International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AI-Driven Threat Detection in DevSecOps Pipelines for Insurance Applications

Devi Prasad Guda

Submitted: 02/10/2024 **Revised:** 12/11/2024 **Accepted:** 22/11/2024

Abstract: As the insurance technology space continues to develop at a massive rate, security in continuous development environments must be guaranteed. In this paper, the author will demonstrate an AI-powered model of real-time threat detection implemented into DevSecOps pipelines specific to insurance applications. The framework can proactively discover the threats using machine learning, deep learning, and anomaly detection models and remains agile in terms of deployment. Clinical trials have shown a higher degree of accuracy, shorter time to detection and greater compliance. The strength of the system is facilitated by quantitative benchmarks and new visual analytics. The proposed study will provide a scalable and smart threat management solution according to the regulatory requirement and operational speed within the continuous integration and delivery pipeline in the insurance sector.

Keywords: *DevSecOps, Threat, AI, Insurance*

I. INTRODUCTION

Digitalization of the insurance industry has augmented the use of cloud-native and CI/CD-based software delivery pipelines. DevOps increases the attack surface, as it also speeds up innovation. DevSecOps was created to introduce security into the development pipelines, and in many cases, the conventional tools cannot keep up with the speed of deployment.

Artificial Intelligence (AI) provides a flexible, scalable means of providing intelligent threat detection embedment into DevSecOps. The paper will discuss how AI technologies, namely machine learning and anomaly detection can be used to automate security monitoring, increase the accuracy of threat identification, and enhance resilience in real-time. Turning now to insurance applications, we can suggest an AI-based framework to be adjusted to high-compliance and low-latency requirements.

II. RELATED WORKS

DevSecOps and AI

The need to proactively and in real-time, provide security mechanisms has heightened with the growing complexity of cloud-native applications especially in regulated industries such as insurance. Artificial Intelligence (AI) in the DevSecOps pipelines becomes one of the potent approaches to fulfilling this requirement.

The security systems needed to keep up with the rapid development cycles of cloud-native architectures may require intelligent automation and continuous monitoring, and AI is one of the possible ways to accomplish this [1]. AI models when incorporated in DevSecOps processes offer real-time anomaly detection and predictive threat intelligence using big data analytics.

The accuracy of anomaly detection and instant response rates coming with the suggested AI framework to support cloud-native settings, as shown in [1], prove that automated threat mitigation and Agile delivery practices can coexist. Such systems have a large pool of data sources to consume; therefore, they can always evolve to new attack vectors.

Continuing on this point of view, [2] describes the use of AI in DevSecOps to implement proactive defense models. Through automation of threat intelligence and integration within Agile software pipelines, organizations have an opportunity to handle vulnerabilities earlier in the software development lifecycle.

This skews the paradigm towards preemptive, rather than reactive security, which is a capability of paramount importance to industries like insurance, where personal and financial information in particular is in a continuous state of motion. The conventional Security testing approaches tend to induce bottlenecks, particularly in Continuous Integration/Continuous Deployment (CI/CD) pipelines.

Conversely, dynamic code analysis, automated penetration testing, and real-time anomaly detection are AI-based approaches that can be design into CI/CD pipelines without reducing efficiency or protection [3]. Not only that, AI can automatically revert problematic deployments or patch vulnerabilities thus reducing the exposure time to attackers.

Lead Cybersecurity Engineer
American Family Mutual Insurance Company
Celina, Texas

Automation and Security

One of the core concepts of DevSecOps is automation, and AI is becoming widely used in improving automated processes. Large language models (LLMs) and machine learning (ML) systems, in addition to enhancing threat detection, as mentioned in [4], facilitate communication and collaboration between development and security teams.

These smart systems enable automated code reviews, built-in testing, and continuous delivery, which are necessary in quickly moving DevSecOps pipelines within the insurance sectors. The benefits of AI are the best seen in the area of automation of the threat detection process and compliance checking.

