Cybersecurity Vulnerability Management

What is vulnerability management?

It is the ongoing process of identifying, assessing, reporting, managing, and remediating cyber vulnerabilities across endpoints, workloads, and systems. Usually, a security team will leverage a vulnerability management tool to detect vulnerabilities and utilize different processes to patch or remediate them.

- **Proactive risk mitigation:** A forward-thinking approach to managing potential threats before they materialize. Instead of reacting to risks after they occur, proactive risk mitigation involves identifying, assessing, and addressing risks in advance to prevent or minimize their impact.
- **Compliance Requirements:** The guidelines and regulations must be followed to ensure they operate legally and ethically.
- **Reduced Attack surface:** Minimize the number of potential entry points that attackers can exploit to gain unauthorized access to a system.

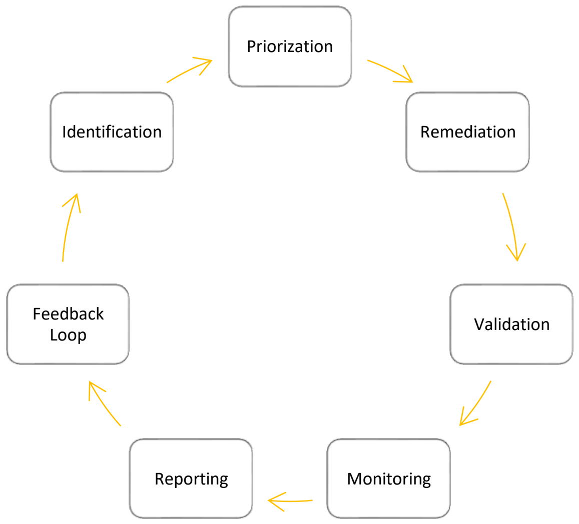
Types of cybersecurity vulnerabilities

- Software vulnerabilities
- Hardware vulnerabilities.
- Configuration vulnerabilities.
- Human Error.
- Zero-Day Vulnerabilities.

The importance of cybersecurity Vulnerability Management

- Preventing Data Breaches
- Compliance and regulations
- Business Continuity
- Cost-Efficiency

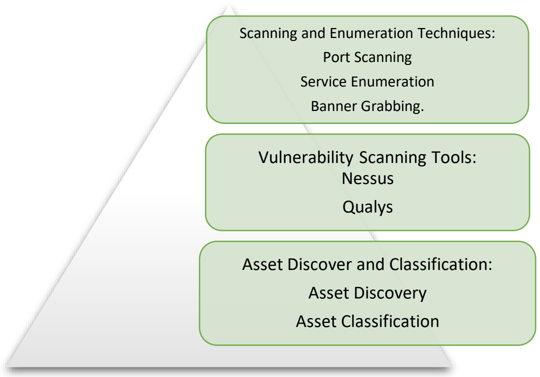
Cybersecurity Vulnerability Management Lifecycle:



Joshua Ortiz
Security Administration Engineer – IT Security Administration

Terminology

1. Vulnerability
2. Threat
3. Risk assessment.
4. Vulnerability Scanning
5. Patch Management
6. Asset Inventory
7. Remediation
8. Vulnerability Management Lifecycle
9. Vulnerability Database
10. Compliance and regulations.



Scanning and Enumeration Techniques:
Port Scanning
Service Enumeration
Banner Grabbing.

Vulnerability Scanning Tools:
Nessus
Qualys

Asset Discover and Classification:
Asset Discovery
Asset Classification

Risk Assessment Methodologies

CVSS (Common Vulnerability Scoring System)

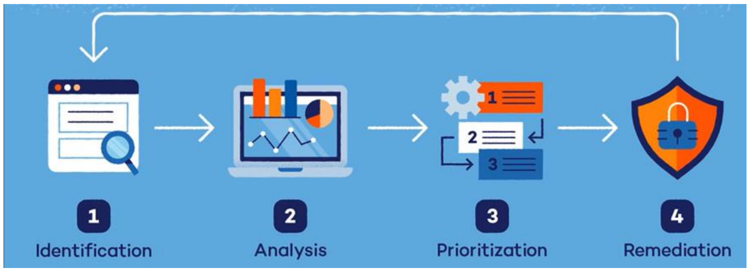
DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)

