

AIOps in Cloud-native DevOps: IT Operations Management with Artificial Intelligence

Sumanth Tatineni

Devops Engineer, Idexcel Inc, USA

ABSTRACT

Businesses often deal with the growing challenge of maintaining IT operations, especially with the increase in technological dependence. Organizations adopting AIOps and organizations elevate IT operations management to address these challenges. This shift comes as a response to the increasing complexities of the huge data, applications, and infrastructure in today's digital scope. Traditionally, managing these systems incorporated manual observation and performance metric analysis, processes which are highly prone to errors and inefficiency. AIOps introduces automation through AI/ML algorithms, which analyze patterns to predict and address issues quickly and rectify discrepancies.

Therefore, recognizing the diverse needs of companies, each facing unique goals and challenges, depicts the role of tailoring AIOps solutions to specific needs. For example, a global e-commerce company managing a huge online platform will ensure a seamless user experience and quick response to customer interactions. In such a situation, the IT team's focus with AIOps could be on real-time analytics to anticipate and mitigate potential disruptions, automated incident response to minimize downtime, and predictive maintenance to address performance issues. This article explores comprehensive insights into how AIOps functions are important in dealing with IT operations challenges within cloud-native DevOps. It aims to explore the benefits of AIOps in improving incident response efficiency, refining system monitoring capabilities, and optimizing IT operations.

*Corresponding author

Sumanth Tatineni, Devops Engineer, Idexcel Inc, USA.

Received: January 07, 2023; **Accepted:** January 16, 2023; **Published:** January 23, 2023

Keywords: AIOps, Cloud-Native DevOps, IT Operations Management, DevOps, Incident Response Automation, IT Automation

Introduction

In business technology, integrating AI has been crucial in reshaping how organizations handle IT operations. According to the IBM Global AI Adoption Index, one in three companies actively use or are considering the implementation of AI to automate their IT processes [1].

This trend has been observed in organizational infrastructure, as depicted in the significant increase in the adoption of cloud-native environments. IBM 2022 survey depicts that there has been an increase in organizations embracing cloud-run systems – compared to 2020, the proportion of respondents with mostly cloud-run environments rose, with 93% of organizations reported depending on cloud-based systems as businesses move towards cloud-native DevOps practices, the complexity of managing IT operations increases, thus posing challenges that require innovative solutions. The adoption of hybrid cloud environments from a Statista survey in March 2022 depicts a trend with 80% of enterprises deploying such environments [2, 3].

Nonetheless, as hybrid cloud adoption grows, so do IT operations teams' challenges in handling the increasing volume of data generated by digital systems. The need to process millions of metrics per second from different tools has become crucial today.

Therefore, with the integration of AI for IT operations (AIOps), scaling operations teams to manage this data volume effectively is practical. The results of not keeping up with this data influx are important, as depicted in the ITIC 2022 Global Server Hardware Security Survey. The survey highlights that 91% of SMEs and larger enterprises recognize the substantial cost of downtime, with a single hour potentially exceeding 300,000 billion dollars in losses [4].

Additionally, 44% of mid-sized and large enterprise respondents reported that one hour of downtimes could surpass one million dollars in potential losses. To respond to all these challenges, AIOps becomes a solution – organizations that implement AIOps adeptly will alleviate the pressure on skilled employees and liberate their time to focus on innovative projects. AI and ML-powered software are huge in handling the escalating volume of metrics, events, and logs while ensuring business operations run seamlessly. Adopting AIOps is key to achieving productivity, efficiency, and informed decision-making in the ever-growing business landscape.

Significance and Background of AIOps in Cloud-Native DevOps

Software development goes through continual transformation. Therefore, introducing new infrastructure techniques and design patterns like cloud computing, SaaS, DevOps, and microservices has become necessary to propel software development further. As organizations shift to cloud-native DevOps practices, managing

and operating IT infrastructure come with different challenges. This transition is mainly noticed when traditional software shifts to SaaS models, thus requiring 24/7 software access for subscription-based users. With these challenges, the use of AIOps and cloud-native DevOps comes as a solution.