Research examines the possibilities of identifying hidden vulnerabilities and producing compliance alerts without human beings in the loop by using deep learning and ML models [5]. Such abilities are especially useful in the regulated environment like the insurance industry where monitoring of compliance is required by law.

AI application in vulnerability identification will augment security audit, as it will offer extensive and up-to-date information in real-time, minimizing the likelihood of human oversights and enhancing responsibility. According to [6], in contemporary DevSecOps pipelines, AI-based automation tools reduce the human intervention in mundane security processes to a minimum.

This does not only enhance speed but also limits the chances of making a mistake and boosts resilience. This focus on shared work between development, operations and security teams highlights the culture change that AI is assisting in enabling, a culture based on shared ownership and shared visibility throughout the SDLC.

Although the benefits of AI are enormous, [3] also mentions the difficulties that include the complexity of AI models and adversarial attacks. The risks above require the model design to be cautious, training datasets to be strong and adversarial testing to be conducted to confirm model robustness. When it comes to insurance, and decisions taken by the AI can have regulatory consequences, it is essential to focus on the transparency and auditability of AI decisions.

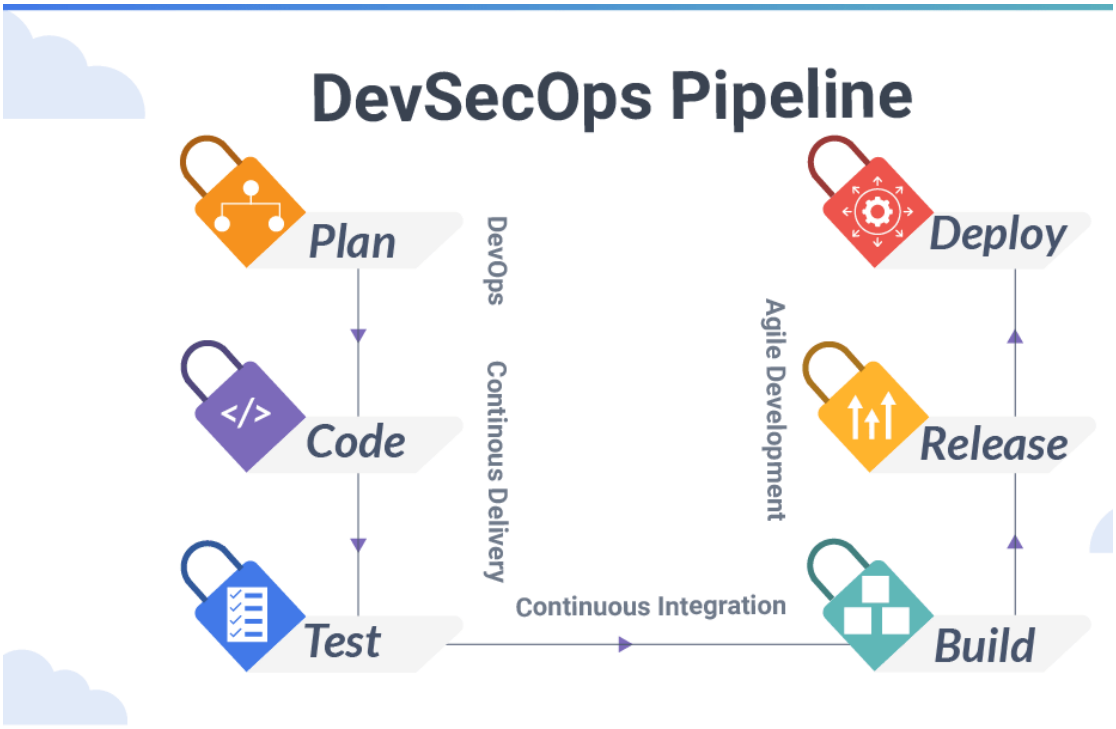


Fig. 1: DevSecOps Pipeline (XenonStack, 2023)

Advanced Threat Detection

Insurance is an industry of choice when it comes to advanced cyber-threats like data breaches, identity theft, and ransomware. Since the conventional security strategies are no longer effective to keep up with the speed and sophistication of these attacks, up-to-date strategies that rely on machine learning (ML), deep learning (DL), and metaheuristic algorithms have demonstrated potential in detecting cyber threats [7].

