Acceleration, Quantum, Information Technology and Algorithm Journal (AQILA)
Vol. 1, No. 1, Juni 2024, pp 16-22
ISSN: 3062-8555, DOI: 10.62123/aqila.v1i1.25

Never Overlook Security Awareness on Deployment

Rizki Sadewa[1*], Muharman Lubis[1], Edi Triono Nuryatno[2]

[1] Telkom University, Jl. Telekomunikasi No. 1, Bandung, 40257, Indonesia
[2] University of Western Australia, Australia

*Corresponding Email: rizkykysadewa@gmail.com

DOI : 10.62123/aqila.v1i1.25

Received : May 17, 2024
Revised : June 04, 2024
Accepted : June 09, 2024

Keywords:
Security Awareness
Deployment
DevSecOps
Kubernetes

ABSTRACT

Since preliminary evidence supports the association between security culture and information security awareness (ISA), more research is needed to determine how it interacts with organizational culture. Beyond variations in respondent nation or gender, the study's findings also demonstrate an association between stronger cyber expertise and level of cyber awareness. Additionally, awareness is linked to defense mechanisms but not the information they were willing to divulge. People play an even more important role in the collaboration between those teams and the security team when security is incorporated into DevOps practices. Furthermore, security is crucial when creating essential systems since it allows us to control objectives, risks, and evidence. Labor only starts after implementing security into the DevOps toolchain. To establish a security culture, we are additionally required to start with behavioral alterations. One of the largest Sharia banks in Indonesia anticipated cyberattacks in 2023, demonstrating to us how crucial security is in the modern world. Although no one could claim that using one of the security solutions would guarantee absolute safety, information security technology is quite dynamic. Future studies could improve on the current findings by taking into account national culture. This study has the aim of proving that we are never satisfied by current security maturity even if you or your company is implementing the best security tools, because the vulnerability can come from that deployment and wherever the environment itself.

1. INTRODUCTION

Agility and quickness are growing in demand in the commercial world. Technology advancements like Continuous Engineering, in particular DevOps, have provided certain businesses a competitive edge [1]. The majority of human aspects of information security research to date has been devoted to discovering the traits that may be connected to and have an impact on information security conduct, with the goal of better understanding human vulnerabilities on an individual level [2]. A assortment of IT associations are grasping DevOps in significant numbers. DevOps is being received by businesses of all sizes, from early-stage new businesses to "unicorns" like Facebook, Amazon, etc. For occurrence, at Flickr, "the near communication and collaboration between the advancement and operations groups improved the discharge time of code by a calculate of ten [3]. Data security mindfulness (ISA) is the state of being mindful and committed to security rules, recognizing potential dangers, understanding the significance of obligations, and acting in like manner. In spite of various data security breaches, especially in knowledge-based teach, coming about from users' hesitance or disappointment to take after security rules, viable measures ought to be executed to moderate negative impacts. In this manner, more noteworthy consideration is required to get it the parts of person, organization, and natural variables in optimizing data security mindfulness [4].

In order to encourage communication between the development and operation teams and decrease discrepancies between development, operations, and releases, DevOps focuses on delivering software quickly using agile methodologies. In this study, we use the definition provided by Leite et al . "DevOps is an organisational collaborative and multidisciplinary effort to automate continuous delivery of new software versions while ensuring their accuracy and dependability." Customers, operations, and quality assurance stakeholders work together with the development team to constantly deliver software products, seize market possibilities, and shorten the time needed to take consideration of client input. In this context, MacDonald, a fellow at Gartner, pointed out that [3] "Development, operations, and cybersecurity are fundamentally intertwined, and DevOps needs to adjust to a new vision of DevOpsSec.". Therefore, recently as software development teams realised the value of addressing security risks early in the development cycle, DevSecOps emerged from the DevOps approach. To facilitate communication between the three

teams responsible for development, operations, and security, DevSecOps involves security management throughout the entire development process.