With AOps using ML and big data, it becomes a central point in automating IT operations processes. The difficulties with modern software operations within cloud-naïve DevOps depict the need for a transition. Traditional boundaries between coding, testing, deployment, and operations blur, demanding DevOps teams to service management and operations, thus improving the importance of seamless integration with AIOps. AIOps are recognized due to their high availability, scalability, and operational efficiency, so they have grown to different levels. As organizations move from manual operations to fully automated AIOps, every stage incorporates varying degrees of AI adoption, thus offering unique solutions to address the evolving challenges of cloud-native DevOps. The adoption of AIOps is expected to reach a market size of 11.02 billion dollars by the end of 2023, with a CAGR of 34% [5]. This growth depicts the increasing recognition of AIOps as a key component in navigating the challenges of cloud-native DevOps environments.

Understanding AIOps

AIOps represents a shift in managing information and data within application environments, mainly in AI, NLP, and ML. It is the next evolution in IT operation analytics by leveraging advanced technologies to streamline and automate different IT processes. AIOps integrates huge amounts of data generated within the modern IT environment by using ML algorithms to automate processes related to anomaly, root cause analysis, and events. The main goal is to enhance the effectiveness and efficiency of IT operations through these technologies. Instead of depending on sequential system alerts, AIOps break down data silos, improve situational awareness, and automate personalized responses to incidents, enabling organizations to enforce IT policies to support business decisions [6]. AIOps goes through different phases before its implementation;

Observe

This phase involves intelligent data collection from IT environments. AIOps enables observability across disparate data sources and devices by deploying ML and data analytics. This phase is crucial in identifying patterns and correlating log and performance data events.

Engage

This phase uses human experts to resolve issues, thus reducing dependencies on conventional IT metrics. AIOps analytics coordinate IT workloads on multi-cloud environments, thus promoting streamlined efforts in assessment and diagnosis. Real-time alerts are raised both in response to incidents and preemptively.

Act

This phase incorporates how AIOps technologies take actions to foster and maintain IT infrastructure. AIOps aims to automate operational processes, thus allowing teams to focus on more critical tasks. Automated responses based on analytics generated by ML algorithms can preempt similar issues with intelligent systems.

Fundamental Algorithms Monitored by AIOps

These algorithms collectively form the backbone of AIOps, thus enabling organizations to navigate the complexities of IT operations with a different approach. Each algorithm addresses distinct facets that contribute to the overall efficacy of AIOps methodologies.

Data Selection Algorithms

As organizations move to cloud-native architecture, the huge volume of data produced can be overwhelming since it incorporates logs, metrics, and events from different sources. To sift through the voluminous and often noisy IT data generated in a contemporary IT environment, thus discerning data features that depict possible problems. Therefore, the data selection algorithms filter through this extensive data repository [7]. It streamlines system monitoring and incident response by violating data features indicative of possible issues. Its algorithm thrives in perfect data curation, thus ensuring only pertinent data is considered for further analysis. This, in return, enhances resource allocation and problem identification, thus ensuring that IT teams prioritize actions based on the most critical and relevant data.

Pattern Discovery

Microservices, APIs, and data storage solutions dynamically interact in cloud-native environments; it is important to uncover relationships and patterns. The pattern discovery thrives in establishing these connections, thus giving them a foundation for comprehensive analysis. Therefore, it automates response and remediation processes to the greatest extent possible, thus enhancing the precision of services. Identifying correlations between data elements pushes IT operation teams to gain insights into the relationships relevant to the performance and behavior of cloud-native applications [8]. This algorithm is instrumental in optimizing incident response and system monitoring within DevOps practices. In addition, the algorithm operates by identifying patterns within data, which are important in subsequent analytical processes. It guides organizations in deciphering the patterns in their IT operations and responding proactively to any potential challenges.

Inference

This algorithm thrives by leveraging ML to analyze historical data and real-time information. Therefore, quickly identifying the root causes allows quick and informed decision-making and intervention, thus perfectly aligning with the responsive and agile attribute of DevOps practices [9]. This algorithm ensures that IT teams promptly identify issues and implement targeted solutions, thus minimizing downtime and optimizing overall IT operations.

