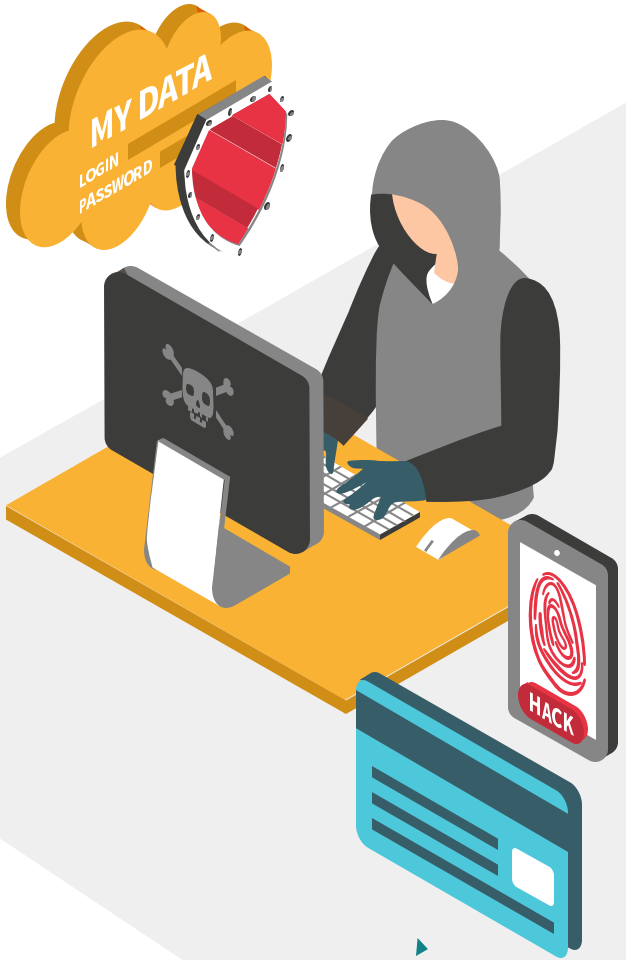
Vulnerability Management



Prepared by : Hazem Mohamed

TABLE OF CONTENTS

01.

What is Vulnerability Management?

Vulnerability Management

Vulnerability management is the process of identifying, evaluating, prioritizing, and mitigating security vulnerabilities in systems and software.

- Vulnerability Management is integral to computer security and network security, and must not be confused with vulnerability assessment.
- Vulnerabilities can be discovered with a vulnerability scanner, which analyzes a computer system in search of known vulnerabilities, such as open ports, insecure software configurations, and susceptibility to malware infections.

Vulnerability Management

- Vulnerability Management is the ongoing, regular process of identifying, assessing, reporting on, managing, and remediating cyber vulnerabilities.

02.

Vulnerability Management process/life cycle

Vulnerability Management process/life cycle

- Vulnerability management is much more than vulnerability scanning or vulnerability assessment . Vulnerability management is a **proactive**, **continuous**, and **systematic** process of **identifying**, **assessing**, **prioritizing**, and **remediating/mitigating** security vulnerabilities in an organization's IT infrastructure.

Vulnerability Management Process Overview

- Identification
- Assessment
- Prioritization
- Remediation
- Verification

Vulnerability Management Process

Identification

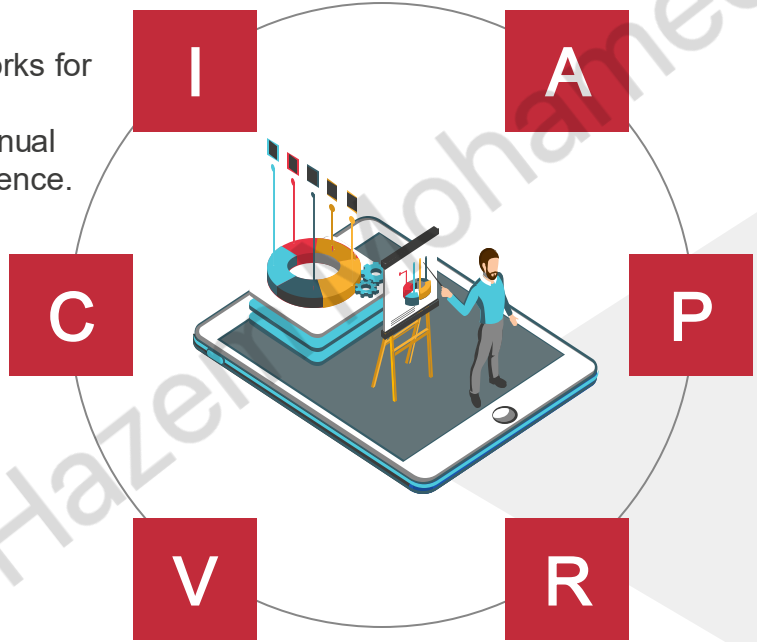
•Scanning systems and networks for vulnerabilities.
•Utilizing automated tools, manual inspections, and threat intelligence.

