Broken Pipeline: Shedding Light on Vulnerability Management and Prioritization

S M Zia Ur Rashid

ABSTRACT

Organizations are struggling to keep up with patching efforts as the number of newly discovered vulnerabilities continues to climb each year. Neither all security issues and vulnerabilities are equally important, nor all of them are exploitable. This is leading to a growing vulnerability backlog and slowing down development and the release of new products. This study aims to explore contextual risk-based approach combination with machine learning techniques for developing better vulnerability management processes that will help the analyst to prioritize vulnerabilities to fix.

ORIGINALITY AND OBJECTIVE

This study will focus on context based risk assessment and vulnerability prioritization which has not been comprehensively studied previously for vulnerability management. This research will try to identify useful factors and metrics that will be helpful for contextual risk assessment and shed a light on the application of ML techniques on vulnerability management to reduce the burden of triaging and prioritizing issues.

Vulnerability Management (VM) is the ongoing practice of continually identifying, classifying, prioritizing, remediating, and mitigating security vulnerabilities in systems, networks and the software that runs on them — whether in the cloud or on-premises. It also applies to browsers and end-user applications. Vulnerability scanner and sometimes endpoint agents are used to find vulnerabilities on them (Source: Rapid7).

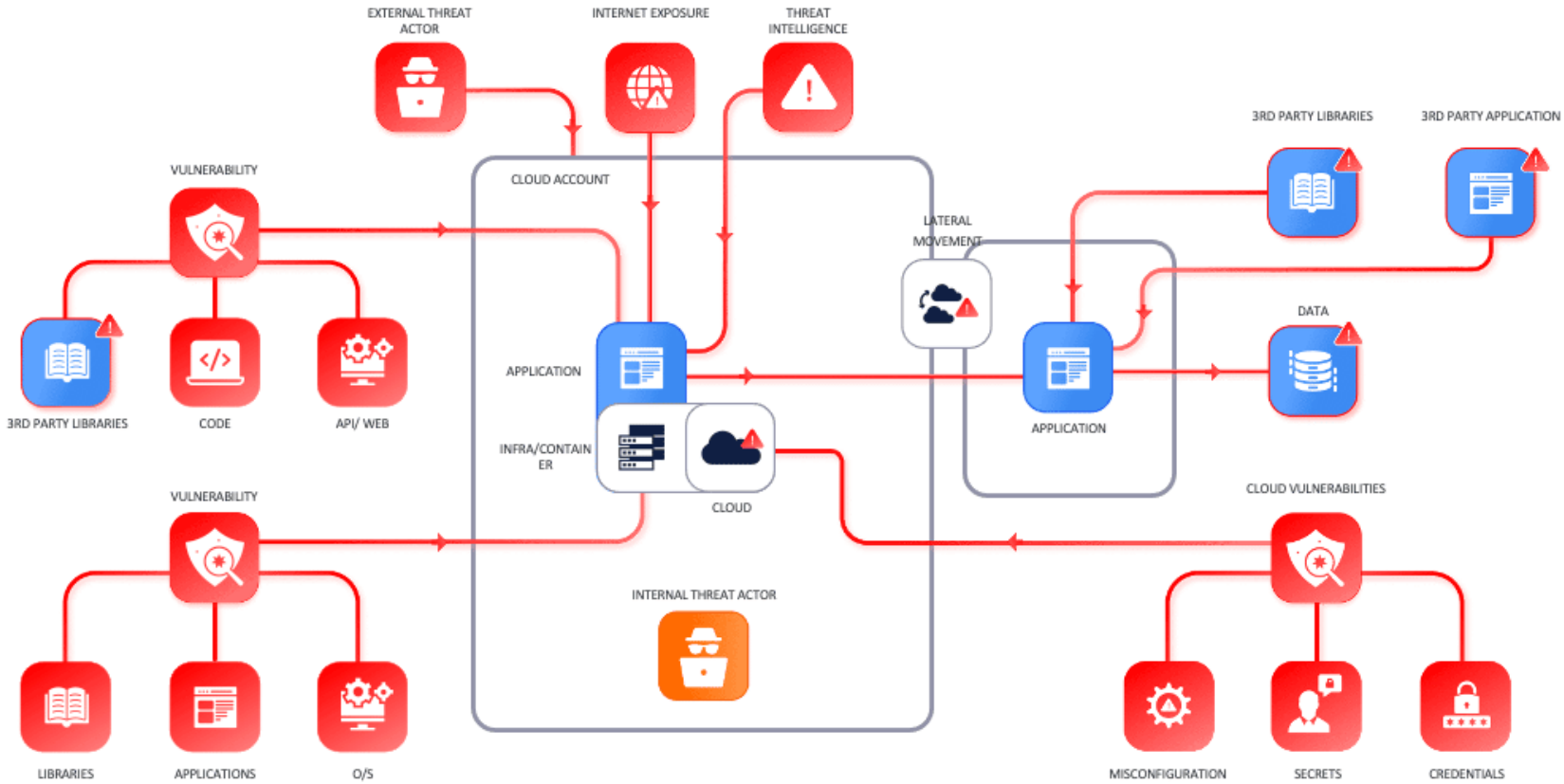


Fig. 1 A topography of IT components in a typical enterprise (Source: AppSec Phoenix)

BACKGROUND AND LITERATURE REVIEW

Most cases these VM tools use Common Vulnerability Scoring System (CVSS) with combination of Common Vulnerabilities and Exposures (CVE) data to evaluate risk and prioritize vulnerabilities [1].

According to Rezilion's analysis on the most popular 20 container images, on average, only 15% of the vulnerabilities are actually exploitable [2].

