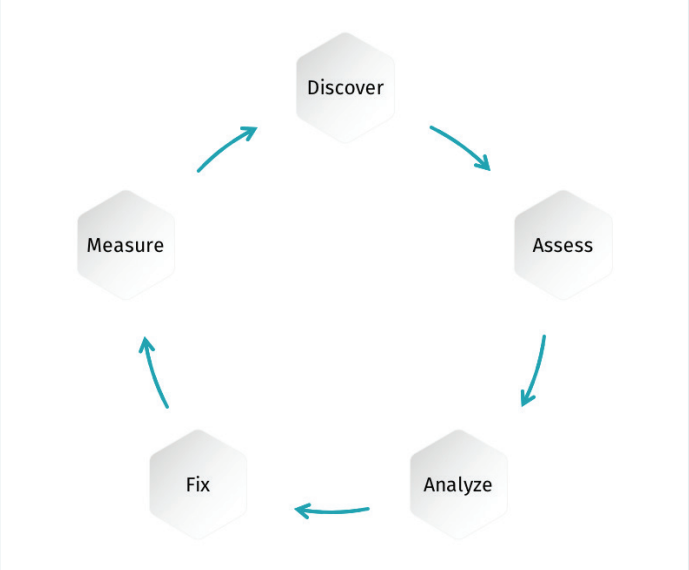
SOLUTION BRIEF

tenable

# Vulnerability Management: Fix

Vulnerability management is an essential part of any organization's security program, and it is foundational to Cyber Exposure, an emerging discipline for managing and measuring cybersecurity risk in the digital era. A mature vulnerability management (VM) program includes all five steps in the Cyber Exposure Lifecycle shown below.




*Cyber Exposure Lifecycle*

This Solution Brief focuses on Fix, the fourth step of vulnerability management.

The Fix objective is to apply the appropriate remediation to remediate exposures that you prioritized in the Analyze phase.

## Key Benefits

- **Reduced attack surface** resulting from remediation of high priority vulnerabilities and misconfigurations.
- **Operational efficiency** gained by providing staff with specific documentation of each exposure and its required remediation.
- **Confidence** that remediation was implemented as expected.

# Challenges

The Fix step is challenging because commonly the staff responsible for identifying and prioritizing exposures must hand off remediation to a completely separate Operations team. Despite good intentions, the hand-off is error-prone. Unclear expectations and instructions often undermine Operations' ability to remediate exposures as required.

Successful remediation requires:

- Clear documentation, including supporting evidence that clearly communicates the exposure to the specific Operations staff members who are responsible for remediation.
- Clearly documented steps Operations must take to fix the exposures.
- Confirmation that fixes were implemented as required.

# Solution

Development of a mature process to Fix exposures typically progresses through four levels.

### LEVEL 1. SEND VULNERABILITY REPORT(S) TO IT OPERATIONS

Unfortunately, many organizations create and distribute a monolithic vulnerability report that includes all vulnerabilities for all assets. Depending on your organization's size, the report can easily be tens of thousands of pages. Such reports are not actionable and rarely result in timely remediation.

At level 1, you fix high and critical vulnerabilities only, not lower priority vulnerabilities and not misconfigurations. Ideally, you will narrowly scope vulnerability reports to include only assets managed by a specific IT Operations staff member. You can generate multiple reports, each for a specific staff member.

### LEVEL 2. CLOSED LOOP REMEDIATION

At this level, you implement an efficient, closed-loop Assess-and Fix process using focused reporting and remediation scanning.

Focused reporting uses the Vulnerability Priority Rating (VPR) to zero in on the highest priority vulnerabilities. This tells IT Operations what to fix first to reduce risk. Focused reporting also groups data by asset owner/administrator so each responsible person knows what must be done. If you have previously accepted the risk of a given vulnerability or selected a compensating control for it, that vulnerability will be excluded from the report.

Remediation scanning evaluates specific tests against a specific target or targets where the related vulnerability was present in an earlier scan. Remediation scans allow you to validate whether your vulnerability remediation actions on the targets have been successful. If a remediation scan cannot identify a vulnerability on targets where it was previously identified, the system changes the status of the vulnerability instances to mitigated.

Additionally, Tenable platforms integrate with leading patch management systems to correlate their patch status reports with vulnerability scan results. Correlating patching with scan results helps you identify patching gaps.

### LEVEL 3. SLA-DRIVEN REMEDIATION AND MITIGATION

At level 3, you perform vulnerability and misconfiguration remediation according to requirements defined in the SLA for each asset class. The following table is an example of how you could define specific Fix SLAs for different asset classes.

| | HIGH Criticality Assets | MEDIUM Criticality Assets | LOW Criticality Assets |
|---|---|---|---|
| Vulnerabilities | | | |
| VPR 9.0-10.0 | 1 day | 3 days | 2 weeks |
| VPR 5.0-8.9 | 3 days | 1 week | 1 month |
| VPR <5.0 | 1 week | 2 weeks | 1 month |
| Misconfigurations | | | |
| Critical Impact | 1 day | 3 days | 2 weeks |
| Moderate Impact | 3 days | 1 week | 1 month |
| Low Impact | 1 week | 2 weeks | 1 month |

## ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.

### LEVEL 4. PERIODICALLY REVISE SLAS

At this level, you can use status reports to help evaluate SLA performance. If SLAs are consistently unmet, you can modify them or develop a corrective action plan to meet them. Additionally, the business processes supported by IT and OT infrastructure are dynamic. For example, a web application may evolve to contain sensitive customer information, or a manufacturing line may generate an increasingly significant percentage of revenue. Therefore, you must periodically review asset criticality to determine if it has changed.

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**