TLP:WHITE

November 2024

Vulnerability Metrics and Reporting

Authors:

Agathe Merle - Abbott
Brian Bizon - Organon
Christopher Castellano - CommonSpirit
David Glosser - Regeneron
Drew Vravick - AbbVie
Gregory Moore - Amgen
Jeff Luckett - Humana
Jason Martin - Highmark Health
Roger Browning - STERIS
Tyler Curry - Health-ISAC

TLP:WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC™
Collaborating for Resilience in Healthcare

Abstract

One of the biggest struggles vulnerability management teams face today is metrics and being able to tell the story of risk in their environment. The programs implemented by vulnerability management teams help prevent breaches, ensure compliance adherence, and demonstrate diligence.

The number of vulnerabilities continues to climb; in 2023, 29,066 CVEs were identified, and in 2024, there are already 24,455 at the time of writing[1]. Metrics and reporting can be one of the most challenging areas to help improve the maturity of your organization and highlight the work being performed by your vulnerability management team. Due to the rapid influx of critical vulnerability disclosures, vulnerability management teams need to monitor and report on the operational health of the program. Peter Drucker's famous quote applies here: "What gets measured, gets managed." The following is not exhaustive; however, this can include evolving and determining the impact of emerging threats, displaying KPIs that might be helpful for other organizations, and monitoring your status from a patching standpoint.

Metrics are the bedrock for assuring that steps such as these and similar are completed, as they illustrate the importance of updating our technology and understanding associated risks. This white paper is a continuation of a series of communications regarding vulnerability management, covering different concepts for metrics and reporting that an organization may be able to use to help develop a vulnerability management program or provide insight into other options that can be implemented into one that already exists.

Executive Summary

In today's always-on interconnected world, vulnerability management is a foundational process for all organizations. Metrics and reporting play a critical role in monitoring the services we provide, implementing detection capabilities, and remediation efforts of application or technology teams. Effective storytelling with metrics and reporting can help showcase improvements or the effectiveness of our technology support personnel. The vulnerability management team should have a scoring system to reflect the organization's remediation timelines. A more mature vulnerability management program will have policies and standards to indicate how risk ratings are determined for vulnerabilities and service level agreements (SLA) for remediation timeframes by risk rating. Risk ratings assist organizations in prioritizing their limited resources to address the highest-risk vulnerabilities first. Simply focusing on the number of vulnerabilities based on severity levels is a fundamental reporting method that is inadequate to help determine the success of the remediation efforts or risk to the organization. To improve this area, metrics can be tailored in separate groups to help effectively tell these stories. Some important segmented areas include technology, network placement or asset context, and tool or service monitoring. For vulnerability management teams to be successful in reporting and metrics, they need to show how they can deliver a compelling message or story. If we cannot use data to show our leaders why something is important or failing, we are doing our jobs ineffectively.

Effective Communications for Metrics

Metrics or key performance indicators (KPIs) can help you tell a story about the state of security for your infrastructure. However, if you cannot engage your audience, the metrics your team spent time and effort putting together may not have the impact you need them to have.

[1] https://www.cvedetails.com/browse-by-date.php

The first step when developing metrics should be considering what and how you want to display and who you are targeting. Your metrics need to tell a story and be engaging. If you display a lot of information, you must keep the format clear while keeping colors and style consistent. Make sure you add legends with your graphics so that if someone were to look at the metrics on their own, they would be able to read the graphs and understand the purpose of showing these numbers. Finally, you will want to show how your metrics tie into the business. Among cybersecurity teams and related departments, therein lies the tendency to sometimes forget these entities are not siloed and have ties to the business's overall mission.

Your metrics should reflect your understanding of the business. For instance, if your organization splits responsibilities by countries/regions, you must ensure you provide vulnerability metrics with those breakdowns. You can show metrics from a cybersecurity point of view (i.e., risk categories, exploits, etc.) while still being able to tailor them to reflect your organization's priorities and workflows. Conclusively, for great metrics, apply consistent and clear formatting, use a storytelling approach, and include legends tailored to your organization's culture, priorities, and workflows.

