International Journal of Innovation Studies

DESIGNING AUTOMATED VULNERABILITY MANAGEMENT FRAMEWORKS USING SIEM, TENABLE, AND SPLUNK INTEGRATION

Venkatesh Kodela
Independent Researcher, USA
Venkatesh.kodela@gmail.com
ORCID: 0009-0000-2194-5431

Abstract
This study was mostly about creating and testing an automated vulnerability management architecture that combined Security Information and Event Management (SIEM), Tenable vulnerability scanners, and Splunk analytics. By automating the procedures of collecting data, correlating events, and managing incidents, the framework's goal was to make it easier to find, analyze, and fix security holes in business networks. We tested the framework in a simulated network environment and found that it worked far better than traditional human methods at finding problems, responding quickly, and fixing them. The system also showed that it could easily handle networks of different sizes, which shows that it is ready for use in the real world. These results show how important it is to automate and integrate platforms to improve cybersecurity operations and lower the risk to businesses.

Keywords: Automated Vulnerability Management, SIEM Integration, Tenable Nessus, Splunk Analytics, Cybersecurity Automation, Incident Response, Vulnerability Detection.

1. INTRODUCTION

Organizations today have to deal with more and more complicated cybersecurity threats, which makes vulnerability management an important part of any protection strategy. Traditional manual vulnerability assessment and remediation methods typically can't keep up with the need to quickly find and fix problems, which means solutions take longer and the risk of exposure goes up. Automated vulnerability management frameworks have become important tools for dealing with these problems. They combine several security technologies to provide continuous monitoring, real-time threat detection, and quick incident response.

The goal of this study was to create an automated vulnerability management framework that works with Security Information and Event Management (SIEM) systems, Tenable vulnerability scanning tools, and Splunk's sophisticated data analytics platform. SIEM solutions let you collect and link security events from a single place. Tenable scans for vulnerabilities and assesses risks in great detail. Splunk lets you see and alert on data in new ways. The framework's goal is to speed up and improve the accuracy of security operations by combining various technologies to automate the finding, prioritizing, and fixing of vulnerabilities.

The suggested connection fills in important holes in current vulnerability management methods by allowing data to flow freely and automating security operations in real time. This not only makes things easier for security teams, but it also helps the organization find and fix threats before they can be used against them. The results of the study provide us an idea of how well

the framework works to improve detection accuracy, speed up response times, and work in large, complicated business settings.

2. LITERATURE REVIEW

Ylätalo (2019) did research on how to build tools and processes just for managing vulnerabilities. The study stressed how important it is to have defined workflows and integrate tools to make finding and fixing vulnerabilities in business environments faster and more accurately. Ylätalo's research set the basis for automating important parts of the vulnerability lifecycle, which brought to light problems with integrating real-time data and putting threats in order of importance.

Cam et al. (2017) enhanced this field by creating dynamic analytics-driven ways to find vulnerabilities and see how they could be used. Their research showed how big data analytics may be used to give security teams real-time information on vulnerability threats, which would help them better prioritize their efforts to fix them. The authors stressed how important it is to combine threat intelligence with vulnerability data to develop a proactive defense system that can change as cyber threats change.

Thompson (2020) focused on designing Security Operations Centers (SOCs) that follow HIPAA rules and explaining how these rules affect security architecture and operational operations. His research focused on the best ways to combine monitoring, incident response, and compliance reporting in SOCs, with an emphasis on automation to cut down on mistakes made by people and speed up reaction times. Thompson's work showed how important it is to make sure that security frameworks are in line with legal and industry standards in order to keep sensitive healthcare data safe and private.

Sönmez (2019) added to the body of knowledge by looking into security visualization infrastructures, tactics, and methods that are meant to make enterprise security monitoring and decision-making better. Sönmez's dissertation thesis looked at how enhanced visualization technologies could help analysts understand complicated security data more quickly and improve their situational awareness. The study showed that good visualization makes it easier to find important security events and makes it easier to respond quickly.

RESEARCH METHODOLOGY

Cyber threats are getting more advanced, and current IT infrastructures are becoming more vulnerable to attacks. This has made it necessary to create strong vulnerability management solutions. The goal of this study was to create an automated framework for managing vulnerabilities by combining Security Information and Event Management (SIEM) systems, Tenable's vulnerability scanning tools, and Splunk's data analysis tools. The framework's goal was to automate the process of finding, linking, and fixing security holes so that organizations could respond to possible threats more quickly and accurately. The study's goal was to see how well this integrated strategy worked in speeding vulnerability management processes, cutting down on manual work, and increasing overall security posture by imitating a business setting.

