DevOps for Better Software Security in the Cloud

Ravi Teja Yarlagadda. *Sr. DevOps SME, Department of Information Technology, USA*
yarlagaddaraviteja58@gmail.com

Abstract— *The DevOps model ensures that the organization's growth and processes are work together. As far as security is concerned, DevOps security tools are significant in relaying information on external attackers which can be traced back to development, allowing for quicker elimination of potential vulnerabilities. It is a process that is particularly critical in cloud deployments, whereby release intervals can be less than24 hours. This paper will explore how DevOps can be used in cloud solutions to increase the overall security of systems and applications [1]. DevOps delivers improved automation across the product delivery chain, prevents errors, nullifies risk and downtime, and enables security to be further integrated into the cloud environment. The paper covers the main facets of DevOps in securing cloud solutions with examples provided on practical applications by companies like IBM. The significance of the research to the U.S is also covered especially for organizations looking to secure their serverless systems.*

Keywords: *DevOps, cloud solutions, Secure by Design, servers, DevSecOps, Software, Development life cycle*

I. INTRODUCTION

Cloud computing has many benefits, but on-demand self-service is probably the most important for device developers; within a small amount of time, computer services can be distributed and scaled up and down via web-accessible interfaces. This, in essence, lays a foundation for DevOps: a new philosophy in software development and operating systems, often simplified in the phrase "You create it, you run it"[2]. While practices that promote the development, delivery, and deployment of applications are phenomenal, it cannot be overlooked that security vulnerabilities are occurring all around us. Software systems have evolved to the extent where we use and rely on them regularly in the same way that we rely on conventional services and infrastructure and infrastructure such as roads. The importance of confidential information in data networks is steadily growing, but the same can be said for related attacks, but efforts to minimize the resulting risk are not being developed at the same rate. The results of this underinvestment in software security may be disastrous.

Enterprise companies with a DevOps system must be thinking of moving forward to DevOps approach in terms of bringing stability into the life cycle of app development. This includes teaching and preparing people of all talents and through all technological disciplines to a higher degree of safety expertise. From checking possible vulnerability exploits to developing business-driven software, the DevOps architecture that uses DevOps technologies means that security is integrated into the operations, services, and production instead of being implemented as an unfortunate necessity [2]. Whilst insisting that security is incorporated at any point of the product delivery lifecycle, one will require continuous integration as compliance costs are minimized and applications are released more easily without any harm. Taking security as an equivalent concern between development and operations minimizes the overall vulnerability of any company interested in the development of applications in the public cloud. When DevSecOps and DevOps are integrated, both developers and administrators have protection at the front of their minds when designing and executing cloud-based services. Security has become a critical feature in the app creation process, instead of being retrofitted later in the cycle. DevOps blends development and processes and helps companies to continually build and deliver cloud services and solutions, integrating customer reviews and new needs as they emerge [3]. Security must be integrated into this strategy from the first step of development: checking that the program works on a stable network, that the code is free from bugs, and that operating threats are easily detected. This paper will discuss the main facets of DevOps in ensuring the security of cloud solutions. The focus is on building and understanding how DevOps is significant, how to incorporate them in the cloud solutions, and illustrates how some companies like IBM applies these principles while designing their cloud offerings.

II. RESEARCH PROBLEM

The main problem that this paper aims at addressing is how DevOps can be integrated into a cloud to address the security issues that may arise. The security matters involve any attacks or vulnerabilities that can occur on a system and therefore DevOps comes in as a reinforcement. The main focus is to understand how the vulnerabilities can be eradicated in software which is important in cloud installations. It is important to address this problem because attacks are common in many companies and to avoid losses, they will need DevOps to improve their overall software security.

III. LITERATURE REVIEW

A. Facets of a secure DevOps

When developing stable cloud services, the key elements that must be incorporated into the DevOps life cycle are explained below:

- Secure engineering to make sure that technologies and facilities are designed and installed with strict protection and privacy controls and work following agreed international, global, regulatory, industrial, and local safety requirements [3].
- Secure deployment and operations will assess the cloud platforms, runtimes, and programs to make sure that they are installed appropriately, constantly monitored for installation and configuration and usability, inspected for security

bugs, and modified with software updates and security fixes.

- Separation of duties means that consumers only have the access necessary to do their work in compliance with the rule of least privilege.
- Availability and business continuity maintenance to maintain the highest standards of availability of the infrastructure, runtime functionalities, and management components [4].
- Security assessment and learning to verify that the security features and assets in the code and programs available are protected as risks emerge and security problems occur.

