Predictive Vulnerability Management

Sruthika Sivakumar **Vedansh Maheswari** **Vanshraj**

1RVU22CSE164 **1RVU22CSE187** **1RVU22CSE526**

Introduction

Predictive Vulnerability Management (PVM) uses advanced analytics and machine learning to reduce potential vulnerabilities before they can be exploited. Unlike traditional methods that react to known threats, PVM handles vast amounts of data from sources such as historical attack patterns, threat intelligence, and assets to predict where and how vulnerabilities might arise.

PVM helps organizations prioritize vulnerabilities based on their potential threat,which allows security teams to focus on the most critical threats first.

PVM improves the overall security and integrates with other cybersecurity functions like threat intelligence and incident response.PVM also helps in regulatory compliance by adopting a security strategy that often exceeds regulatory requirements, thus building greater trust with customers and stakeholders.

Literature Review

1) *Yung-Yu Chang, Pavol Zavarsky, Ron Ruhl, Dale Lindskog, 09-11 October 2011 "Trend Analysis of the CVE for Software Vulnerability Management"* The research found a 28% decrease in the frequency of vulnerabilities and a reduction in high severity incidents from 2007 to 2010. Over 80% of vulnerabilities were exploitable via network access without authentication. Analysis of 18,427 vulnerabilities across 15 types revealed significant trends in frequency, severity, and CVSS base metrics, leading in security strategy development.

2) *Samuel Ndichu,Sylvester McOyowo, and Henry Okoyo ,Cyrus Wekesa ,08 October 2020 "A Remote Access Security Model based on Vulnerability Management"*

Information security threats exploit remote access vulnerabilities, with external devices posing higher risks. VPNs, despite secure connections, have exploitable vulnerabilities that encryption can hide. The study identifies weaknesses in traditional remote access security and proposes a machine learning-based solution to enhance security.

3)*Kalliopi Sapountzaki,14 August 2011 "Vulnerability management by means of resilience"*
The article insights about resilience functions in social-ecological systems, focusing on how actors manage vulnerability through re-arrangement. It centers on V Actors navigating various hazards by reconfiguring vulnerabilities across spatial and temporal scales, potentially reallocating resources and affecting others' vulnerabilities in the process.

4) *Michał Walkowski,Jacek Oko, Sławomir Sujecki, 19 September 2021 "Vulnerability Management Models Using a Common Vulnerability Scoring System"*
The article prioritizes vulnerabilities in data networks, crucial for effective management. The existing solutions lack organizational context, while commercial tools lack transparency. An open-source solution was introduced, the Vulnerability Management Center (VMC), which integrates CVSS to improve prioritization accuracy. Testing in real environments shows that the VMC software effectively speeds up fixing serious problems and lowers the risk for organizations.

5) *Ju An Wang, Minzhe Guo,13 April 2009,"OVM: an ontology for vulnerability management"*
The article proposes an ontological approach to improve the Information Security Automation Program (ISAP). By creating an ontology for vulnerability management (OVM) populated with NVD data, it uses inference rules and data-mining to understand vulnerabilities, attacks, and countermeasures, aiming to improve ISAP's effectiveness.

6)*O.H. Alhazmi; Y.K. Malaiya, 28 August 2006,"Prediction capabilities of vulnerability discovery models"*
The study explores quantitative methods for software security, focusing on vulnerability discovery models (VDMs) for risk assessment. It evaluates predictive accuracy using partial data, comparing logistic and linear models. Static approaches estimate vulnerability attributes, enhancing early model application. Results show constraints improve prediction errors, suggesting potential for combined model approaches.

7)*Katheryn A. Farris, John Sullivan, George Cybenko,5 May 2017,"Vulnerability survival analysis: a novel approach to vulnerability management"*The article addresses enterprise network security by examining how long vulnerabilities persist. Using the Cox proportional hazards regression model on real IT data, it checks vulnerability "time-to-death" and identifies factors for lower survival rates. This approach brings in better understanding and reduces network vulnerabilities.

8) *Marc A. Rosen, 5 April 2017,"Digital Threat and Vulnerability Management: The SVIDT Method"* The article introduces the SVIDT method for managing vulnerabilities in human systems against digital threats. It assesses system strengths and vulnerabilities, identifies potential threats, and evaluates interventions to improve resilience. Applied to a Swiss casino facing online gaming challenges, the method shows its benefits and limitations.

9)*Mart´ın Barrere, R`emi Badonnel and Olivier Festor,2014,"A SAT-based Autonomous Strategy for Security Vulnerability Management"* The article discusses a new method for autonomously assessing and fixing vulnerabilities in computer and network systems. Using a detailed mathematical model and formalizing the process as a SAT problem, the framework evaluates vulnerabilities and performs corrections. The feasibility is tested through various experiments, showing its effectiveness.

10)*Yolanta Beres, Jonathan Griffin, Simon Shiu, September 30, 2008,"Security Analytics: Analysis of Security Policies for Vulnerability Management"*The article introduces a new method using mathematical models and motivates to guide security investments and policy decisions. It examines standard patch management, emergency policies, and early mitigation measures. The study shows how these factors affect risk exposure, offering a new approach to security investment decisions beyond traditional risk analysis.

11)*Benjamin L. Bullough, Anna K. Yanchenko, Christopher L. Smith, and Joseph R. Zipkin, 24 March 2017,"Predicting Exploitation of Disclosed Software Vulnerabilities Using Open-source Data"*Thousands of software vulnerabilities are reported, posing security risks if unpatched. While many aren't exploited, prioritizing patches for likely-exploited vulnerabilities can save resources. Machine learning gives moderate success in predicting exploitation. This study reflects prior work, revealing how data selection impacts predictive model performance.