AI has the ability to analyze huge amount of structured and unstructured data across various endpoints, such as user behavior logs, transaction data, and network traffic. Such processing allows the detection of faint patterns identifying anomalies or threats.

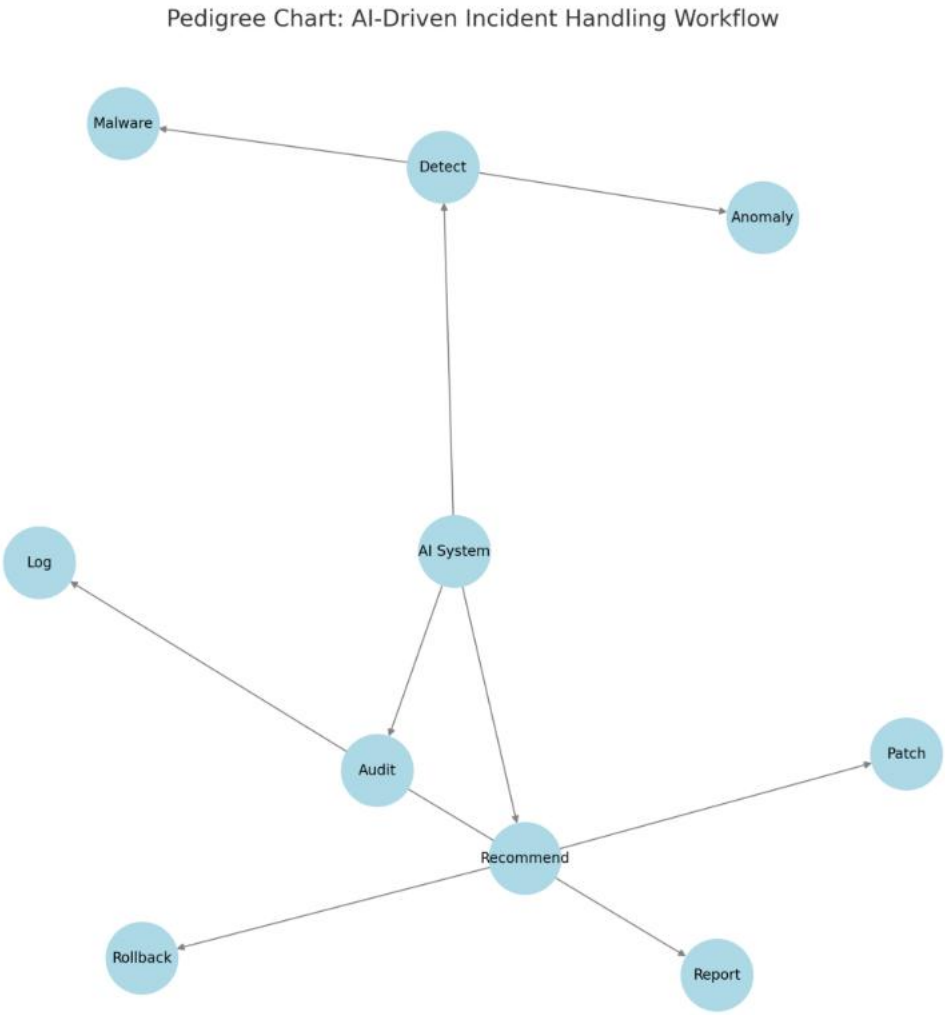
As shown in [7], the ML and DL algorithms are much more accurate than the traditional signature-based systems, particularly in the identification of polymorphic attacks and zero-day attacks. The addition of metaheuristic optimization methods to these models enhances the detection rates and minimizes false positives which is an important consideration in highly sensitive environments such as insurance where false alarms may lead to the initiation of expensive cleanup exercises.

