ZEROHEALTH CORP
PENETRATION TESTING REPORT

UNCOVERING RISKS
EMPOWERING RESILIENCE

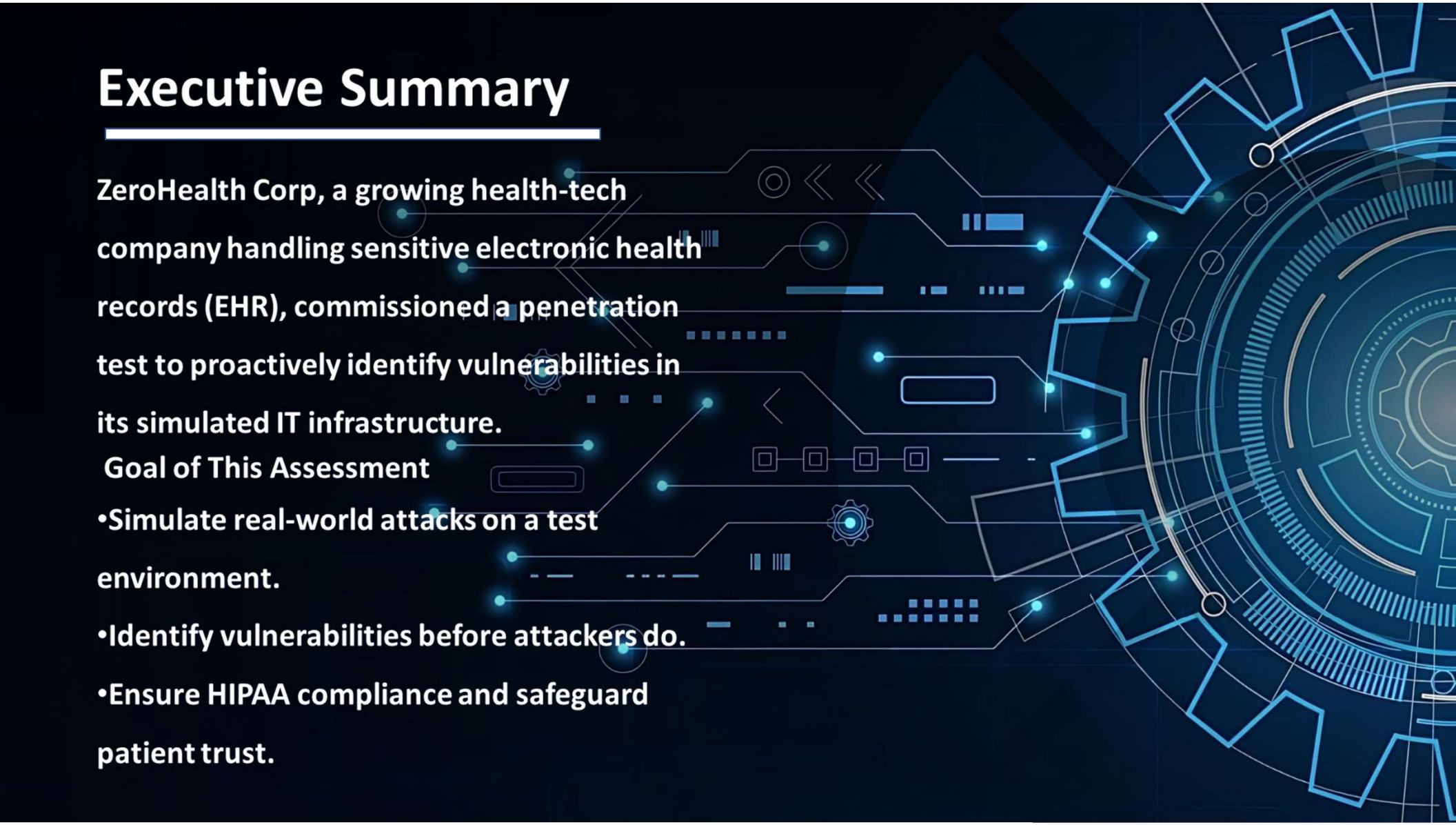
PREPARED BY:
KIRIDI DAVID EBI
PROJECT LEAD
DATE:
JULY 2025

Executive Summary

ZeroHealth Corp, a growing health-tech company handling sensitive electronic health records (EHR), commissioned a penetration test to proactively identify vulnerabilities in its simulated IT infrastructure.

