International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST5231096

Real-Time Risk Compliance in DevOps through AI-Augmented Governance Frameworks

Sandeep Belidhe
Independent Researcher, USA

Article Info
Publication Issue
Volume 10, Issue 1
January-February-2023

Page Number
778-782
Article History
Accepted: 20 Jan 2023
Published: 09 Feb 2023

ABSTRACT

In a constantly growing DevOps environment, there is a need to monitor the risks needing compliance in real time to meet security and regulation needs. This paper focuses on applying AI systems in governance structures where machine learning (ML) and predictive analytics enhance risk detection and mitigation. Compliance checks lower human interaction in identifying deviations and operational risks. An example of AI in action for DevOps pipeline risk detection is shown through a simulation; a case study from the financial industry shows its relevance. This paper discusses issues like integration, security, and possibly increasing the capacity of the AI system and possible solutions like deploying compact AI systems, anonymizing data, and cloud computing. Here, AI requires secure, efficient, and self-healing DevOps systems.

Keywords: Real-Time Risk Compliance, AI-Augmented Governance, DevOps, Continuous Monitoring, Predictive Analytics, Risk Management, Automation in DevOps, Compliance Automation, Machine Learning, Regulatory Adherence, Risk Detection, Security and Compliance, Cloud-Based Platforms.

Introduction

DevOps is an essential practice in today's software development and technology operations to serve as the bridge between development and operation while highlighting the role of efficiency, automation, and frequent delivery. CD and collaboration make it easy for DevOps teams to release quality software faster since they are aligned with nominals of software delivery. However, due to the enhanced velocity and integration of the DevOps process, instances of security law and data protection violations are also likely. In such dynamic contexts, threats can rapidly go out of hand if not controlled and managed – resulting in doubts, security incidents, or fines.

AI-augmented governance frameworks present a solution for checking compliance and coupling real-time monitoring of DevOps processes. These tools can identify dangers from the beginning, estimate threats that may become an issue, and guarantee that all work on development and deployment complies with the legislation. It is, therefore, the aim of this report to discover if and how AI can make risk management real-time and simultaneous with the processes in DevOps without compromising on either security or productivity. In conclusion, only real-time compliance reduces risk to money and other violations, fortifies the organization, and increases adherence to regulatory standards to avoid later overturns and generate sustainable innovations free of vital risks.

Simulation Report

This report incorporates an example of a conventional DevOps pipeline that can also contain and leverage AI tools to address risk assessment and compliance and offer continuous monitoring. The pipeline's stages include code development and testing, deployment, and maintenance. It also consists of a governed risk compliance process, followed several times. All these AI tools are integrated to perform different tasks, perform risk analysis, and anticipate problems before they malfunction.

Thus, in this environment, innovations such as machine learning (ML) and natural language processing (NLP) are adopted for compliance and to improve security. Artificial intelligence and machine learning models read through historical data in search of new signs of threats to security or instances of infringement of compliance (Aziz & Dowling, 2019). In the development processes, NLP is employed to understand code and documentation to guarantee adherence to regulatory requirements. These technologies enable or facilitate risk management in DevOps based on multiple spectrums (Halper, 2019).

An essential application of AI's predictive analytics is to anticipate different risks before they occur, including security threats or compliance issues. This proactive risk detection enables the team to mitigate the problems before they get out of hand. AI also monitors the development and deployment environment at intervals to ensure compliance throughout the SDLC. Moreover, AI validates compliance across all designed processes, like handling of data and data encryption, to meet regulatory standards (Gokani, 2017).

The results introduced from the simulation were quite encouraging. AI also tracked possible weaknesses in real time and promptly addressed such deficiencies. Implementing the automated checks greatly enhanced productivity compared to manual interventions and validation. In general, with the assistance of AI, the governance improved the DevOps pipeline, augmented the risk management and compliance, ensured that the system did not become vulnerable to any malicious attacks and the DevOps thus was safe from any security threats and hence less prone to delays or costly hacks (Jain, 2018).

Real-Time Scenario

In this case, a financial institution uses AI to keep risk compliance up to date within its DevOps processes. The firm operates in a financial industry with strict rules to the standards it seeks to adopt, like the PCI DSS for protecting payment card industry data. As part of the DevOps system, CD cycles are used for swift app development, delivery, and adherence to company regulations. Into this pipeline are incorporated AI tools that detect security threats, compliance issues, and other risks (Alsheiabni et al., 2019).

AI in this scenario is essential in risk estimation and mitigation during code development and deployment. The deep learning model scans the code for various security threats and reports probable compliance issues in advance, impacting the system. However, it also produces compliance reports with the regulation of activities in compliance with the requirements of the sectors and standards, such as PCI-DSS. In case of a breach, AI issues a real-time alert with other features like risk assessment and possible solutions. Consequently, compliance failures decrease since the monitoring system uses artificial intelligence, as noted by Khanna (2018). In addition, it helps to make decisions faster by offering information immediately; thanks to the AI model, the team can respond to compliance risks quickly.