Collaboration

As development teams leverage cloud-native technologies, the physical dispersion of team members can pose different challenges to effective collaboration. This algorithm addresses this by promoting improved interaction among relevant teams and operators. It fosters collaborations, especially in scenarios where individuals are geographically dispersed, while concurrently maintaining event data that expedites future identification of similar issues. Customized reports and dashboards ensure teams can quickly grasp and act upon their tasks. In addition, maintaining event data that accelerates the discovery of similar issues contributed to a collective learning environment [10]. It, therefore, promotes cohesion and agility, thus ensuring that teams can effectively collaborate regardless of their locations, thus optimizing the overall efficiency of cloud-native practices.

Automation

This algorithm's remediation and response capabilities seamlessly align with the core principles of DevOps, where CI/CD demands quick and accurate solutions. By automating response mechanisms based on AI insights, the automation algorithm reduces the manual intervention needed for incident resolution. This accelerates the remediation process and ensures reliability and consistency in responding to incidents [11]. This algorithm enables IT teams to manage incidents efficiently, optimize resource allocation, and maintain the agility needed in DevOps practices.

Why Businesses Should Adopt AIOps IT Noise Elimination

Traditional IT operations often deal with noise, thus leading to false positives, obscured root-cause events, and increased difficulty in outage detection. This noise can lead to performance issues, increased operating risks, costs, and tampering with enterprise digital initiatives. AIOps tools are important in eradicating and mitigating this noise by constructing correlated incidents directly pointing to the root cause. This approach thus enhances the precision of incident detection and resolution.

Improved Customer Experience

In times when customer experience is important for driving profitability, AIOps helps provide predictive analysis and automated decision-making for future events. Through comprehensive data analysis, AIOps predicts events that might affect the availability and performance of IT systems. In addition, it quickly identifies the root cause of IT issues, thus facilitating instant resolution and consequently ensuring an enhanced customer experience.

Enhances Better Collaboration

By breaking down functional silos within organizations, AIOps fosters a seamless workflow for IT groups and other business units. This collaborative technique fosters organizational responsiveness and agility. In addition, customized reports and dashboards generated by AIOps tools empower teams to comprehend their tasks quickly and take prompt actions, thus fostering a culture of effective collaboration.

Better Service Delivery

Integrating AI, ML, and automation within AIOps facilitates efficient query resolution by analyzing usage patterns, support tickets, and user interactions. Applying probable cause analytics, AIOps anticipate underlying performance issues, thus enabling proactive resolution strategies that streamline service delivery and contribute to the enterprise's overall operational resilience.

Understanding Cloud-Native DevOps

DevOps hastens seamless collaboration among stakeholders in the SDLC, thus fostering cohesion between QA, developers, and infrastructure management teams. Automation is important in DevOps as it ensures continuous testing, integration, and delivery, thus empowering different contributors to work concurrently for enhanced agility and speed. The merger between cloud-native principles and DevOps is important for maximizing flexibility, efficiency, and productivity. Both emphasize key aspects like cross-team collaboration and CI/CD [12].

Without adopting DevOps, meeting the demands of cloud-native DevOps seamlessly combines these principles like optimization of processes and tools, workflow automation, and collaborative encouragement. A cloud-native approach involves conceptualizing, developing, testing, and releasing software within a cloud

environment. Core aspects of cloud-native development include CI/CD processes, containerization, orchestration, and immutable infrastructure. Orchestrating automated configurations, updates, management tasks, and deployment is crucial.

Containerization incorporates building in lightweight, modular containers with granular infrastructure management. CI/CD allows continuous testing and delivery, thus contributing to the repetitive development cycle. Immutable infrastructure depicts using unmodifiable configurations by replacing servers with new ones when updates are necessary [13]. The word cloud-native denotes applications curated to utilize the advantage of distributed computing in cloud delivery models. The Cloud Native Computing Foundation (CNCF) discusses cloud-native technologies that allow scalable public, private, and hybrid cloud applications.

Key characteristics like service meshes, containers, microservices, immutable infrastructure, and declarative APIs. These features allow loosely coupled, manageable, observable, and resilient systems, thus allowing engineers to make impactful changes effortlessly. Microservices are important to cloud-native development, breaking applications into small, granular components for flexibility and scalability. Cloud-native practices incorporate these features, thus representing the future of software development [14]. This technique allows the creation of efficient, scalable, and flexible applications tailored to long-term business and computing needs.

