Vulnerability Management System

Naif Alkelaibi

DOI: https://doi.org/10.5281/zenodo.7092162

Published Date: 19-September-2022

Abstract: **Past efforts to protect and mitigate attacks have resulted in the development of security systems, targeting different types of attacks on isolated computer systems. The different IT systems yield data with varying formats that cannot be aggregated into a singular learning corpus. As a result, vulnerability scans on computer systems have limited value for cybersecurity experts and managers. This project introduces a centralized vulnerability management system (VMS) capable of hosting organizational security findings in a unified format that permits, among other things, offers vulnerability discovery, vulnerability validation, alerting and event notification, continuous asset profiling, metrics measurements, API integration, and bespoke development. Primarily, the system aggregates all vulnerability reports from different systems in an organization and presents them in a harmonized format using a web application.**

Keywords: **IT systems, security systems, vulnerability management system (VMS).**

1. INTRODUCTION

The world is becoming increasingly computerized every passing day. A troubling characteristic of this change is the emergence of new cybersecurity risks, challenging every aspect of modern computer systems. Organizational IT infrastructure and its components are becoming more and more connected. Connecting to the internet serves as the gateway for attacks targeting IT assets. Today's cybercrime is a big business and the motivation to attack organizations and governments globally has never been higher. Monetary and reputational impacts of cybersecurity attacks are higher, especially if an organization lacks an appropriate cybersecurity plan.

The National Cyber Security Centre has indicated that over four in ten businesses and two in ten charitable organizations globally suffer two cyberattacks annually. The survey indicates further that the numbers keep growing, especially as a significant percentage of small businesses continue lacking proper protection plans against cybersecurity threats. The study reported that the threats experienced by organizations vary widely across systems and the type of IT assets targeted. A wide range of primary means by which cybersecurity risks affect and destroy organizations exists. There is always the risk that a malicious actor might obtain sensitive information stored in an organizational database and sell it in the open markets on the dark web (Ozkaya and Aslaner). Another popular cybersecurity risk in today’s computerized world is ransomware. Recent cybersecurity research has hinted that ransomware campaigns have adopted commercially oriented business models, increasing the attack motivations and investment in the development of stronger encryption methods (Cascavilla et al.; Habibzadeh et al.; Ozkaya and Aslaner). Such advances in cybersecurity threats call for more stringent and strong governance to protect organizations from financial and reputational damage.

A part of a cybersecurity plan includes making sure that an organization’s IT assets are safe from both internal and external threats castigated by malicious or disgruntled actors. Accordingly, cybersecurity governance and risk management plan have transformed from an offbudget to a core budget item for all organizations – large and small. However, these resources have traditionally been channeled into the development of attack countermeasures and remediation for different IT systems in an organization. Past efforts to protect and mitigate attacks have resulted in the development of security systems, targeting different types of attacks on isolated computer systems. The different IT systems yield data with varying formats that cannot be aggregated into a singular learning corpus. As a result, vulnerability scans on computer systems have limited value for cybersecurity experts and managers.

The events of the infamous WannaCry ransomware attack that targeted Microsoft Windows operated system and encrypted data led to major losses to organizations and individuals globally. Reports indicate that a Server Message Block (SMB) port was exposed and vulnerable, creating an avenue for the operating system to be exploited. The attack affected close to half a million-computer systems in a hundred and fifty countries within a day. More than 50 organizations globally were affected with the costs of the attack topping $4 billion (Habibzadeh et al.). The interesting question that remains unanswered is whether victims of the attacks could have avoided the losses. It later emerged that Microsoft Windows had released a fix for the vulnerability, but most organizations had not taken up the update on their systems – that is the problem and where the need for a vulnerability management system (VMS) as part of cybersecurity governance and risk management plan becomes vital. The idea of developing a VMS is motivated by the existing vulnerability management lifecycle that helps organizations anticipate and respond to cybersecurity threats better and more timely.