Kubernetes, an open-source computer program outlined to robotize the administration of computerised administrations like holders, is broadly embraced by specialists. Its use stems from its capacity to streamline and dispense with tedious manual assignments included in conveying and overseeing holders. Kubernetes is recognized as one of the foremost popular container coordination instruments within the open-source domain, being grasped by associations such as Adidas, Nokia, Spotify, and the U.S. Division of Defense (DoD). The focal points of utilizing Kubernetes have been well-documented. For occurrence, the execution of Kubernetes within the U.S. DoD come about in a exceptional lessening of computer program sending time from eight months to fair one week. Essentially, Adidas experienced outstanding enhancements, counting a 50% lessening in e-commerce site stack time and a critical increment in discharge recurrence, from once each 46 weeks to 34 times per day [5]. Whereas Kubernetes offers various focal points, clients have communicated misgivings with respect to its security. A study conducted by the Cloud Local Computing Establishment, including 1,337 specialists, uncovered that 40% of the members communicated concerns almost the security of Kubernetes. Recounted prove encourage substantiates these concerns raised by professionals. For occurrence, in 2018, there was an occurrence where pernicious people misused an uncertain Kubernetes support to pick up unapproved get to to Tesla's Amazon Web Administrations (AWS) assets [5]. Given this, in spite of the presence of a auxiliary think about on DevOps culture, to the finest of our information, no investigate has been done on the social angles of DevSecOps particularly on Sending for Kubernetes. Therefore, this paper aims to appear the significance of security within the arrangement handle.

2. LITERATURE REVIEW

2.1 DevOps

DevOps, which merges Development and Operations, is a fresh perspective in software engineering that has garnered significant attention recently. Since DevOps is a newly coined term and an innovative idea, there isn't a widely accepted definition of it yet. As a result, current definitions of DevOps usually only capture aspects pertinent to the overall concept [6]. Since DevOps is a relatively new subject, there isn't a standardized definition for it yet [7]. Therefore, in this paper, we aim to conceptualize DevOps through the following contributions:

1. Analyzing and comparing definitions of DevOps found in the research literature.
2. Identifying and classifying practices linked to DevOps.
3. Comparing DevOps with other development methodologies.

Another researcher noted that software engineering experts are keen to identify and define the characteristics of DevOps to bridge the gap between academia and industry and clarify the meaning of DevOps. In this study, we performed a systematic literature review to explore and assess how DevOps has been evaluated in peer-reviewed literature [6]. The study aimed to:

1. Distinguish and indicate DevOps standards.
2. Recognize and indicate hones and exercises related with DevOps.
3. Recognize and indicate challenges in receiving DevOps and relate them to particular hones.
4. Recognize and indicate the claimed and illustrated benefits of DevOps.
5. Synthesize the discoveries by (a) deciding the conditions between hones and (b) building up the joins between hones and their comparing benefits.

Erich et al.[8] state that "DevOps automation is bolstered by various design patterns that enhance the continuous delivery of software applications on cloud platforms." DevOps asserts it enables "faster delivery of builds, features, and bug fixes, thereby creating a continuous build pipeline" [9]; however, adopting DevOps is complex [10]. To effectively adopt DevOps for IS development, it is crucial to clearly understand its underlying concepts, practices, tools, benefits, and challenges. We can also highlight identified elements such as communication and collaboration, continuous deployment, continuous delivery, continuous planning, and automated pipelines [11].

2.2 DevSecOps

Joining security into DevOps has been challenging since ordinary security strategies cannot coordinate the nimbleness and speed of DevOps. DevSecOps may be a development pointed at creating and coordination present day security strategies that adjust with DevOps hones. This consider gives an outline of DevSecOps, its execution, the benefits it offers, and the challenges organizations experience amid its appropriation. To realize this, we conducted a multivocal writing audit, analyzing a choice of dim literature [12]. In later a long time a expansive portion of computer program improvement companies have changed center from creating program as a item (SaaP), where companies created the computer program and conveyed a wrapped up item to a client that at that point introduced and ran it locally, to create program as a benefit (SaaS), where computer program is centrally facilitated on a cloud foundation and gotten to through for illustration a webbrowser [1], or other channels that conveys it straightforwardly to a customer's machine or gadget [2]. The utilize of it is at that point advertised through authorizing and memberships. With SaaS, the clients don't control the fundamental cloud framework or the application's usefulness [1], as that's

done by the supplier. This gives the supplier the opportunity to ceaselessly move forward and convey their computer program without having to redistribute it to all their clients as they essentially upgrade the computer program on their possess cloud framework. This advanced program engineering process of creating whereas ceaselessly joining and conveying computer program is complex. Nonstop integration (CI) implies to consequently coordinated modern code from a few designers into the same form of the computer program and at the same time, check for errors [3]. Ceaseless Conveyance (CD) implies to send unused program to generation, with the varying figure from conventional computer program sending being the recurrence of sending, which can happen numerous times each day [3]. "Continuous conveyance empowers businesses to diminish cycle time so as to urge speedier criticism from clients, decrease the hazard and taken a toll of arrangements, get way better perceivability into the conveyance handle itself, and oversee the dangers of computer program conveyance more effectively" [4]. These forms require a huge number of devices and data frameworks [5]. These forms, devices and frameworks are regularly overseen by free operations groups [6]. Numerous challenges when implementing CI/CD brought about from need of collaboration and communication between the administrators and developers [2][3][6][7]. Endeavors at overcoming these challenges have come about in a concept, named DevOps [2].

