VULNERA™

SOLUTION BRIEF

VULNERABILITY INTELLIGENCE

Vulnerability Management Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs)

Vulnerability Intelligence

Security metrics provide quantitative data that you can use to support your vulnerability management program. These metrics help you make the right decisions as it pertains to your strategy and the future of your program.

There are many real-time and historical metrics which you may choose to track regularly. But you can only analyze and manage the vulnerabilities that you are aware of. VULNERA solutions give you continuous asset and service discovery to help identify what is connecting to your internal, external, and cloud networks.

The data collected is aggregated over the assessment period to identify new, open and resolved vulnerabilities. It is then categorized, classified, analyzed, and assigned a risk score to help security teams prioritize the most critical vulnerabilities for mitigation and remediation. This vulnerability intelligence helps organizations track trends over time and to reduce overall risk.

VULNERA's real-time dashboard enables teams to create a report to satisfy the needs of your executives, technology and security teams, and operations and project management teams. It provides insight into the week-to-week, month-to-month and year-to-year progress, without requiring domain-specific knowledge.

Our solutions go a step further than traditional solutions by retesting the environment, validating that remediation activities have been successful, and reporting your success via the dashboard – saving you valuable time and resources tracking activities via spreadsheets.

Quantitative Indicators

The most common and important types of KPI. They are easy to understand because they are measurable characteristics represented as a number.

- Number of assets (e.g., Windows, Linux servers, workstations, applications, etc.)
- Number of vulnerabilities per type (low, high, critical, exploitable)
- Number of scanned IP addresses / networks
- Number of internet-facing assets, applications
- Number of internal, external and cloud servers, applications

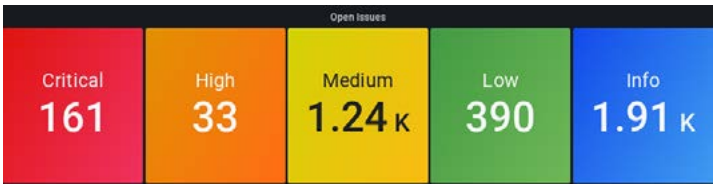

Figure 1. Counts of Open Issues by Severity Level

Figure 2. Counts of Remediated Issues by Severity Level

Key Risk Indicators

Critical predictors of unfavorable events that could adversely impact organizations. They monitor changes in the levels of risk exposure and contribute to early warning signs that enable you to report risks, prevent crises, and mitigate them in time.

- Number of open vulnerabilities: total number of applicable vulnerabilities that are not yet analyzed or have work in progress
- Percentage of numbers of open vulnerabilities related to closed issues in a month
- Status and the number of vulnerabilities per asset: status of the remediation progress
- Overview of the remediation solution type: indicate the number of the remediation solution types (patch, config change, etc.)
- Number of open vulnerabilities per site

Figure 3. Exploitability Risk Factors

Figure 4. SLA Violations by Severity

Input Indicators

Used to measure resources needed for a business process or project. They are necessary for tracking resource efficiency and to help determine if additional funding or extra staff may be needed.

- Time to resolve or remediate a vulnerability
- Items needed to resolve the vulnerability or to patch systems

Figure 5. Mean Time to Resolution (MTTR)

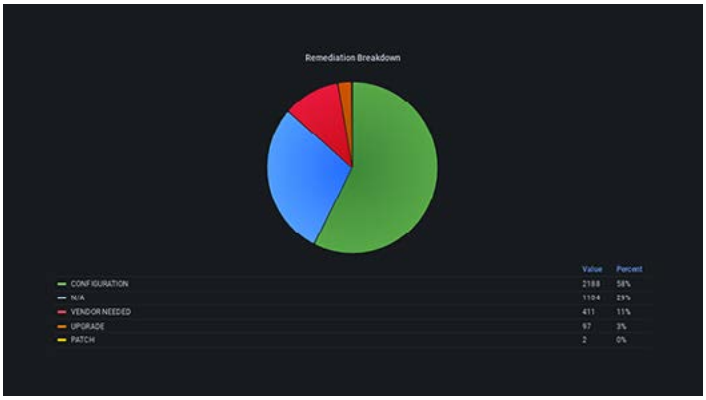

Figure 6. Remediation Actions Required

Output Indicators

Used to measure resources needed for a business process or project. They are necessary for tracking resource efficiency and to help determine if additional funding or extra staff may be needed.

- Number of vulnerabilities remediated (also by criticality, system type, etc.)

