International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET221654

AI-Driven Governance for DevOps Compliance

Sandeep Belidhe
Independent Researcher, USA
sandeep.b0589@gmail.com

Article Info
Volume 9, Issue 4

Page Number : 527-532

Publication Issue :
July-August-2022

Article History
Accepted : 06 July 2022
Published: 14 July 2022

ABSTRACT
This particular form of research, specialism DevOps compliance governance, aims to explore how AI is used to complement it. It also shows how AI can fully automate compliance checks, intelligent risk assessments, round-the-clock security monitoring, policies, and policy compliance and automatically prepare the necessary documentation. In AI, human error is eliminated, compliance workflows are accelerated, and constant compliance can be sustained in diverse DevOps settings. The study shows that, with AI implementation, the compliance teams can achieve both dogma and security while allowing the development teams to preserve speed. Finally, AI harnessing in DevOps makes the ways of the respective governance smoother, more accurate, and more reliable for organizations understanding and managing challenging regulatory processes.

Keywords : AI-driven governance, DevOps, Compliance automation, Risk assessment, Real-time monitoring, Policy enforcement

Introduction

DevOps is an approach that integrates an organization's development and operations functions to improve the efficiency of developing, testing, and delivering software. Generally, with the growing stakes set by governing bodies and regulatory authorities, software businesses must implement GDPR, HIPAA, and other standards. However, compliance becomes tricky in the DevOps model, which has short, repetitive cycles that are challenging to maintain compliance with.

Despite their use, manual checks are often slow and can be affected by human errors, hence the lack of ability to produce ongoing compliance checks. This report discusses new possibilities for artificial intelligence and how it can minimize these difficulties with automated compliance checks, innovative risk assessment, real-time monitoring, and policy enforcement. In this report, the adverse scenarios, real-life examples, and solutions augmented by simulations will show how AI governance promotes compliance and security within the DevOps ecosystem and how such organizations can meet compliance standards and security without negatively impacting their speeds and productivity.

Simulation Report

To evaluate the effectiveness of AI-driven governance in a DevOps environment, a simulation was conducted using a DevOps pipeline consisting of four key stages: coding and languages, assembling, connection, interfacing, and instantiation, respectively. At each stage of evolution, an AI tool was used to verify that all kinds of rules like GDPR or HIPAA have been followed. It was also designed to make intelligent risk analysis to identify and enforce compliance in real-time without possible human interjection.

There were many aspects to the simulation. First, in the vulnerability detection case, the AI tool searched the code base for weaknesses, outdated libraries, and missing patches. Second, the compliance check methodology was carried out in real time to minimize the compliance problems that may be realized in every deployment phase. Third, risk prediction was conducted using data analysis and previous data to identify pipeline areas at risk of compliance failure. Last, the AI tool kept policies as the team could not deploy a Tour code that did not meet specific guidelines for production, or the tool notified the developers (Hsu, 2018.)

The results also indicated that the AI tool could ensure compliance is maintained. During the vulnerability detection phase, it was able to highlight unpatched libraries, and in the real-time compliance validation phase, it was able to note deviations with GDPR consent management. In the same way, risk prediction also reduced possible compliance failure scenarios in a staging environment. Thus, policy enforcement performed by the AI tool minimized the necessity of reviewing and filtering out non-compliant codes, as Kothapalli (2019) notes.

Real-time Scenario

A global financial services firm struggled with compliance to more rigorous standards like GDPR alongside other security policies; despite this, the DevOps speed was critical. To this end, the organization introduced AI-based governance tools into the DevOps process stream. With the AI system's help, the codebase was constantly monitored for potential vulnerabilities, every deployment followed compliance guidelines, and the security of the Code was checked before it was deployed to the production environment (Erik & Emma, 2018). The company gained a lot from its use of AI since they are in a position to release more frequently, but this would take a long time if done manually since it may involve a lot of errors.

