📅 Insider Threat Simulation Log Day 13: Visible Security Misconfigurations Across Workstations

Date of Entry: 6/28/2025
Observer: Michael Warner
Location: Facility-Wide
Classification: Internal Security Simulation

🧾 Incident Overview

On the thirteenth day of my insider threat simulation, I made a facility-wide observation regarding common security misconfigurations visible on many active pharmacy workstations. While walking through various work zones, I noticed that multiple Windows-based terminals displayed red warning icons in the system tray, specifically on the Windows Security shield.

This red indicator is typically associated with disabled antivirus, inactive firewall settings, or missing updates — all of which significantly degrade a system's security posture. These devices were in live production use, and at no point did I touch or interact with any of the computers. My observations were entirely based on screen visibility from normal walking routes during my shift.

The fact that these misconfigurations were both visible and persistent across multiple systems suggested a systemic issue with workstation management and endpoint security enforcement.

⚠️ Risk Assessment

- Neglected endpoint security creates real and scalable vulnerabilities:
- Disabled antivirus or firewalls increase malware and ransomware exposure
- Unpatched systems are susceptible to known exploits and privilege escalation attacks
- Visible misconfigurations reflect poor centralized control over endpoint settings
- Insider threats could intentionally disable protections, assuming no one checks
- Patients' protected health information (PHI) is put at risk via weakened device hardening

🕵️ Speculative Insider Perspective

As a malicious insider, I could:

- Wait for a shift at a station with the red shield, knowing it has lower protection
- Introduce malicious USBs or files without triggering endpoint defense software
- Use known Windows vulnerabilities to escalate privileges on poorly maintained systems
- Take advantage of security negligence to bypass detection or local logging

The fact that these signs of weakness were visible to anyone in the pharmacy only highlights the severity of the oversight.

🛡️ Initial Thoughts & Actions

I did not interact with or test any workstation. This observation was made purely from screen glances while working my regular duties. I documented these recurring misconfigurations because they directly influenced my decision to draft a formal business proposal (see Day 14). I believed that a policy or infrastructure change was needed to address these issues proactively.

✅ Recommendations (Low-Impact Suggestions)

- Conduct a full audit of active pharmacy endpoints to verify antivirus, firewall, and update compliance
- Implement centralized endpoint management (e.g., Microsoft Intune, SCCM)
- Configure systems to alert IT when protections are disabled or misconfigured
- Limit local admin rights so users cannot disable security settings
- Include visible workstation indicators in routine employee training (what to report, who to notify)

🟠 Severity Rating

Moderate to High — Misconfigured systems in sensitive areas like a pharmacy pose an unacceptable risk. The widespread nature of these issues suggests a breakdown in endpoint security enforcement and monitoring.

- End of Entry