12) *Emrah Yasasin , Julian Prester , Gerit Wagner , Guido Schryen ,12 September 2019 ,"Forecasting IT security vulnerabilities – An empirical analysis"*Organizations face numerous IT security threats and need to predict and allocate resources for vulnerabilities. While much research focuses on source code analysis, limited work addresses post-release vulnerability forecasting. This study uses methodologies like exponential smoothing and ARIMA on NVD data, finding optimal forecasting methods vary by software package and robustness in error metrics.

13)*Soumyadeep Hore , Ankit Shah , Nathaniel D. Bastian , 28 February 2023 ,"Deep VULMAN: A deep reinforcement learning-enabled cyber vulnerability management framework"*Cyber vulnerability management is important for cybersecurity operations centers. Traditional methods are not adequate due to rising vulnerabilities and resource limits. The Deep VULMAN combines deep reinforcement learning and integer programming to allocate resources and prioritize vulnerabilities under uncertainty, outperforming current methods in simulations and real world data over a year.

14)*Jon M Heberlin , May 2023 ,"A Risk Based Approach to Technical Vulnerability Management"*This study evaluates risks related to vulnerabilities, focusing on the relationship between Exploit Code Maturity (ECM), Remediation Level (RL), and Report Confidence (RC) on CVSS scores. It uses data from the National Vulnerability Database, One-ANOVA analysis shows that temporal metrics can evaluate technical vulnerability risk, and provide recommendations for better management.

15)*Jaipal Reddy Padamati ,Laxmi Sarat Chandra Nunnaguppala, Karthik Kumar Sayyaparaju,18 September 2021 , "Evolving Beyond Patching: A Framework for Continuous Vulnerability Management"*This report shows regulatory compliance in cloud computing, focusing on Security Orchestration, Automation, and Response (SOAR), SIEM, and advanced threat detection. It points out continuous vulnerability management beyond regular patching, supporting sustained readiness against evolving threats. The findings show effective technology utilization and strategic recommendations for improving company security and compliance.

16)*Raghavendra Rao Althar, Debabrata Samanta, Manjit Kaur, Abeer Ali Alnuaim, Nouf Aljaffan, Mohammad Aman Ullah, 27 December 2021, "Software Systems Security Vulnerabilities Management by Exploring the Capabilities of Language Models Using NLP"* this paper examines data science methods to create a knowledge management system to have secure software development. With insurance domain data being used, it explores practical challenges and language modeling's role. The model assesses security during development, showing efficient vulnerability classification in experiments.

17)Rahi, K., Bourgault, M., & Preece, C, 2022-01-26 "Risk and vulnerability management, project agility and resilience: a comparative analysis. International Journal of Information Systems and Project Management"This paper shows project management literature on risk management, vulnerability management, project agility, and project resilience. It develops a framework highlighting their differences and convergences.It also shows risk and vulnerability management are active, project agility is reactive, and project resilience is both, helping recovery from disruptive events.

18)*Seth P. Tuler , Thomas Webler , Colin Polsky, 15 October 2012 "A rapid impact and vulnerability assessment approach for commercial fisheries management "* Fisheries managers need data and tools to assess socio-economic impact. The rapid impact and vulnerability assessment (RIVA) method efficiently assembles decision-relevant information, linking management actions to consequences. In this paper it is shown how RIVA helps managers to reduce negative impacts and give more positive responses.

19)Kylie McClanahan, Sky Elder, Marie Louise Uwibambe, Yaling Liu, Rithyka Heng, Qinghua Li , 2024,"When ChatGPT Meets Vulnerability Management:the Good, the Bad, and the Ugly"In their assessment of language models' utility in vulnerability management, researchers noted significant time savings potential. Models like ChatGPT had difficulty finding specific information when asked questions directly but they were very good at taking lots of documents about security issues and making short summaries. This could help make it faster and easier for people to decide which problems to fix first and how to fix them.

20)*Su Zhang, Xinming Ou & Doina Caragea,30 Nov 2015,"Predicting Cyber Risks through National Vulnerability Database"*This paper researches software vulnerabilities using NVD data which aims to predict future vulnerabilities important for cybersecurity management amid rising zero-day attacks. Despite efforts with data mining and machine learning, results showed poor predictive capability across NVD data, which suggested limited effectiveness in showing vulnerabilities except in select cases.

Theoretical background

Predictive Vulnerability Management has several theoretical areas, including machine learning, data analytics, risk management, and threat intelligence. PVM uses machine learning algorithms to analyze large datasets, identifying patterns and trends that can predict future vulnerabilities. These predictive models are informed by both supervised and unsupervised learning techniques, which help find potential vulnerabilities before they become critical issues.

Data analytics plays an important role by processing and interpreting this data to provide insights which involve descriptive, diagnostic, predictive, and prescriptive analytics to understand past vulnerabilities, identify root causes, future threats, and recommend preventive measures.

Risk management principles focus on identifying, assessing, and prioritizing risks. This involves evaluating the likelihood and impact of potential vulnerabilities and determining the most critical assets to protect. Threat intelligence improves PVM by providing

context about current and emerging threats, gathered from various sources and analyzed to understand threat actors and their methods. Traditional vulnerability management practices, such as scanning for known vulnerabilities and applying patches, form the foundation of PVM. By integrating these theoretical components, PVM creates a security strategy that anticipates and reduces potential threats before they can be exploited.

Research gap

The research gap in Predictive Vulnerability Management is improving data quality, developing transparent algorithms, improving real-time prediction, integrating with existing systems, understanding vulnerabilities, recognizing human and organizational factors, and ensuring regulatory compliance. Addressing these will improve PVM's effectiveness and scalability in these cybersecurity strategies.