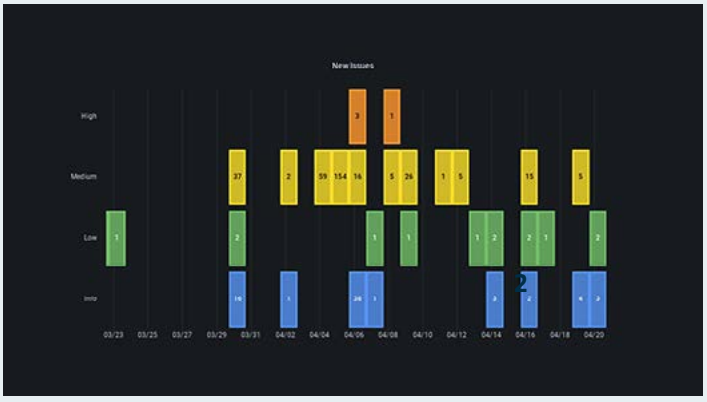

Figure 7. Remediation by Day and Severity

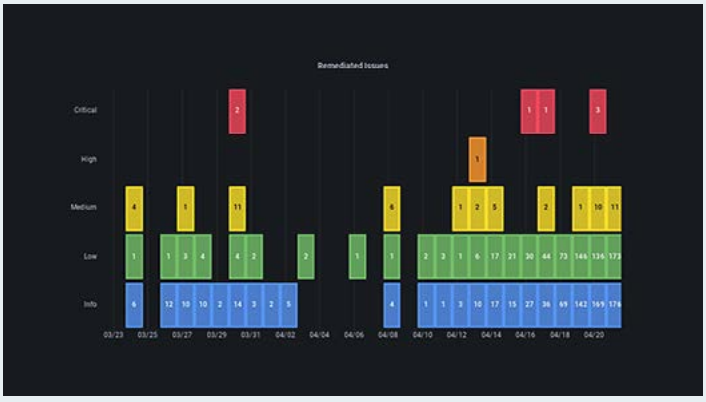

Figure 8. New Issues by Day and Severity

Leading Indicators

Used to predict the outcome of a change in a process and confirm long-term trends in the data.

- Trends such as increasing or decreasing number of found vulnerabilities
- Trends in the criticality of a vulnerability

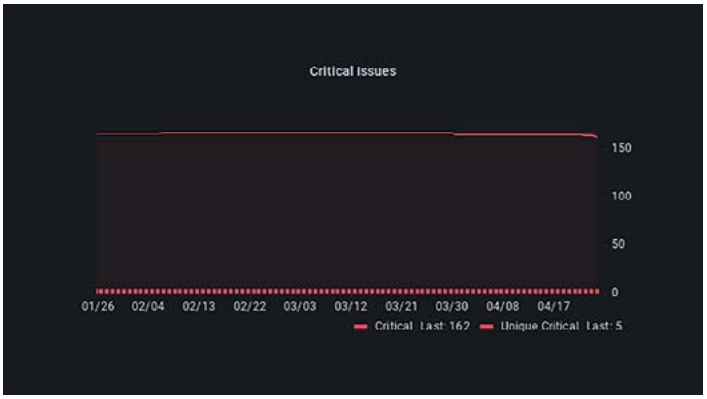

Figure 9. Total and Unique Issues by Severity and Day

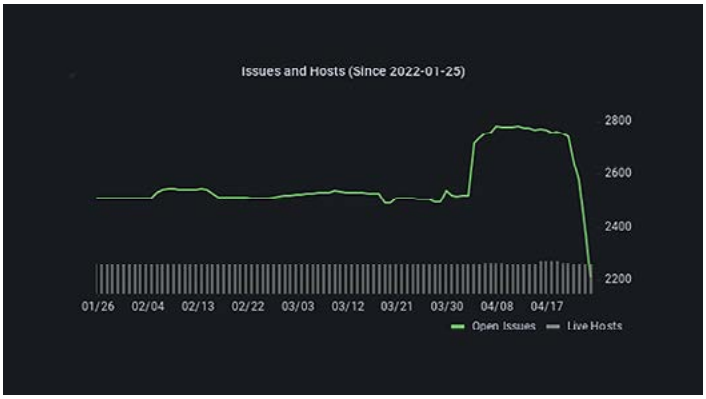

Figure 10. Issue and Host Count by Day

Lagging Indicators

Compares your current performance against your past performance. Used to measure results after an action has taken place to reflect upon the success or failure of that initiative.

- Results at the beginning of a time frame (found vulnerabilities at the beginning of scan)
- Results at the end of a time period (e.g. remediated vulnerabilities at the end of week/month)
- Historical data

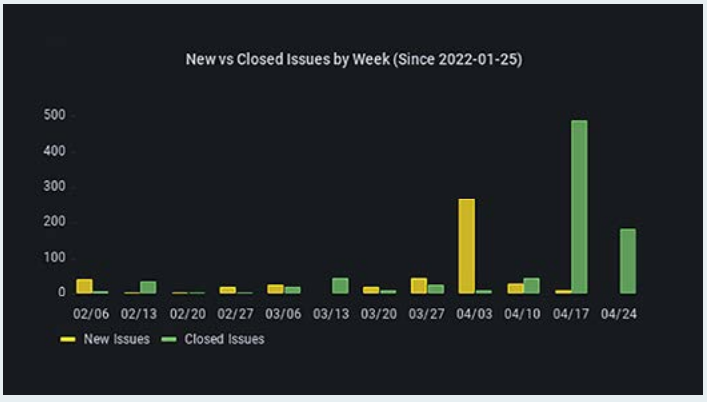

Figure 11. Open and Closed Issues by Week

Operational Indicators

Used to monitor and evaluate the efficiency of day-to-day operations. These help management identify which strategies are effective and those that inhibit the company.