RATING	CVSS SCORE
NONE	0.0
LOW	0.1 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 8.9
CRITICAL	9.0 - 10.0

Damage	Impact of an attack
Reproducibility	How Easily attack can be reproduced?
Exploitability	How easy is it to launch the attack
Affected users	How many users will be impacted?
Discoverability	How easily the vulnerability can be found.

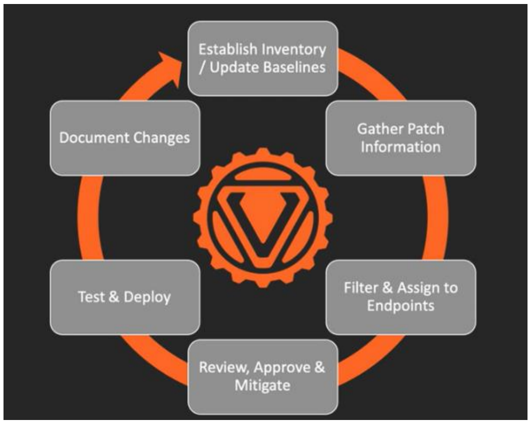
Conducting Vulnerability Scans

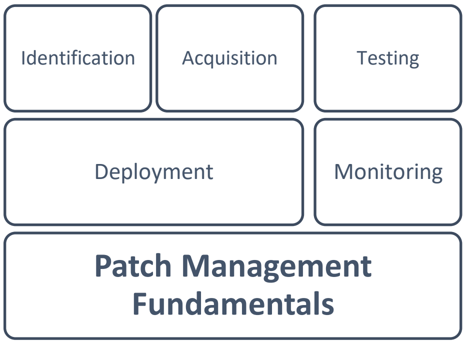
- Scope Definition
- Selection Tools
- Scanning
- Analysis



Vulnerability Databases and Repositories

- National Vulnerability Database (NVD)
- Common Vulnerabilities and Exposures (CVE)
- Vendors Specific Resources


Establish Inventory / Update Baselines
Gather Patch Information
Filter & Assign to Endpoints
Review, Approve & Mitigate
Test & Deploy
Document Changes



Identification

Acquisition

Testing

Deployment

Monitoring

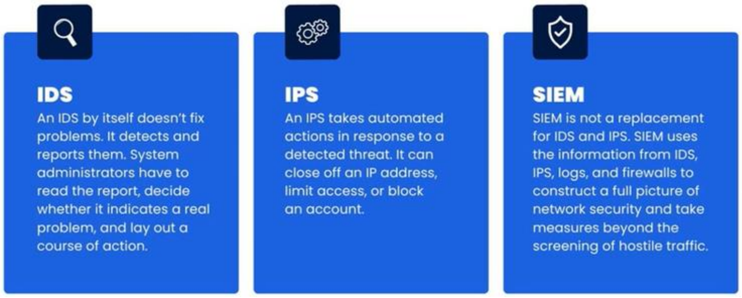
Patch Management Fundamentals

Implementing Continues Monitoring

IDS (Intrusion Detection Systems)

IPS (Intrusion Prevention Systems)

SIEM (Security Information and Event Management)



IDS

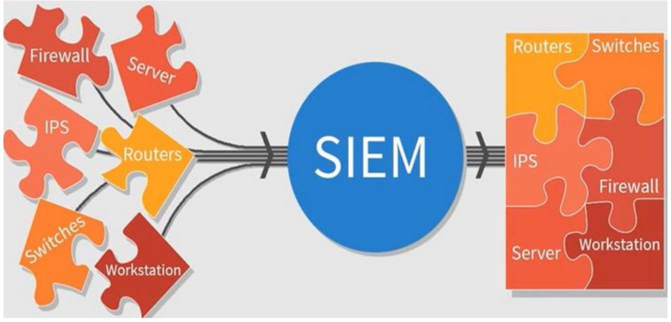
An IDS by itself doesn't fix problems. It detects and reports them. System administrators have to read the report, decide whether it indicates a real problem, and lay out a course of action.

