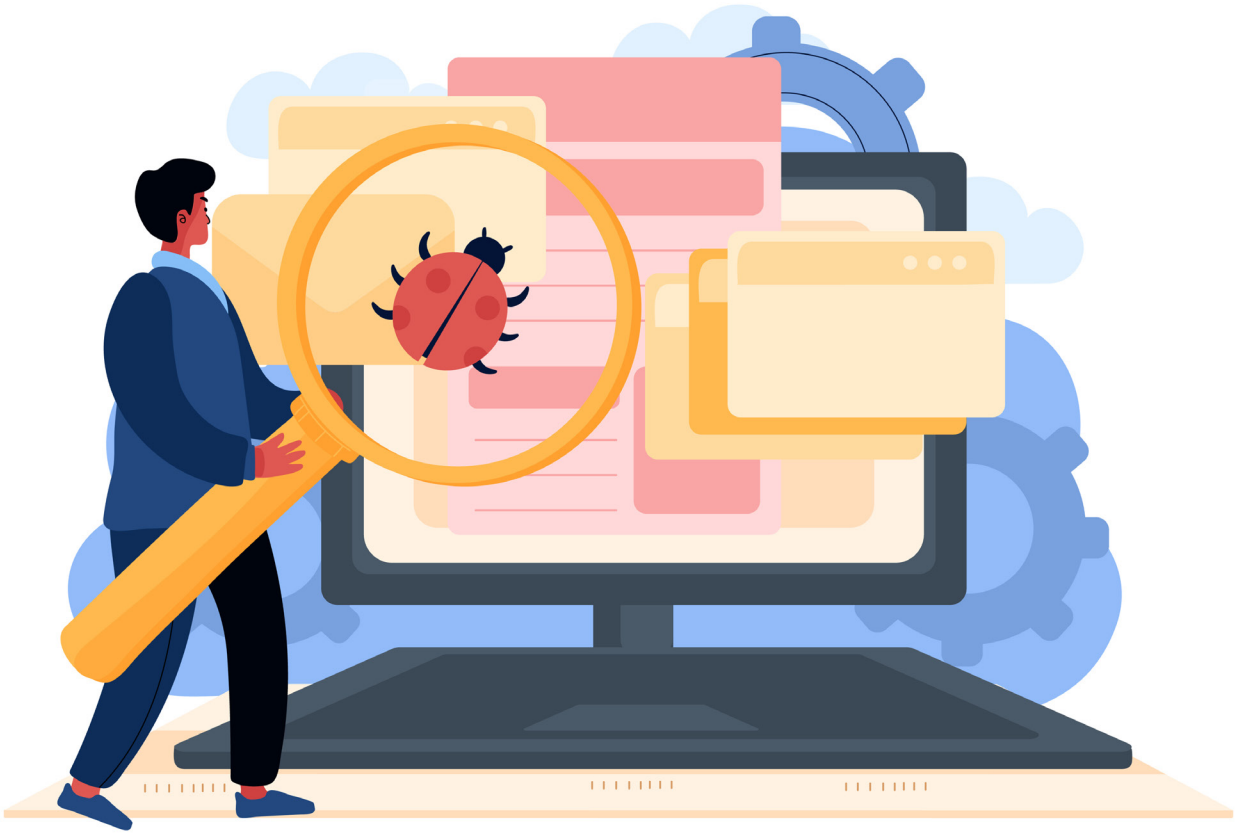
VULNERA™

YOUR TOP 10 VULNERABILITY MANAGEMENT QUESTIONS ANSWERED

Given the complexity of the modern attack surface, organizations are overwhelmed with a flood of concerns about how to protect their organizations from cyberattacks. Not only is there pressure to reorganize priorities around vulnerability management, corporate boards and stakeholders are now taking an active role in developing security strategies.

This eBook was compiled to help organizations like yours to answer ten of the most frequently asked questions related to vulnerability management.

Use the table of contents below to jump to a section that appeals to you.



01

How frequently should I be assessing my network?

With new vulnerabilities published regularly by the National Vulnerability Databases (NVD) and CISA publishing alerts of known exploited vulnerabilities, ICS advisories, or nation state attacks, you should review reported vulnerabilities at least on a monthly basis, preferably weekly or daily. In addition, you should also assess your environment when major changes to infrastructure and internal network security capabilities occur.