- Time from detection to remediation per vulnerability
- Remediation done in set timeframe
- Type of remediation solution

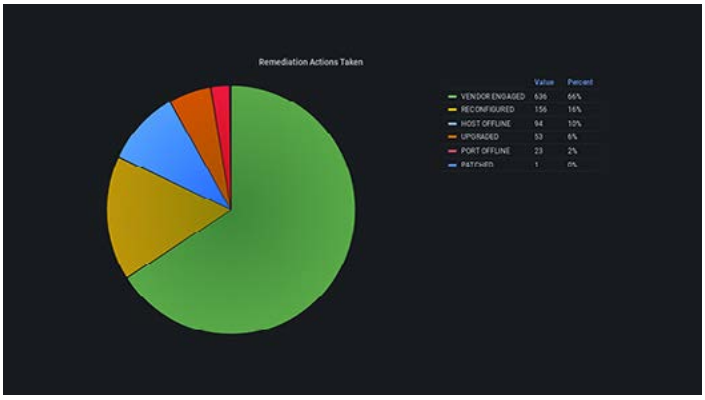

Figure 12. Remediation Actions Taken

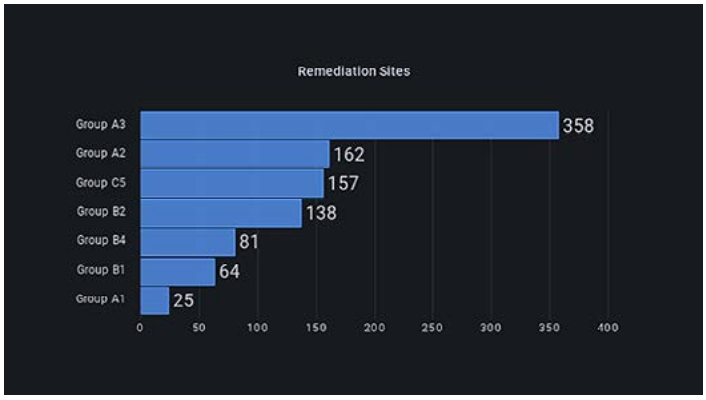

Figure 13. Remediation Activities by Site

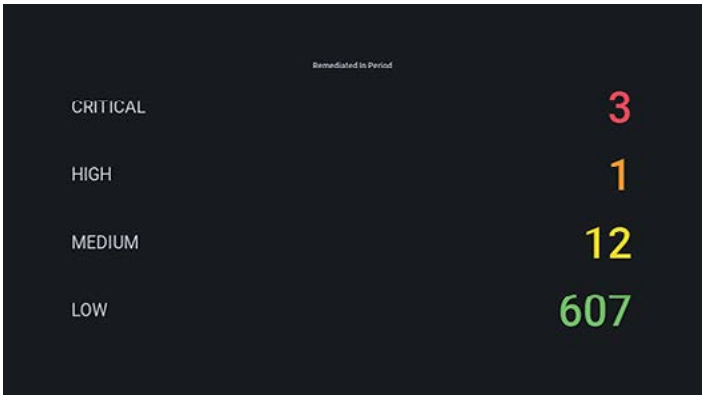

Figure 14. Issues Remediated in Period by Severity

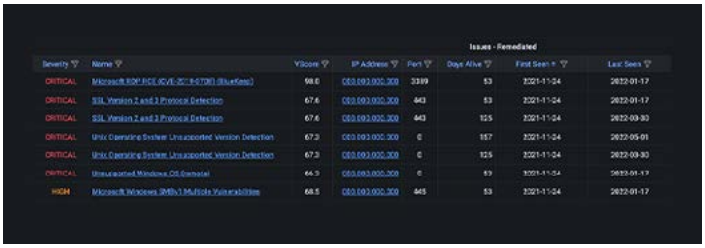

Figure 15. Issues Remediated

Recognizing the unique challenges of tracking vulnerability management success, VULNERA has responded to this demand with solutions that track performance in real-time and historically over time. This helps security teams document the progress and ROI of your program as well as gives you an early warning when tools or processes are no longer effective. Vulnerability intelligence helps you communicate performance to key stakeholders, including the board, as well as supports decisions for budgeting and additional security spending.

CONTACT

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

+1 626.515.5523
www.vulnera.com | info@vulnera.com

SB1012 REV A 05/2022