DATA PROTECTION

Building Cyber Resilience for the iDempiere Environment

About Me

Aishwarya Gore

Ethical Hacker and
Cyber Security Professional

I am an electrical engineer with a passion for cyber security.

6 years of experience in VAPT, Security Audits, Risk Assessment & Management, Compliance Audits.

Certifications –
CEH, CISA, HIPAA, ISO27001 LA, MITRE ATT&CK Defender, Executive Vulnerability Management.

The future is Open-source

But, IS IT SECURED?

In 2022, the National Vulnerability Database had **206059** entries. This means **more than 560 new vulnerabilities were found per day.**

80% of **exploits** are published before the CVEs are released. The average gap between the publication of an exploit and the corresponding CVE is **23 days**.

60% of data breaches are caused by the failure to apply available patches.

A study shows that **84%** of companies have **high-risk** vulnerabilities half of which could be removed with a simple **software update.**
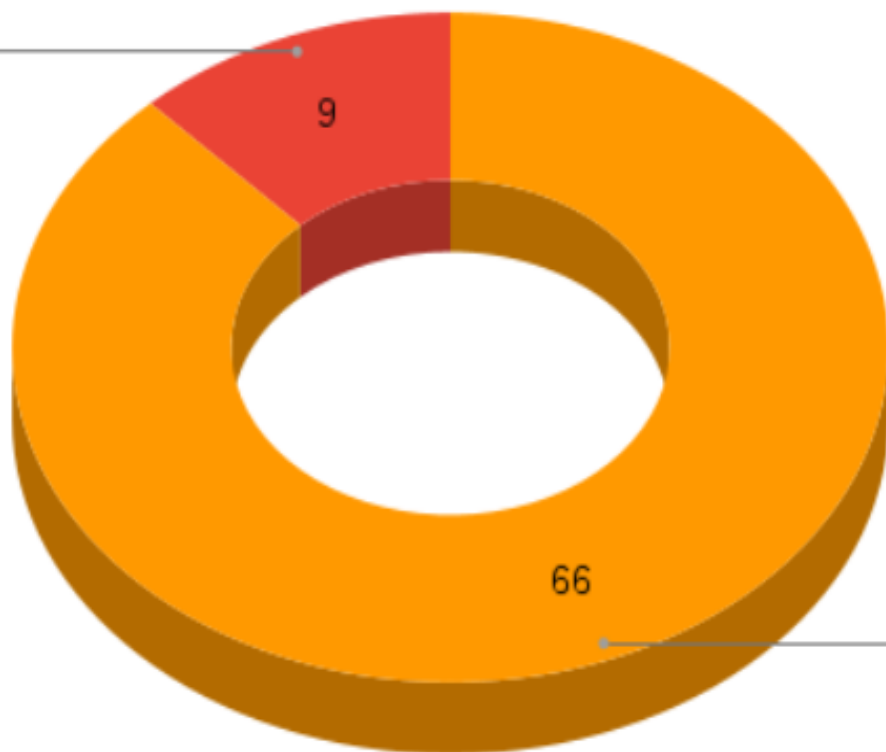
| **9** CRITICAL | **66** IMPORTANT | **0** MODERATE | **0** LOW |

Microsoft patched 75 CVEs in its February 2023 Patch Tuesday Release, with nine rated as critical and 66 rated as important.

Critical
12.0%

9

66

Important
88.0%

Top 10 Vulnerabilities In 2022

Log4Shell
Follina
Spring4Shell
Google Chrome Zero-Day
F5 BIG-IP
Microsoft Office Bug
ProxyNotShell
Zimbra Collaboration Suite Bugs
Atlassian Confluence RCE Flaw
Zyxel RCE Vulnerability