Your organization may also be subject to various compliance requirements like PCI, HIPAA, and Sarbanes Oxley. When answering to a regulatory agency or auditor, it is common for them to request evidence of vulnerability management efforts. You will need to provide proof of your existing program.

02

What are the steps in vulnerability management?

The vulnerability management lifecycle is a cyclical and ongoing process in order to strengthen an organization's cybersecurity posture. These are the broad steps in a typical vulnerability management process.

Step 1 - Discover

Inventory the assets which are accessing your network. Get a more detailed understanding of your internal workforce as well as third parties and vendors that interconnect with the company. You cannot protect what you can't see.

Step 2 - Assess

A vulnerability assessment will help you to pinpoint risks these identified assets pose to the environment. Your organization's internal, external, and cloud attack surface is constantly changing, so it is best to continuously assess.

Step 3 - Prioritize

Risk prioritization answers the question of which risks should be remediated first by evaluating the likelihood of exploitation in the environment. Then, those identified as most critical should be targeted for remediation first.

Step 4 - Resolve

The ultimate goal of any security program is to reduce the level of risk within the environment. Eliminating vulnerabilities through patching, or at least reducing the risk through other mitigation controls, is necessary to ensure a successful, long-term fix.

Step 5 - Validate

Testing the effectiveness of your security controls is critical to protecting your environment. It allows you to ensure your security controls are working as intended as well as discovers any additional security gaps or misconfigurations that should be addressed before they can be exploited.

Step 6 - Report

Finally, a thorough report should document the state of affairs in terms of identified and fixed vulnerabilities. This provides critical security information to all levels within the organization as well as helps prove compliance with various regulations.

03

When do I need a vulnerability assessment vs. a pentest?

Penetration testing can be considered the gold standard when it comes to technical cybersecurity assessments – but it's not the best place to start for most organizations.

When determining which you need, a question to ask yourself is whether you are wanting to validate the effectiveness of your controls. Or, do you want to know where issues exist so that they can be fixed. It is more likely the latter.

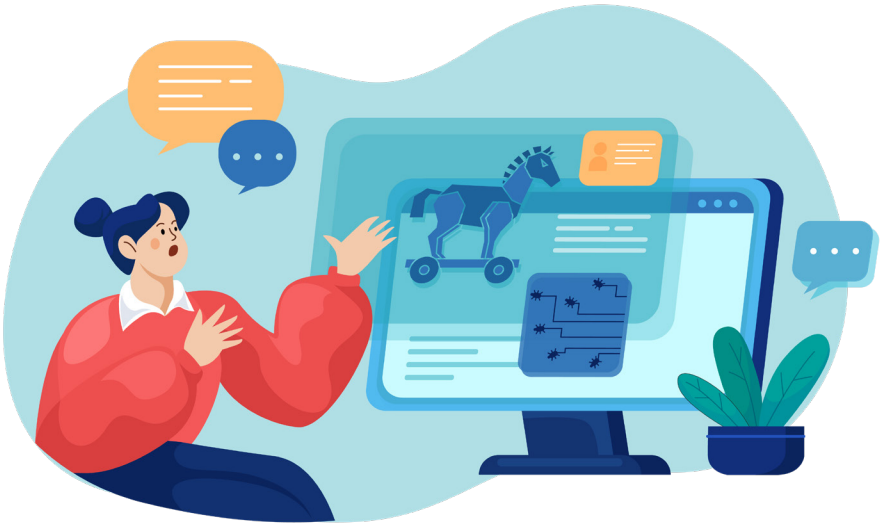
Most organizations start with a vulnerability assessment to identify and resolve security issues. Then after a few months, schedule a penetration test to test security controls.

Another thing to consider is whether you are required to do a penetration test as part of a compliance requirement. These are some common scenarios:

- An audit or compliance mandate (PCI, CMMC, etc) requiring a penetration test
- Aligning to a framework (e.g. NIST CSF, CIS) that requires or recommends a penetration test
- Has an established vulnerability management program and a penetration test is 3rd party validation of the vulnerability management programs health
- A 3rd party requirement to perform a penetration test by name

04

What are the main types of vulnerabilities and how do I address them?



A vulnerability is a weakness in a host or system, such as a missed software update or system misconfiguration, that can be exploited by cyber criminals to compromise your internal, external, and cloud environments. Identifying vulnerabilities is one of the most important steps that an organization can take to improve and strengthen their overall cybersecurity posture.

