Top 5 Common Security Gaps Discovered

This one-page summary highlights the most frequent defensive weaknesses identified by Validato during initial baseline simulations.

Validato

1. EDR Misconfiguration

Even top-tier Endpoint Detection and Response (EDR) tools are often left in "monitor only" mode or have critical protection features disabled, allowing standard attacker techniques to execute unchallenged.

2. Over-Privileged Standard Users

Adversaries frequently manipulate standard operating system features. If standard users have unnecessary permissions, attackers can perform credential dumping or privilege escalation without triggering traditional alerts.

3. SIEM Invisibility (Log Gaps)

Many organisations assume their SIEM is receiving all necessary telemetry. Validato often discovers that critical security logs for lateral movement or persistence are not being forwarded, leaving the SOC blind to an active breach.

4. Ransomware Execution Paths

While perimeter defences may be strong, internal configurations often allow ransomware-associated behaviours — such as shadow copy deletion or mass file encryption — to proceed because the internal "behavioural" controls were never tested.

5. Persistence through Standard Features

Attackers often maintain access by using legitimate OS tools like Scheduled Tasks or Registry modifications. Validato identifies where these standard features are being manipulated to ensure they are properly restricted and monitored.

The Validato Solution:

Instead of finding software vulnerabilities, we find defensive gaps. We provide the guided remediation steps your IT team needs to harden these areas, ensuring your existing security investments perform exactly as you expect.

Validato

+44 (0) 124 237 4181

justask@validato.io

https://validato.io/