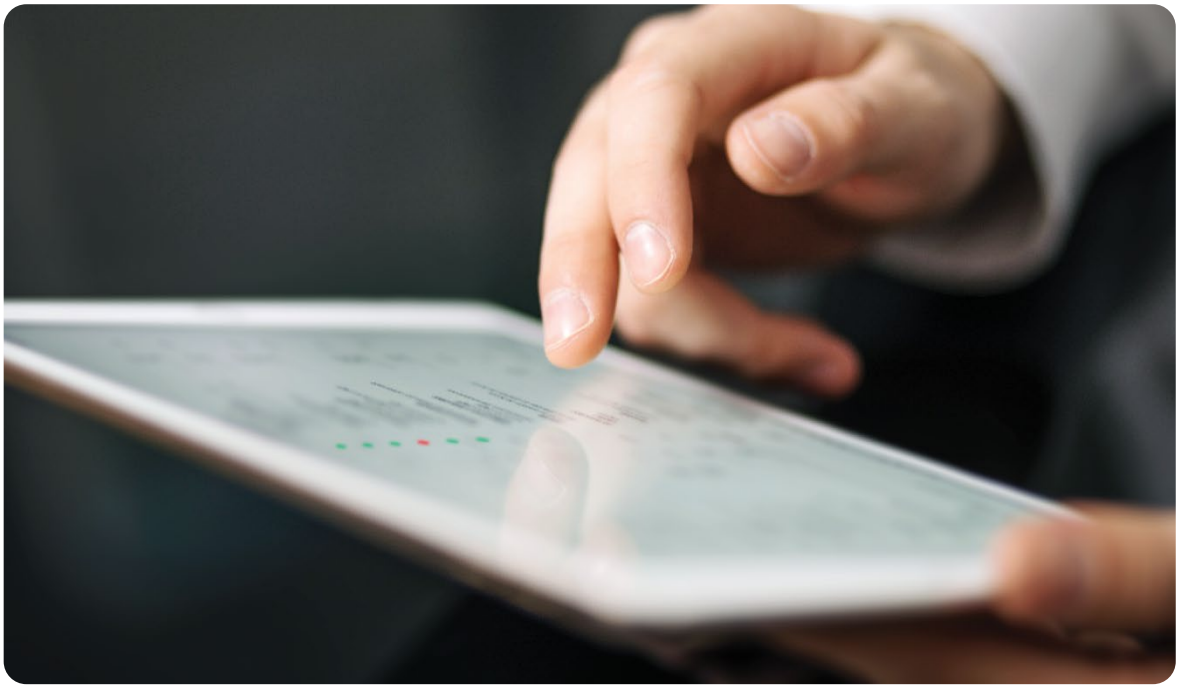
An information infrastructure security assessment is a comprehensive process aimed at identifying vulnerabilities and potential threats that could allow unauthorized access to your network. Regular assessments are essential for maintaining the effectiveness of security measures and detecting new threats that may arise from changes in your information infrastructure or applied technologies.

The presence of vulnerabilities in your network gives attackers opportunities to exploit them, gain access to sensitive data, disrupt ongoing operations, or even halt them entirely. Timely detection and mitigation of these vulnerabilities are critical for safeguarding your information infrastructure.

Information infrastructure can be exposed to various threats for several reasons. Below are the primary types of vulnerabilities that may exist within information systems:

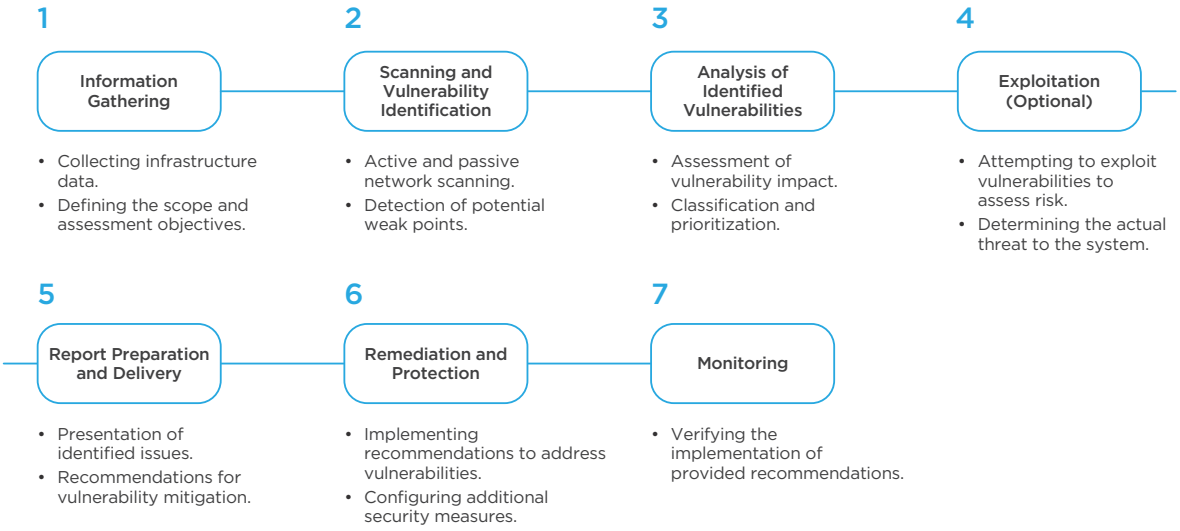
- Software Vulnerabilities: Flaws in software or outdated applications that can be exploited by attackers.
- Network Vulnerabilities: Weak points in the network caused by improper configuration of network equipment, insufficient protection against external attacks, or inadequate security of connected devices.
- Access Management Vulnerabilities: Issues such as weak passwords, lost or stolen devices, or poorly managed access rights.
- Physical Infrastructure Vulnerabilities: Insufficient security measures for facilities that house servers and other devices containing sensitive information.

While vulnerabilities related to physical infrastructure and access management are primarily administrative and organizational issues that companies or organizations can often address internally, software and network vulnerabilities are technical in nature and require the expertise of cybersecurity specialists for proper analysis and resolution.



infocom
TRUSTED SECURITY

The first four stages involve gathering information and analyzing existing risks. This requires close cooperation between Infocom representatives and the client. During these stages, potential threats are identified, their likelihood and impact are assessed, and priorities for security measures are established. Factors such as potential threat sources (internal or external), attack methods (network, hardware, or social), and targeted assets (corporate data, workflows, etc.) are also considered.



Assessment Stages

Infocom specialists then proceed to examine the network infrastructure (equipment configuration, connection schemes, etc.) and conduct a “scan” using specialized software. The data collected helps identify all weaknesses in the information system, such as open ports, outdated software versions, weak network protocols, and misconfigured or improperly connected equipment.

After completing the assessment, Infocom delivers a report detailing all identified vulnerabilities and providing comprehensive recommendations for mitigation, along with suggestions to enhance the overall security level of the infrastructure. Upon request, Infocom can perform a follow-up audit to evaluate the implementation of previous recommendations.

Benefits of infoScan:

- Identifying and addressing existing vulnerabilities in your infrastructure.
- Reducing business disruption risks through proactive threat detection.
- Enhancing cybersecurity levels without additional investments.
- Comprehensive reports with recommendations to improve your security posture.
- Experts support and consultation.