IPS

An IPS takes automated actions in response to a detected threat. It can close off an IP address, limit access, or block an account.

SIEM

SIEM is not a replacement for IDS and IPS. SIEM uses the information from IDS, IPS, logs, and firewalls to construct a full picture of network security and take measures beyond the screening of hostile traffic.



Creating Vulnerability Reports

Identify Vulnerabilities:

Prioritize vulnerabilities:

Document Findings:

Provide Remediation Recommendations:

Include Risk Assessment:

Establish a Reporting Timeline:

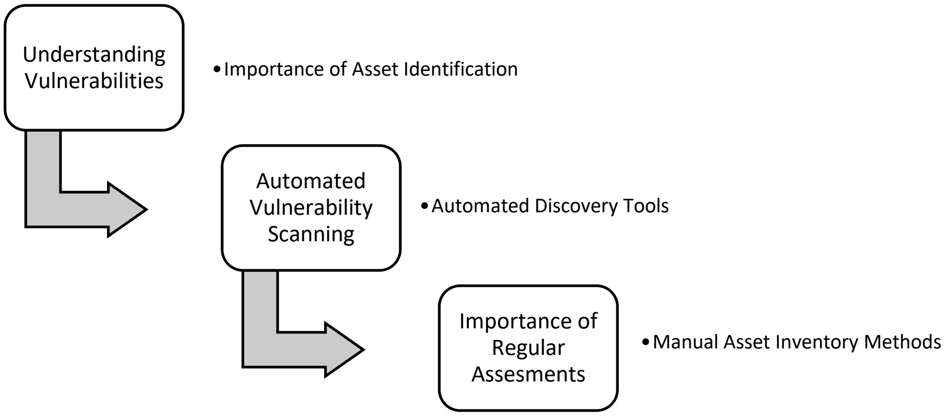
Metrics & KPIs

- Vulnerability Managment Metrics
- Incident Response Metrics
- Compliance Metrics
- Risk Assessment Metrics
- User Awareness Metrics

Navigating the Cybersecurity Landscape.

Understanding the impact of Vulnerabilities

- Consequences of Exploitation
- Financial and Reputational Risks
- Legal Implcations


Understanding Vulnerabilities
Importance of Asset Identification
Automated Vulnerability Scanning
Automated Discovery Tools
Importance of Regular Assesments
Manual Asset Inventory Methods

Security Audits and Assessments

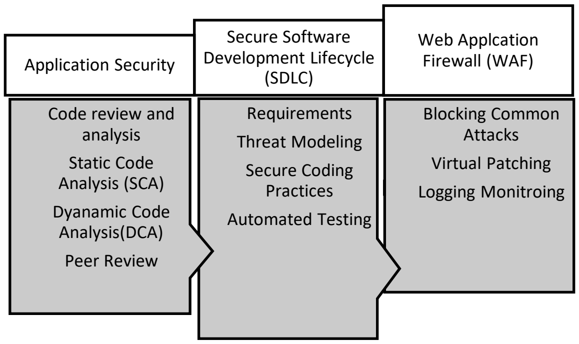
Internal vs. External Audits:

Internal Audits:

External Audits:

Continues Monitoring:

Application Security



Application Security	Secure Software Development Lifecycle (SDLC)	Web Applcation Firewall (WAF)
Code review and analysis Static Code Analysis (SCA) Dyanamic Code Analysis(DCA) Peer Review	Requirements Threat Modeling Secure Coding Practices Automated Testing	Blocking Common Attacks Virtual Patching Logging Monitroing