1.1 Problem Statement

As organizations ramp up investments in cybersecurity risk countermeasures, the need for a VMS becomes more evident but vaguely appreciated. Different computer systems and cybersecurity tools report vulnerabilities from different sources and in different formats. Owing to the unstructured nature of the reports, it becomes significantly difficult for technical teams to relearn their strategies from experiences and mitigate attacks. The information cannot be summed up into a single dashboard where the management can monitor and anticipate attacks. The problem is understood to cut across the various phases, namely, identification, analysis, report, and remediation, of countering attacks.

Problems in the identification phase of cybersecurity risk are mostly associated with false positive scan results. False positive results in cyber vulnerability scans occur when the scanning process and tools access only a section of the targeted resources, preventing an accurate exposure of all possible vulnerabilities. For example, a vulnerability scanner may read only the configuration data from the service banners, thereby ignoring the back-reported vulnerability updates. Challenges associated with the analysis phase include the inconsistent time of reports, duplicate items, ambiguous reporting, and escalation issues. These challenges become more sophisticated when coupled with the reporting problems, such as lack of validation and finding statuses, as well as communication difficulties between stakeholders.

1.2 Project Execution (Milestones)

We identified current challenges in the industry for handling security findings. As part of our approach, we considered the following points. First, we focused on identifying the current pain points, which consist mainly the ambiguous security reports. The users of the proposed solutions include system administrators, security analysis, and management. Data for the project came from vulnerabilities findings from security scanning tools. The addressable problem was the lack of a system that had multiple sources of vulnerability reports. A reconnaissance survey was undertaken to identify gaps for technical security teams and management. The main outcomes of the survey were, first, a large number of vulnerabilities reported from different scanning tools made it hard for the technical team to analyze. Second, there is no method for the management to track the vulnerability status of the organization. More details about the outcomes of the survey are described in Section 1.3.

1.3 Progress and Deliverables:

The first step involved selecting the right methodology to manage our project. The team settled on the agile methodology because it is a development project. A feasibility study followed to identify current gaps in the industry. A survey of the technical security team and management has been shared to better understand current gaps and suggest improvement options. Multiple workshops were conducted to analyze survey input and find possible solutions.

1.4 Background and Feasibility Research

A review of past cybersecurity efforts revealed that past investments in cybersecurity governance and risk management have focused solely on the development of attack and vulnerability countermeasures, but little has targeted vulnerability acumen. We consider it a major challenge going forward, especially as computer systems become more complex and interconnected. Currently, security findings are generated from multiple systems. Each system generates security findings with its format and view. It becomes difficult for security professionals and strategists to aggregate this information into a single learning corpus that could be used to develop helpful insights for attack preparedness and mitigation strategies. As a result, security analysts have to read multiple security reports in different formats. It is also difficult for the management to track and implement tracking security findings.

Background research was carried out to substantiate the problem as hypothesized above. Chart 1 summarizes the perception of the respondents concerning their experiences with their organizational vulnerability management process. Over 70% of the respondents perceive their organizational cybersecurity vulnerability management processes as difficult, while slightly above 20% consider the processes tolerably difficult. Only a few (less than 5%) consider the processes simple. The study also sought to understand the ease with which users read vulnerability findings from their current systems. Over 80% of the respondents consider reading vulnerability findings a painful exercise. Consequently, it becomes much more difficult for close to 70% of the respondents to track the vulnerability status of their organization.