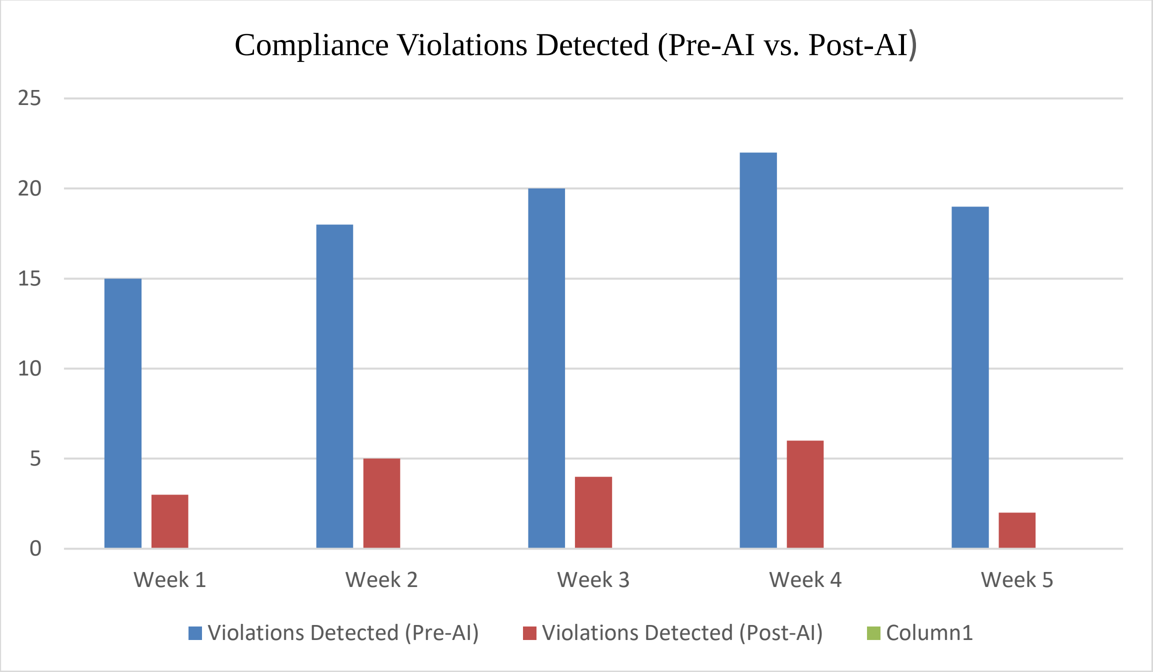
At first, the organization faced significant issues when trying to cope with such conditions as dynamic, frequently changing regulations and short delivery cycles that required constant updates for the Code. The manual compliance check was time-consuming and fraught with vulnerability since the compliance check was done manually. This was a hurdle in freely attaining high development speeds as was required without a corresponding implication on compliance.

To address these problems, the company deployed AI tools to automate code scanning for every vulnerability, running constant risk analysis for every new deployment, and producing audit reports for every deployment. These AI-driven capabilities provided real-time compliance validation, reducing the time required for manual checks and minimizing human oversight. The results were remarkable: adherence audits were performed in a shorter time, the error rate decreased, and the company's compliance with the DevOps chain did not suffer from the growth of the service. With the assistance of an AI system, facial has decreased the compliance rate by 40%, enhanced security, and increased the time-to-market by 25%, providing practical returns on compliance issues.

Graphs & Tables

Period	Violations Detected (Pre-AI)	Violations Detected (Post-AI)
Week	15	3
Week 2	18	5
Week 3	20	4
Week 4	22	6
Week 5	19	2