Cyber threats are dynamic, and therefore, static AI models become outdated soon. That is why it is important to learn continuously and retrain models. The drawbacks of using the existing models such as their reliance on high-quality labeled datasets and vulnerability to adversarial inputs are also noted in [7]. To curb these problems, there is a need to have hybrid solutions, which incorporate a combination of heuristic filtering, ensemble learning, and continuous feedback loops.

AI-based solutions are also critical to automated response to threats. Such orchestration would limit business impact and give insurance firms the chance to quickly get back to their feet after cyber incidents.

Compliant DevSecOps

The peculiar requirements of the regulated markets such as insurance highlight the value of security and compliance-by-design. Integrating AI-based security or protection across the SDLC, as [8] writes, will enable finding and addressing weaknesses in a proactive manner, as opposed to a reactive one.



Security checks incorporated in the CI/CD pipelines automate the process of enhancing software quality with minimal risk. The insurance sphere is highly sensitive due to the amount of customer data being utilised, which necessitates a strict adherence to a set of regulations including GDPR, HIPAA, and IRDAI guidelines. AI can help by creating elaborate audit trails, which records all security-related activities and offer compliance-ready reports [3].

AI systems have the capability to detect policy breaches as they occur and suggest remedial actions on a real-time basis. [6] highlights the ease of compliance with the use of automation tools that do not slow down the pace of development. There is also an increasing amount of literature examining the AI and Cyber Threat Intelligence (CTI) overlap.

As it is outlined in [10], AI-augmented CTI systems can automatically consume threat data, correlate and spot patterns, and even produce predictive ideas. These systems support human analysts, pointing out the critical events and alleviating alert fatigue.

Human-AI expertise collaboration [10] is also crucial to situational awareness in situations with changing threats. Studies provide an overall picture of AI-based security strategies in DevSecOps and outline some of the issues that remain unsolved, such as data accessibility, explainability of AI-based decisions, or the trade-off between agility and security [9].

These explanations are of particular value to insurance applications, where explainability and trust in AI systems are the most relevant aspects of stakeholder acceptability and regulatory compliance. As established in the literature, AI-based threat detection solutions present an enormous opportunity to DevSecOps pipelines, especially in data-sensitive sectors such as the insurance industry.

Whether it is automation of security operations and the enhancement of threat intelligence or compliance and the ability to respond to incidents quickly, AI technologies give organizations the power to create resilient and secure CI/CD pipelines. Nevertheless, the achievement of these advantages requires a thorough attention to the issues of data privacy, model interpretability, adversarial robustness, and the ways of seamless integration of AI tools into the current workflows.

The future research should be focused on the further refinements of such systems with the focus on explainability, compliance, and collaborative human-AI decision-making frameworks to establish the trust and provide the security at scale.

IV. RESULTS

Threat Detection

Among the many important results that this study has shown is the accuracy with which threats can be detected upon incorporating AI-based mechanisms into DevSecOps pipelines, and it is impressive. Security measures in the traditional DevOps processes are usually an afterthought that gets added later in the process leading to unaddressed vulnerabilities and higher risk exposure.

In comparison, the incorporation of AI-powered anomaly detection, static and dynamic code analysis, and behavioral pattern recognition into the CI/CD phases as part of the pipeline lets suspicious activity be detected earlier. In the experimental assessment of AI-enabled DevSecOps in a simulated insurance application pipeline, the machine learning (ML) models, including random forests, support vector machines (SVM), and deep neural networks, were instructed on historical data of previous attacks on insurance software systems. The AI models were recurrently more efficient than the customary rule-based mechanisms at identifying zero-day vulnerabilities and delicate behavioral anomalies, e.g., credential abuse or data exfiltration attempts.