Iterative Testing

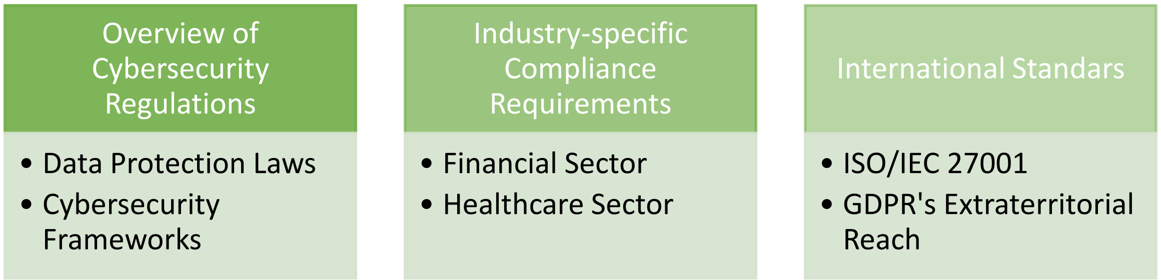
Scheduled Assessments:

Adaptive Strategies:

Collaborative Approach:

Joshua Ortiz
Security Administration Engineer – IT Security Administration

Compliance and Regulatory Considerations



Overview of Cybersecurity Regulations

- Data Protection Laws
- Cybersecurity Frameworks

Industry-specific Compliance Requirements

- Financial Sector
- Healthcare Sector

International Standars

- ISO/IEC 27001
- GDPR's Extraterritorial Reach

User Awareness and Training in Cybersecurity

Role of Users in Security

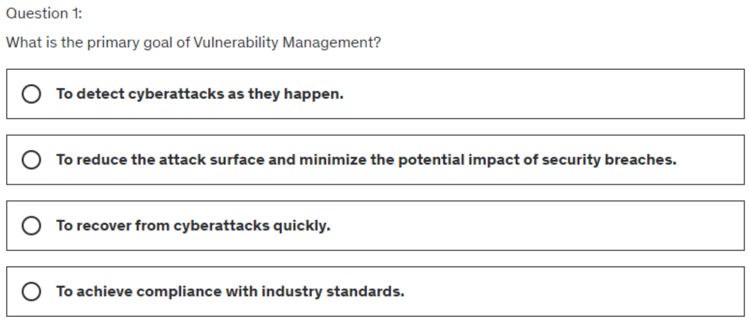
Common Security Pitfalls

Importance of User Education

Ethical Hacking Case Studies	Identifying Vulnerabilities Ethically	Reporting and Remediation
Social Engineering Attack Mitigation	Scope Definition	Vulnerability Assessment
Web Application Security Enhancement	Reconnaissance	Exploitation Details
	Scanning	Risk Assessment

Vulnerability Scanning Software

1. **Nessus:** Comprehensive scanning and assessment.
2. **OpenVAS:** Open-source, network, and web application scanning.
3. **Qualys:** Cloud-based vulnerability management.
4. **Nmap:** Network mapping with vulnerability scanning.
5. **Acunetix:** Web application security.
6. **Burp Suite:** Web application security testing.
7. **Retina CS:** Vulnerability management.
8. **OpenSCAP:** SCAP-based vulnerability assessment.
9. **Nexpose (InsightVM):** Network, OS, and application scanning.
10. **MBSA:** Windows security misconfigurations and updates.



Question 1:

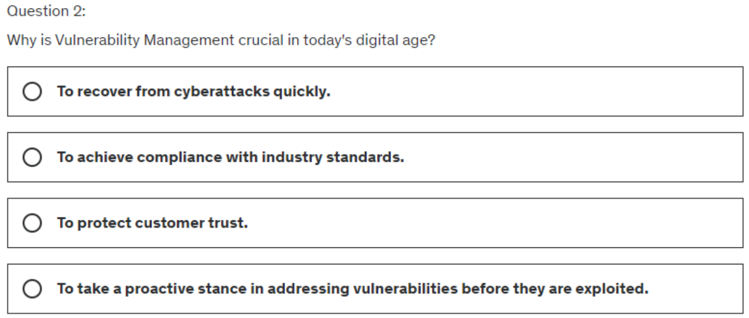
What is the primary goal of Vulnerability Management?

