

What Vulnerability Management Actually Is (and Why You're Doing It)

Wed, Aug 12, 9:00 AM EDT · <https://scottslab.io/posts/vulnerability-management-fundamentals>

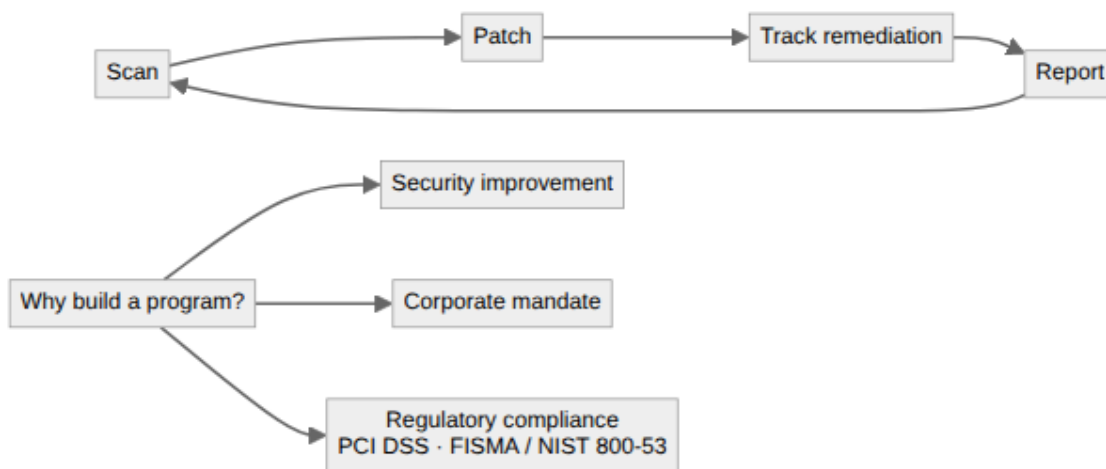


TL;DR

Vulnerability management is the whole loop, not just the scan: find issues, apply patches, track remediation, and report on it. Programs get built for one of three reasons: general security improvement, a corporate mandate, or regulatory compliance. The driver shapes everything. When it's compliance, the regulation writes your requirements for you: PCI DSS demands quarterly internal and external scans (external via an approved vendor) with a rescan-until-clean rule; FISMA/NIST 800-53 wants regular scans and remediation of real findings.

People collapse "vulnerability management" down to "running Nessus," and that's the smallest part of it. The actual program is a loop: scan to find the issues, apply patches, track remediation so nothing falls through the cracks, and report on where you stand. Scanning without the tracking and the reporting is just generating anxiety on a schedule.

Before you build one, it's worth being honest about *why*, because the driver shapes the whole thing. There are three. The first is plain security improvement: you want to find and fix your weak spots. The second is a corporate policy or mandate. Leadership or a customer contract requires it, which usually comes with strings attached: specific tools, deadlines, centralized reporting. The third is regulatory compliance, and that's the one that stops being optional.



When compliance is the driver, the nice thing is the regulation writes your requirements for you. PCI DSS, for anyone touching cardholder data, is explicit: quarterly internal and external scans, external scans run by an Approved Scanning Vendor, a requirement to rescan until you get a clean result, and a fresh scan after any significant change. There's no ambiguity to argue about. The standard hands you the cadence and the bar. FISMA and NIST 800-53 do the same for federal systems: regular vulnerability scanning and risk-based remediation of legitimate findings, under control RA-5.

The reason to name your driver out loud is that it sets your floor. A security-improvement program can be pragmatic and risk-based. A compliance program has a minimum you cannot go under no matter how you feel about a particular finding. "We decided it wasn't worth patching" is a fine sentence right up until an auditor holding the PCI DSS text disagrees. Know which game you're playing before you tune the rest of the program.