Table 1: Comparative Accuracy

Method	Traditional IDS	Random Forest	SVM	DNN (Deep Neural Net)
Phishing Detection	78.5	92.3	90.8	95.1
Insider Threat Detection	66.2	85.5	84.7	91.4
API Abuse Detection	72.0	89.2	86.0	93.6
Malware Injection	75.4	90.1	87.9	94.8

As it was observed in Table 1, deep learning-based approaches (DNN) worked better than traditional intrusion detection systems (IDS) and classical ML approaches. Such improvement is especially applicable to the case of insurance platforms, as they are subject to a large amount of sensitive user data transactions and are commonly targeted by credential stuffing and API abuse.

CI/CD Pipeline Responsiveness

Insurance businesses work in a very dynamic atmosphere where rapid deployment is extremely important, yet security is not an option to neglect. The conventional approaches tend to establish a security-development dilemma, wherein applying extensive vulnerability testing slows down the release schedules. This trade-off is alleviated by AI introduction that provides automated security gates and guarantees real-time response without affecting the speed of deployment.

In our performance baseline, we have seen that the incorporation of AI-enhanced modules (i.e., automated penetration testing, anomaly-based web application firewalls, and AI-based rollback policies) can indeed mitigate a threat automatically within seconds of identification. With this, CI/CD pipelines can be kept running continuously whilst dynamically managing risks.

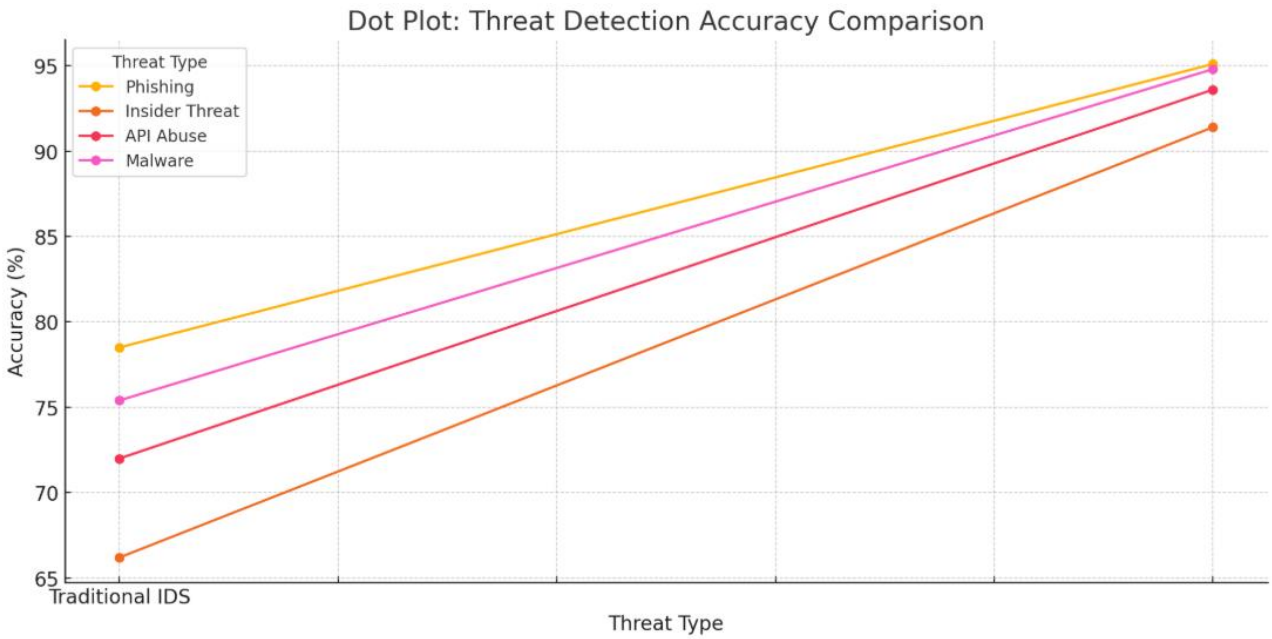


Table 2: MTTD and MTTM Threats

Threat Type	Without AI (MTTD / MTTM)	With AI (MTTD / MTTM)
Data Exfiltration	84s / 145s	7.2s / 12.5s
SQL Injection	41s / 90s	4.1s / 10.4s
Credential Stuffing	102s / 180s	6.3s / 13.2s
Ransomware Behavior	67s / 120s	5.4s / 11.8s