DevOps is important in aligning with cloud-native principles to streamline automation and collaboration, thus ensuring organizations are poised for success in the ever-evolving scope of software development. To successfully implement cloud-native DevOps practices, crucial transformations are needed in their different domains;

Cultural Change by Transitioning from Silos to Devops

A culture shift is indispensable, especially moving away from traditional silos towards a cohesive DevOps technique. While cloud infrastructure is not mandatory for cloud-native status, DevOps is important. The main objective of DevOps is to synchronize all stakeholders through shared tools and a given set of priorities.

Organizational Change Incorporating Buy-In From Everyone

The organizational scope requires a huge shift with a unanimous team commitment to collaborate to get a shared objective. The emphasis is on fostering a quicker feedback loop between developers and end-users, thus expediting application development and generating actionable insights for organizations.

Technical Change

Technical shifts are integral, particularly in creating applications. One example is the transition from a monolithic architecture to microservices, which ensures a more modular and scalable application framework with the principles of cloud-native DevOps.

How to Implement Cloud-Native DevOps

Implementing cloud-native applications needs an understanding beyond just cloud deployment. For true cloud-native status, cloud-native DevOps must depict specific characteristics that align with contemporary software development principles. One main aspect incorporates embracing microservices patterns. Traditional monolithic applications should go through a shift by breaking down into smaller, independent services that enable autonomous development [15].

The key aspect is ensuring each service adheres to a strong contract, thus enabling repetitive enhancements. The collaborative merge of these microservices forms the comprehensive application framework. In addition, containerization is important in achieving cloud-native objectives. By packaging code independently of underlying system issues, containerization promotes an environment where applications become more scalable and portable. This technique frees developers from concerns about diverse deployment environments, thus streamlining the development-to-production pipeline.

A declarative communication pattern is another essential characteristic, thus demanding a reliance on the network for message delivery, along with failure outcomes or explicit success. This technique standardizes communication models by shifting functional implementation details away from the application itself to a remote service endpoint or API, as it ensures a more modular and streamlined communication framework within the cloud-native environments. Implementing container orchestration is important in the cloud-native space. Kubernetes is a key platform that brings its capacity to abstract the complexities associated with underlying storage, networking, and computing resources, greatly contributing to the seamless management and deployment of cloud-native applications.

Consequently, adhering to the 12-factor application principles ensures clean, declarative contracts for deployment on cloud platforms, enhancing the scalability and maintainability of cloud-native applications. Amplifying automation within CI/CD pipelines is important in navigating the increased complexity introduced by cloud-native paradigms, which demand a strong automation plan to navigate the deployment pipeline effectively.

It is important to expose health checks from applications to the platform, which enhances visibility into the application's operational state and aids in monitoring and promptly responding to any deviations from the expected functionality.

Lastly, telemetry data is collected incorporating metrics like requests per minute and latency by using data points that are key indicators for evaluating whether the application aligns with predefined Service Level Objectives (SLOs) [16].

Implementing alerting mechanisms based on telemetry data ensures proactive responsiveness in maintaining the cloud-native health of the application. While cloud-native DevOps isn't a cure-all, it is a potent technique for companies looking to expedite automation and curate production environments for improved customer service.

How AIOps Works in Cloud-Native DevOps

AIOps utilizes different comprehensive processes that enable IT teams to proactively manage incidents, optimize resources, and elevate operational efficiency, which reduces manual effort and enhances IT systems' overall performance and reliability.

Data Aggregation and Correlation

AIOps thrives in aggregating and correlating this varied data to present a unified view of the cloud-native IT scope. In a cloud-native DevOps pipeline scenario, AIOps incorporates events, metrics, and logs generated across different stages. For example, it correlated deployment events with changes in application performance metrics, thus offering insights into the impact of code change on system behavior. This process promoted the visibility

of interconnected components, thus facilitating streamlined monitoring [17].

Data Collection and Analysis

AIOps starts by collecting different data from the dynamic IT environment. For example, a cloud-native application leveraging microservices architecture – AIOps would gather log data, metrics from containerized applications, and events triggered by orchestration tools such as user interaction data and Kubernetes. Therefore, this comprehensive data collection ensures that AIOps has an integrated understanding of the cloud-native ecosystem, which is important for effective incident optimization and response [18]. The gathered data goes through proper analysis using advanced ML algorithms that aim to discern anomalies that may necessitate attention from IT personnel, thus ensuring that genuine issues are identified while minimizing false noise or alarms, which enhances the accuracy of issue identification within the operational ecosystem.