○ **To detect cyberattacks as they happen.**

○ **To reduce the attack surface and minimize the potential impact of security breaches.**

○ **To recover from cyberattacks quickly.**

○ **To achieve compliance with industry standards.**



Question 2:

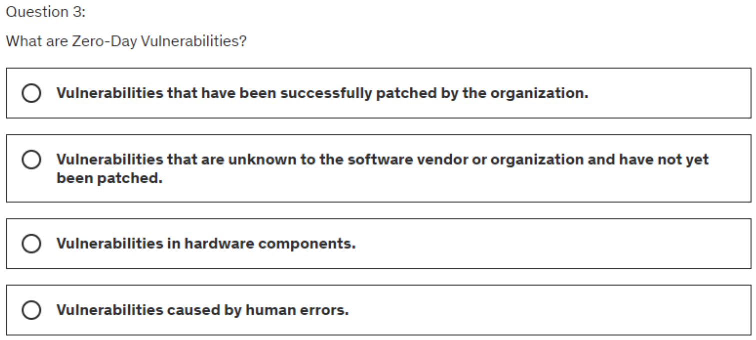
Why is Vulnerability Management crucial in today's digital age?

○ **To recover from cyberattacks quickly.**

○ **To achieve compliance with industry standards.**

○ **To protect customer trust.**

○ **To take a proactive stance in addressing vulnerabilities before they are exploited.**



Question 3:

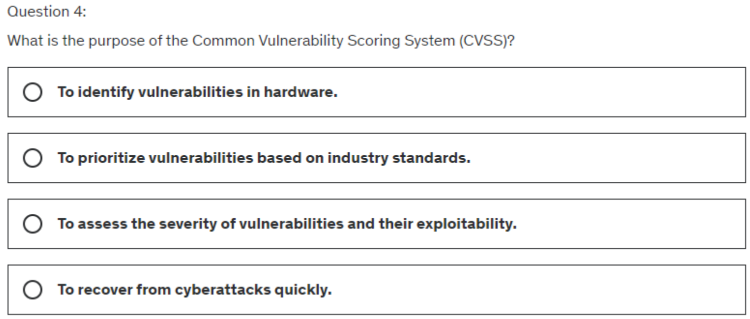
What are Zero-Day Vulnerabilities?

○ **Vulnerabilities that have been successfully patched by the organization.**

○ **Vulnerabilities that are unknown to the software vendor or organization and have not yet been patched.**

○ **Vulnerabilities in hardware components.**

○ **Vulnerabilities caused by human errors.**



Question 4:

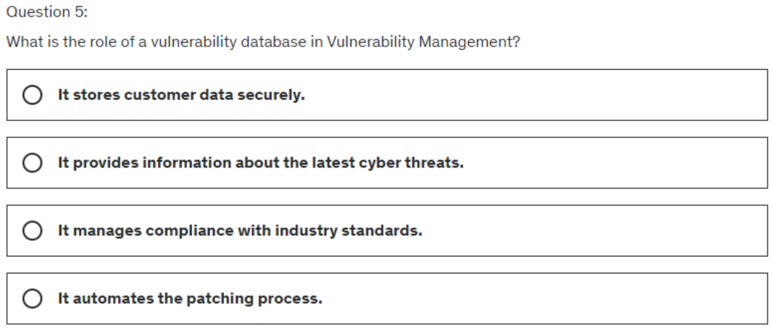
What is the purpose of the Common Vulnerability Scoring System (CVSS)?

○ **To identify vulnerabilities in hardware.**

○ **To prioritize vulnerabilities based on industry standards.**

○ **To assess the severity of vulnerabilities and their exploitability.**

○ **To recover from cyberattacks quickly.**



Question 5:

What is the role of a vulnerability database in Vulnerability Management?

○ **It stores customer data securely.**

○ **It provides information about the latest cyber threats.**

○ **It manages compliance with industry standards.**

○ **It automates the patching process.**