Continuous Monitoring

•Implementing continuous monitoring to detect new vulnerabilities.
•Regularly updating vulnerability databases and scanning systems.

Verification

•Verifying that vulnerabilities have been effectively mitigated.
•Conducting post-remediation testing and validation.



Assessment

•Analyzing vulnerabilities to determine their severity and potential impact.
•Considering factors like exploitability, affected systems, and available patches.

Prioritization

•Ranking vulnerabilities based on their risk level.
•Considering factors such as criticality, exposure, and business impact.

Remediation

•Developing and implementing a plan to address vulnerabilities.
•Applying patches, configuration changes, or other mitigation measures.

Life Cycle

Scanning

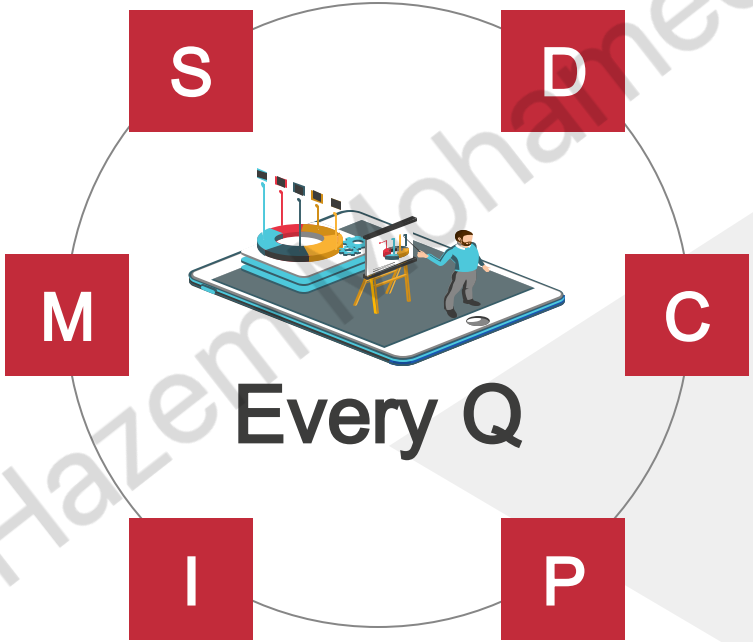
Scanning Using Tools

Mitigate

Set mitigation solutions after studying and testing them.

Identify

Identify and deliver to each owner



Detect Vulnerabilities

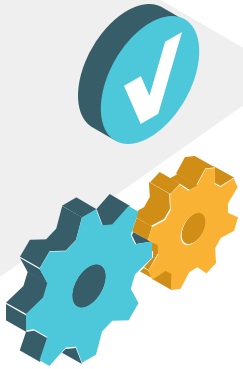
Detect Vulnerabilities in each Sub-net

Check Every Vulnerabilitiy

Check if it’s a false positive

Prepare Report

Prepare the Detailed Report



03.

Importance of VM

Vulnerability management is a **critical** aspect of maintaining a secure digital environment.

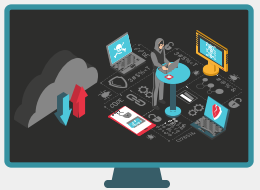
—Here are key points about its importance:

- **Risk Reduction**: By continuously identifying, assessing, and addressing security weaknesses, organizations can **minimize the risk** of cyberattacks and data breaches.
- **Proactive Approach**: Vulnerability management is **proactive**, helping prevent attacks rather than reacting after a breach occurs.
- **Automated Scanning**: Tools like vulnerability scanners automatically scan assets for vulnerabilities, threats, and risks, ensuring timely detection.
- **Patch Management**: Keeping systems up-to-date with the latest security patches is essential to prevent exploitation of known vulnerabilities.
- **Configuration Management**: Ensuring secure device configurations and compliance with security policies enhances overall security posture.

Remember that vulnerability management should be **continuous** to adapt to evolving threats and changing environments

04.

Patch Management



Patch management is the process of **applying vendor-issued updates** to close security vulnerabilities and optimize the performance of software and devices. It is sometimes considered a part of **vulnerability management**. In practice, patch management aims to **balance cybersecurity** with the operational needs of a business.