Vulnerabilities can be broken down into network vulnerabilities, operating system vulnerabilities, and human vulnerabilities.

Network Vulnerabilities

A network vulnerability is a flaw or weakness in the organizational processes, hardware, or software that could result in a security breach. Network vulnerabilities may come in many forms. The most common include:

- **Misconfigured firewalls or operating systems.** When this happens, breaches may occur due to inadvertent exposure of sensitive or internal network services. In some cases, misconfiguration simply relates to the fact that default settings have not been changed.
- **Malware.** This is any type of malicious software, including viruses, worms, or Trojans, that are installed on a host server or user's machine. These days, malware is most commonly delivered through drive-by web browser attacks or after host compromise due to another vulnerability.
- **Unpatched or outdated software.** With this, the systems running applications and services are exposed, potentially allowing for full system compromise with subsequent attacks on the entire network once access to the initial network device is achieved.
- **Social engineering or "Phishing" attacks.** With these, users are "fooled" into providing personal information like their username and password.
- **Credential stuffing attacks.** This is when attackers use credentials they've acquired in a previous breach to continue to break into additional user accounts.

You must address these factors when assessing the security of your systems. If left unchecked, it may lead to more advanced attacks which

Operating System Vulnerabilities

In operating system vulnerabilities, malicious actors typically exploit to gain access to an asset on the operating system (OS) that is installed or to cause damage in another manner. Some common examples include superuser or admin accounts that may be present on OS installs or control of administrative features (user management, application installation, antivirus disable, etc).

There are several types of these vulnerabilities, including:

- **Remote code execution.** Commonly called RCE, this type of vulnerability lets attackers run arbitrary code remotely on vulnerable workstations or servers.

- **Denial-of-service.** Also called DoS, this is a serious threat that makes individual hosts, network services, or sometimes the entire network to not function properly. There are two types of DoS attacks:
  - **Flood attacks.** The system receives excessive requests, causing a significant slowdown and eventual stop.
  - **Crash attacks.** Work by exploiting vulnerabilities causing a service or system to crash.

- **Elevation of privilege.** Also called EoP or privilege escalation, it allows attackers authorization permissions beyond what had been granted.

- **Information disclosure.** Hackers capture personal information and disclose it.

- **Spoofing.** This is a process that includes impersonating someone by tampering with the authentication processes in place.

One of the most effective ways to avoid dealing with operating system vulnerabilities is by ensuring that all operating systems are "patched" meaning that new updates, bug fixes, or added security patches from the developers are automatically installed.

Human Vulnerabilities

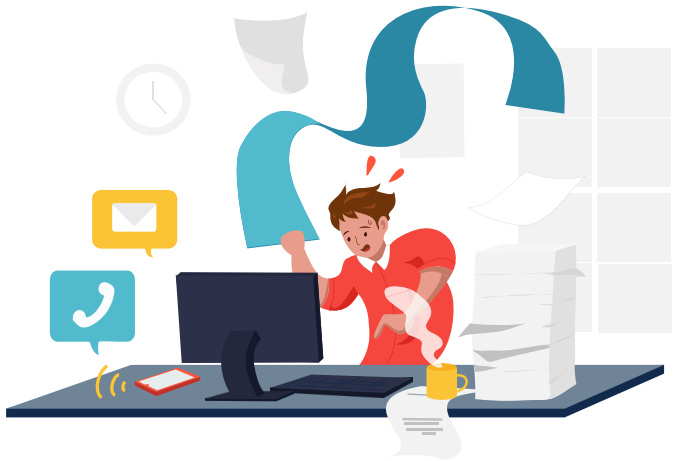
People represent one of the main weaknesses of cybersecurity. In fact, human vulnerabilities can cause much more damage and be more costly than any of the other vulnerability types on this list. Even though advanced hacking skills and powerful malware bolster the capabilities of a cyber attacker, it is, in the end, humans that represent the only un-patchable risk in cybersecurity.

Some of the human vulnerabilities that exist today include:

- **Social engineering.** Defined as the art of gaining access to data, systems, or buildings by exploiting human psychology.

Today, most cyberattacks utilize several social engineering techniques, ranging from phishing to the strategic placement of devices like USB charging outlets or flash drives that access data or upload malware without the user realizing it.