Since many VM tools prioritize and provide remediation recommendations based on CVSS scores, and what gets lost is the organizational context [3]; the understanding of how to distinguish the relevant 15% of vulnerabilities from the remaining 85%.

Contextual aspects are based on:

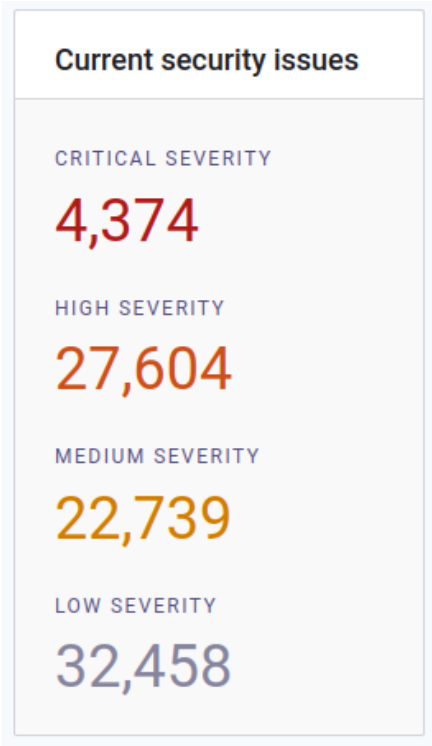
- The severity of a vulnerability – CVSS
- Probability of exploitation – how likely is that vulnerability to be exploited
- Locality - location of the asset
- Business Impact - how important the asset is and how much damage it can cause if exploited
- Cyber Threat Intelligence (CTI) data

Security teams need to provide extra manual effort to assess the risk of all identified vulnerabilities and prioritize them for fixes maintaining the SLAs which increase their workloads.

A recent survey disclosed that among 602 security professionals who participated in that survey, 54% are considering quitting their jobs due to overwhelming amounts of responsibilities and workforce shortages within their departments [4].

PROBLEMS

- Vulnerabilities have been increasing in number year on year, around 25K cve published this year. (https://www.first.org/epss/data_stats)
- Assets, Scopes and Environment complexity are also increasing.
- Security team needs to put manual effort to review large amount of findings and prioritize them which is time-consuming and increases their workloads. Also, subject matter expertise is required to accomplish the task.
- Organization needs to maintain SLA, compliance and maturity level (e.g., SANS).



RESEARCH QUESTIONS

1. Does CVSS-based vulnerability management reflect the actual risk and business impact, and help to prioritize vulnerabilities to fix without putting extra manual effort to analyze the vulnerability?

2. What are the metrics and factors different vulnerability management tools considered to evaluate risk and prioritize vulnerabilities?

3. How could machine learning help to prioritize security vulnerabilities and recommend context-driven remediation plans?

METHOD 1 : SURVEY

Survey research means collecting information about a group of people by asking them questions and analyzing the results. This study will conduct an online survey via surveymonkey or similar platform.