Goal of This Assessment

- Simulate real-world attacks on a test environment.
- Identify vulnerabilities before attackers do.
- Ensure HIPAA compliance and safeguard patient trust.

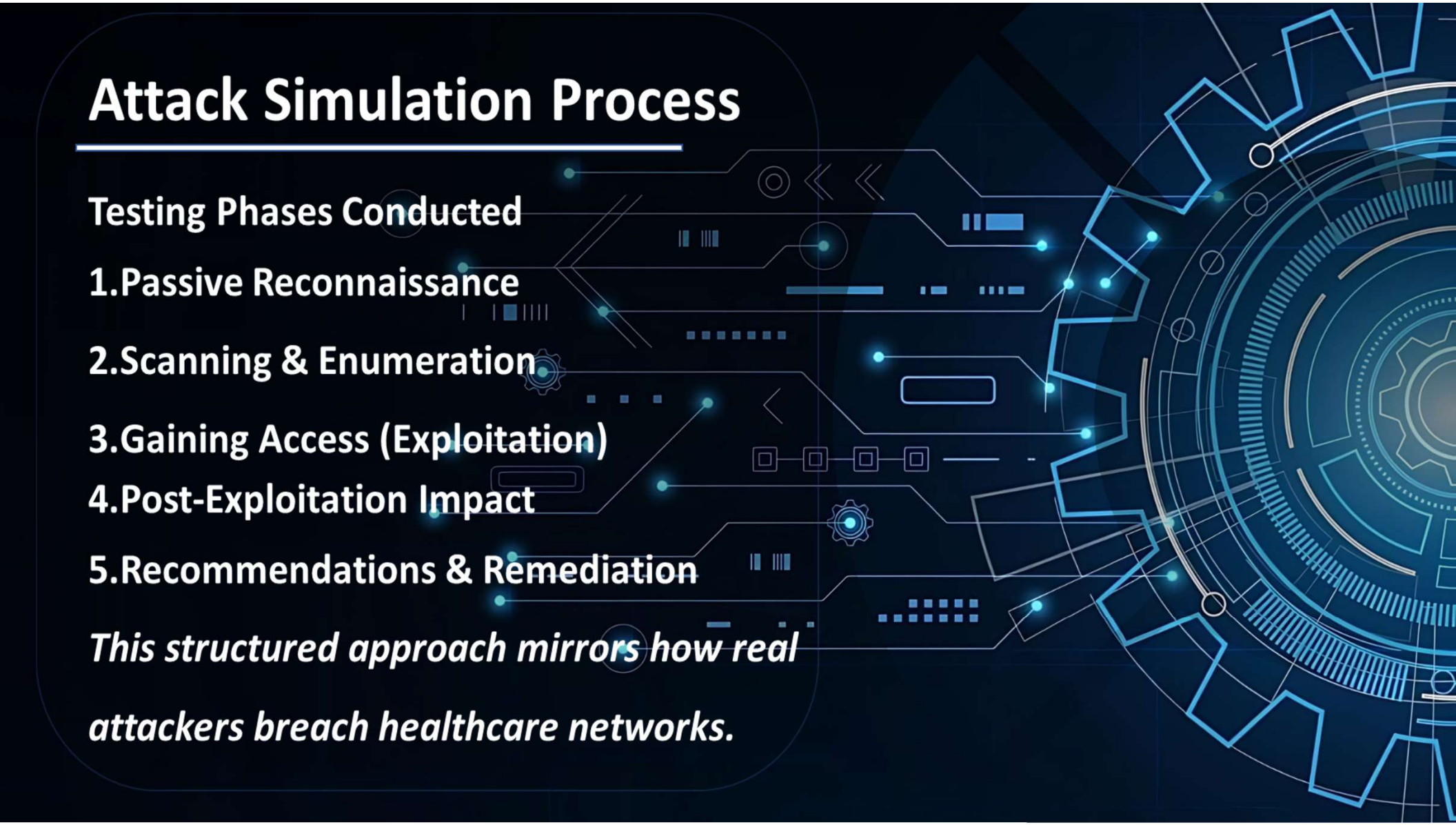