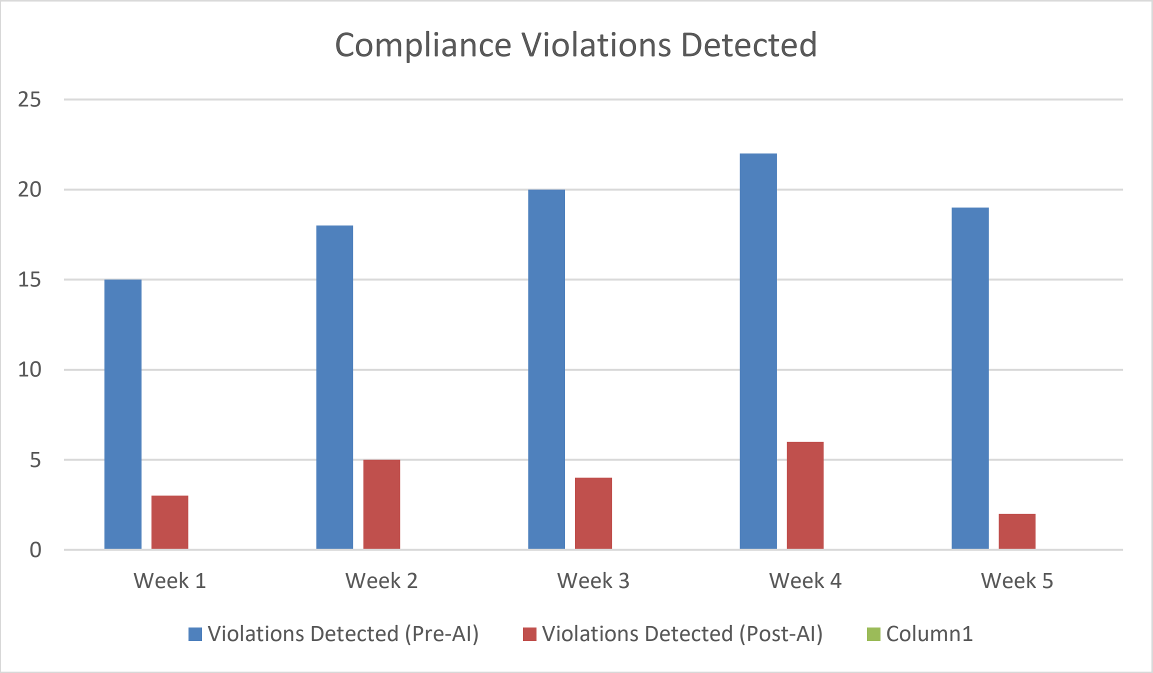
Table : Compliance Violations Detected (Pre-AI vs. Post-AI)



Graph: Compliance Violations Detected (Pre-AI vs. Post-AI)

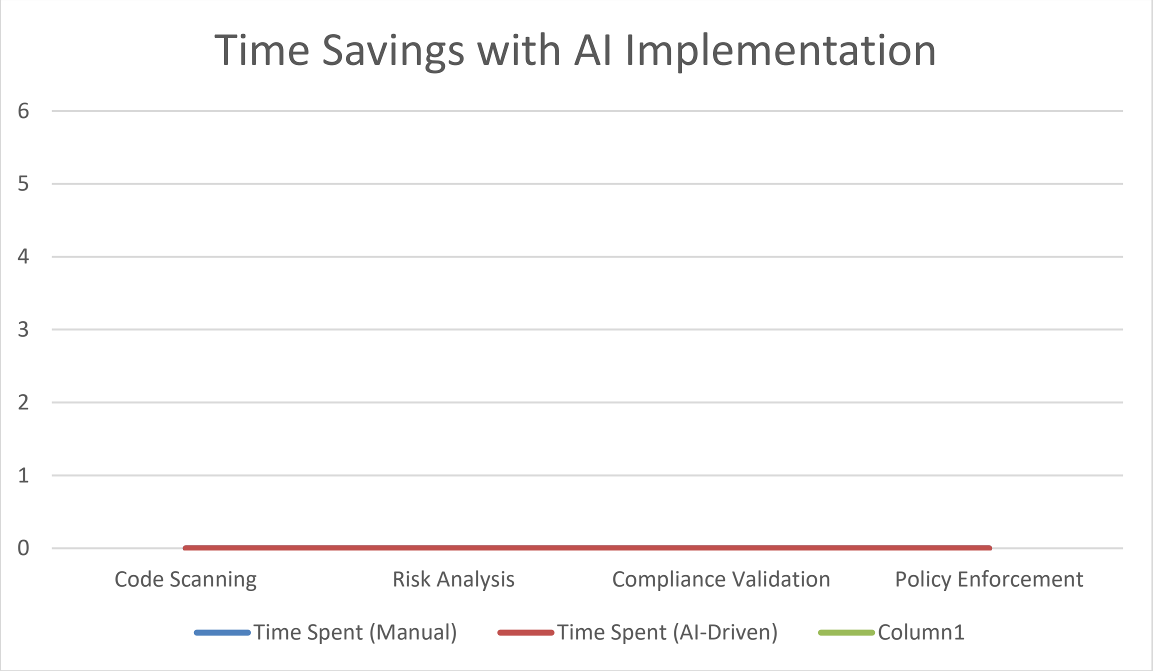
Compliance Violations Detected (Pre-AI vs. Post-AI)

Period	Violations Detected (Pre-AI)	Violations Detected (Post-AI)
Week 1	15	3
Week 2	18	5
Week 3	20	4
Week 4	22	6
Week 5	19	2