In later a long time, numerous computer program advancement companies have moved their centre from Computer program as a Item (SaaP), where a completed computer program item is conveyed to a client for neighbourhood establishment and utilize, to Computer program as a Benefit (SaaS). SaaS includes centrally facilitating program on a cloud foundation, available through web browsers or other coordinate channels to the customer's gadget [13]. This demonstrate is advertised through authorizing and memberships, with the supplier overseeing the basic foundation and application usefulness. Thus, the supplier can persistently progress and upgrade the program without requiring to redistribute it to all clients, as overhauls are made on the cloud framework [14]. This cutting-edge program designing approach, which includes nonstop integration and conveyance, is complex. Ceaseless Integration (CI) includes consequently coordination unused code from different engineers into a single program adaptation whereas checking for blunders. Persistent Conveyance (CD) involves habitually sending unused computer program to generation, frequently different times a day. CD permits businesses to decrease cycle times, get quicker client criticism, lower sending dangers and costs, pick up superior perceivability into the conveyance handle, and oversee computer program conveyance dangers more viably [15]. These forms require various devices and data frameworks, ordinarily overseen by free operations groups. Challenges in actualizing CI/CD regularly stem from a need of collaboration and communication between administrators and designers. Endeavours to address these challenges have driven to the concept of DevOps.

2.3 Security Awareness

Security mindfulness is habitually dismissed in data security programs. Whereas organizations contribute in progressed security innovations and progressing preparing for their security experts, small exertion is made to improve the security mindfulness of customary clients, who in this way gotten to be the weakest interface within the organization. Thus, organized cyber hoodlums are progressively centering on creating modern hacking strategies to take cash and data from the common open. Also, the quick growth of web entrance within the Center East, coupled with constrained client security mindfulness, makes the locale an engaging target for cyber offenders [16].

Hackers are constantly discovering new methods to steal information. Unfortunately, "uneducated" users within an organization become easy targets for hackers and are susceptible to privacy attacks [17]. Education and training for users are essential to combat IT security threats. Users need to not only learn the material but also apply it in their daily activities. Achieving this is challenging and requires a collective effort, not just from the users or the organization. Multiple groups must collaborate to cultivate IT security awareness. Below, we summarize some recommendations [16]:

1. Governments ought to create legislation concerning cybercrime and ensure its enforcement. Collaboration with other nations is crucial, given that many attacks originate from overseas. Additionally, establishing dedicated Computer Emergency Response Teams (CERT) for the detection, prevention, and response to cyber security incidents is essential.
2. Setting up Computer Crisis Reaction Groups (CERT) is urgent for boosting residents' security mindfulness. CERTs can play a part in forming modern cybercrime laws, preparing computer scientific groups, and supporting organizations and people in combating cybercrime. Additionally, organization a cyber security mindfulness month can increase open consideration to cyber security issues. Eminently, nations just like the UAE, Saudi Arabia, and Qatar have recently set up CERT centers within the Center East
3. Police Offices ought to shape specialized computer forensics groups proficient at collecting, recouping, analyzing, analyzing, and displaying electronic prove from computers or electronic gadgets. Endeavors got to give security preparing to both representatives and clients, either through online or onsite strategies, or a mix of both, conducted frequently to address advancing IT security dangers. Additionally, endeavors ought to run nearby mindfulness campaigns utilizing custom fitted substance and conveyance strategies to suit diverse users' dialect, culture, and inclinations. Compliance with measures like ISO 27001 can be encouraged through learning administration frameworks to track client learning action. Reviews ought to be conducted to survey security mindfulness levels and the adequacy of mindfulness campaigns, guaranteeing protection security. Setting up a central point of contact for IT security things is significant for client communication, and instruction fabric ought to cover IT security approaches

and related punishments. Enterprises should embrace a proactive position toward security mindfulness instead of a responsive one.
4. Telecommunication companies (ISPs) should provide guidance on safe internet usage and secure configuration of internet devices.
5. Media outlets should consistently disseminate IT security advice, report on IT security incidents, and highlight the penalties imposed on attackers.
6. Clients ought to ceaselessly teach themselves by perusing magazines, books, and online articles on IT security dangers and measures for self-protection.
7. Non-Governmental Organizations (NGOs) ought to initiate IT security mindfulness campaigns and offer back to those with questions or security issues.
8. Schools and colleges ought to conduct security mindfulness campaigns and join IT security points into their computer courses.