Your vulnerability management program metrics should cover several areas and offer different breakdowns, including:

- **Risk Breakdowns:** You need to evaluate vulnerabilities using a scoring system of your choosing and share the numbers of both instances and unique vulnerabilities for each predefined risk category.

- **Type Breakdowns:** Breaking down your vulnerabilities by type will help you tell the story to your leadership and help the teams working on remediation.

- **Business Units Breakdowns:** These may include divisions, departments, countries, or regions. The breakdown metrics you offer should reflect whichever units your organization uses to organize itself.

Organizations will have tens of thousands, hundreds of thousands, or even millions of vulnerability instances. Your role as the vulnerability team is to break down those numbers in ways that are useful to your organization and can help drive remediation.

Supplemental Metrics

Simplicity and relevance are fundamental when presenting vulnerability metrics. Using concepts like the "Keep It Simple and Straightforward" (KISS) principle ensures you share only the essential information by cutting out unnecessary details. It is critical that you understand who your audience is, which is a vital part of this approach. Additionally, tailoring your message to fit their level of understanding and focus on what they need to know is conducive to clear communication. Conversely, providing too much data can overwhelm and confuse rather than clarify the key points you want to convey.

Using stories and analogies can make technical data more relatable and comprehensive. These tools help bridge the gap between complex details and everyday experiences, making the information more memorable. Building trust is also essential. Presenting your data confidently and clearly reassures your audience that you are an expert on the topic and should be trusted. By focusing on simplicity, audience relevance, and engaging storytelling, you can effectively communicate vulnerability metrics, helping your audience make informed decisions.

In addition to providing KPI metrics to leadership, an organization can leverage data analytics-driven insights to expand leadership's understanding of patch performance and effectively communicate necessary changes for further risk reduction. Supplemental vulnerability metrics offer a nuanced view beyond standard KPIs, guiding informed decision-making processes.

A helpful supplemental metric can include analyzing the aging trend of high-risk vulnerabilities, explicitly focusing on security flaws that are 60 days or older and more likely to be exploited. This metric offers a clear view of the attack surface landscape and highlights areas where older, potentially unpatched vulnerabilities pose the greatest risk. This categorization metric provides leadership with the tools they need to identify areas of concern where remediation should be prioritized.

The following are examples of vulnerable software categorization:

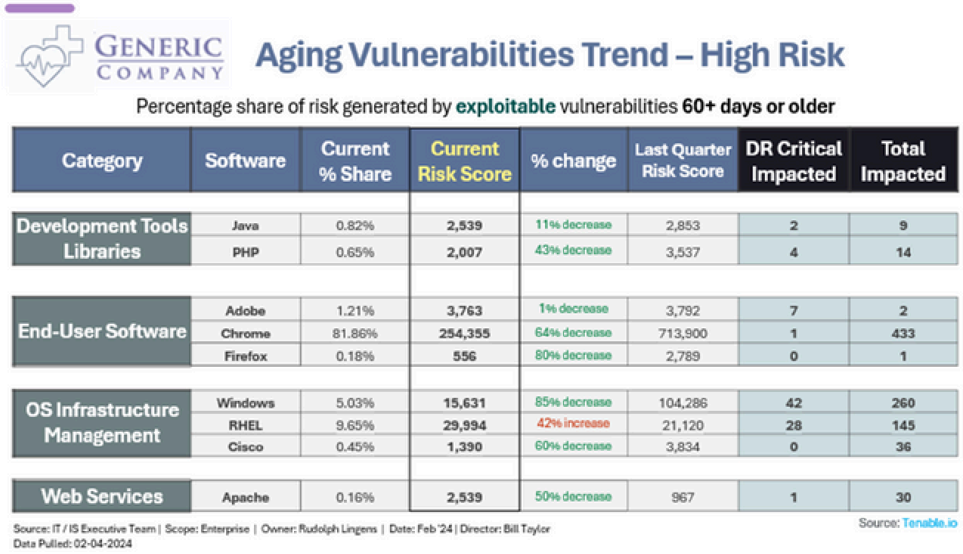
- **Development Tools / Libraries:** Software tools and libraries used in the development process.
- **End User Software:** Applications and software directly utilized by end users.
- **OS Infrastructure Management:** Operating systems and infrastructure management tools.
- **Web and Enterprise Services:** Web applications and enterprise services.

