ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/venkat-soma/248

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 2

Review

Compliance/Vulnerability Scanning Using Prisma Cloud for Cloud Deployments

Venkat Soma*

Citation: Soma V. Container Orchestration with Kubernetes. *J Artif Intell Mach Learn & Data Sci 2024*, 2(2), 1046-1049. DOI: doi.org/10.51219/JAIMLD/venkat-soma/248

Received: 03 June, 2024; **Accepted:** 28 June, 2024; **Published:** 30 June, 2024

***Corresponding author:** Venkat Soma, New York Mets, USA

ABSTRACT

In the present era of widespread cloud technology adoption, it is necessary to ensure the compliance and security of cloud deployments. This research examines the effectiveness of the Prisma Cloud for the enhancement of the security level within the cloud environments through compliance and vulnerability scanning. The Prisma Cloud is a cloud-native security platform that assists in maintaining compliance and scanning vulnerabilities. Through leveraging the cloud security posture management and cloud workload protection, the Prisma cloud provides continuous monitoring, real-time alerts and automated remediation for maintaining regulatory compliance and identifying security issues. This study tries to explore the functionalities and features of the Prisma cloud related to compliance and vulnerability scanning through the identification of the strengths and limitations. This research study also offers probable recommendations for the optimisation of its utilisation in organisational settings.

Keywords: Cloud security, compliance management, Prisma Cloud, vulnerability scanning, automated remediation, cloud workload protection.

1. Introduction

1.1. Project specification

In the present landscape of increasing adoption of cloud technologies, it is necessary to ensure the compliance and security of cloud deployments become a necessary concern for organisations. The Prisma Cloud refers to the native security solution which provides "*Cloud Workload Protection*" (CWP) and "*Cloud Security Posture Management*" (CSPM) components that assist in preserving the cloud environments[1]. The present research focuses on leveraging the Prisma cloud for the enhancement of the security posture of cloud deployments through the identification of the issues associated with vulnerability and compliance management. This project includes a comprehensive examination of the abilities of Prisma Cloud in the conduction of vulnerability and compliance scanning for cloud deployments.

1.2. Aims and objectives

This research aims to evaluate the effectiveness of Prisma cloud to ensure compliance and address the vulnerabilities in cloud deployments.

The key objectives are as follows:

- To explore the functionalities of Prisma cloud relevant to vulnerability and compliance scanning
- To analyse the outcomes of the assessment and address the main strengths and limitations of Prisma Cloud
- To provide recommendations for organisations to optimise the use of Prisma Cloud for compliance and security

1.3. Research questions

- RQ 1: What functionalities of Prisma cloud are relevant to compliance and vulnerability scanning?
- RQ 2: What are the results of the assessment related to the identification of strengths and limitations of Prisma cloud?
- RQ 3: What are the main recommendations for the optimisation of the use of the Prisma cloud?

1.4. Research rationale

Issues: The research will address the complications of the cloud environments which make it challenging to maintain compliance and consistent security. It focuses of the identification of vulnerabilities and ensures the timely improvement of large-scale cloud environments.

Reason for the issues: Cloud environments evolve continuously with frequent alterations in deployments and configurations. The scale of the cloud environments makes it difficult to conduct a holistic and continuous vulnerability assessment.

Present issues: The present landscape of cloud security presents several challenges. Many organisations lack detailed visibility into the cloud environments which hinders their effective compliance and vulnerability management[2]. The traditional vulnerability management techniques are not well-suited for the cloud leading to the ineffective detection and elimination of the issues.

2. Literature review

2.1. Research background

The adoption of cloud computing has transformed the IT landscape which offers better scalability, cost-efficiency and flexibility. This shift introduces significant security issues as the traditional security measures are inappropriate for the dynamic and distributed nature of the cloud environments. Many organisations face dual challenges to ensure compliance with regulatory standards and protect against vulnerabilities. The Prisma Cloud is developed by Palo Alto Networks which is the cloud-native security platform. It is structured for the identification of issues through delivering detailed tools for compliance and vulnerability scanning across multi-cloud and hybrid environments[3].