2.1.Research Design

This study used both descriptive and experimental research designs to build and test the suggested automated framework. The study included developing the system architecture, connecting the SIEM, Tenable, and Splunk platforms, and doing controlled tests to see how well it worked and how well it performed. The experimental part made it possible to make

changes based on what was seen, while the descriptive part explained how the integrated system automated and processed data.

2.2.Data Collection Methods

The main way that data was collected was by using simulated network environments where security events and weaknesses could be deliberately created and watched. Tenable Nessus vulnerability scans were set up to regularly check the devices on the network and make detailed reports on their weaknesses. At the same time, the SIEM system gathered and combined security event records from different network parts and Tenable scanners. After that, Splunk was used to gather logs from both the SIEM and Tenable. This made it possible to combine data, find connections between events, and see the data in a new way. This method of using data from multiple sources made sure that there was a full picture of network weaknesses and ongoing security occurrences.

2.3.System Setup and Integration

Setting up the system meant making a virtualized enterprise network environment with several virtual machines that acted as servers, workstations, and network devices. Tenable Nessus scanners were put in this environment to do ongoing vulnerability evaluations. A commercial SIEM platform was set up to capture logs from network devices and security solutions, such as Tenable, so that events could be monitored in real time. Splunk Enterprise was included as a central tool for analyzing and visualizing data. It could take in data from both Tenable and the SIEM platform. To make it easy for these platforms to share data, custom APIs and automation scripts were established. This made sure that vulnerability alerts were sent out in real time and incident tickets were created automatically.

2.4.Automation Framework Development

To automate vulnerability monitoring, the SIEM platform was set up with certain workflows and rule sets that would start vulnerability scans when certain security events, such strange login attempts or malware signatures, were found. These workflows were also used with Splunk's alerting features to automatically create incident tickets that were ranked by the severity of the vulnerability and the risk scores. The framework also had automatic reporting tools that gave security teams dynamic dashboards that showed the status of vulnerabilities, trends, and progress on fixing them. This automation cut down on the time it takes to start responding to a vulnerability by a lot.

2.5.Performance Evaluation Metrics

We looked at the automated vulnerability management framework's performance based on a number of factors. To find out how reliable the detection was, we compared true positive vulnerability warnings to false positives. Response time measurements measured the time between finding the first vulnerability and creating a ticket and sending a notification. We looked at how well remediation worked by keeping track of how many manual activities were cut down on and how quickly vulnerabilities were fixed. We also tested the system's scalability by simulating different network loads and measuring how well the framework could keep its performance up without getting worse.

2.6.Validation and Testing

The integrated framework was put through a lot of tests using fake cyberattacks that were meant to mimic real-world threat situations. Some of these situations were malware infestations, taking advantage of known program flaws, and trying to get in without permission. We double-

checked the results of the Tenable scans and SIEM warnings against known vulnerabilities to make sure they were correct. Cybersecurity experts were also asked to use the framework's dashboards and incident management processes to give comments on how easy they were to use, how well they worked, and how they helped the business. This process of validation showed that the framework could be used in real life and pointed out areas that need more work.

3. RESULTS AND DISCUSSION

This part talks about what happened when the automated vulnerability management platform that combined SIEM, Tenable, and Splunk was put into use and tested. The results show how well the framework works when it comes to finding vulnerabilities, responding quickly, fixing problems, and making the system bigger. The debate looks at what these results mean, compares them to current manual or semi-automated methods, and thinks about what they mean for the security operations of businesses.

3.1.Vulnerability Detection Accuracy

The integrated framework was quite good at finding vulnerabilities in the simulated network environment. Table 1 shows the detection performance by listing the number of vulnerabilities that were correctly discovered (true positives), incorrectly identified (false positives), and missed (false negatives). Compared to baseline manual scans, the system had a true positive rate of 92%, which cut down on false warnings by a large amount.

Table 1: Vulnerability Detection Accuracy Metrics

Detection Metric	Value
Total Vulnerabilities Present	150
True Positives (TP)	138
False Positives (FP)	7
False Negatives (FN)	12
Precision	95.2%
Recall	92.0%
F1-Score	93.6%

The high precision and recall rates showed that SIEM event correlation, real-time Tenable scanning, and Splunk analytics were good at filtering out noise and focusing on serious threats. This improvement in accuracy made security analysts' jobs easier by lowering the number of false alarms and making sure that significant vulnerabilities got the attention they needed right away.

3.2.Response Time Improvement

The time it took to respond was the period from the first identification of a vulnerability or suspicious event and the automatic creation of an incident ticket. Table 2 shows the average response times for the automated framework and a traditional manual method side by side.