When categories are simplified and grouped, executives can quickly identify the areas they are responsible for patching without delving into specific details. They can then share the presented data with their management teams for an immediate response or insight into pending actions.

A concise format facilitates informed decision-making, enabling swift action to mitigate vulnerable assets. For instance, a clear table is a straightforward and readily digestible method for presenting vulnerability data, eliminating the need for complex charts or graphs.

Real-World Example

In the chart below, Generic Company provides a compelling example of the impact of supplemental metrics. After implementing these metrics, they identified a significant opportunity within their OS infrastructure management category, specifically focusing on workstations. This tailored approach resulted in an impressive 85% reduction in the observed risk score for this asset category in the following quarter. This achievement was directly attributed to the insights provided by the supplemental metrics, which prompted leadership to direct IT teams to remediate these vulnerabilities. Furthermore, this initiative uncovered a broader lifecycle issue, leading to an enterprise-wide effort to enhance software asset lifecycle management across the organization.



GENERIC COMPANY

Aging Vulnerabilities Trend – High Risk

Percentage share of risk generated by **exploitable** vulnerabilities **60+ days or older**

Category	Software	Current % Share	Current Risk Score	% change	Last Quarter Risk Score	DR Critical Impacted	Total Impacted
Development Tools Libraries	Java	0.82%	2,539	11% decrease	2,853	2	9
	PHP	0.65%	2,007	43% decrease	3,537	4	14
End-User Software	Adobe	1.21%	3,763	1% decrease	3,792	7	2
	Chrome	81.86%	254,355	64% decrease	713,900	1	433
	Firefox	0.18%	556	80% decrease	2,789	0	1
OS Infrastructure Management	Windows	5.03%	15,631	85% decrease	104,286	42	260
	RHEL	9.65%	29,994	42% increase	21,120	28	145
	Cisco	0.45%	1,390	60% decrease	3,834	0	36
Web Services	Apache	0.16%	2,539	50% decrease	967	1	30

Source: IT / IS Executive Team | Scope: Enterprise | Owner: Rudolph Lingens | Date: Feb '24 | Director: Bill Taylor
Data Pulled: 02-04-2024

Source: Tenable.io

In summary, supplemental vulnerability metrics offer a strategic advantage by providing detailed, actionable insights that complement traditional KPIs. These metrics enable leadership to pinpoint and address high-risk areas effectively, ultimately contributing to a more secure and resilient organization.

Patch Management Metrics

Patch management is a crucial aspect of cybersecurity. It involves timely and efficient software updating to mitigate vulnerabilities. Effective patch management requires a set of metrics to ensure that vulnerabilities are promptly identified and addressed, minimizing potential risks. These metrics help organizations evaluate their patch management processes, identify areas for improvement, and maintain a robust security posture.

Key metrics for patch management can include:

- **Patch Compliance Rate:** The patch compliance rate measures the percentage of systems that are up to date with the latest patches. This metric provides insight into the effectiveness of the patch deployment process and helps identify gaps in coverage. A high compliance rate indicates a well-maintained and secure environment, while a low rate may highlight areas where systems are vulnerable due to unpatched software.

- **Mean Time to Patch (MTTP):** Mean Time to Patch (MTTP) is the average time taken to apply patches after they are released. This metric is critical for assessing the responsiveness of an organization’s patch management process. A shorter MTTP indicates a proactive approach to vulnerability management, reducing the window of exposure to potential threats. Conversely, a longer MTTP suggests delays in addressing vulnerabilities, increasing the risk of exploitation.

- **Patch Success Rate:** The patch success rate measures the percentage of successfully applied patches without causing disruptions or failures. This metric helps organizations evaluate the reliability of their patching processes and the compatibility of patches with their existing systems. A high success rate indicates that patches are being effectively tested and deployed, while a low rate may indicate issues with patch validation or conflicts with existing configurations.

