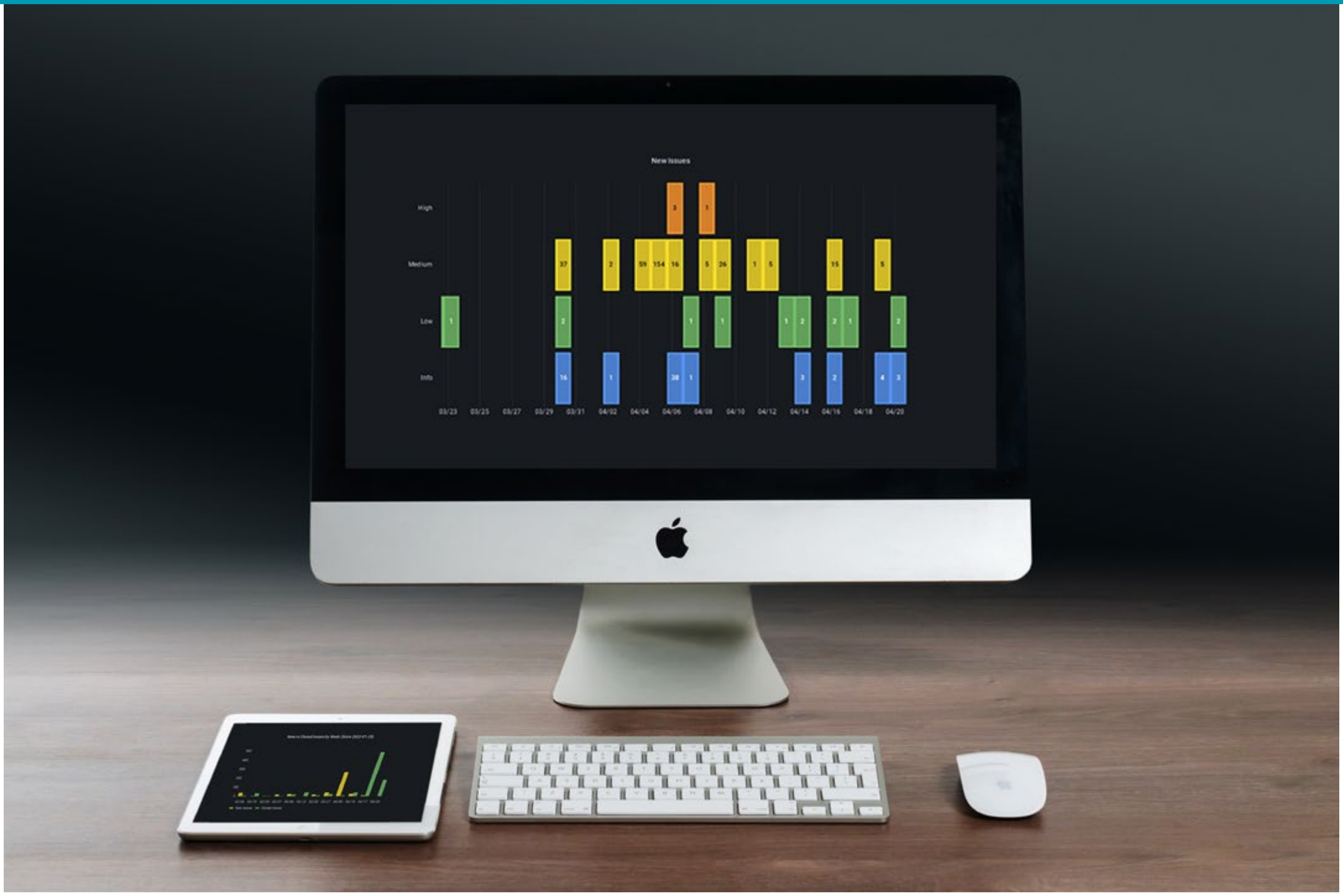
SOLUTION BRIEF

REMEDIATION TRACKING

Assess the Success of your Remediation Efforts



Remediation Tracking

Vulnerabilities provide openings for attackers to enter your systems. Once exploited, they can steal data, deny access to services, and abuse resources. Identifying and fixing security vulnerabilities is a continuous process. Risks can change daily – and bad actors are not taking a break in finding innovative ways to exploit vulnerabilities.

When creating a vulnerability management program, there are several stages that should be planned and documented:

- Assessment of the environment
- Classifying and prioritizing vulnerabilities
- Mitigation activities
- Remediation validation and reporting

Vulnerability management is not always as easy as scanning, patching, and validating. When a vulnerability has been remediated, it's important to retest to ensure that it has been corrected. Fixes may be more complex than applying a simple patch.

Mitigation actions may include policy, process and procedure modifications, security architecture changes, deployment of new security technologies, and deployment of OS and application patches. It may take several iterations of change requests and final approvals before remediation is complete.

Plus, various audits, standards, and regulations require various testing and reporting to ensure compliance.

Solution Overview

VULNERA's remediation tracking feature helps organizations with automated tracking and validation that vulnerabilities have been successfully remediated. Retesting focuses on outcomes – and on your success.