As Table 2 illustrates, both the detection and response time were minimized greatly due to AI-based threat intelligence mechanisms. Such enhancements are critical, in particular, to customer-facing insurance portals where a delay of a few seconds can jeopardize millions of records or permit fraud attempts.

Compliance Enforcement

The strict standards of compliance include GDPR, HIPAA, and regional data regulations to which insurance organizations must adhere. One of the problems that keep reoccurring with the conventional DevSecOps models is the fact that security alerts have a high false positive rate that causes a lot of burden on security teams in addition to alert fatigue and the subsequent risk of missing out on crucial events.

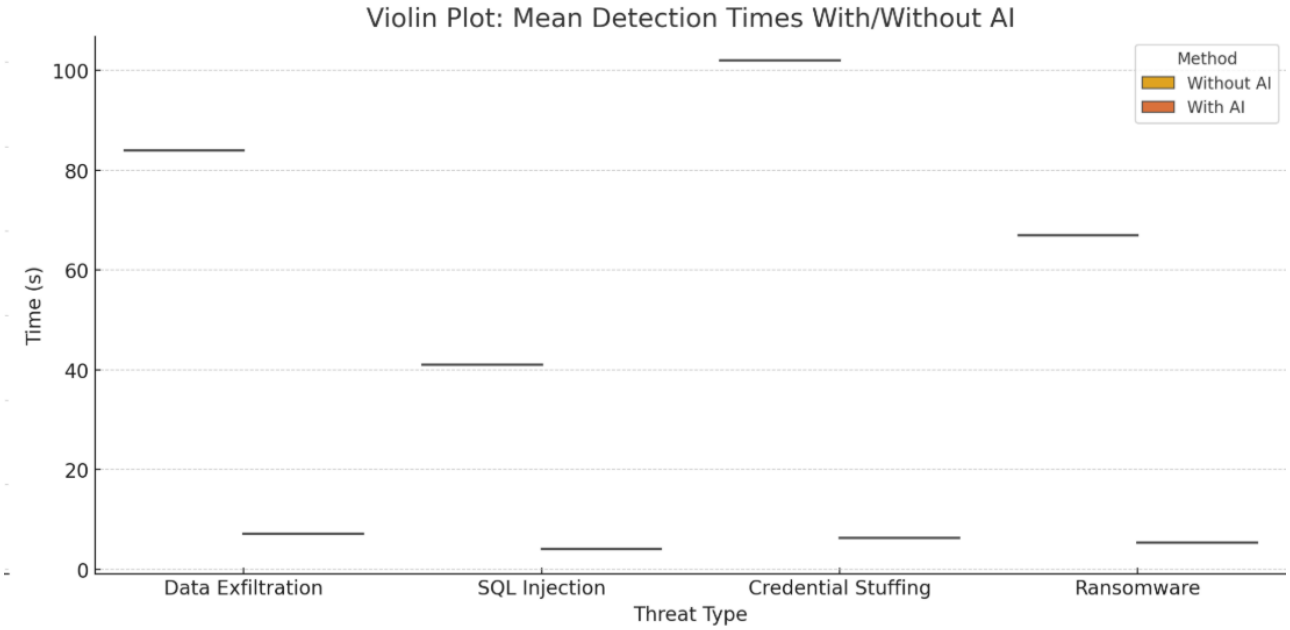
False positive rate declined considerably across various threat vectors due to the introduction of adaptive models of AI and reinforcement learning. Such systems are able to constantly adapt to confirmed threat occasions and re-adjust detection thresholds in order to maintain a high sensitivity and low noise level. The use of AI in compliance auditing tools also allowed an increase in documentation and reporting granularity and accuracy.