3. RESEARCH METHODS

The chosen approach for investigating deployment attack detection models was the systematic literature review (SLR) methodology. This method encompasses comprehending, assessing, and recognizing the existing research evidence in order to address specific review inquiries [18]. Conducting a literature review is an essential initial phase in research, allowing for a comprehensive grasp of the current advancements and identification of gaps and obstacles in the field. A systematic literature review follows a structured approach, involving a series of methodical steps to systematically organise the review process [19].

3.1 Research question

Population, Intervention, Comparison, Outcomes, and Context (PICOC) criteria were utilised to create these inquiries. Table 1 illustrates the population, intervention, comparison, outcomes, and context (PICOC) criteria. Conducting a literature review is an essential initial phase in research, allowing for a comprehensive grasp of the current advancements and identification of gaps and obstacles in the field. A systematic literature review follows a structured approach, involving a series of methodical steps to systematically organise the review process [8]. The following research inquiries will be addressed in this study:

Table 1. Population, Intervention, Comparison, Outcomes, and Context (PICOC) Criteria

Criteria	Value
Population	Security Awareness on Deployment
Intervention	Deployment Vulnerability
Comparison	Not Available
Outcomes	Deployment Security Practices on Kubernetes and VM in other Cloud Computing Environment.
Context	Review the existing studies of security practices

RQ1 : What are the current challenges of Deployment Security Practices on Kubernetes systems that support the decision-making of Security Awareness on Deployment?
RQ2 : Which technique is most appropriate to support decision-making for Review the existing studies of security practices in Security Awareness on Deployment?
RQ3 : In which scenarios are deployment security used to provide Deployment Security Practices on Kubernetes in Review the existing studies of security practices for Security Awareness on Deployment?

3.2 Research process

The journals, conferences, and sources listed in Table 2 were chosen based on their track record of featuring empirical studies, literature surveys, and being frequently referenced in systematic literature reviews within the field of software engineering.

Table 2. Sources Journals, Conferences, and Resources

Source	Acronym
DevSecOps: A Multivocal Literature Review	DSOAMLR
Security as Culture: A Systematic Literature Review of DevSecOp	SACAAA
DevSecOps Metrics	DSOMEM
Preliminary Findings about DevSecOps from Grey Literature	PFADGL
Toward successful DevSecOps in software development organizations: A decision-making framework	TSDEISD
Self-Service Cybersecurity Monitoring as Enabler for DevSecOps	SSCMED

3.3 Quality assestment

Every Systematic Literature Review (SLR) underwent assessment utilizing the criteria from the York University, Centre for Reviews and Dissemination (CDR) Database of Abstracts of Reviews of Effects (DARE) . These criteria revolve around four questions aimed at assessing quality.

4. DISCUSSION AND RESULT

Deployment security practices encompass a set of protocols and strategies aimed at fortifying the security of software or systems during the deployment phase. These measures are critical to mitigate potential risks and vulnerabilities that may arise when deploying applications or systems.

4.1 Security education

Security education plays a pivotal role in equipping individuals and organizations with the knowledge and skills needed to understand, mitigate, and respond to security threats effectively. It encompasses various aspects:

1. Awareness Programs: These initiatives aim to raise general awareness about security risks and best practices among individuals within an organization. They cover topics like phishing, password security, social engineering, and the importance of regular updates.
2. Training Sessions: Comprehensive training programs delve deeper into specific areas of security, providing in-depth knowledge on topics such as network security, secure coding practices, data protection, incident response, and compliance regulations.
3. Specialized Certifications: Recognized certifications in security domains—like Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or CompTIA Security+—validate expertise and encourage continuous learning.
4. Hands-on Workshops and Simulations: Practical exercises, simulations, and workshops simulate real-world scenarios, allowing individuals to apply theoretical knowledge and develop practical skills in a controlled environment.
5. Tailored Curriculum: Educational institutions and training providers offer specialized programs tailored to different roles and industries, ensuring that professionals gain relevant knowledge aligned with their responsibilities.
6. Promotion of a Security Culture: Beyond formal education, fostering a culture of security awareness is crucial. This includes integrating security practices into everyday operations, encouraging reporting of security incidents, and emphasizing collective responsibility for security.
7. Continuous Learning and Updates: Given the evolving nature of cybersecurity threats, ongoing education and staying updated with the latest trends, vulnerabilities, and defense mechanisms are essential.