Pattern Recognition and Anomaly Detection

As mentioned, AIOps uses ML algorithms to discern patterns and identify anomalies. For instance, a situation where a cloud-native application experiences fluctuations in resource utilization during CI/CD. AIOps understand these patterns and detect anomalies that may depict unexpected performance deviations or inefficient resource allocation [19]. Therefore, by learning from historical data, AIOps adapt to the unique patterns relevant to cloud-native architectures, thus contributing to strong anomaly detection.

Inference and Root Cause Analysis

AIOps correlates events and metrics to uncover the sequence leading to incidents. For example, if there's a spike in resource utilization within a Kubernetes cluster, AIOps can trace it back to specific containerized applications [20]. This correlation allows IT teams to determine whether the issues come from increased demand, potential flaws, or misconfiguration in the underlying infrastructure. Therefore, root cause analysis helps maintain the resilience of cloud-native applications.

Automation and Remediation

AIOps automate routine tasks and help in incident resolution. For instance, if AIOps detects abnormal behavior in a cloud-native application, it can automatically trigger alerts to the relevant DevOps teams. In addition, it may suggest predefined remediation steps based on historical incidents. This automation expedites incident response and aligns with the principles of CI/CD. AIOps further enhances operational efficiency by reducing manual intervention. Automated responses like resource scaling, service starts, or the execution of predefined scripts allow quick and precise issue resolution.

Predictive Analytics

AIOps uses predictive analytics by forecasting future incidents, performance trends, or capacity needs. Based on historical data from a cloud-native environment, AIOps can predict increased traffic during specific operational periods [21]. This predictive ability empowers IT teams to scale resources proactively, thus ensuring the handling of anticipated workload, which is important in efficient cloud-native DevOps management.

Challenges in Implementing AIOps in Cloud-Native DevOps Interoperability

One of the key challenges in implementing AIOps in cloud-native DevOps is the interoperability with existing data and tools. Legacy

tools often need more integration characteristics, thus making it easier to seamlessly and seamlessly incorporate them into a modern AIOp environment. Tickets or incidents originating from service desks may be left out of AIOps analysis, thus creating a possible blind spot. In addition, there might be a dependency on underlying tools for deeper analysis, thus hindering the comprehensive utilization of AIOps insights. Therefore, organizations can focus on comprehensive data ingestion strategies by integrating modern and legacy sources to address this challenge. An AIOps platform with built-in data can allow data access anytime, thus reducing the dependency on disparate tools.

Service and Asset Interdependencies

Service and asset interdependencies require a clean configuration management database (CMDB) [22]. However, getting a clean CMDB is rare and can result in extended time-to-value due to the need for tools, instrumentation, scripts, and tagging. This introduces resource overhead costs, thus impacting operational efficiency. A possible opportunity lies in automating service and application dependency mapping using ML models and self-learning. In addition, automating alert enrichment through context resolution and extraction can enhance the efficiency of AIOps platforms. Thus, having built-in asset intelligence can further streamline the management of service interdependencies.

Culture Change

Implementing AIOps demands a huge shift in organizational culture and processes. The difficulty in changing the system of engagement and gaining trust in AIOps decisions can hinder progress. Black-box platforms that lack customization and flexibility add to the challenge. Promoting continuous bi-directional integration and collaboration with existing engagement tools is important to handle this [23]. Open-box ML models and fully customizable algorithmic behavior push organizations to adapt AIOps to their specific needs. The platform should allow users to understand and validate algorithmic decisions, thus promoting a more adaptable and transparent culture.

Limited Support

Another common challenge is the limited support for outcomes and use cases that resonate with different stakeholders. Most tools are metric-driven or KPI, thus needing a broader understanding of outcomes required for driving results and gaining sponsorship. Use cases often focus narrowly on IT operations management or DevOps, thus neglecting the broader operational and business impact. The opportunity is to adopt an outcome-driven approach encompassing operational and business perspectives. Use cases should be curated to cater to the needs of different IT stakeholders like IT operations, DevOps, IT service management (ITSM), and IT planning, thus ensuring a more impactful AIOps implementation.