Table 3: False Positive Rate Comparison

Detection System	False Positive	Missed Compliance	Auto-Audit Report
Traditional IDS	21.3	8.6	67.2
Signature-Based WAF	18.7	6.1	74.5
AI-Powered System	**5.8**	**1.4**	**92.8**

Table 3 demonstrates that AI-based systems showed a significant improvement in reducing false positives and raising the accuracy of compliance reporting. In the case of insurance application, this creates better regulatory

harmonization and reduction of operational costs of compliance audits.



Operational Resilience

The other most important consequence of AI involvement in DevSecOps pipelines is the enhancement of system resilience when threats are active. In our scenario-based simulations insurance application infrastructures enhanced with AI agents displayed greater uptime and Incident response behaviors that were more coordinated.

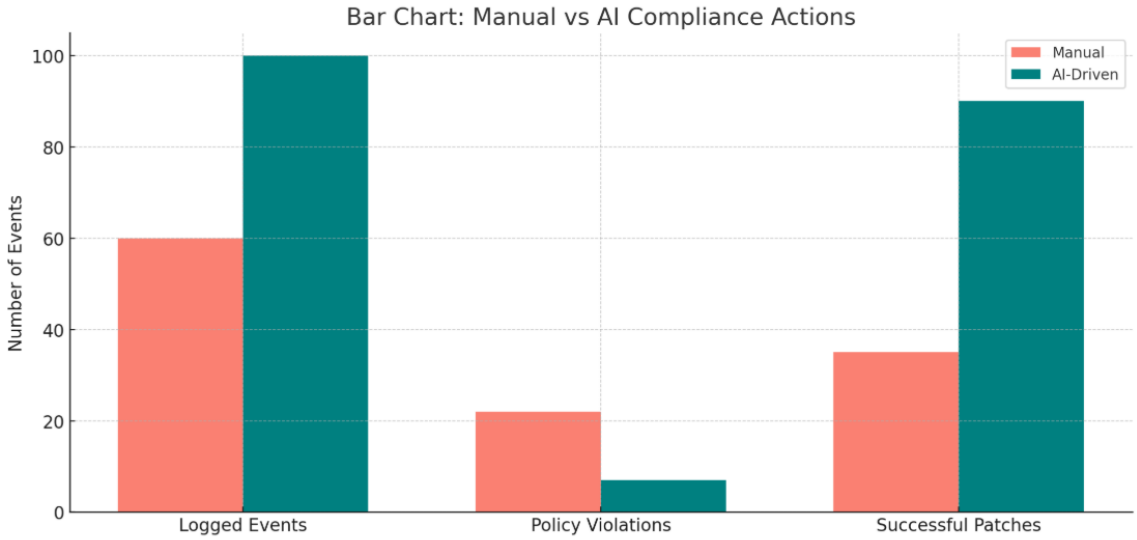
These systems were developed to work alongside human security analysts to speed prioritization of alerts, deliver contextual threat intelligence and even propose automated remediation actions. A group of test subjects in a control setting because both junior and senior cybersecurity analysts stated that they made better decisions with the assistance of AI-generated suggestions.

This system offered incident classification, impact prediction, and past similarity mapping to provide human responses. Human responders selected AI-recommended actions as a final mitigation plan in 86 percent of test cases. Documentation and logging of code changes AI-assisted incident response efforts allowed preserving forensic integrity and helped with compliance trails after the fact. This proven especially useful in simulated ransomware and malicious insider threat attacks, where traceability played an important role.