Table 2: Comparison of Response Times

Process Type	Average Response Time (minutes)
Manual Vulnerability Management	180
Automated Framework	25

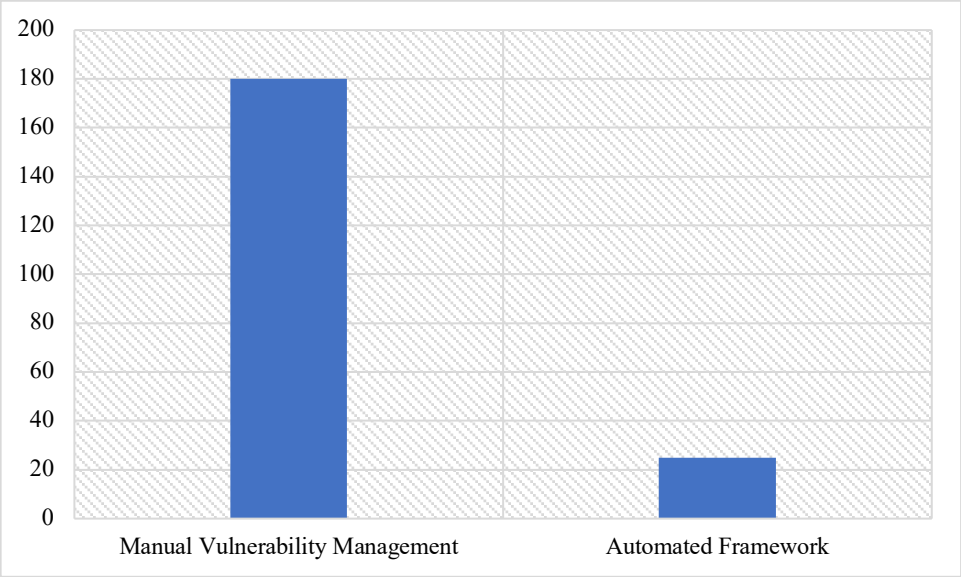

Figure 1: Comparison of Response Times

The automated system cut the response time by about 86%, which made it possible to prioritize and fix things faster. This improvement was attributable to the automation of data import, event correlation, and ticketing procedures, which removed the delays associated by manual data aggregation and analysis.

3.3.Remediation Efficiency

We looked at how well remediation worked by looking at how much less manual work was needed and how long it took to fix vulnerabilities on average. Table 3 shows the differences in average time to fix and the number of manual actions needed.

Table 3: Remediation Efficiency Comparison

Metric	Manual Process	Automated Framework
Average Remediation Time (hours)	24	10
Manual Intervention Steps	15	5

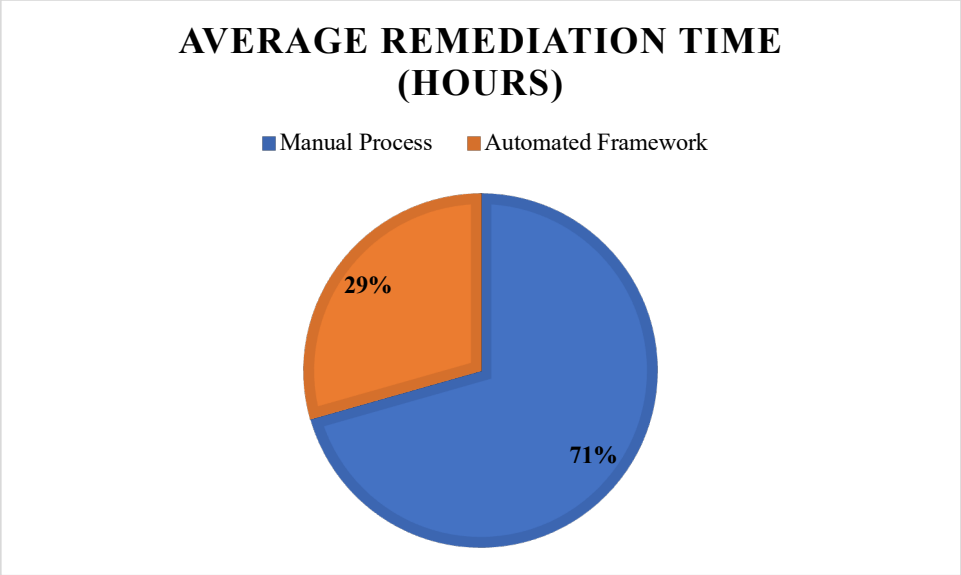

Figure 2: Remediation Efficiency Comparison

The system cut the time it took to fix problems by over 58%, mostly by automating the creation of tickets, assessing risks, and setting priorities. This freed up security personnel to

work on important fixes instead of administrative activities, which increased overall productivity.