Lack of On-Premises Option for Security and Compliance

The challenge of deployment options, particularly the lack of on-premises choices for security and compliance, is a concern for organizations with stringent regulatory requirements. Most tools offer either SaaS or on-premise deployment exclusively, which limits flexibility. Some vendors retrofit legacy architectures for enterprise deployment, while others over-provision infrastructure to address scalability concerns [24]. However, an opportunity arises to adopt a solution that supports different deployment options like fully managed SaaS, cloud, and on-premise. Modern applications with a cloud-native architecture leverage microservices and containers, thus providing the necessary flexibility for scalable,

distributed, and secure deployments. This technique aligns with the principles of vertical and horizontal scalability, thus ensuring that the chosen AIOps platform can evolve in line with the organization's needs while adhering to relevant security and compliance standards.

Benefits of Combining AIOps with Cloud-Native DevOps Manageability and Independence

Cloud-native applications depict a distinctive architecture allowing independent development, management, and deployment of individual components. This inherent modularity facilitates autonomous evolution, thus streamlining the development lifecycle. This independence is further augmented when complemented by AIOps, which utilizes the power of ML and AI. AIOps can intelligently optimize and manage each component, thus ensuring seamless coordination within the cloud-native ecosystem.

Fosters Resilience

The strong architecture of cloud-native applications, fortified by AIOps, contributes to increased resiliency. When infrastructure outages pose a threat, AIOps algorithms actively identify potential vulnerabilities and initiate preemptive measures. The technique and the adaptability of cloud-native designs ensure applications remain operational and stay online even in diverse conditions.

Interoperability

Cloud-native services often depend on open-source and standards-based technologies, thus promoting workload portability and interoperability. When AIOps is integrated into this framework, it operates within the standardized protocols, thus fostering seamless collaboration and communication between disparate components. The result is a reduced vendor lock-in, thus allowing for greater adaptability and flexibility in the cloud-native ecosystem.

Enhanced Business Agility

Cloud-native applications, by their design, thus provide unparalleled flexibility in deployment options across the network. When infused with AIOps capabilities, business agility reaches new points. AIOps streamlines operational processes, automates routine tasks, and ensures CI/CD through DevOps techniques [25]. The merge allows for smaller, more manageable applications, thus facilitating rapid development, deployment, and repetitive improvements.

Increased Automation

Automation is the backbone of both cloud-native DevOps and AIOps. Cloud-native applications leverage DevOps automation features to allow continuous delivery and deployment, thus promoting a culture of frequent software updates. AIOps further refines and amplifies this automation with its ML algorithms, thus providing intelligent insights for optimizing software changes. Techniques such as canary releases and blue-green deployments are necessary to allow improvements without disrupting the customer experience.

Zero Downtime Deployments

Container orchestrators like Kubernetes are key to cloud-native architectures, which ensure the deployment of software updates with minimal to zero downtime. AIOps merged with container orchestration adds an extra layer of sophistication. It optimizes the deployment process, mitigates risks, and ensures that updates integrate with the operational environment seamlessly, thus leading to a seamless user experience without downtime [26].

Improving Incident Response with AIOps

Adding AIOps into cloud-native incident management brings about capabilities that hugely enhance the efficacy and efficiency of incident response strategies. This integration helps in the timely detection and diagnosis of issues and streamlines the coordination of responses, thus leading to a more cost-effective and resilient incident management framework.

Driven Anomaly Detection

In cloud-native ecosystems, where the scale and complexity often result in information overload, AIOps helps detect anomalies that may depict possible incidents. Monitoring performance metrics like memory utilization, network bandwidth, and CPU usage provides a baseline for normal system behavior. AIOps uses ML algorithms like local outlier factor or isolation forest and identifies deviations from these baselines. This technique allows teams to quickly detect and respond to incidents, thus preventing possible disruptions before they escalate.