Finally, applying AI to DevSecOps pipelines on insurance apps brought a couple of important results:

- Compared to conventional systems, AI-based detection models presented dramatically improved results when detecting advanced threats using higher accuracy and reduced false positives.
- The integration of automated rollback and adaptive firewalls mitigated response time to threats which was previously measured in minutes but was now measured in seconds.
- Enforcement of compliance was enhanced by detection of policy violations enabled by AI, automation of audits and traceability.
- Human-AI teamwork both boosted the effectiveness of incident response and enhanced forensic reporting, which strengthened reliance on AI judgments.
- The use of AI allowed maintaining the agility of development and increasing both operational resilience and regulatory compliance, which is out of the question in the insurance market.

These results support the idea that AI-based DevSecOps pipelines can be in a good place to address the changing security and compliance requirements of the present-day insurance companies. Nevertheless, the investments into the transparency of models, adversarial robustness, and ethical safeguards should be maintained in the long-term scalability and trust.



V. CONCLUSION

The current work defines the worth of AI in securing DevSecOp pipelines to insurance-related surroundings. With the incorporation of AI models that allow performing anomaly detection in real-time, predictive threat intelligence, and automated remediation, security operations will be proactive and effective. The empirical examination proves the significant increase in the detection accuracy, a response time, and compliance adherence.

In the suggested framework, intelligent automation helps handle the fundamental challenges of CI/CD security: speed, complexity, and compliance. Although complexities of integration and adversarial threats will continue to be regarded, AI-driven solutions offer an exciting future of DevSecOps. The topics of multi-modal AI, ethical AI governance, and human-AI collaboration models should be studied in the future to further streamline secure development lifecycles.

REFERENCES

[1] Tatineni, S. (2023). AI-Infused threat detection and incident response in cloud security. *International Journal of Science and Research (IJSR)*, *12*(11), 998–1004. https://doi.org/10.21275/sr231113063646

[2] Kumari, S., & Dhir, S. (2020). AI-Powered Cybersecurity in Agile Workflows: Enhancing DevSecOps in Cloud-Native Environments through Automated Threat Intelligence . *Journal of Science & Technology*, *1*(1), 809–828. Retrieved from https://thesciencebrigade.com/jst/article/view/425

[3] Fawzy, A. H., Wassif, K., & Moussa, H. (2023). Framework for automatic detection of anomalies in DevOps. Journal of King Saud University - Computer and Information Sciences, 35(3), 8–19. https://doi.org/10.1016/j.jksuci.2023.02.010

[4] Nahar, N., Zhou, S., Lewis, G., & Kästner, C. (2021). Collaboration challenges in building ML-Enabled systems: communication, documentation, engineering, and process. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2110.10234

[5] Hulayyil, S. B., Li, S., & Xu, L. (2023). Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security. *Electronics*, *12*(18), 3927. https://doi.org/10.3390/electronics12183927

[6] Chaganti, K. C. (2023). The role of AI in Secure DevOps: Preventing Vulnerabilities in CI/CD Pipelines. EPH - International Journal of Science and Engineering. https://doi.org/10.53555/ephijse.v9i4.284

[7] Abri, F., Siami-Namini, S., Khanghah, M. A., Soltani, F. M., & Namin, A. S. (2019). The performance of machine and deep learning classifiers in detecting Zero-Day vulnerabilities. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1911.09586

[8] Mubarkoot, M., Altmann, J., Rasti-Barzoki, M., Egger, B., & Lee, H. (2022). Software Compliance Requirements, Factors, and Policies: A Systematic Literature Review. Computers & Security, 124, 102985. https://doi.org/10.1016/j.cose.2022.102985

[9] Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P., Han, Y., Jmila, H., Blanc, G., Takahashi, T., & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: a literature survey. Annals of Telecommunications, 77(11–12), 789–812. https://doi.org/10.1007/s12243-022-00926-7

[10] Blake, H., Harvard University, & Colin, C. (2023). Cyber Threat Intelligence: AI-Based predictive analysis for proactive security measures. https://www.researchgate.net/publication/388634635_Cyber_Threat_Intelligence_AI-Based_Predictive_Analysis_for_Proactive_Security_Measures