One of the best ways to do reduce this risk is by investing in regular cybersecurity or security awareness training. When users are aware of the vulnerabilities and possible manipulation methods, they are more prepared to deal with the situations when they present themselves.



05

What is the difference between remediation and mitigation?

While the terms “remediation” and “mitigation” are often used interchangeably, they are different.

Remediation is the process of eliminating detected vulnerabilities in your network. This is often accomplished through patching. Making yourself aware of the typical patch release schedule from relevant companies like Microsoft and VMware can help reduce your exposure to cyberattack. CISA also releases regular updates and keeps a catalog of Known Exploited Vulnerabilities.

But, there are instances in which patches are not feasible.

- The patch has not been released by the vendor. It takes time to prepare and distribute them so there may be some delay in patching.
- The patch may create additional problems across the network – or bring it down altogether

Mitigation, on the other hand, is more like damage control. The vulnerability cannot be eliminated immediately but it can be minimized. This is often a temporary solution or workaround to decrease the possibility of the vulnerability being exploited.

Examples of mitigation include:

- Disabling the software temporarily
- Blocking a port on a firewall
- Removing unneeded or unexpected hardware

REMEDIATION	MITIGATION
Remediate means to correct or improve a deficiency or a problem.	Mitigation means to reduce, lessen, or decrease.

Additional mitigation strategies can be found in NSA’s Top Ten Cybersecurity Mitigation Strategies document.

06

What is vulnerability management vs. patch management?

While vulnerability management and patch management are closely related, they are distinct processes with different goals.

Vulnerability management is a cyclical process of discovering, assessing, prioritizing, remediating, validating, and reporting security vulnerabilities across an organization's endpoints and systems. IT teams conduct this process continuously to keep up with new assets and applications added to the network, changes made to systems, and the discovery of new security threats over time.

Patch management, on the other hand, is a process to update applications and operating systems. It is a software update from a vendor that can include anything from security fixes to new software features. It is just one part of vulnerability management.

	Vulnerability Management	Patch Management
Purpose	Manage all vulnerabilities	Manage software patching
Functions	Discover, assess, prioritize, remediate, validate, and report vulnerabilities	Patch or upgrade software to remove security holes, fix bugs, and add features
Key Steps	▪ Inventory systems and software ▪ Scan networked systems ▪ Identify vulnerabilities ▪ Assess and prioritize vulnerabilities ▪ Remediate (patch or reconfigure) ▪ If fix is unavailable or doesn't work, mitigate or accept risk ▪ Validate controls were effective ▪ Report (dashboard, analytics, compliance	▪ Inventory systems and software ▪ Standardize software versions ▪ Discover and acquire patches ▪ Test ▪ Create and approve plan ▪ Install ▪ Document

07

How often should I be patching?

CISA provides guidance around remediation timelines, but most organizations maintain their own internal SLA for how fast an issue should be remediated, based on acceptable risk.

CISA recommends the following remediation timelines:

- Critical vulnerabilities should be remediated within 15 calendar days of initial detection.
- High vulnerabilities should be remediated within 30 calendar days of initial detection.
- If vulnerabilities cannot be remediated within the recommended timeframes, develop a remediation plan for action and coordination across the organization.

The remediation plan should include:

- Vulnerability remediation constraints
- Interim mitigation actions to overcome constraints
- Final actions required to remediate vulnerability

> ***"60% of data breaches are caused by a failure to patch. If you correct that, you've eliminated 60% of breaches".***

CISA has recently published the Stakeholder-Specific Vulnerability Categorization Guide (SSVC) designed to assist in prioritizing the remediation of a vulnerability based on the impact expolitation would have to the organization.

08 What do CVSS scores mean?

The Common Vulnerability Scoring System (known as CVSS Scores) provides a numerical representation of the severity of an information security vulnerability. This score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help assess and prioritize vulnerability management processes.