Attack Simulation Process

Testing Phases Conducted

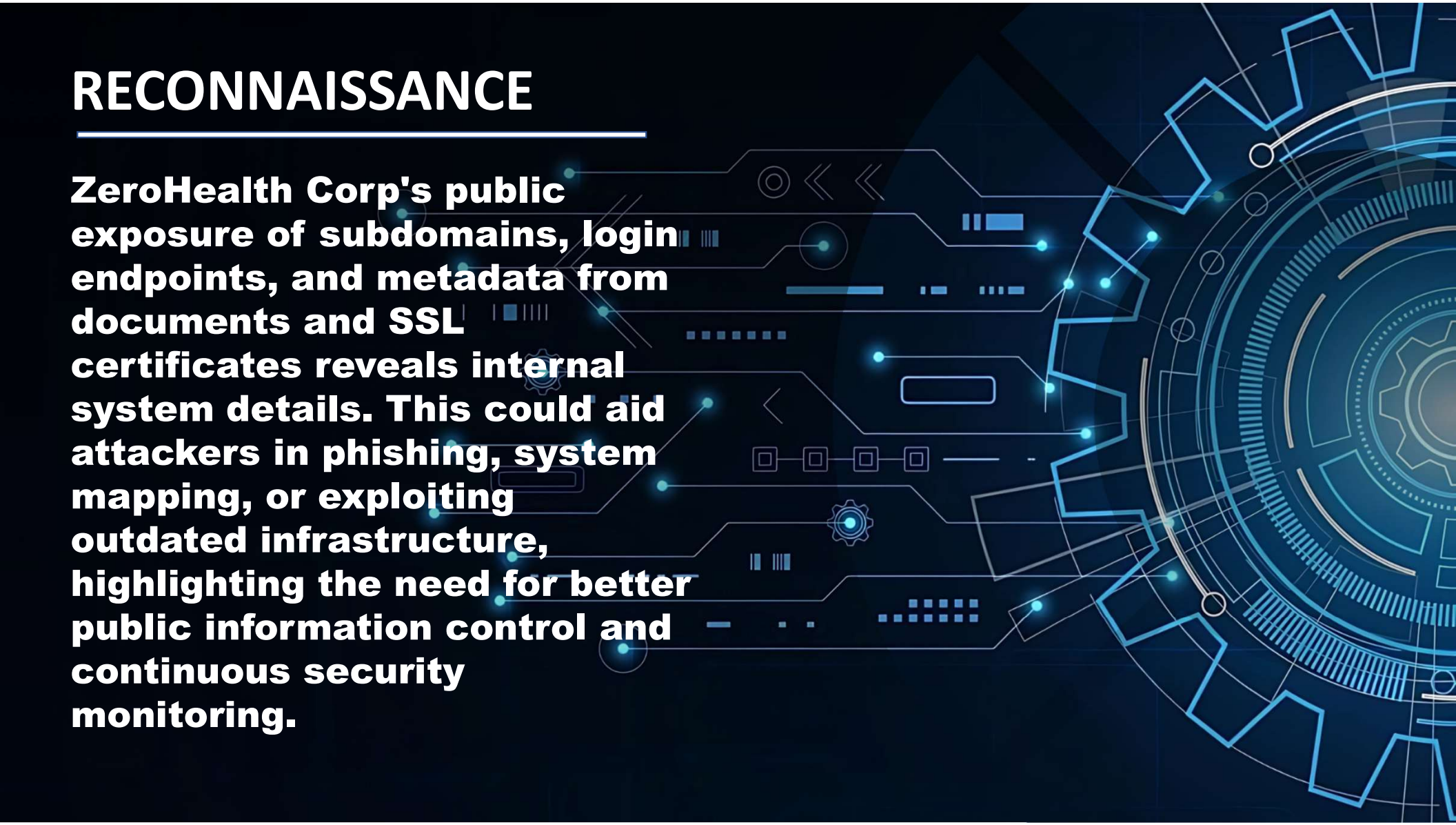
1. Passive Reconnaissance
2. Scanning & Enumeration
3. Gaining Access (Exploitation)
4. Post-Exploitation Impact
5. Recommendations & Remediation

