digitaldefense
by HelpSystems

9 Vulnerability Management Pitfalls to Avoid

Vulnerability management (VM) can seem unmanageable at times. But the key to successful VM is working simply and strategically. If you approach VM practically and prioritize appropriately, you can keep the number of your resulting tasks at a very manageable level.

As with any on-going security practice, there are countless ways you can botch VM, making it inefficient or ineffective. That's why it's a good practice to step back and evaluate your vulnerability management program from end to end. Below we list a few common pitfalls organizations need to avoid when it comes to vulnerability management.

Vulnerability Scanning Slipups

Limited scanning

Are you limiting your scanning to server-only or external-only scans? If so, you are missing the big picture. It's important to examine both internal and external assets so you can make informed decisions

Incomplete scanning

If you aren't using an up-to-date Configuration Management Database (CMDB), your scans could be inadvertently skipping vital assets. Be sure your CMDB is a complete and accurate representation of your assets and their interdependencies. This will help prevent the creation of scanning blind spots.

Wasted scanning

Are you running scans and ignoring the results? Perhaps you put off remediation because your team is small with limited bandwidth. Using risk context and threat intelligence can help you prioritize and shorten your to do list to those vulnerabilities most critical to your unique organization.

Restricted Scanning Results

Refusing to whitelist your vulnerability scanner leads to an inaccurate read on potential vulnerabilities. A firewall can see scanning results as malicious and therefore deny scanner traffic. This will give you artificially positive results and a false sense of security.

Careless Vulnerability Resolution

Mismanaged Scanning Results

Have you been tossing giant lists of unprioritized, unvetted vulnerabilities to your team? If so, you are most likely "helping" them become less effective. Don't overwhelm your team. Use agreed upon criteria in conjunction with a risk-based vulnerability management tool so you can sort, filter, and prioritize lists before they're handed over.

Mitigation Without Remediation

Are you just performing fixes or stop-gap measures without any cause analysis? When addressing vulnerabilities, you must identify how they arose to avoid reoccurrence. Addressing the root of the issue rather than each instance will set your team up for successful remediation.

Endless exceptions

Do you have a list of exceptions that don't have an expiration date? If so, you could be permanently ignoring some vulnerabilities that still require remediation. Be sure to assign expiration dates and avoid creating an ever-growing list of vulnerability exceptions with endless shelf lives.

Needless VM Complications

Complicated vulnerability management is a thing of the past. Choose an easy to use VM solution with robust filtering, sorting and ranking capabilities that can help you effectively prioritize tasks and maximize your IT team's productivity.

Learn how Frontline Vulnerability Manager™ (Frontline VM™) from Digital Defense combines powerful technology with a user-friendly interface to simplify and streamline your VM efforts.