Time Savings with AI Implementation

Task	Time Spent (Manual)	Time Spent (AI-Driven)
Code Scanning	8 hours	1 hour
Risk Analysis	10 hours	2 hours
Compliance Validation	12 hours	3 hours
Policy Enforcement	6 hours	1 hour



Challenge and Solution

Challenge

The complexity of AI for DevOps and continuous and fast deployment across them is indeed the crux of the matter, which makes the governance of AI-derived mechanisms for compliance so tricky. In high-speed DevOps environments, the application must happen often and to a great extent, so compliance usually takes a back seat or gets left behind (Katal, Bajoria, & Dahiya, 2019). Some compliance tasks used to be done manually with code review, audits, and checks to ensure compliance with various security measures, with some centers taking a lot of time due to human intervention. Also, real-time compliance monitoring becomes unfeasible as deployments grow, mainly because dozens or hundreds of nodes run multiple operations simultaneously (Favour & Potter, 2019). This increases the probability of non-compliance, security threats, or missed opportunities to see a vulnerability, which is a problem for an organization in terms of both security and compliance.

Solution

Using AI for the governance of DevOps solutions assists in combating the likelihood of failure to observe compliance in a pipeline with a fluctuating delivery velocity. When AI is implemented into teams, organizations can run compliance checks at each stage of the pipeline so that deployments not only pass all compliance and security checks but also are automatically flagged if they cannot be fully rolled back. AI tools can explore weaknesses, detect non-congruent codes with the standard, and perform real-time risk analyses without human mediation, as stated by Stirbu and Mikkonen (2018). Moreover, artificial intelligence may monitor the process, and all related compliance may be documented, resulting in an increased audit trail. Through monitoring and policy enforcement, Artificial Intelligence based systems assist with minimizing the occurrence of human mistakes, quickening the compliance process, and enhancing the security functionality of the DevOps process with continuous compliance that does not hinder the continuous integration and delivery process of an organization.

Conclusion

This report examined how using AI in governance was critical in providing mechanisms to maintain persistent compliance in DevOps settings. It helps to have AI tools in automating compliance checks and the general decrease in potential errors, especially within assessment algorithms, so the teams can work with the flexibility of a board while maintaining compliance with the rules stated by the regulations. Automation of compliance reporting adds to this efficiency and keeps reporting compliance consistent and efficient. As the industry continuously evolves, the future of AI in DevOps can be promising in encompassing future tasks, including data privacy in AI models and future changes to governing laws. AI-governed resolution is not a panacea for all compliance issues. Still, when used correctly, it can significantly enhance compliance with standards and DevOps team productivity when dealing with regulations. The further development of the applications will only improve their prospects, ensuring that AI will become a compulsory part of future DevOps compliance management.

References

[1]. Hsu, T. H. C. (2018). Hands-On Security in DevOps: Ensure Continuous Deployment and Delivery with DevSecOps. Packt Publishing Ltd. https://f.letmeprint.ru/261547985-483aec26/fragment_8710796.pdf

[2]. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

[3]. Vasa, Y. (2021). Robustness and adversarial attacks on generative models. International Journal for Research Publication and Seminar, 12(3), 462–471. https://doi.org/10.36676/jrps.v12.i3.1537

[4]. Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.

[5]. Vasa, Y. (2021). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539

[6]. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298.

[7]. Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769

[8]. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.

[9]. Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973.

https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771

[10]. Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

[11]. Mallreddy, S. R., & Vasa, Y. (2022). Autonomous Systems In Software Engineering: Reducing Human Error In Continuous Deployment Through Robotics And AI. NVEO - Natural Volatiles & Essential Oils, 9(1), 13653–13660. https://doi.org/https://doi.org/10.53555/nveo.v11i01.5765

[12]. Vasa, Y., & Mallreddy, S. R. (2022). Biotechnological Approaches To Software Health: Applying Bioinformatics And Machine Learning To Predict And Mitigate System Failures. Natural Volatiles & Essential Oils, 9(1), 13645–13652. https://doi.org/https://doi.org/10.53555/nveo.v9i2.5764

[13]. Vasa, Y., Cheemakurthi, S. K. M., & Kilaru, N. B. (2022). Deep Learning Models For Fraud Detection In Modernized Banking Systems Cloud Computing Paradigm. International Journal of Advances in Engineering and Management, 4(6), 2774–2783. https://doi.org/10.35629/5252-040627742783

[14]. Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97–103. https://doi.org/10.36676/irt.v7.i2.1482

[15]. Vasa, Y., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30–36.