2.2. Critical assessment

The primary cloud offers a wide range of features designed for the enhancement of the security posture of cloud deployments. The Prisma cloud monitors the cloud environment continuously to maintain compliance with the various regulatory standards such as PCI-DSS, GDPR and many more through delivering comprehensive reports and real-time alerts[4]. Prisma Cloud provides automated improvement of the capabilities which enables the organisation to address the vulnerabilities quickly. This platform integrates with various security tools such as DevOps facilitate seamless workflows and the automation of the security process[5].

2.3. Linking with aim

The primary aim of this research is to evaluate the efficiency of the Prisma cloud to ensure compliance the address the vulnerabilities in the cloud deployments. Through the critical assessments of the capabilities of Prisma Cloud, this research tries to provide actionable insights along with the best practices for the organisation's aims to enhance its cloud security. The critical assessment highlights the strengths and the limitations of Prisma cloud which sets the stage for a detailed investigation and practical recommendations.

2.4. Vulnerability scanning process and its benefits

The vulnerability scanning process started with the findings of the cloud resources including the virtual machines and serverless functions. The Prisma Cloud conducts a thorough assessment of the discovered resources and scanning of the vulnerabilities. The identification of the vulnerabilities is prioritised depending on the severity and exploitability which enables the organisation's focus on the most critical issues. Incorporation of the Prisma Cloud increases the pace of scanning that identifies the security gaps before exploitation[6]. Through ensuring compliance with the regulatory standards, various organisations can able to avoid costly penalties and enhance their reputations.

2.5. Theoretical framework

This proposed research is grounded in the principles of cloud security and compliance management which have been drawn from the establishment of the theories and the models in this field. ***Cloud Security Alliance and the Cloud Control Matrix*** refer to a framework for the assessment of cloud security controls and compliance with industry standards[7]. The ***shared responsibility model*** relies on the concept that cloud security is a shared responsibility among the cloud service provider and customer[8]. This further emphasises the need for vigorous security measures on each side.

2.6. Literature Gap

Though there exists vast varied enriched literature on cloud security along with compliance, specific research on the practical application and the effectiveness of comprehensive platforms such as Prisma remain limited. There is a lack of empirical studies for the evaluation of the real-world effectiveness of Prisma Cloud in diversified cloud environments.

3. Methodology

3.1. Research philosophy

The interpretivism research philosophy has been used in this research as it focuses on understanding the context-specific gradation of the organisations in the implementation of the Prisma Cloud for vulnerability and compliance scanning. This philosophy provides values to the complications of the cloud environments and aims to interpret the actual implications and meanings of the features embodied into Prisma clouds within these environments. Through the utilisation of the interpretivism research philosophy, this research can be able to provide in-depth insights about the process of perceives of Prisma cloud and its usage through the different stakeholders. This further assist in the captivation of the practical realities and the challenges faced in the current phenomenon.

3.2. Research approach

A deductive approach in implemented in this research as this research study started with the establishment of the frameworks and theories associated with the cloud security. Deductive approach is concerned about the development of the theories related to the existing study[9]. These theories are used in the formulation of the hypothesis about the effectiveness of the Prisma clouds. The incorporation of the various theories through the empirical observations leads to the testing of the validity of these theories within the data collection process. Through following the deductive approach, this research study can bale to verify the theoretical assumptions in a systematic manner and evaluate the performance of the prisma cloud. This further ensures the structured analysis of the capabilities of Prisma cloud in identifying and eliminating vulnerabilities issues.

3.3. Research design

The descriptive research design is selected in this study to deliver a vigorous overview of the prisma cloud's functionalities and its implementation of the prisma process and its result. The descriptive research design includes the utilisation of a ranger of quantitative and qualitative research methods for the collection of the data that assists in the accurate description of the research problem[10]. This research design allows the researchers for the detailed documentation and the analysis of the process through which prisma cloud is used for the compliance along with the vulnerability scanning in various cloud environments. Through focusing on the description, this research can comprehensively capture and showcase the present state of the cloud security practices and the identification of the common issues and best practices. Incorporation of this research design ensures that the findings are practical and informative enough for the organisations looking for the enhancement of the cloud security.