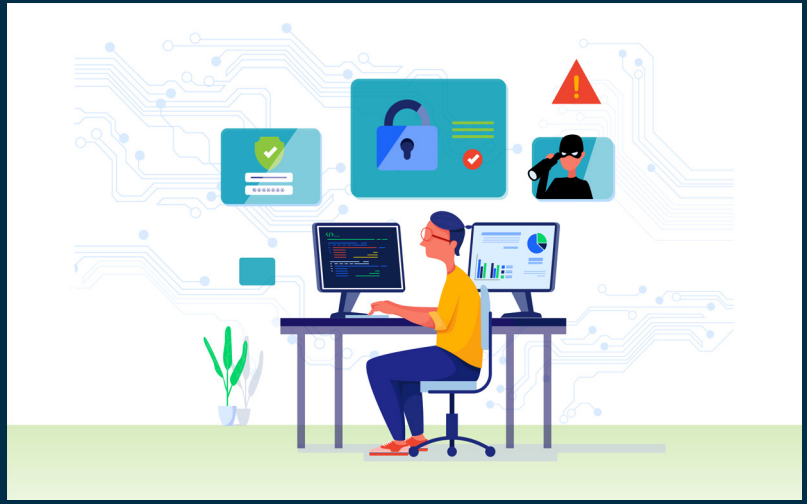
While they are useful in prioritizing risk, their value is limited due to the fact this number does not reflect the risk the vulnerability poses to your environment. In other words, CVSS answers the question, "Is this dangerous?", but not "is this dangerous to my organization".

> ***"Research shows that 2 to 5% of your vulnerabilities will be exploited, but CVSS can assign as many as 40% a score of 7 or higher."***

In the end, CVSS alone cannot be used to measure and quantify cyber risk. CVSS does not allow stakeholders to properly understand a vulnerability's impact, nor does it provide the information needed to create a proper remediation strategy.

At VULNERA, we use CVSS to measure the criticality of attack scenarios and then add the contextual information including information regarding exploitability. Our VSCORE evaluates:

- Active exploits available on the internet or in exploit packs
- Are remotely exploitable
- Often result in arbitrary code execution
- Being used in known exploit campaigns
- Have active advisories from vendors and regulating bodies



09

Is agent-based or agentless scanning better?

Proactive identification and remediation of vulnerabilities are critical to the strength of any cybersecurity program. But where do you start? You know you need vulnerability scanning, but how do you know what solution best fits your needs?

Vulnerability scanning comes in both agent-based or agentless scanning – or a hybrid of the two. Which to choose depends on your environment and your organizational needs. Let's explore both options.

Agent-Based Scanning

Agents are a software package deployed to each asset to collects data. The agent passes data back to a collection server which is then aggregated for analysis including identification of vulnerabilities.

Works best for: Environments that are widely distributed, have numerous remote workers, or devices that are seldom connected to the network.

Advantages:

- Designed to circumvent the need for credentials as the agent is installed directly on a device
- Assets using dynamic addressing or that are located offsite behind private subnets can still be scanned
- Ability to scan personal devices

Challenges:

- Operating system dependent and generally cannot scan network assets like routers, switches, firewalls and printers
- Administrative overhead as new devices are added and must have agents installed

Agentless Scanning

Does not require agents to be installed on each asset and instead reaches out from the server to the asset. This lightweight method for scanning for vulnerabilities eliminates installing and managing additional software on all devices.

Works best for: For all environments, agentless scanning leverages a blackbox approach – meaning unknown assets will be identified on the network, regardless of whether its in a known inventory.

Advantages:

- Agentless scanning may provides some gap data that isn't stored on the device
- Ability to identify and scan assets that may be missed by agent-based scanning
- No OS compatibility requirements

Challenges:

- A consistent network connection is required so remote assets are not accessible for scanning
- Does not have the depth of visibility into local system vulnerabilities

10

Why is remediation validation important?

Vulnerability management is more than just scanning and detecting vulnerabilities. The ultimate goal of any program is to reduce the level of risk within your environment.

Vulnerability management is a cyclical process that includes discovery, prioritization, remediation, and monitoring to ensure a successful, long-term fix.

How this is accomplished will be influenced by the cybersecurity framework that your organization has chosen to use. Often this is dictated by the type of operation that you run. Some of the well-known and popular frameworks used by organizations include NIST, PCI DSS, and CMMC.

Testing the effectiveness of your security controls along with ongoing monitoring of the environment is critical to protecting your network from cyberattacks.

Remediation Validation helps security teams by:

- Ensuring that any security controls in place are actually working as required
- Discovering any additional security gaps, so they can be addressed before they can be exploited
- Identifying if misconfigurations may have occurred which may result in new threats and vulnerabilities
- Monitoring when issues are closed and gives insight into actions taken to reduce risk

VULNERA™

www.vulnera.com

EB1022 REV A 202211