Faster Resolution from Response History

A historical record of past incidents is important for accelerating incident resolution. AIOps tools with techniques like K-means clustering help ease delving into incident histories, thus identifying similarities and patterns between past and current issues. By leveraging this knowledge base, incident response teams can gain insights into effective resolution strategies. AIOps tools suggest optimal courses of action by drawing from the incidents, thus expediting the resolution process and minimizing downtime.

Automated Notification

Timely and automated notification is key for effective incident responses. AIOps thrives in this area by automating notifying relevant teams when incidents or critical events happen. By intelligently collating essential information and using AI to filter noise from notifications, AIOps promptly inform the correct teams [27]. This accelerates incident response and minimizes alert fatigue, thus allowing responders to focus on actionable reports and prioritize their efforts efficiently.

NLP for Ticket Interpretation

During widespread incidents, the influx of tickets can easily overwhelm support teams. AIOps employ NLP algorithms, which are important in interpreting tickets quickly by sorting through free-text information in tickets, categorizing them based on similarities, and quickly pointing out issues. NLP allows faster incident report interpretation, which expedites response and communication, thus ensuring that support staff can swiftly address specific concerns and meet client's expectations for quicker interactions.

Root Cause Analysis

Identifying the root cause of incidents is often a difficult and time-consuming task. AIOps deals with this challenge by applying unsupervised ML techniques to monitor metrics and correlate logs, thus expediting root-cause analysis [28]. Therefore, by consolidating data from disparate sources into a centralized dashboard, AI allows a comprehensive view of incidents. This streamlines the identification of optimization opportunities and empowers teams to respond to crises and predict and prevent future incidents.

Conclusion

This article shows that organizations are fast steering towards increased security integration by embracing intelligent automation and cloud-native practices. Recognizing the huge role of cultural

shifts, collaboration, and the need for continuous improvement, businesses are positioning themselves to survive and thrive in IT operations [29].

Moving forward, the future of AI in DevOps is poised to transform from the increased usage of ML models for predictive resource optimization to the development of complex AI-driven monitoring tools; the merge of AI with emerging technologies like serverless architecture and edge computing is changing the DevOps ecosystem.

AI's capability moves beyond autonomously optimizing software performance, enhancing code quality, and generating code based on high-level needs or business objectives. In times when IT operations are crucial for business functionality, AIOps is the solution for organizations looking to thrive in a technology-driven world. According to Gartner's research, by 2025, 70% of organizations need to adopt a service/product orientation to be able to support their business [30], depicting the role of embracing AIOps to foster unparalleled operational efficiency and moving towards a future where adaptability and innovation are key.

References

1. Kumar D, Sampath AK (2022) Orchestration of ML/AI models using MLOps/AIOps frameworks. Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022 1-7.
2. Shi L, Yao W, Chen M, Liang H, Chen Y, et al. (2022) A solution on cloud and digital transformation for IT system using DevOps yundao platform. In 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA) 868-871.
3. Vázquez-Rodríguez Á, Giraldo-Rodríguez C, Chaves-Diéguéz D (2022) A Cloud-Native Platform for 5G Experimentation. In 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) 60-64.
4. Chen T, Suo H (2022) Design and Practice of DevOps Platform via Cloud Native Technology. In 2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS) 297-300.
5. CHEN Yong, YAO Wensheng, CHEN Jingxiang, LIANG Huan, LI Jing (2020) Cloud native approach of agile cloud-network converged application delivery. Telecommunications Science 36: 96.
6. Zhang J, Wang Y, Liu X (2022) Cloud-Native CI/CD platform. In NCIT 2022: Proceedings of International Conference on Networks, Communications and Information Technology 1-5.
7. Raj P, Vanga S, Chaudhary A (2022) Cloud-native computing: How to design, develop, and secure microservices and event-driven applications. John Wiley & Sons <https://www.wiley.com/en-sg/+native+Computing:+How+to+Design,+Develop,+and+Secure+Microservices+and+Event+Driven+Applications-p-9781119814764>.
8. Bagehorn F, Rios J, Jha S, Filepp R, Shwartz L, et al. (2022) A fault injection platform for learning AIOps models. In Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering 1-5.
9. Di Stefano Alessandro, Di Stefano A, Morana G, Zito D (2021) Prometheus and AIOps for the orchestration of Cloud-native applications in Ananke. In 2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) 27-32.
10. Long XUE, Gang LU, Qi ZHOU, Huiyan ZHANG,