OWASP TOP 10 SECURITY RISKS & VULNERABILITIES

#	
1	Broken Authentication
2	Injection
3	XML External Entities (XXE)
4	Sensitive Data Exposure
5	Security Misconfiguration
6	Broken Access Control
7	Insecure Deserialization
8	Cross-Site Scripting (XSS)
9	Insufficient Logging and Monitoring
10	Using Components with Known Vulnerabilities

iDempiere Environment

MySQL, MariaDB, MSSQL, PostgreSQL, Oracle

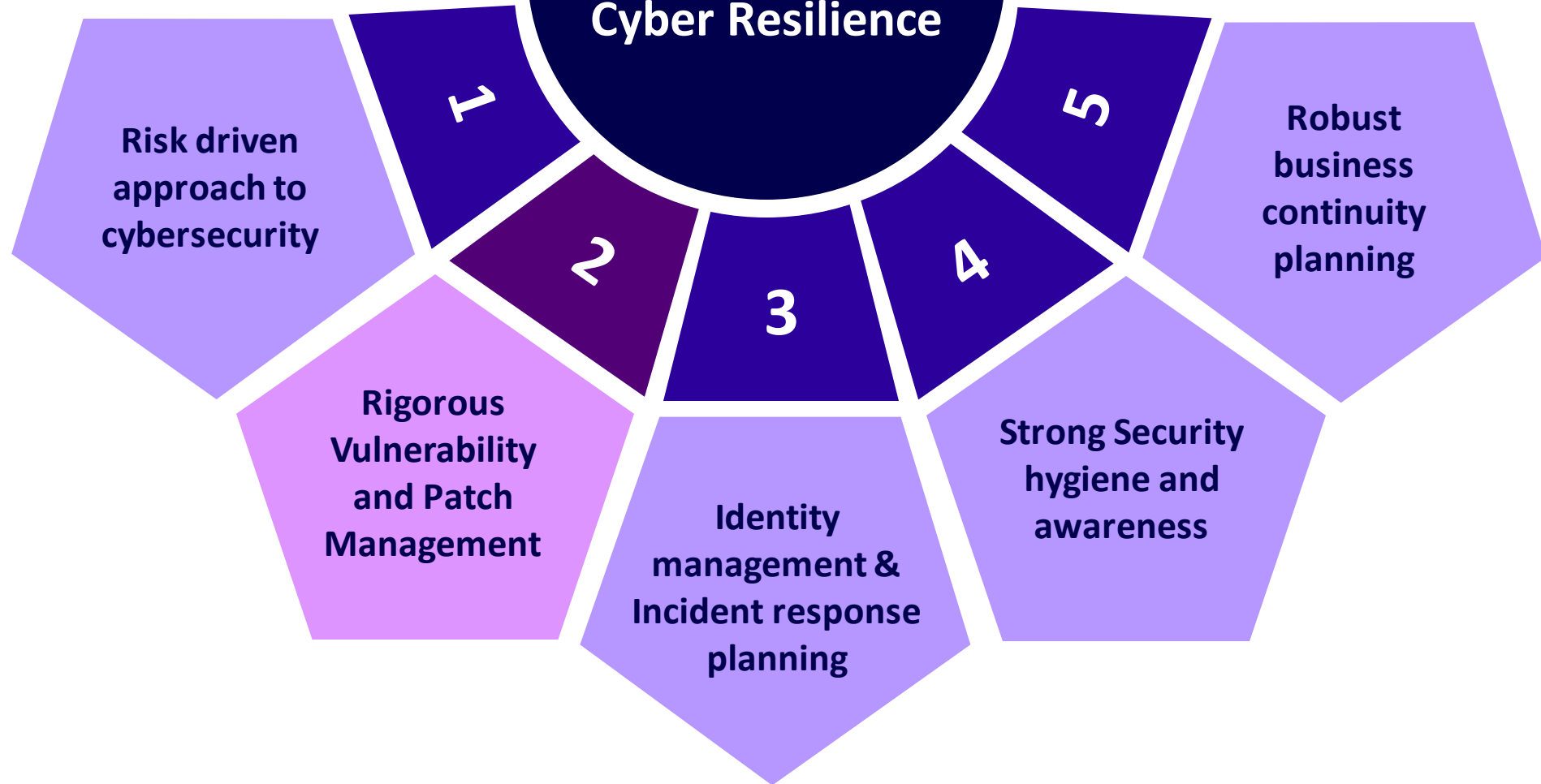AWS, Azure, GCP, OpenStack, OpenNebula