- **Vulnerability Detection Rate:** This metric assesses the organization’s ability to identify vulnerabilities that require patching. It measures the number of detected vulnerabilities against the total potential vulnerabilities in the environment. A high detection rate indicates effective monitoring and scanning processes, ensuring vulnerabilities are identified and patched promptly. A low detection rate may suggest gaps in vulnerability assessment and scanning capabilities.

- **Patch Risk Score:** Patch risk scoring involves evaluating the severity and potential impact of vulnerabilities that patches aim to fix. This metric helps prioritize patching efforts based on the criticality of the vulnerabilities. Patches for high-risk vulnerabilities should be prioritized to reduce the potential for significant security breaches. Effective patch risk scoring ensures limited resources are allocated to the most critical areas, enhancing overall security.

Challenges and Best Practices

Effective patch management has challenges. Organizations often face difficulties coordinating patching across diverse environments, ensuring minimal disruption to operations, and dealing with the sheer volume of patches released regularly. To overcome these challenges, organizations should adopt best practices such as maintaining a comprehensive inventory of assets, prioritizing patches based on risk, and automating patch deployment where possible.

Regular review of patch management metrics allows organizations to improve their processes and continuously adapt to evolving security landscapes. By focusing on key metrics such as compliance rate, MTTP, patch success rate, vulnerability detection rate, and patch risk score, organizations can enhance their patch management practices and fortify their defenses against cyber threats.

Asset Context Metrics

Considered one of the most vital metrics in your vulnerability management program, asset context and knowing what you own are invaluable for accurately assessing risk. As an organization's asset count grows, so does the challenge of properly inventorying the different exploitable points of the attack surface.

Below are key details to consider when building contextually aware vulnerability management metrics:

- **Critical Assets:** Critical assets are typically deemed the organization's crown jewels as they are considered business-critical and are pivotal for adequately maintaining the business's mission. Knowing what is considered a business-critical asset is an evolving process involving stakeholders responsible for business operations and infrastructure. An organization can effectively identify business-critical assets via a common set of determinants. These typically include systems where one or more are in play: intellectual property, customer data (PII), systems subject to regulatory requirements, or client-facing/internet-facing systems. You will want to ensure enhanced actions cover these systems, as many implications for the business's mission are tied to the uptime of these assets.

- **Public-facing Assets:** Public-facing assets serve various business needs, including providing external users access to interactive portals, building brand awareness, and conducting other operations conducive to the organization's operability; however, these assets can also be one of the many initial access vectors as part of the external attack surface. Therefore, the posture and prioritization of remediation efforts concerning these assets are crucial to the resiliency of an organization's security apparatus. Considering the average mean time to exploitation for vulnerabilities is 44 days, it is essential to have an inventory of public-facing assets for proper monitoring and remediation processes.[2] Another factor regarding public-facing assets is shadow IT as the ease of deploying cloud instances creates an added challenge for companies of all sizes.

- **Metrics Set:** Generally, a sufficient set of metrics to report on includes time to remediate by severity, mean time to acknowledge for analysts to review and assess severity, and time to communicate for tracking an issue from detection to notification. Additionally, incorporating a service level agreement (SLA) when informing teams of vulnerabilities brings awareness and helps facilitate a solution. Implementing these guidelines can be helpful, especially when addressing risks associated with supply chain attacks.

- **Asset Inventory:** It is essential for organizations to develop a comprehensive software inventory. This information can be derived from sources such as installed software detections from vulnerability management tools or a software bill of materials (SBOM). Accounting for all open-source and third-party software leveraged in your environment is invaluable to understanding exposure to potentially malicious or vulnerable software components. Organizations compromised by supply chain attacks would have benefited from knowing all software components deployed in their environment. As such, leveraging SBOMs serves as a solution to this issue. In this instance, a vulnerability management team can capture metrics, such as the number of software packages deployed and associated known vulnerabilities.