Tables and Graphs

Stage	AI Tool Used	Risk Type	Detection Efficiency (%)	Response Time (Seconds)
Code Development	Machine Learning (ML)	Security Threats	92	30
Code Deployment	Predictive Analytics	Compliance Issues	88	25
Code Maintenance	Natural Language Processing (NLP)	Regulatory Non-compliance	85	40
Continuous Monitoring	Deep Learning	Security Breaches	95	15

Table 1 : AI Tools for Risk Detection and Compliance in DevOps Pipeline

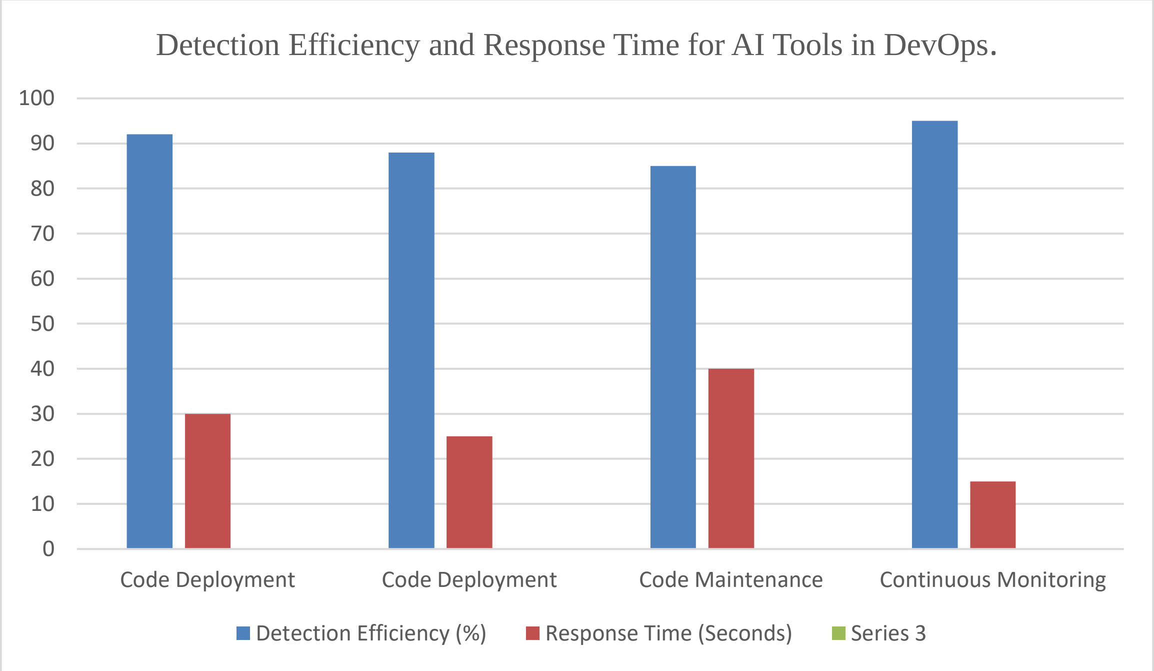

Fig 1; Detection Efficiency and Response Time for AI Tools in DevOps.

Challenge and Solution

Integrating AI for real-time risk compliance in DevOps means several limitations must be considered for effective and efficient integration. One of the challenges, therefore, is the issue of integration with AI. AI can be a challenge when adopted to an existing DevOps process, even with systems that an organization has inherited. Dayalan (2017) suggests that modular integration must be used to counter this. When embedding AI in a particular manner, it becomes possible to implement these tools in parallel with the existing DevOps tools, thus keeping things comparatively simple and not interrupting process flow.

Another problem is data protection. One of the concerns arising from using AI systems, since the systems rely on data to make risk predictions, is that input data into the system may be leaked or violate regulation. To fix this, AI tools can adopt data anonymization or encryption measures so that data can remain secure while AI can always track compliance and risks (Pattyam, 2019).

Another problem is scalability; the solutions must be scalable in many cases. However, AI must be scalable as environments and DevOps flow continue to expand and the inherent code and operation amounts expand. Cloud-based AI platforms seem to address these issues in a scalable manner because these can be adapted depending on how the DevOps environment's demands may grow over time, and integration with continuous monitoring and risk management across large environments is also possible (Begoli et al., 2019). Lastly, one major disadvantage of using AI systems is that they might have false positives and negatives wherein the system identifies non-threatening issues as risks or fails to identify actual risks. More precisely, AI models should involve the process of continuous learning to avoid low accuracy. This makes it easier for these agencies to tweak their algorithms as they appear to eliminate false positives and negatives.

Conclusion

Therefore, AI-based governance frameworks are crucial for real-time risk compliance in DevOps organizations. Risk assessment can be proactive and always on, and compliance checks – are always automated. Thanks to AI, all of these make the process more effective and less reliant on errors. Real-time compliance enables an organization to manage compliance risks and prevent them from arising concurrently, minimize physical interference with the compliance process, and monitor compliance continually. The future of AI in DevOps governance is therefore projected to have better prospects, with self-healing systems and better risk models as possibilities for improving risk management and operational security.

References

1) Alsheiabni, S., Cheung, Y., & Messom, C. (2019). Factors inhibiting the adoption of artificial intelligence at organizational-level: A preliminary investigation. In Americas Conference on Information Systems 2019 (p. 2). Association for Information Systems. https://research.monash.edu/files/287736273/287674072_oa.pdf
2) Mallreddy, S.R., Nunnaguppala, L.S.C., & Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799. https://resmilitaris.net/issue?volume=Volume%20-12&issue=Issue%20-6&year=2022
3) Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2022). AUTOMATED MACHINE LEARNING FRAMEWORK USING LARGE LANGUAGE MODELS FOR FINANCIAL SECURITY IN CLOUD OBSERVABILITY. International Journal of Research and Analytical Reviews , 9(3), 183–190.
4) 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.
5) 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
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., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30–36.
8) 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.

9) 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

10) 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

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

12) 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