-- Here are key points about the importance of patch management:

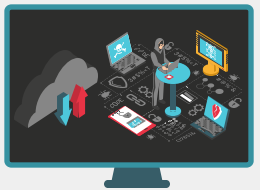
- **Risk Reduction**: By continuously identifying, assessing, and addressing security weaknesses, organizations can **minimize the risk** of cyberattacks and data breaches.
- **Proactive Approach**: Vulnerability management is **proactive**, helping prevent attacks rather than reacting after a breach occurs.
- **Automated Scanning**: Tools like vulnerability scanners automatically scan assets for vulnerabilities, threats, and risks, ensuring timely detection.
- **Patch Types**:
  - **Security Updates**: Address specific security risks by remediating vulnerabilities. Unpatched assets are often targeted by hackers.
  - **Feature Updates**: Improve asset performance and user productivity by introducing new features.
  - **Bug Fixes**: Address minor issues that affect performance but don't cause security problems.
- **Minimizing Downtime**: Formal patch management processes allow organizations to prioritize critical updates, gaining benefits with minimal disruption to employee workflows.
- **Regulatory Compliance**: Patch management helps organizations keep critical systems compliant with regulations like GDPR, HIPAA, and PCI-DSS.

Remember that patch management is a **continuous lifecycle**, adapting to evolving threats and changing IT environments

05.

Patch Management

Life Cycle



Patch Management Process

Identification

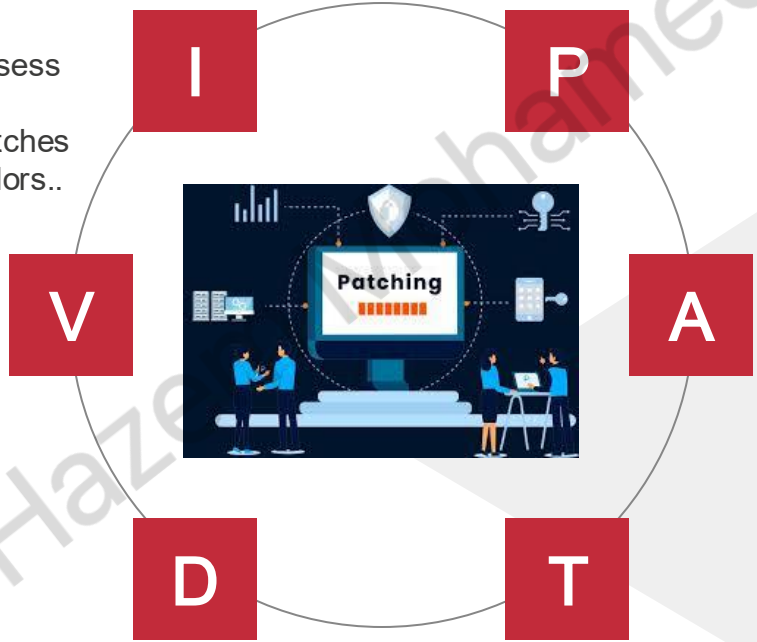
•Identify vulnerabilities and assess their impact on systems.
• Stay informed about new patches and updates released by vendors..

Verification

•Confirm successful patch installation.
• Validate that systems are functioning correctly after patching.

Deployment

• Deploy patches to production systems.
• Schedule deployments during maintenance windows to minimize disruption.



Prioritization

• Prioritize patches based on severity, criticality, and potential impact.
• Focus on high-risk vulnerabilities that could lead to security breaches.

Acquisition

•Obtain the necessary patches from reliable sources (vendor websites, security advisories, etc.).
• Ensure the authenticity and integrity of the patches.

Testing

• Test patches in a controlled environment (sandbox or test systems).
• Verify compatibility with existing software and configurations.