[2] https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one

- **Leverage reputable frameworks:** The role of a vulnerability manager is continuously evolving as the complexity of technology and the interplay thereof present unique and unprecedented challenges. It is important to consider potentially integrating frameworks to foster risk-based prioritization. For example, stakeholder-specific vulnerability categorization (SSVC) is a framework that focuses on the impact of a vulnerability and enables the vulnerability manager to incorporate context specific to their organization.[3] [3] Additionally, the exploit prediction scoring system (EPSS) is another helpful framework as it provides updates that reflect changes in the exploitability of a vulnerability.[4]The dynamic monitoring capability of EPSS provides updated information regarding exploitation risks associated with a vulnerability.

With the ever-evolving threat landscape, vulnerability management teams must prioritize risks effectively. To determine the severity of a vulnerability, teams should consider its likelihood and potential impact, often measured using the Common Vulnerability Scoring System (CVSS). Additionally, prioritization tools like EPSS can assist in this process. Understanding the context of vulnerable assets is crucial for assessing their impact on the organization. By focusing on high-risk vulnerabilities, teams can significantly reduce their organization's overall risk profile and improve their security posture.

Vulnerability Management Program Health Metrics

Many metrics discussed in this whitepaper focus on vulnerabilities and their remediation speed. However, the overall health of the vulnerability management program is often overlooked. A critical metric in this area is scanning coverage, which represents the number of devices assessed for vulnerabilities or the percentage of an organization's fleet covered by the program. This is difficult to calculate because this metric relies on the organization maintaining an accurate configuration management database (CMDB). Due to cloud computing, ephemeral systems, and asset owners' control over configuration items (CIs), most organizations experience difficulties identifying every device in their environment. It is important to note that this metric is an estimate, as precise device inventory can be challenging to maintain.

To consider a device covered, vulnerability data should be collected through network-based scans, agent-based scans, or passive network traffic monitoring. To enhance data richness, scan frequency and depth (authenticated vs. unauthenticated) can be analyzed. Categorizing data points by device type, operating system, network location, or business unit can promote scanning adoption.

The number of exceptions can refine the accuracy of scanning coverage. Exceptions include systems not scanned due to compliance, availability, or potential risks. For instance, vulnerability management teams might avoid scanning operational technology (OT) equipment in manufacturing sites to prevent disruptions. If other methods (OT security tools, passive sensors) cannot gather vulnerability information from such devices, they may fall under the exception category.

Ad Hoc Reporting

Ad-hoc reporting presents a significant challenge for vulnerability management teams. Frequent requests for updates or data often require time-consuming preparation. These reports may address new critical vulnerabilities, even before detection tools are in place, or provide a count of end-of-support internet-facing devices. Effective communication with leadership about the status of these requests is crucial. When creating ad-hoc reports, identifying impacted assets and distinguishing between external and internal systems is essential for timely updates. Basic reports can compare remediation percentages internally and externally. Centralized data repositories, such as SIEMs, custom databases, or cloud/SaaS vulnerability management solutions, can facilitate efficient reporting on asset counts and remediation progress.

[3] https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

[4] https://www.first.org/epss/#:~:text=The%20Exploit%20Prediction%20Scoring%20System,be%20exploited%20in%20the%20wild.

Suppressing findings for systems without the relevant configuration, like Log4j not being used by an application, is vital. Providing context for these exclusions is crucial for understanding the overall security posture. Additionally, reporting on security controls on external end-of-life assets can help assess potential vulnerabilities. Ultimately, a central repository for data enables rapid assessment of impact and remediation progress, streamlining ad-hoc reporting.

Conclusion

Effective vulnerability management teams are crucial in safeguarding organizations by identifying and mitigating risks. Clear and timely communication of metrics and findings is essential to ensure stakeholders have the information needed to make informed decisions and maintain business operations. By tracking key metrics and effectively communicating their significance, vulnerability management teams can demonstrate their value in protecting the organization’s assets, mitigating risks, and ultimately supporting achieving business objectives.

This whitepaper was developed by Health-ISAC's Vulnerability Management Working Group. To join this working group, please send an email expressing your interest to contact@h-isac.org.