This structured approach mirrors how real attackers breach healthcare networks.



RECONNAISSANCE

ZeroHealth Corp's public exposure of subdomains, login endpoints, and metadata from documents and SSL certificates reveals internal system details. This could aid attackers in phishing, system mapping, or exploiting outdated infrastructure, highlighting the need for better public information control and continuous security monitoring.



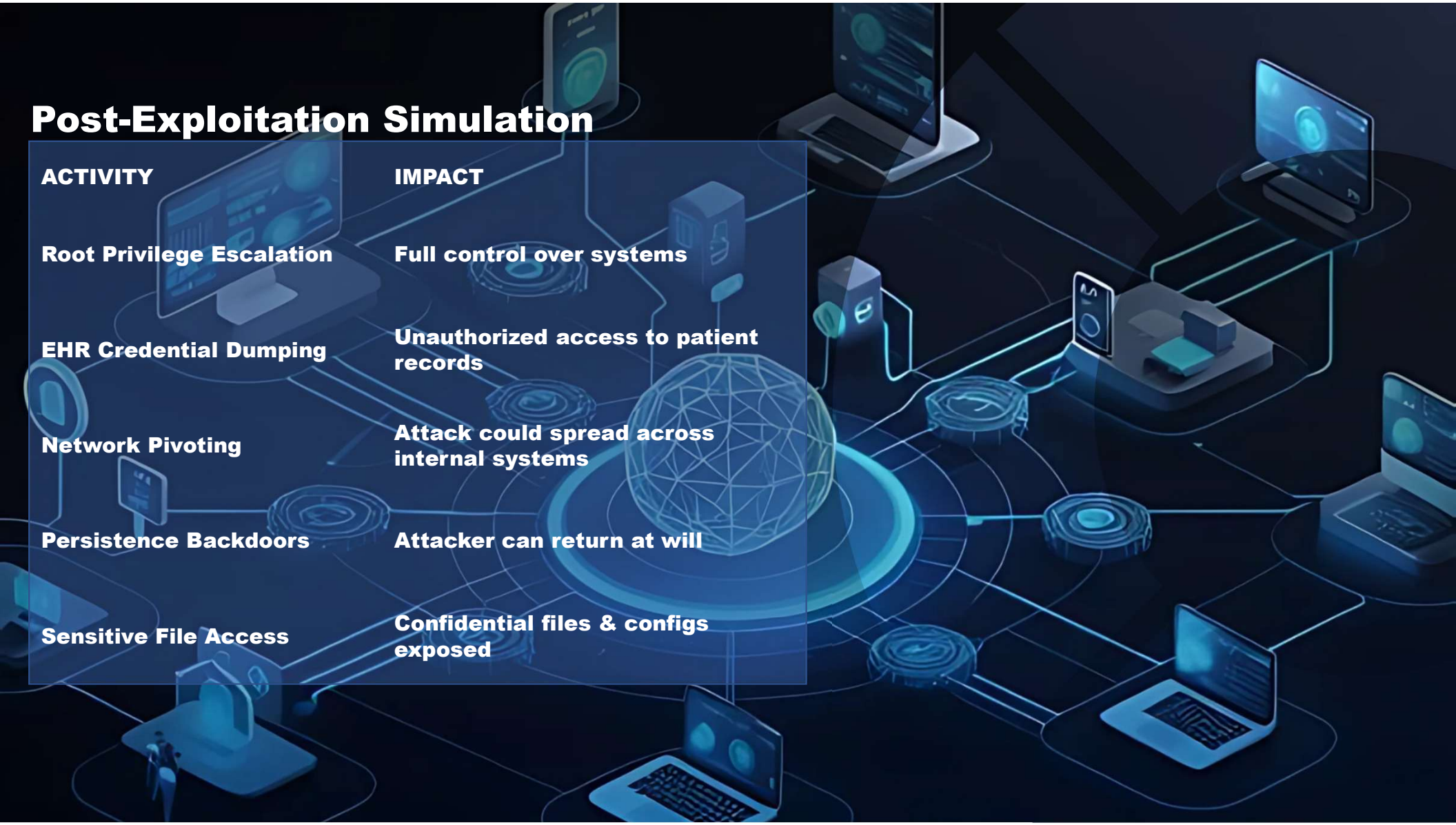
Vulnerability & Port Scan Overview

Discovered Open Ports: 25+ Services

PORT	SERVICE	RISK LEVEL
21 vsfTPD	This leads to data breaches, system manipulation, or full takeover depending on the system's permissions.	Critical 9.8
22 OpenSSH	OpenSSH 4.7p1 vulnerable to a cryptographic weakness that could allow attackers to recover session keys under certain conditions.	Medium5.9
80:Apache /DVWA	Apache httpd 2.2.8 outdated, known for multiple exploits	High7.5
139 Samba	A vulnerability that allows attackers to remotely run malicious code by uploading a specially crafted library to a shared folder and then triggering it through a network mechanism—much like how the notorious EternalBlue exploit works.	Critical 9.8
