Improsec performs an independent security analysis and assessment of the security state of a selected Windows client or server. The assessment can either be performed on a standard laptop or server with a Windows image deployed with standard business applications.

**Methodology**

Based on our extensive knowledge of current attack vectors, we analyse how specific configurations and installed applications can be circumvented and exploited. We test for modern attack vectors, such as: credential theft, lateral movement, privilege escalation, persistence techniques, anti-malware bypass, application whitelisting bypass and arbitrary code execution.

During our analysis we investigate areas such as: boot process, data protection, assigned permissions, patch management, Group Policies, services, scheduled tasks, administrative practices, supported protocols, firewall configuration, drivers, etc.

**Involvement**

The delivery requires minimal involvement of your technical staff.

---

**Value**

- Assess your Windows client/server platform’s resilience against modern threats
- Identify misconfigurations and insufficient hardening, that could lead to loss of confidentiality and integrity
- Tangible recommendations based on recognized best practices for improving security of the Windows platform

**Product**

The deliverable of the analysis is a written report containing the following:

- A non-technical section with an Executive Summary for management and decision makers
- A technical section including detailed observations and tangible recommendations to improve the security level and hardening of the system