Continuous assessment of the target environment tracks the lifecycle of vulnerabilities – whether they are still open, being retested, or if the issue has been closed. Reported within the real-time dashboard, security teams and other stakeholders can understand the status at any point in time.

Remediation tracking also provides independent confirmation that mitigation efforts are working – so that compliance can be maintained across the environment.

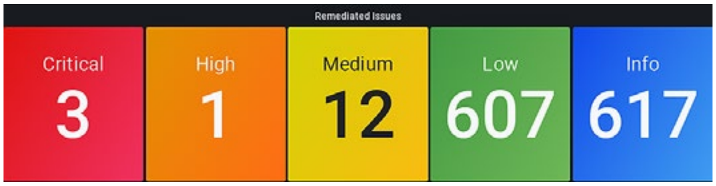
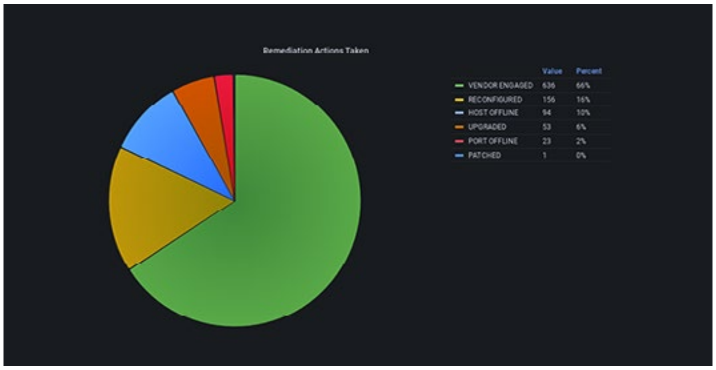


Figure 1. Counts of Remediated Issues by Severity Level



	Value	Percent
VENDOR ENGAGED	636	66%
RECONFIGURED	156	16%
HOST OFFLINE	94	10%
UPGRADED	53	6%
PORT OFFLINE	23	2%
PATCHED	1	0%

Figure 2. Remediation Actions Taken

How It Works

After every scan completes, a retest of the environment is conducted and remediation testing activities are tracked and updated, including the observed remediation reason. A dedicated dashboard highlights resolved issues accompanied with the remediation reason and confidence level. Additionally, new vulnerabilities may be uncovered during follow-up security tests.

Remediation tracking helps answer the questions:

- Did the patch resolve the issue?
- How many issues were closed with the patch?
- How and why was the issue closed?

Each vulnerability has its own audit trail including what remediation actions were performed and when. The environment continues to be monitored for additional instances of the vulnerability. Additional instances may indicate that the root cause has not been addressed.

Retesting (and tracking of any issues) monitors for changes in the environment, including:

- Changes in permissions
- Newly disabled or enabled services
- Disrupted services
- Appliance failures / misconfigurations

In addition, remediation activities are reported against prescribed SLAs so teams know how many issues are in violation of SLA policies.

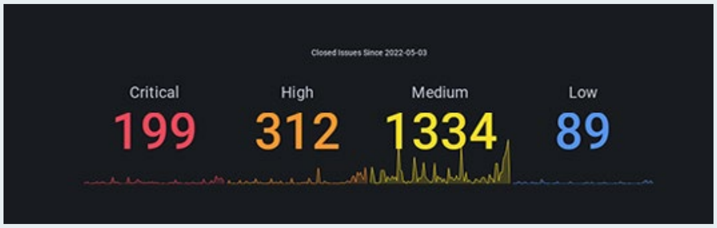
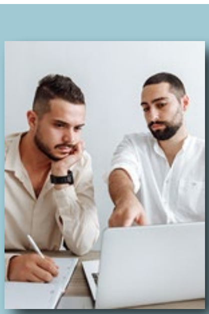


Figure 3. Closed Issues

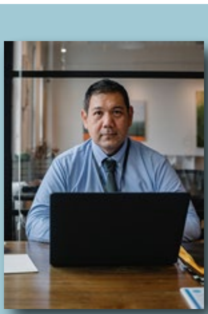
Validate Security Controls are Effective

No matter your role on the team, remediation tracking helps satisfy the needs of executives, technology and security teams, and operations and project management teams.



For IT & Security Teams

- Requires little manual intervention beyond remediation
- Automation closes the risk-remediation feedback loop, enabling autonomy amongst team members
- Dashboard provides real-time and historical tracking of closed issues



For CISOs

- Provides insight into cyber threats and remediation progress
- Improves decision-making based on real-time vulnerability intelligence
- Answers stakeholder questions regarding security and operational risk

For Risk & Compliance Teams

- Monitors when issues are closed and provides insight into actions taken
- Meets reporting requirements and fulfills multi-test requirements for various regulations
- Simplifies teamwork and reduces time spent manually managing the process

About VULNERA

Security assessments should empower companies to achieve compliance while also improving the security of the organization. The industry is riddled with variances in quality, fragmented offerings, logistical constraints, and resource limitations. That's why VULNERA has built vulnerability management solutions that help organizations with the heavy-lifting so stakeholders can focus on what matters – remediating security issues.

CONTACT

To learn more about how VULNERA's remediation tracking and other security challenges, please visit www.vulnera.com or call +1 626.515. 5523 for a discussion with a vulnerability expert.