Nginx, Apache, Vmware, HANA, IIS

Jquery, AngularJS, VueJS, ReactJS, NodeJS, JRE, JDK

Open VPN, ExpressVPN, NordVPN, AWS/Azure VPN

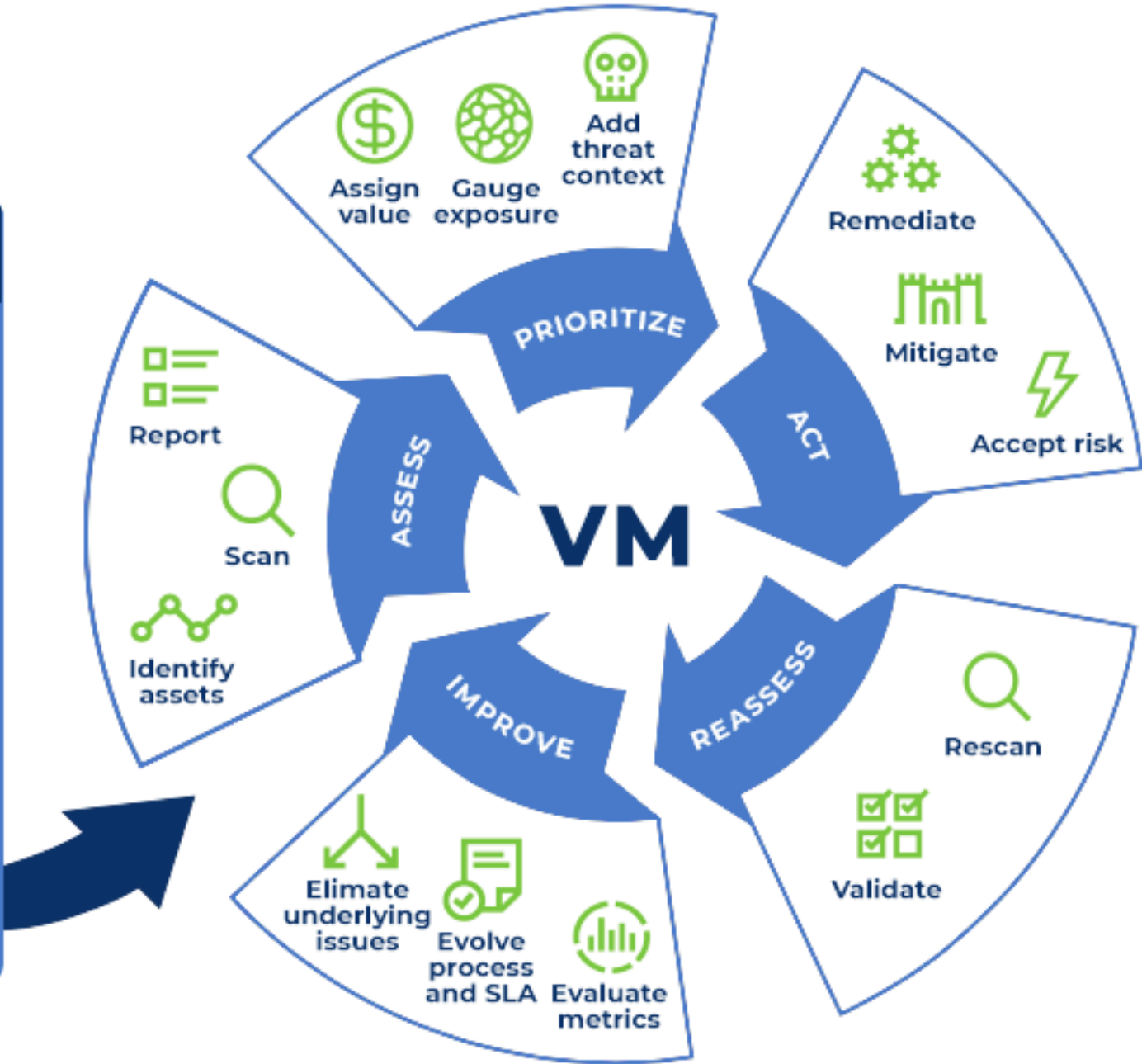Proxy – Zscaler, Fortinet, PaloAlto, Checkpoint, Cisco, Symantec

Recommendations for building Cyber Resilience

1. Risk driven approach to cybersecurity
2. Rigorous Vulnerability and Patch Management
3. Identity management & Incident response planning
4. Strong Security hygiene and awareness
5. Robust business continuity planning