3.4. Data collection method

In this research, the secondary data collection method is used to analyse the vulnerability scanning by using Prisma Cloud for the cloud deployments. This method is used in this research as it allows the researchers to navigate the existing information and the actionable insights from the previous studies, databases and the reports related to the cloud security through Prisma cloud. The secondary data offers a broader range historical context and perspectives which enhance the in-depth analysis of the proposed research. This approach is cost-effective and time-efficient which allows the wider foundation of knowledge without the requirement for the extensive primary data collection.

3.5. Ethical considerations

Ethical considerations are the baseline for the research that used secondary data to ensure the credibility and integrity of the research. It is necessary to verify and validate the sources through ensuring that the data is relevant and unbiased. The proper citation and the attribution of the secondary data sources are essential for maintaining intellectual property rights and avoid plagiarism. The researchers have to be aware of the context when interpreting the secondary data. It is also essential to ensure the confidentiality and privacy of any type of personal data within the secondary data to foster the ethical standards in this research.

4. Results

4.1. Critical analysis

There exist various security control tools such as CSA Cloud control matrix and the NIST cybersecurity framework which provides holistic guidelines for the cloud security along with the compliance[11]. However, the Prisma Cloud contributes significantly in the cloud security through monitoring, automated remediation and the vulnerabilities scanning. The prisma cloud accelerates to provide holistic compliance and the vulnerabilities scanning features. The automated remediation along with the real-time alerts fosters the operational efficiency. However, the complications in this area may poses issues for the newly engaged users. The integration with the existing tools can become challenging which requires comprehensive management and configuration.

4.2. Findings and discussion

The prisma cloud enhance the cloud security through the continuous monitoring and the identification of the vulnerabilities. Prisma cloud scans the open-sourcing dependencies in the source packaging, registries and deployment of images and compares these with the public databases such as NDV. This assist in the in-depth identification of the vulnerabilities at any dependency point. This platform integrates with the Ci/CD pipeline which allows an individual to scan the container images during the building process of central dashboards[12]. This offers the vigorous automated remediation through the integration with the DevOps workflows. AS the Prisma Cloud significantly enhance the cloud security, it is necessary for the sports organisations to increase investment level in the training and management of integration.

Theme 1: Functionalities of prisma cloud relevant to vulnerability and compliance scanning.

The prisma cloud provides a centralised insights of the vulnerabilities across the public and private cloud and the on-promises environments. The vulnerability scanning process of the prisma cloud includes the acquirement of visibility into the vulnerabilities across virtual machines, Kubernetes, misconfiguration and serverless functions[13]. The prisma cloud assist in the visualisation of the potential risk factors across the container images, host operating system and the serverless functions within the vigorous risk sourcing. Through the conduction of correlation between the vulnerabilities with the various risk factors such as excessive permissions, external exposure and misconfigurations, Prisma cloud can foster its remediation efforts. The Prisma cloud scans across the languages with the accuracy and identify the issues in the open-sourcing package. This supports the popular languages and leverage more than 300 data sources for the minimisation of the false positives.

Theme 2: The result related to the identification of strengths and limitations of Prisma cloud.

The Prisma cloud provides a combined view of the vulnerabilities across various cloud environments such as private, public and on-promises environments[14]. The Prisma cloud supports the agent based this includes the containers, hosts and serverless functions which ensures the comprehensive visibilities[15]. As well as the agentless scanning which allows various organisations of the sports industry to select the most suitable approach for its organisational infrastructure.

Theme 3: Key recommendations for the optimisation of the use of the Prisma cloud.

4.3. Evaluation

The prisma cloud is evaluated depending on the capability to deliver the continuous compliance monitoring and the efficient vulnerabilities scanning and the seamless integration with the existing security tools. The performance of the cloud environments is assessed in the various cloud environments through investigating its scalability, user-friendliness and the accuracy.