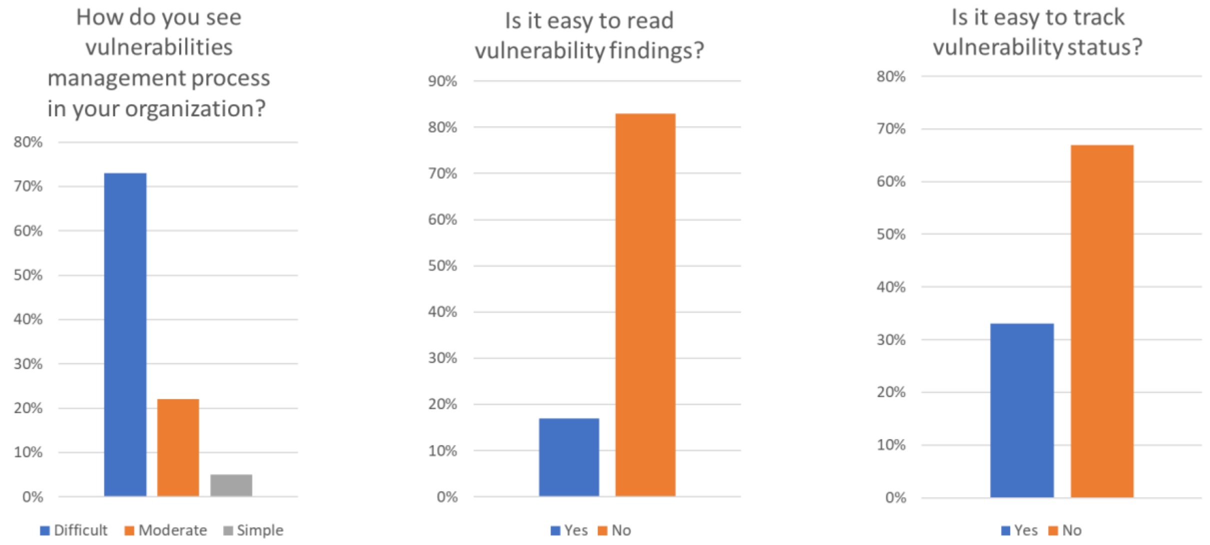


Chart 1: User perception of current vulnerability management processes, ease of reading vulnerability findings, and tracking vulnerability status

The challenges identified by the respondents cut across four areas, namely, complexity, false positive scan results, difficulty tracking vulnerability status, and the decentralized nature of the current vulnerabilities management processes. Users consider the processes complex for lack of a unified report about the vulnerabilities. There are also multiple false positives arising from different scanning tools identifying the same vulnerabilities but in different formats. In addition to false positive scans and process complexity, users find the lack of appropriate tracking tools challenging. The decentralized nature of existing cybersecurity vulnerability management systems kills the prospects of developing a vulnerabilities dashboard, and technical teams often resort to using emails to identify the reported vulnerabilities. Users desire a platform to manage cybersecurity vulnerabilities that has the following technical outcomes.

Table 1: Desirable outcomes of a cybersecurity vulnerability management system

Apparent	Validated	Workflow	Centralized
Unified report for the vulnerabilities report.	Validate all vulnerabilities generated from the scanning tool to ensure no duplicate vulnerabilities are reported.	Assure vulnerabilities are closed with evidence.	Centralized system for both management and technical team

1.5 Project Motivation

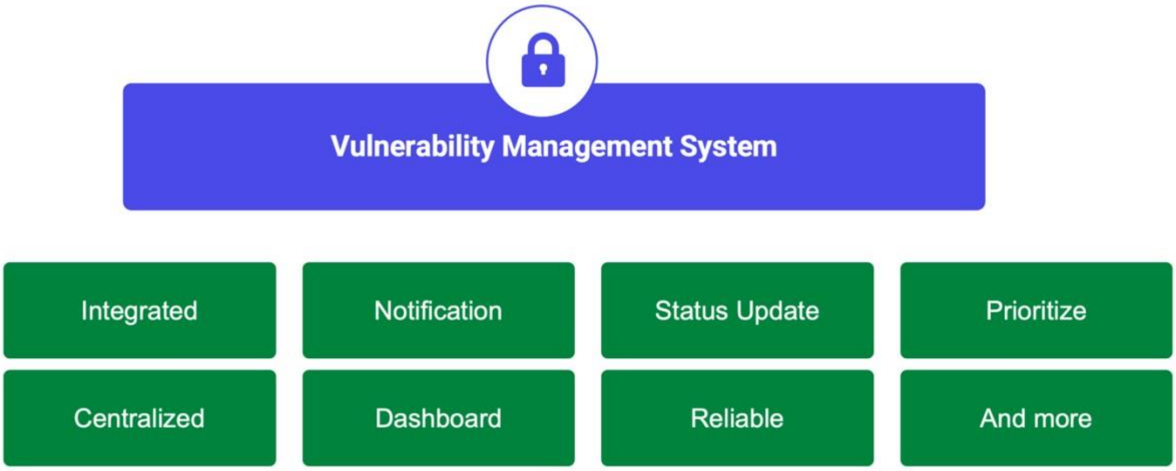
With the adoption and implementation of a robust vulnerability system, an organization can continually improve its cybersecurity prospects and ensure high-security levels for critical IT infrastructure and assets. The main motivations for developing a vulnerabilities management system include:

- The need to have a platform that helps technical teams to identify vulnerabilities from internal and external actors timely
- The need to have a system that enables an organization to understand in real-time, its security position
- The need to reduce the cybersecurity threat and risk profile of an organization and bring it to an acceptable level
- The need to mitigate the time organizations take to mitigate security threats

2. THE SOLUTION: VULNERABILITY MANAGEMENT SYSTEM

2.1 Unique Features

The project appreciates that vulnerability management is not a straightforward task. It involves extensive complexities, stretching beyond the choice of features needed in the system but also covering the desirable actions of the organization itself and its employees. Overall, the project aims to develop a vulnerability management system that is highly integrated, centralized, and reliable. Desirable features of the system include sending vulnerability notifications, an interactive dashboard, self-managed vulnerability status updates, and the ability to prioritize vulnerabilities. Figure 1 details the unique features of the proposed vulnerability management system.



VMS is a highly integrated, centralized, and reliable capable of sending vulnerability notifications, an interactive dashboard, self-managed vulnerabilities status updates, and the ability to prioritize vulnerabilities.

Figure 1: Unique features of the proposed vulnerability management system

2.2 Project Scope

The scope of this project is to have an interactive application to host all vulnerabilities in a unified format for the technical security team to handle security findings easily. The system will have multiple features for technical security teams and management. Features include a management dashboard, findings distribution, a unified report, reducing false positives, and removing duplicated items. Based on the background research undertaken (Section 1.2), the proposed vulnerability management system improves the following areas.

Table 2: Vulnerability management improvements promised by the new system

The current vulnerability management process	Vulnerability management system
Highly complex	Apparent: Unified report for the vulnerabilities report.
Multiple false positive reports	Validated: Validate all vulnerabilities generated from the scanning tool to assure no duplicate vulnerabilities reported
Difficulties tracking vulnerability status	Workflow: Assure vulnerabilities are closed with evidence.
Non-centralized, hence, too much email traffic	Centralized: Centralized system for both management and technical team

2.3 Vulnerability Management System (VMS)

VMS is an interactive application to host all organization vulnerabilities. The system reads organization vulnerability reports and aggregates them into a simple and unified format.

This is achieved by having multiple methods in the back-end and front-end to further enhance vulnerability representation in the application. Key capabilities of the system include removing duplicate findings, escalation tags, and interactive dashboards, among others. Figures 2&3 are screenshots of the vulnerability management system.

2.3.1 System Design

To achieve the above features, the system uses multiple tools as described in Table 2.

Table 2: VMS design tools

Development Tool	Role/Outcome
HTML5	This is the platform where the web application is created and deployed. It reinforces JavaScript interactive tools
CSS	For interface customization and design
JavaScript	Used for adding interactive behavior to the web application, such as interactive database query systems and output filter systems for removing duplicates, resolving vulnerabilities, and escalating scan results using notifications on the dashboard

2.3.2 Testing and Benchmarking

In addition, to the front-end features described in Table 2, the initial back-end has already been developed and tested successfully the connection from the front-end using API. We have implemented the solution as a beta in small organizations and there are positive indications the organizations will adopt the system. The test results revealed that our vulnerability management system overcomes typical limitations of the existing vulnerability management tools. Table 3 is a descriptive benchmark chart of the vulnerability management system.