Hypothesis:

- CVSS alone are insufficient to assess business risk and impact, and prioritize vulnerability to fix.
- Existing vulnerability management tool doesn't satisfy the needs fully.
- Vulnerability management without proper context requires more manual effort to prioritize vulnerabilities.
- Analyst considers different factors during manual assessment which may be varied organization to organization.

Participants:

The study will use a sample of 300 participants designated as Security Engineer, Security Manager or equivalent designated person who oversee vulnerability management programs and responsible to triage or prioritize vulnerabilities.

METHOD 1 : SURVEY (PROS AND CONS)

Pros:

- Easier to administer and can be developed in less time
- Online surveys are cost-effective
- Conducted remotely can reduce or prevent geographical dependence
- Capable of collecting data from a large number of respondents

Cons:

- Respondents may not feel encouraged to provide accurate, honest answers
- Respondents may not feel comfortable providing answers that present themselves in a unfavorable manner.
- Question wording can bias respondent's answers

METHOD 2 : COMPARATIVE STUDY

Comparative study is the process of comparing items to one another and distinguishing their similarities and differences. This study will conduct a comparative analysis on different vulnerability management tools including both open source and commercial tools. To identify the existing vulnerability management tools from both industrial offerings and the latest research, academic literature and web search will be performed using different keywords

Participants:

This study doesn't involve any human participants directly. However, it's expected to select popular or known vulnerable management tools for this study that offer or claim to provide state-of-art features and solutions, and has a free or evaluation version.

Measures:

This study will try to measure performance of different vulnerability management tools, their features and identify what kind of metrics they use to assess risk and prioritize vulnerability. The following two questions will be tried to answer:

- What are the differences between vulnerability reports produced by the different vulnerability management tools?
- What metrics and factors are considered by the tools to aid in the risk assessment and prioritize vulnerabilities?

METHOD 2 : COMPARATIVE STUDY (PROS AND CONS)

Pros:

- Helps to identify similarities and differences.
- Broaden our thinking about product functionality.
- Helps to understand what the most successful products are doing and try to figure out how they do it.

Cons:

- Requires collaboration, access to commercial tools
- Requires advance technologies (such as server to install VM tools and applications)

METHOD 3 : APPLIED RESEARCH

Applied research is a type of examination looking to find practical solutions for existing problems. These can include challenges in the workplace, education and society. It focuses on answering one specific question for a client or sponsor.

Research Question:

How could ML help the analyst by providing in-depth context and prioritizing vulnerabilities through analyzing risk and exploitation probability?

Approaches:

- Systematic review of existing risk calculation frameworks such as Factor Anlysis of Information Risk (FAIR), and metrics or factors that can be considered for contextualize risk for prioritizing vulnerabilities.
- Systematic review of ML techniques that are being used to prioritize issues and visualize the attack paths.
- Based on the findings, develop a ML-based solution to solve the question or problem.

METHOD 3 : APPLIED RESEARCH (PROS AND CONS)

Pros:

- Helps in solving specific problems in business
- Findings can be used to develop new technologies and improve existing systems.

Cons:

- Costly and time-consuming
- Requires industry collaboration and sponsorship
- Requires subject matter expertise to solve the problem

CONCLUSION

Organizations cannot rely on CVEs and CVSS metrics alone to measure and quantify cyber risk. Context-driven risk scoring and vulnerability prioritization with the help of ML techniques could help improve the vulnerability management process and optimize time for security teams.

REFERENCES

[1] Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). A comparison of cybersecurity risk analysis tools. Procedia computer science, 121, 568-575. https://doi.org/10.1016/j.procs.2017.11.075

[2] Rezilion (2022, May 26). Researchers Find 85% of Vulnerabilities Pose No Risk. Rezilion. https://www.rezilion.com/blog/rezilion-researchers-find-85-of-vulnerabilities-pose-no-risk/

[3] Devaux, T., Massip, T., Ulliac, A., Simoni, J. L., & Varela, P. (2021). Automation of Risk-Based Vulnerability Management Based on a Cyber Kill Chain Model. Proceedings of the 28th C&ESAR, 233.

[4] Stone, Brain (2022, April 7). 54% of security professionals currently want to quit their jobs. CX Online. https://www.techrepublic.com/article/54-of-security-professionals-currently-want-to-quit-their-jobs/


Thank
You

QUESTIONS

ziaurrashid.com

ziaur-rashid@utulsa.edu