4.2 Security design

Secure by design refers to an approach where security measures and considerations are integrated into the design phase of a system or product from its inception. This proactive strategy aims to minimize vulnerabilities and reduce the likelihood of security breaches by prioritizing security features and considerations throughout the entire development lifecycle.

Key principles of a "secure by design" approach include:

1. Preventative Measures: Anticipating potential security threats and implementing measures to prevent vulnerabilities rather than simply reacting to security issues after they occur.
2. Default Security Settings: Setting secure configurations and default settings to minimize the attack surface and ensure that the system starts with a secure baseline.
3. Risk Assessment: Identifying potential risks and threats early in the design phase and implementing controls to mitigate these risks.
4. Least Privilege Principle: Granting minimal access and privileges to users or components to limit potential damage if compromised.
5. Strong Encryption and Authentication: Implementing robust encryption methods and authentication mechanisms to protect data and control access.
6. Modularity and Isolation: Designing systems in a modular fashion and isolating components to contain potential security breaches and limit their impact.
7. Regular Updates and Maintenance: Building mechanisms for easy updates and maintenance to address vulnerabilities and stay resilient against emerging threats.

By integrating security into the foundational design of systems or products, the "secure by design" approach aims to create inherently more secure and resilient solutions. This strategy not only helps in reducing the risks of security breaches but also saves time and resources that might otherwise be spent on retrofitting security features after the fact.

4.3 Security automation

Security automation in DevSecOps refers to the integration of automated security practices and tools throughout the software development lifecycle (SDLC) to embed security measures seamlessly into the process. This approach emphasizes the collaboration between development, security, and operations teams to create a more secure and efficient software delivery pipeline. Here's an overview:

1. Continuous Security Testing: Automated security testing tools are integrated at various stages of development, including static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), and interactive application security testing (IAST). These tools continuously scan code, dependencies, and applications for vulnerabilities and compliance issues.
2. Shift Left Approach: Security checks are moved earlier in the SDLC, enabling issues to be identified and resolved during the development phase rather than after deployment. This "shift left" strategy helps in catching and fixing vulnerabilities at their inception, reducing the cost and effort of addressing them later.
3. Infrastructure as Code (IaC) Security: Automation tools are used to validate the security configuration of infrastructure components (like cloud services or containers) defined through code. This ensures that security measures are incorporated into the infrastructure setup itself
4. Policy Enforcement and Compliance: Automated checks enforce security policies and regulatory compliance standards throughout the development process. This ensures that code and applications adhere to security guidelines and industry regulations
5. Continuous Monitoring and Response: Automated monitoring tools continuously track system behavior and security metrics in real-time. They can alert teams about potential security incidents, enabling rapid response and mitigation
6. Integration with CI/CD Pipelines: Security checks and controls are seamlessly integrated into the continuous integration/continuous deployment (CI/CD) pipelines. This ensures that security measures are an integral part of the automated build, test, and deployment processes.

Security Orchestration and Automation Response (SOAR): Utilizing SOAR platforms, security incident response tasks can be automated, enabling faster and more efficient handling of security incidents and threats.

5. CONCULUSSION

DevSecOps speaks to a social move and a set of hones that coordinated security into each stage of the computer program advancement lifecycle. It's not fair a strategy; it's a mentality alter that cultivates collaboration, communication, and shared obligation among improvement, security, and operations groups. In conclusion, DevSecOps isn't around including security checkpoints; it's a all encompassing approach that implants security as an indispensably portion of the computer program improvement lifecycle. It's a social change that empowers organizations to construct and convey secure, high-quality computer program more effectively and viably.

REFRENCES

[1] M. Sánchez-Gordón and R. Colomo-Palacios, "Security as Culture: A Systematic Literature Review of DevSecOps," in *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, 2020, pp. 266–269, doi: 10.1145/3387940.3392233.