Patch Management Process

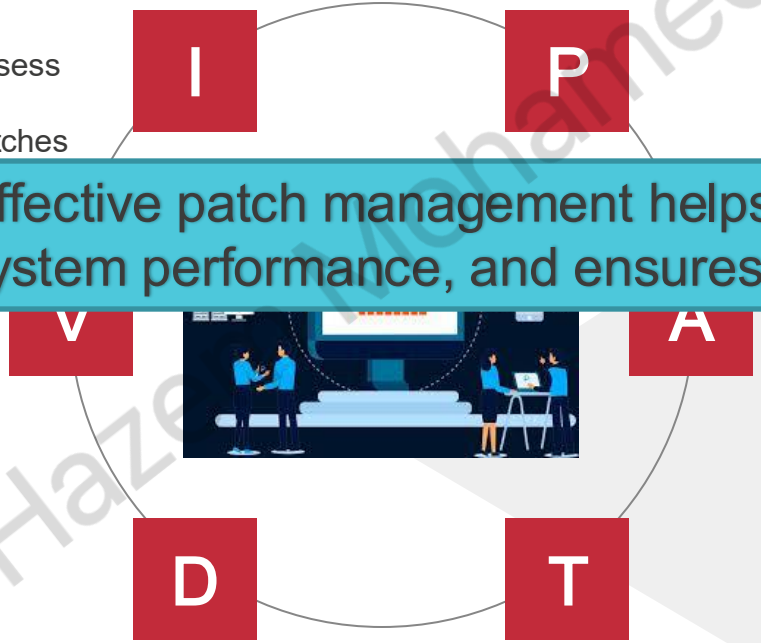
Identification

•Identify vulnerabilities and assess their impact on systems.
• Stay informed about new patches

Prioritization

• Prioritize patches based on severity, criticality, and potential impact.
• Focus on high-risk vulnerabilities

Remember that effective patch management helps prevent security breaches, enhances system performance, and ensures regulatory compliance



•Confirm successful patch installation.
• Validate that systems are functioning correctly after patching.

reliable sources (vendor websites, security advisories, etc.).
• Ensure the authenticity and integrity of the patches.

Deployment

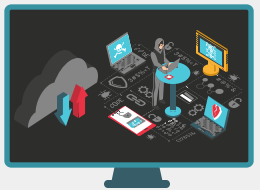
• Deploy patches to production systems.
• Schedule deployments during maintenance windows to minimize disruption.

Testing

• Test patches in a controlled environment (sandbox or test systems).
• Verify compatibility with existing software and configurations.

06.

Relationship Between VM and PM



Relationship Between VM and PM

	Vulnerability Management	Patch Management
Scope	VM operates within a relatively **broad scope**. It encompasses a range of preventive measures to fortify the system against security threats.	PM operates within a **narrower scope**. It concentrates on patches and updates provided by software vendors or security teams.
Objectives	VM aims to identify, classify, prioritize, and mitigate vulnerabilities in software and systems.	PM aims to apply software updates (patches) to address known vulnerabilities and improve functionality.
Activities	VM involves vulnerability scanning, risk assessment, and remediation planning.	PM includes testing, deploying, and verifying patches.
Approach	**Proactive Approach**: It focuses on preventing vulnerabilities from being exploited.	**Reactive Approach**: It responds swiftly to security holes before threats can exploit them.

Challenges

Volume & Complexity of Vulnerabilities

The sheer volume and complexity of vulnerabilities can overwhelm organizations, making it difficult to prioritize and address them effectively.

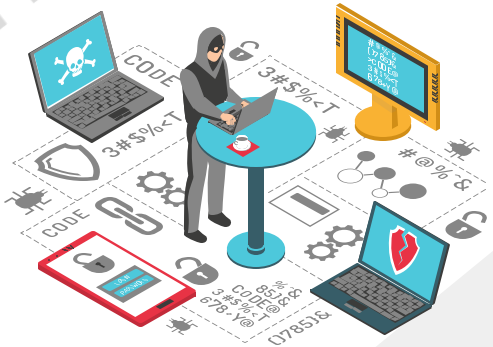
Resource Constraints

Limited resources, including time, budget, and expertise, can pose challenges to effective vulnerability management, particularly for small and medium-sized organizations.

Patch Management in Large and Diverse Environments

Patching systems in large and diverse environments can be challenging due to compatibility issues, downtime concerns, and the need to coordinate across multiple teams and stakeholders.

Tools



VM and PM Tools

- **Vulnerability Scanning Tools:** Automated vulnerability scanning tools such as Nessus, Qualys, and OpenVAS help organizations identify and assess vulnerabilities in systems and software.
- **Patch Management Solutions:** Patch management solutions such as SCCM (System Center Configuration Manager) and WSUS (Windows Server Update Services) help organizations deploy patches and updates to systems efficiently.

Action1.
ManageEngine.

OpenVAS
Open Vulnerability Assessment Scanner

Nessus vulnerability scanner

secpod

Qualys.

Microsoft System Center Configuration Manager

Action1
#1 for patch management

ManageEngine Patch Manager Plus

THANKS

DO YOU HAVE ANY QUESTIONS?

hmohamed200@gmail.com

https://itsysadmins-eg.info/