1524 Bind Shell	Opens a listener (e.g., port 4444/TCP) for attacker connections; allows remote commands and stays active until stopped.	Critical 10.0
6667 UnrealIRCd	A backdoored UnrealIRCd (2009–2010) let attackers run OS commands by sending 'AB;<command>' to the IRC server.	Critical 9.8

Top 5 Critical Exploited Vulnerabilities

VULNERABILITY	PORT(S)	CVSS	EXPLOITATION TOOL	BUSINESS IMPACT
Apache httpd 2.2.8	80	7.5 High	BurpSuite/ OWASP ZAP	Exposed Electronic Health Record (EHR) credentials, risking patient data and system control.
Samba Usermap Exploit	139/445	9.8 Critical	Metasploit	Root access, full system takeover
Bind Shell Access	1524	10. Critical	Netcat	Direct root shell, system compromise
DistCC RCE	3632	9.8 Critica	Metasploit	Remote commands, lateral movement
UnrealIRCd Backdoor	6667	9.8 Critica	Metasploit	Root access via backdoor, data exfiltration



Post-Exploitation Simulation

ACTIVITY	IMPACT
Root Privilege Escalation	Full control over systems
EHR Credential Dumping	Unauthorized access to patient records
Network Pivoting	Attack could spread across internal systems
Persistence Backdoors	Attacker can return at will
Sensitive File Access	Confidential files & configs exposed