Table 3: Descriptive benchmark chart

Existing vulnerability management tools	Proposed vulnerability management system
Use rule-based approaches and can only scan known vulnerabilities	VMS is a learning system that continuously updates its vulnerability catalog. It offers a continuous assessment of systems across the full stack dedicated to the discovery of vulnerabilities, leveraging multiple engines and toolchains.
Tools have low accuracy and do not provide updates to IT asset inventory data	Uses a correlation technology to validate newly discovered vulnerabilities to remove false positives, while updating IT asset inventory through constant interrogation of the entire IT ecosystem
Scanning is episodic, with periodic point-in-time scans	Real-time threat intelligence, correlation, and machine learning models automatically prioritize the riskiest vulnerabilities
Vulnerability tools typically only scan enterprise-owned managed IT assets	Automatically discovers and categorizes known and unknown assets continuously identifies unmanaged assets and creates automated workflows to manage them

2.3.3 Metrics for Evaluating the VMS System

Metric	Performance Expectations
Vulnerability discovery	Continuous evaluation of systems across the full stack dedicated to the discovery of vulnerabilities
Vulnerability validation	Ability to analyze and correlate vulnerabilities to minimize false positive alerts
Alerting and event notification	Ability to create situational awareness through an integrated ticketing system to inform the technical team and management about the vulnerability status of the system
Continuous asset profiling	Ability to interrogate the entire ecosystem and update IT asset inventory
Metrics and measurements	Ability to measure improvements and efficiency of key vulnerability management processes and flag risk areas
API integration	Ability to integrate vulnerability intelligence into a unified system with custom reports

3. CONCLUSION, LIMITATIONS, AND FUTURE WORKS

The goal of the project is to have a centralized vulnerability management system that is capable of hosting organizational security findings in a unified format that permits, among other things, vulnerability discovery, vulnerability validation, alerting and event notification, continuous asset profiling, metrics measurements, API integration, and bespoke development. Primarily, the system will aggregate all vulnerability reports from different systems in an organization and present them in a harmonized format using a web application. The new system trounced existing vulnerability management tools in various ways.

First, as opposed to the existing tools that rely on rule-based approaches and can scan only known vulnerabilities, the new VMS is a learning system that continuously updates its vulnerability catalog. It offers a continuous assessment of systems across the full stack dedicated to the discovery of vulnerabilities, leveraging multiple engines and toolchains. Second, the new VMS overcomes the accuracy limitations of existing tools by using correlation technology to validate newly discovered vulnerabilities to remove false positives, while updating IT asset inventory through constant interrogation of the entire IT ecosystem. It also shifts from episodic and point-in-time scans offered by traditional tools to real-time threat intelligence, correlation, and machine learning models that automatically prioritize the riskiest vulnerabilities. It automatically discovers and categorizes known and unknown assets, continuously identifies unmanaged assets, and creates automated workflows to manage them, overcoming the limitation of scanning only enterprise-owned managed IT assets. Other capabilities of the system include allowing users to assign vulnerabilities to themselves. The supervisor can assign the vulnerabilities to a specific member of his/her team for appropriate action.

3.1 Limitations and Future Work

The main limitation of this project was the short timeframe. The project execution was limited to two months. With an adequate timeline, a future improvement on the project would involve testing the novel vulnerability management system in large organizations with a largescale vulnerability spectrum.

REFERENCES

[1] Cascavilla, Giuseppe, et al. “Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review.” *Computers & Security*, vol. 105, Elsevier, 2021, p. 102258.

[2] Habibzadeh, Hadi, et al. “A Survey on Cybersecurity, Data Privacy, and Policy Issues in CyberPhysical System Deployments in Smart Cities.” *Sustainable Cities and Society*, vol. 50, Elsevier, 2019, p. 101660.

[3] National Cyber Security Centre. “New Figures Show Large Numbers of Businesses and Charities Suffer at Least One Cyber Attack in the Past Year - GOV.UK.” *Department for Digital, Culture, Media & Sport, Information Commissioner’s Office, National Cyber Security Centre, and Margot James*, 25 Apr. 2018, https://www.gov.uk/government/news/new-figures-show-large-numbers-of-businessesand-charities-suffer-at-least-one-cyber-attack-in-the-past-year.

[4] Ozkaya, Erdal, and Milad Aslaner. *Hands-On Cybersecurity for Finance: Identify Vulnerabilities and Secure Your Financial Services from Security Breaches*. Packt Publishing Ltd, 2019.