[2] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput. Secur.*, vol. 88, p. 101640, 2020, doi: https://doi.org/10.1016/j.cose.2019.101640.

[3] M. A. Akbar, K. Smolander, S. Mahmood, and A. Alsanad, "Toward successful DevSecOps in software development organizations: A decision-making framework," *Inf. Softw. Technol.*, vol. 147, p. 106894, 2022, doi: https://doi.org/10.1016/j.infsof.2022.106894.

[4] A. R. Ahlan, M. Lubis, and A. R. Lubis, "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures," in *Procedia Computer Science*, 2015, vol. 72, doi: 10.1016/j.procs.2015.12.151.

[5] M. S. Islam Shamim, F. Ahamed Bhuiyan, and A. Rahman, "XI Commandments of kubernetes security: A systematization of knowledge related to kubernetes security practices," *Proc. - 2020 IEEE Secur. Dev. SecDev 2020*, pp. 58–64, 2020, doi: 10.1109/SecDev45635.2020.00025.

[6] R. Jabbari, N. bin Ali, K. Petersen, and B. Tanveer, "What Is DevOps? A Systematic Mapping Study on Definitions and Practices Ramtin," in *DevOps on the Microsoft Stack*, Berkeley, CA: Apress, 2016, pp. 3–8.

[7] J. Roche, "Adopting DevOps Practices in Quality Assurance: Merging the art and science of software development," *Queue*, vol. 11, no. 9, pp. 20–27, Sep. 2013, doi: 10.1145/2538031.2540984.

[8] F. Erich, C. Amrit, and M. Daneva, "Report: DevOps Literature Review," *https://www.researchgate.net/publication/267330992_Report_DevOps_Literature_Review*, no. October, pp. 1–27, 2014, doi: 10.13140/2.1.5125.1201.

[9] M. Soni, "End to End Automation on Cloud with Build Pipeline: The Case for DevOps in Insurance Industry, Continuous Integration, Continuous Testing, and Continuous Delivery," in *2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 2015, pp. 85–89, doi: 10.1109/CCEM.2015.29.

[10] J. Wettinger, V. Andrikopoulos, and F. Leymann, "Automated Capturing and Systematic Usage of DevOps Knowledge for Cloud Applications," *Proc. IEEE ...*, 2015, [Online]. Available: http://www.iaas.uni-stuttgart.de/RUS-data/INPROC-2015-01 - Automated Capturing and Systematic Usage of DevOps Knowledge for Cloud Applications.pdf.
[11] G. B. Ghantous and A. Gill, "DevOps: Concepts Practices, Tools, Benefits andChallenges," *PACIS 2017 Proc.*, p. 1, 2017, [Online]. Available: http://aisel.aisnet.org/pacis2017/96.
[12] H. Myrbakken and R. Colomo-Palacios, "DevSecOps: A Multivocal Literature Review," 2017, pp. 17–29.
[13] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," 2011.
[14] B. Fitzgerald and K.-J. Stol, "Continuous software engineering: A roadmap and agenda," *J. Syst. Softw.*, vol. 123, pp. 176–189, 2017, doi: https://doi.org/10.1016/j.jss.2015.06.063.
[15] Humble Jez and Molesky Joanne, "Why Enterprises Must Adopt Devops to Enable Continuous Delivery," no. August, pp. 6–12, 2011, [Online]. Available: www.cutter.com.
[16] F. A. Aloul, "The Need for Effective Information Security Awareness," *J. Adv. Inf. Technol.*, vol. 3, no. 3, 2012, doi: 10.4304/jait.3.3.176-183.
[17] Z. A. Khattak, J. A. Manan, and S. Sulaiman, "Analysis of Open Environment Sign-in Schemes-Privacy Enhanced & Trustworthy Approach," *J. Adv. Inf. Technol.*, vol. 2, no. 2, pp. 109–121, 2011, doi: 10.4304/jait.2.2.109-121.
[18] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, and H. Fahmy, "Monitoring Real Time Security Attacks for IoT Systems Using DevSecOps: A Systematic Literature Review," *Information*, vol. 12, no. 4. 2021, doi: 10.3390/info12040154.
[19] A. Carrera-Rivera, F. Larrinaga, and G. Lasa, "Context-awareness for the design of Smart-product service systems: Literature review," *Comput. Ind.*, vol. 142, p. 103730, 2022, doi: https://doi.org/10.1016/j.compind.2022.103730.