Risk to Business

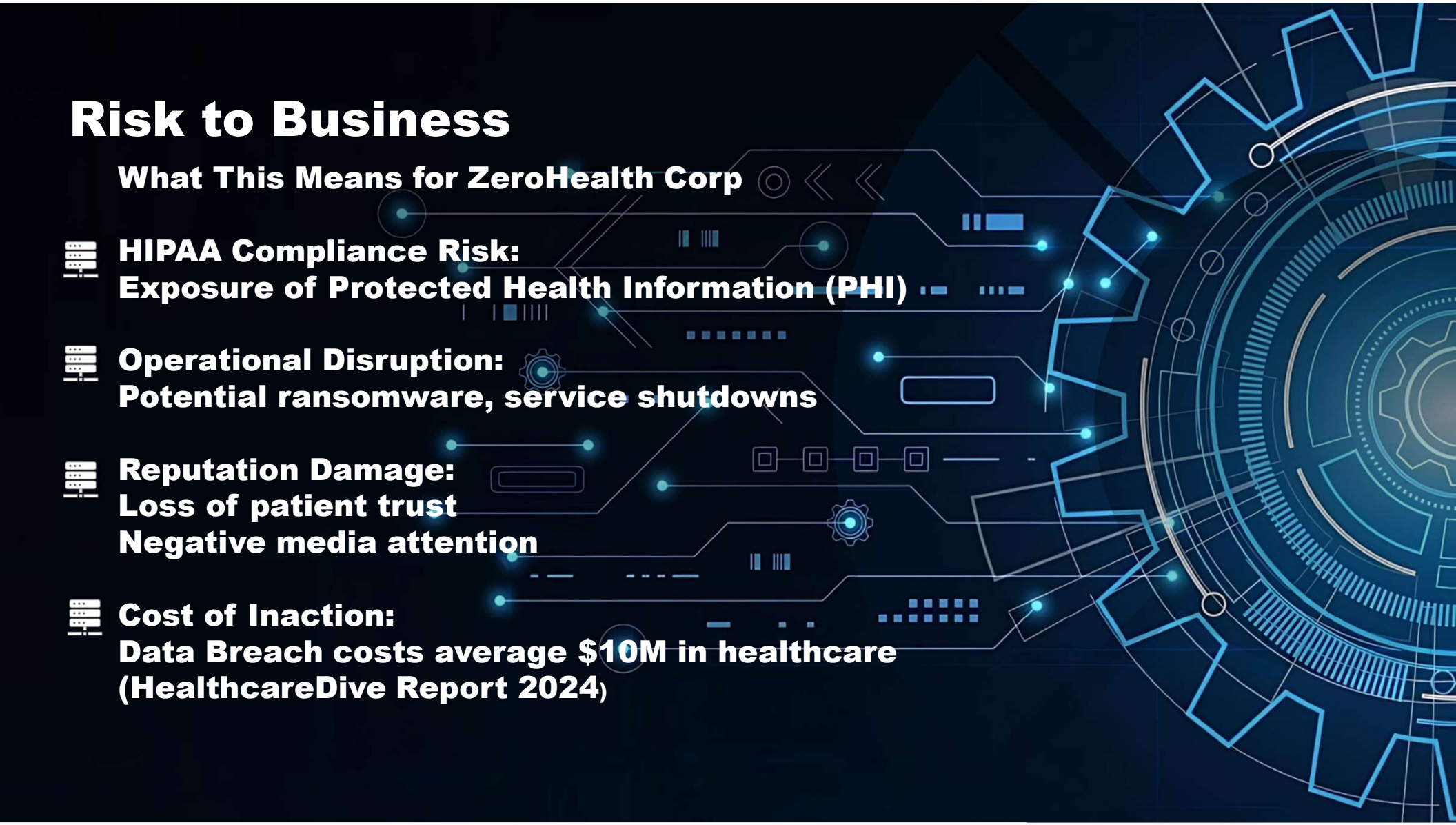
What This Means for ZeroHealth Corp

HIPAA Compliance Risk:
Exposure of Protected Health Information (PHI)

