OPENPHARMA CYBERSECURITY AUDIT ACTION PLAN

Luis Cruz

03/2025

Open Pharma

Overview of the Audit

- OpenPharma handles highly sensitive data, including proprietary research, patient records, and regulatory compliance information.
- A recent cybersecurity audit revealed 14 key vulnerabilities, posing risks to data integrity, regulatory compliance, and business operations.
- Due to resource constraints, we prioritized 8 critical vulnerabilities for immediate remediation.

Open Pharma

Overview of the Audit

THE 8 SELECTED VULNERABILITIES

1. Outdated Operating Systems
2. IPv6 Networking Poisoning
3. LLMNR Network Poisoning
4. MDNS Network Poisoning
5. NBT-NS Poisoning
6. ASREP-Roastable Users
7. Kerberoastable Users
8. Machines Without Required SMB Signing

VULNERABILITIES RANKED BY SEVERITY AND IMPACT

Open Pharma

Business Impact Example

Vulnerability:

NBT-NS Poisoning

Risk:

Exploited to intercept name resolution traffic, enabling attackers to capture credentials.

Business Impact

Regulatory Risk

- Violates data protection requirements (e.g., HIPAA, FDA cybersecurity guidelines).

Operational Risk

- May expose internal systems to impersonation and unauthorized access.

Reputational Impact

- A breach of credentials could lead to loss of trust and financial liability.

Open Pharma

Key Remediation Action Example

Vulnerability: ASREP-Roastable Users

- **Proposed Fix:**
  - Enforce stronger password policies and enable Kerberos pre-authentication.
  - Implement MFA for privileged accounts and monitor for suspicious Kerberos activity.

- **Business Benefit:**
  - Protects against credential theft and lateral movement within the network.
  - Safeguards sensitive research and patient data from unauthorized access.

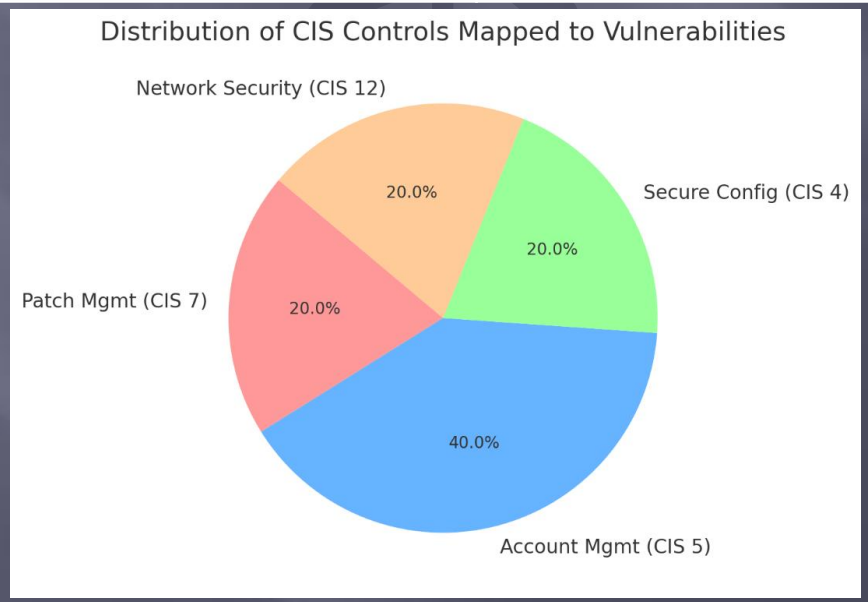
CIS Control Alignment: CIS Control 5 (Account Management)

Open Pharma

CIS Controls Alignment

OpenPharma aligns each selected vulnerability with CIS Controls (IG1 level) for strong foundational security.

	Examples of Safeguard Implementation	
CIS Control 7	Patch Management	Address outdated operating systems
CIS Control 5	Account Management	Strengthen authentication & access control
CIS Control 12	Network Infrastructure Management	Mitigating network poisoning (IPv6, LLMNR, MDNS, NBT-NS)



Open Pharma

Next Steps & Recommendations

- **Immediate Actions:** Remediate critical vulnerabilities, focusing on network poisoning and outdated OS updates.
- **Mid-Term Goals:** Implement MFA, Active Directory hardening, and network segmentation.
- **Long-Term Strategy:** Conduct regular security awareness training, implement SIEM tools, and test incident response plans.
- **Final Thought:** These actions will help OpenPharma protect sensitive assets, reduce attack surfaces, and ensure regulatory compliance.

Open Pharma