- Tingjun WAN (2020) Cloud native intelligent operation and maintenance technology. *Telecommunications Science* 36: 105-112.
11. Rao S (2020) AIOps with the Oracle Autonomous Database. In 2020 IEEE 36th International Conference on Data Engineering Workshops (ICDEW) 1-3.
12. Sojan A, Rajan R, Kuvaja P (2021) Monitoring solution for cloud-native DevSecOps. In 2021 IEEE 6th International Conference on Smart Cloud (SmartCloud) 125-131.
13. Battina DS (2020) Devops, A New Approach To Cloud Development & Testing. *International Journal of Emerging Technologies and Innovative Research* 7: 982-985.
14. Laszewski T, Arora K, Farr E, Zonooz P (2018) Cloud Native Architectures: Design high-availability and cost-effective applications for the cloud. Packt Publishing Ltd <https://www.perlego.com/book/800670/cloud-native-architectures-design-highavailability-and-costeffective-applications-for-the-cloud-pdf>.
15. Tola B, Jiang Y, Helvik BE (2020) On the resilience of the NFV-MANO: An availability model of a cloud-native architecture. In 2020 16th International Conference on the Design of Reliable Communication Networks DRCN 2020 1-7.
16. Chen Z, Kang Y, Li L, Zhang X, Zhang H, et al. (2020) Towards intelligent incident management: why we need it and how we make it. In *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* 1487-1497.
17. Masood A, Hashmi A, Masood A, Hashmi A (2019) AIOps: predictive analytics & machine learning in operations. *Cognitive Computing Recipes: Artificial Intelligence Solutions Using Microsoft Cognitive Services and Tensor Flow* 359-382.
18. Notaro P, Cardoso J, Gerndt M (2021) A survey of aiops methods for failure management. *ACM Transactions on Intelligent Systems and Technology (TIST)* 12: 1-45.
19. Thakore U, Ramasamy HV, Sanders WH (2019) Coordinated Analysis of Heterogeneous Monitor Data in Enterprise Clouds for Incident Response. In 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) 53-58.
20. Hua Y (2021) A Systems Approach to Effective AIOps Implementation (Doctoral dissertation, Massachusetts Institute of Technology) <https://dspace.mit.edu/bitstream/handle/1721.1/139422/hua-huay-sm-sdm-2021-thesis.pdf?sequence=1&isAllowed=y>.
21. Sabharwal N, Bhardwaj G (2022) AIOps Supporting SRE and DevOps. In *Hands-on AIOps: Best Practices Guide to Implementing AIOps* 73-88.
22. Malec A, Prasad PWC (2023) Assessing Organisational Incident Response Readiness in Cloud Environments. In *Conference on Innovative Technologies in Intelligent Systems and Industrial Applications* 387-396.
23. Dhamija P, Bag S (2020) Role of artificial intelligence in operations environment: a review and bibliometric analysis. *The TQM Journal* 32: 869-896.
24. Bogatinovski J, Nedelkoski S, Acker A, Schmidt F, Wittkopp T, et al. (2021) Artificial intelligence for IT operations (AIOps) workshop white paper. arXiv preprint <https://arxiv.org/abs/2101.06054>.
25. Helo P, Hao Y (2022) Artificial intelligence in operations management and supply chain management: An exploratory case study. *Production Planning & Control* 33: 1573-1590.
26. Dhamija P, Bag S (2020) Role of artificial intelligence in operations environment: a review and bibliometric analysis. *The TQM Journal* 32: 869-896.
27. Sandeep SR, Ahamad S, Saxena D, Srivastava K, Jaiswal S, et al. (2022) To understand the relationship between Machine learning and Artificial intelligence in large and diversified business organisations. *Materials Today: Proceedings* 56: 2082-2086.
28. Lipai Z, Xiqiang X, Mengyuan L (2021) Corporate governance reform in the era of artificial intelligence: research overview and prospects based on knowledge graph. *Annals of Operations Research* 326: 105.
29. Kosińska J, Zieliński K (2020) Autonomic management framework for cloud-native applications. *Journal of Grid Computing* 18: 779-796.

Copyright: ©2023 Sumanth Tatineni. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.