5. Conclusion

This research showcases that the Prisma cloud is an efficient tool for the enhancement of cloud security through the holistic vulnerabilities along with compliance scanning abilities. The Prisma cloud assists in continuous monitoring and automated remediation is paramount in maintaining compliance with the different regulatory standards and the protection against security issues. The findings suggested that the Prisma cloud significantly

enhances cloud security. There exist various challenges in the integration along with the user management which require proper identification. The optimisation of the Prisma Cloud performance can be conducted by the organisations through the improvement of automation capabilities and the integration of advanced machine learning algorithms for early detection of security threats. It further enhances the user interface and develop more customizable reporting options.

6. Research Recommendations

- Improve the automation capabilities for the compliance checking and the vulnerabilities which requires the integration of the CI/CD pipeline.
- Implement advanced machine learning algorithms for the detection of threats and challenges clearly.
- Enhance the user interface for providing more congenital navigation and easier access to the essential features.
- Develop more comprehensive and customizable reporting options which allows the users to generate those reports that includes different regulatory needs and internal security policies.
- Foster strong communication through creating webinars, cloud-based programmes and training initiatives.
- Expand the integration abilities with the other compliance and security tools which enables the more holistic security ecosystem.

7. Future Work

Future work for the proposed research should focuses on the various aspects related to the Prisma cloud features for the maintenance of compliance and scanning of the vulnerabilities. The further research on this topic should examine the application of the advanced AI and machine learning techniques for the enfacement of the threat detection along with the predictive analysis. The future research has to study the integration of the Prisma Cloud with the emerging technologies including edge computing, serverless commuting and IoT. Through the exploration of the methods for ensuring consistent compliance coupled with the security across the multiple cloud providers in the sports industry. The further research can conduct the user studies for the collection of feedback on the usability and the effectiveness of the Prisma Cloud to maintain compliance and mitigate vulnerabilities. Through focusing on these areas, the future research significantly contributes in the enhancement of the capabilities and thew applicability of Prisma Cloud in the various cloud deployment contexts.

8. References

1. https://www.theseus.fi/handle/10024/406583
2. https://ieeexplore.ieee.org/abstract/document/9441298/
3. https://search.proquest.com/openview/0814f5b72cc9655547426a7e94acbbc7/1?pq-origsite=gscholar&cbl=18750&diss=y
4. https://elibrary.kubg.edu.ua/id/eprint/48589/
5. https://repository.ihu.edu.gr/xmlui/handle/11544/30461
6. https://www.sciencedirect.com/science/article/pii/S0167404823002936
7. https://www.mdpi.com/2673-8732/3/3/18
8. https://doi.org/10.1016/j.cose.2021.102580
9. L. Varpio, E. Paradis, S. Uijtdehaage, et al. The distinctions between theory, theoretical framework, and conceptual framework. Academic Medicine, 2021; 95: 989-994.
10. SL Siedlecki. Understanding descriptive research designs and methods. Clinical Nurse Specialist, 2020; 34: 8-12.
11. https://www.researchgate.net/profile/Angelia-Chandra/publication/346510456_Measurement_of_the_Cloud_Security_Level_at_Company_using_Cloud_Control_Matrix/links/5fc5b09492851c3012993c7c/Measurement-of-the-Cloud-Security-Level-at-Company-using-Cloud-Control-Matrix.pdf
12. https://www.researchgate.net/profile/Manish-Abhishek/publication/360379894_Framework_to_Deploy_Containers_using_Kubernetes_and_CICD_Pipeline/links/628319477da61013d7484662/Framework-to-Deploy-Containers-using-Kubernetes-and-CI-CD-Pipeline.pdf
13. https://elibrary.kubg.edu.ua/id/eprint/48589/
14. https://doi.org/10.3390/jsan10030042
15. Y. Li, Y. Lin, Y. Wang, et al. Serverless computing: state-of-the-art, challenges and opportunities". *IEEE Transactions on Services Computing*, 2022; 16: 1522-1539.