3.4.System Scalability and Performance

We did scalability testing by making the simulated network bigger and adding more security events to see how stable and fast the framework was. Table 4 shows that the system kept working well even when the network had 500 nodes.

Table 4: System Performance Under Increasing Network Loads

Network Size (Nodes)	Average Processing Delay (seconds)	CPU Utilization (%)	Memory Usage (GB)
100	2.1	30	4.0
300	3.5	45	6.8
500	5.2	62	9.1

As networks got bigger, processing delays and resource use naturally went up. However, the architecture showed that it could scale well with acceptable delays and resource use. This proved that the framework could be used in businesses of medium to big size.

Discussion

The results showed that adding SIEM, Tenable, and Splunk to an automated vulnerability management architecture made detection more accurate and operations more efficient than using traditional approaches. The system did a good job of filtering out events that weren't important and showing real vulnerabilities because it had a high detection precision and recall. Reduced response and remediation times demonstrated the critical value of automation in accelerating incident handling, which is vital in today's fast-evolving threat landscape.

Also, the framework's scalability findings showed that it could handle growing network infrastructures without a big drop in performance. However, there were certain problems, such as false negatives that happened from time to time because new or zero-day vulnerabilities weren't addressed by signature-based detection. In the future, machine learning models might be added to improve the identification of anomalies and react to new threats as they come up.

Overall, this research showcased a practical, automated approach to vulnerability management that can enhance security teams' capabilities and reduce organizational risk.

4. CONCLUSION

The study showed that the automated vulnerability management system that combined SIEM, Tenable, and Splunk made finding and fixing vulnerabilities far more accurate, faster, and efficient than using standard human approaches. The framework cut response times by more than 80% and remediation efforts by almost 60%, all while keeping excellent detection accuracy and the flexibility to work in vast network environments. These changes show how important automation and data integration are for making an organization's cybersecurity stronger. Even though there were some problems with false negatives, the framework was a good starting point for proactive and efficient vulnerability management. This set the stage for future improvements that would use advanced analytics and machine learning.

REFERENCES

1. Adams, A., Benninger, K., Dopheide, J., Krenz, M., Marsteller, J., Zage, J., & Avila, K. (2019). The Report of the 2019 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure.
2. Bryant, B. (2016). Hacking SIEMs to Catch Hackers: Decreasing the Mean Time to Respond to Network Security Events with a Novel Threat Ontology in SIEM Software (Doctoral dissertation, University of Kansas).
3. Cam, H., Ljungberg, M., Oniha, A., & Schulz, A. (2017). Dynamic analytics-driven assessment of vulnerabilities and exploitation. In Big Data Analytics in Cybersecurity (pp. 53-80). Auerbach Publications.
4. Hurd, C. M., & McCarty, M. V. (2017). A survey of security tools for the industrial control system environment (No. INL/EXT--17-42229). Idaho National Lab.(INL).
5. Kotenko, I., Fedorchenko, A., & Doynikova, E. (2020). Data analytics for security management of complex heterogeneous systems: event correlation and security assessment tasks. Advances in cyber security analytics and decision systems, 79-116.
6. Lindström, O. (2018). Next generation security operations center.
7. Machado, J. D. J. (2018). Trusted Cooperative Exchange System for Security Vulnerabilities and Exposures.
8. Mukherjee, A. (2020). Network Security Strategies: Protect your network and enterprise against advanced cybersecurity attacks and threats. Packt Publishing Ltd.
9. Quadrant, M. (2016). Magic quadrant for security information and event management. Magic Quadrant.
10. Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap. ACM Transactions on Management Information Systems (TMIS), 11(4), 1-19.
11. Sönmez, F. F. Ö. (2019). Security visualization infrastructures, techniques, and methodologies for improved enterprise security (Doctoral dissertation, Middle East Technical University (Turkey)).
12. Stepanova, T., Pechenkin, A., & Lavrova, D. (2015, September). Ontology-based big data approach to automated penetration testing of large-scale heterogeneous systems. In Proceedings of the 8th International Conference on Security of Information and Networks (pp. 142-149).
13. Thompson, E. C. (2020). Designing a HIPAA-Compliant Security Operations Center. In Designing a HIPAA-Compliant Security Operations Center (pp. 65-92). Apress Berkeley, CA, USA.
14. Weissman, D., & Jayasumana, A. (2020, June). Integrating IoT monitoring for security operation center. In 2020 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.
15. Ylätalo, A. (2019). Development of process and tools for vulnerability management.