Operational Disruption:
Potential ransomware, service shutdowns

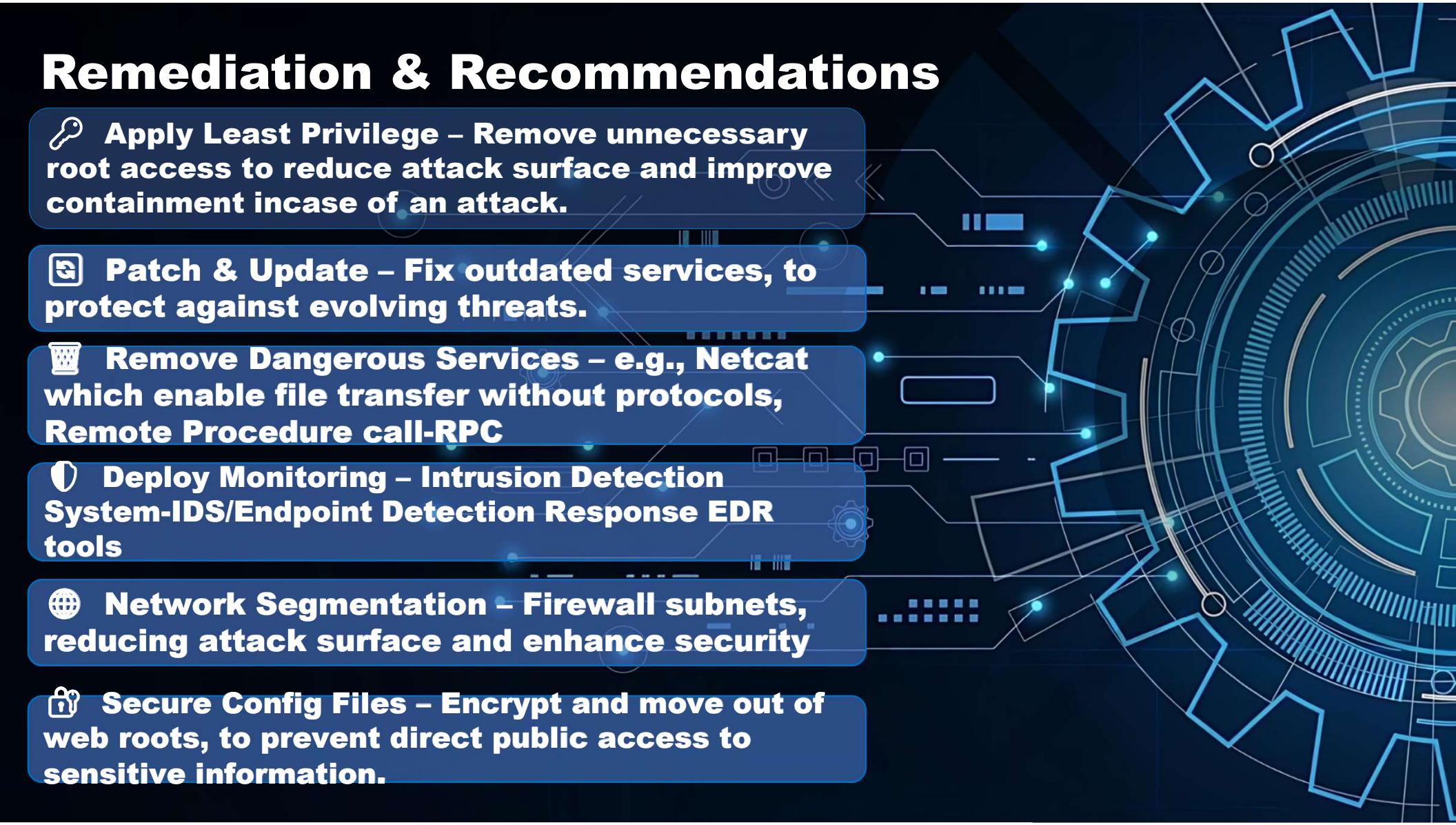
Reputation Damage:
Loss of patient trust
Negative media attention

Cost of Inaction:
Data Breach costs average $10M in healthcare
(HealthcareDive Report 2024)



Remediation & Recommendations

- **Apply Least Privilege** – Remove unnecessary root access to reduce attack surface and improve containment incase of an attack.
- **Patch & Update** – Fix outdated services, to protect against evolving threats.
- **Remove Dangerous Services** – e.g., Netcat which enable file transfer without protocols, Remote Procedure call-RPC
- **Deploy Monitoring** – Intrusion Detection System-IDS/Endpoint Detection Response EDR tools
- **Network Segmentation** – Firewall subnets, reducing attack surface and enhance security
- **Secure Config Files** – Encrypt and move out of web roots, to prevent direct public access to sensitive information.




THANK YOU