Advantages of Continuous Vulnerability Management

- Accurate visibility of the attack surface at all times
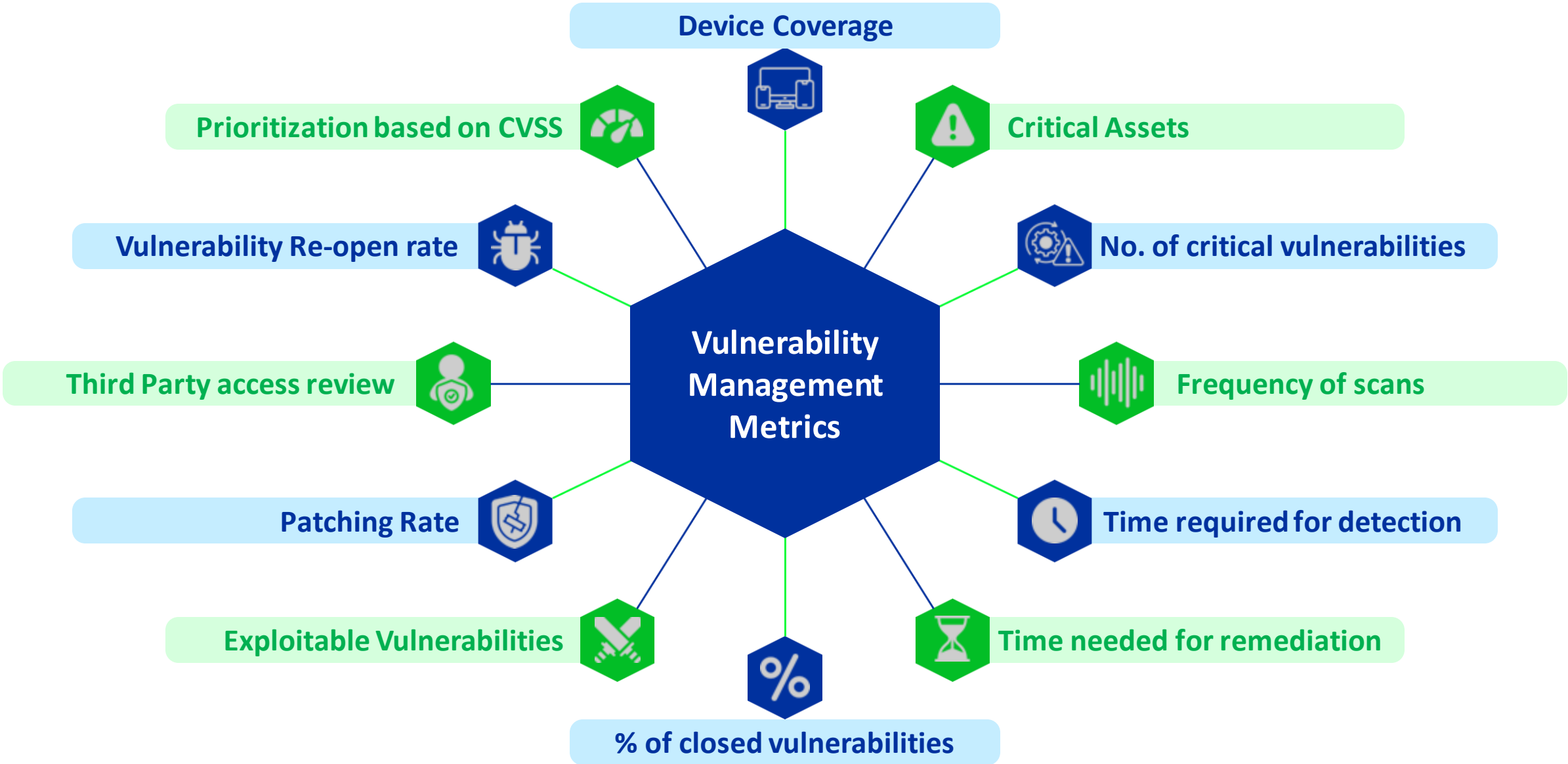- Faster detection and mitigation cycles
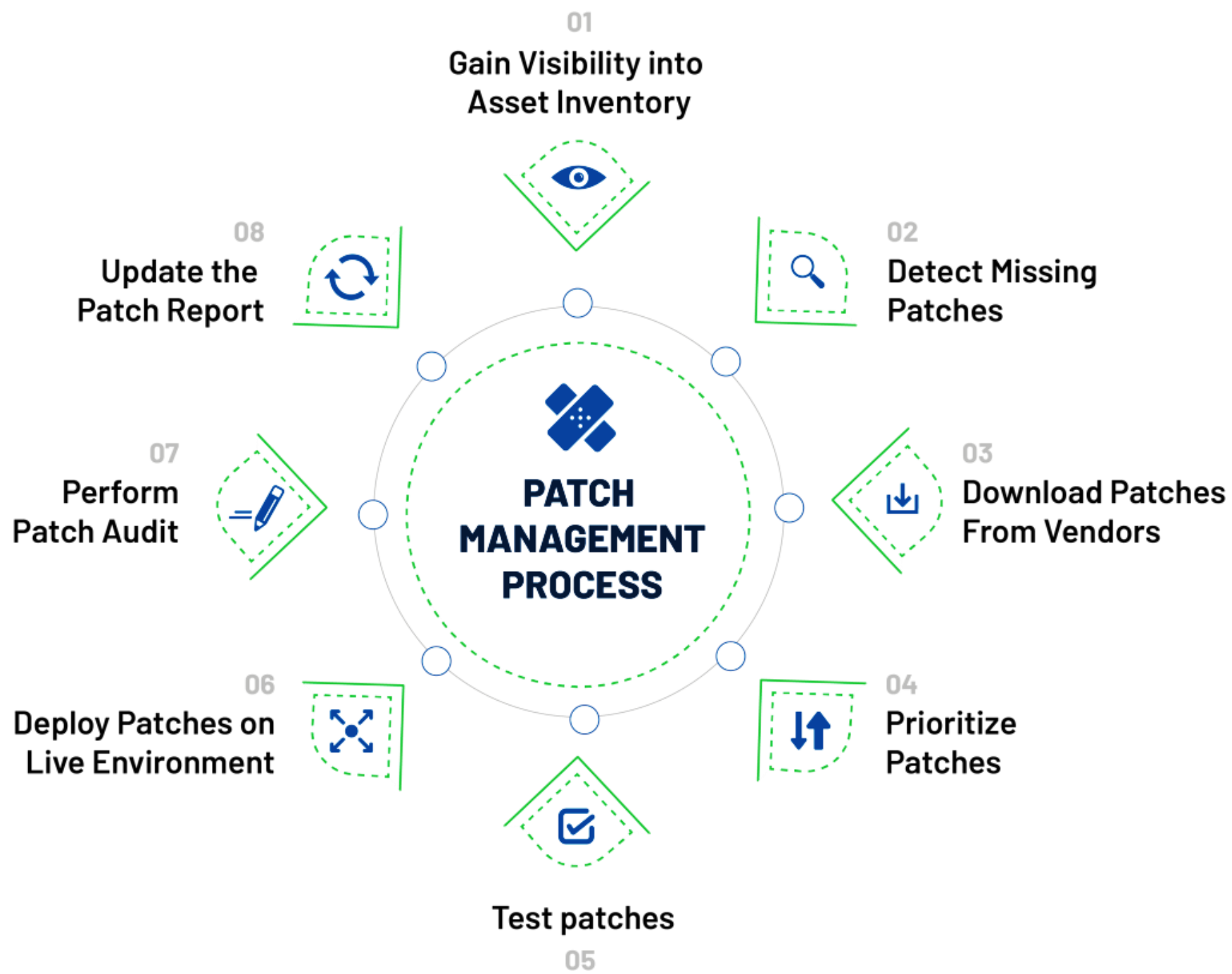- Effective utilization of IT resources for configuring scans
- Continuous compliance with security standards
- Reduced team fatigue and improved productivity

PATCH MANAGEMENT PROCESS

01 Gain Visibility into Asset Inventory

02 Detect Missing Patches

03 Download Patches From Vendors

04 Prioritize Patches

05 Test patches

06 Deploy Patches on Live Environment

07 Perform Patch Audit

08 Update the Patch Report

Incident Response

THANK YOU!

Aishwarya Gore
aishugore@gmail.com