I. Safe Engineering

Cloud systems, cloud resources, and cloud services need to be designed to counter the risks identified in the operating environment [4]. The key strategies for secure engineering are explained below:

1. Security and design specifications

To develop safe applications, developers need to start with well-defined security specifications. Secure software is defined as these criteria are added to the specification. Designing guides security in coding, integration, deployment, and operations [5]. Security specifications and architecture is a development-centric practice that provides a framework for the security of the program, device, or service being designed. Secure applications may provide or incorporate features that are a key component of end-user experience, particularly secure login and authorization and entitlement verification. Secure applications can also provide or incorporate features that are unknown to the end-user, like data security in transit or at rest, monitoring and response to threats and assaults, and more. Protection specifications can embody both end-user security functions and device security functions [5]. These standards can be implemented by the design of applications and the design of security solutions to protect normal functions. Security specifications should also be articulated in ways that consumers of the applications can understand. Developers need to match the security specifications of the program with the safety standards of the organization and with the changing user requirements of the applications. Based on the jurisdiction, industry, and consumers the program represents, any of the various international, state, legislative, industry, and regional security requirements may apply. These specifications define security features and deployment procedures in the application or on the network and networks on which the software runs [6].

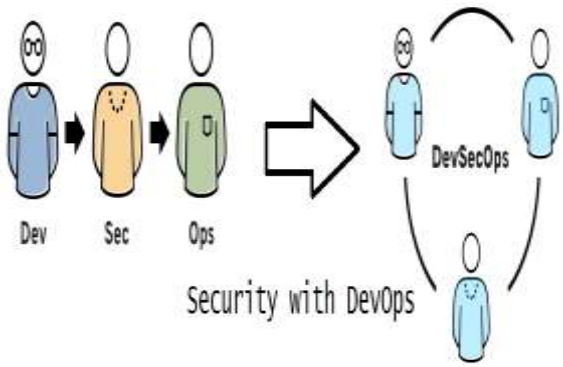

Fig i: Security with DevOps

2. Threat Modelling

Software packages, networks, and facilities operating on or near the Internet are vulnerable to risks and attacks that lead to security breaches, including corrupted systems and the disappearance or leakage of confidential information. Cybercriminals and malicious code can test software, systems, and services to find potential vulnerabilities in a program and its integration. These breaches can manipulate bugs and flaws to crack targeted applications, compromise target processes, or steal confidential data that could be contained in the service. Threat Modeling provides the development team with insight into behaviors, actions, or situations that could cause security breaches. With this experience, the development team will prepare for a safe architecture, scripting, setup, integration, and security checking to avoid allowing for such abuses [1].

3. Secure coding and integration

Secure coding is a development process that helps to reduce the risk of security-related architecture flaws, coding vulnerabilities, and integration failures arising in applications, code defects, and systems. Developers work on safe coding by adopting the danger model instructions to prevent unsafe code, device setup, and deployment errors. Secure coding focuses on maintaining correct syntax, development, integration, and setup to eliminate bugs and weaknesses relevant to these and other aspects of software development.

4. Security testing

Security testing affirms the accuracy of the design, coding, and deployment of applications, systems, and services. Security monitoring operations may take place at each of the varying stages in the software and resources cycles of DevOps. Developers will need to select a method or software and techniques that can authenticate the efficient execution of secure scripting, setup, and integration tasks.

5. Vulnerabilities and incident management

Vulnerability and incident management are a method shared by production and operations. Vulnerability protection relates to the detection and management of bugs in applications and services installed. Operational infrastructure must be tested and constantly monitored to ensure that the quality of the application, system, or service remains strong. The development team must review vulnerability feeds for suppliers and other public outlets to learn about recently found bugs in modules that are important to their applications, programs, and services [7]. When a vulnerability is found, the implementation team must review the warning promptly and overcome, distribute and deploy security deficiencies and security issues. User notice of vulnerabilities can be requested by an organization's regulation, subscription agreement, or legal duty.

vi. *Validation and enhancement of operational controls*

Validation and enhancement of operational controls is an activity shared by production and operations. Security risks and technological issues continue to develop. It is important to provide a continual phase of change throughout operations and production. Strong security requires a mix of good architecture, better procedures, good vulnerability management techniques, rigorous security monitoring practices, and vulnerability assessment intelligence [7]. Viable security includes an overview of the efficiency of security in applications, processes, and facilities, as well as the background check of security issues and operational requirements. The findings will support the next iterations in secure development and help make sure that previous security shortcomings are not reassessed, and new challenges are easily resolved.

II. *Secure deployment and operation*

Secure deployment guarantees that software delivery systems, pipelines, and performance metrics are secured and free from security breaches. Secure DevOps can also guarantee that the code, modules, and services are safely deployed with proper oversight. A new or modified delivery is ready to launch in a secure environment if it has been tested to make sure that the delivery meets the specific vulnerabilities in the security framework [8]. Delivery can involve new or modified features, patches to fix current malfunctions, or patches to correct security issues. Depending on the process of delivery, changes to manufacturing processes and facilities can be routine, expedited, or emergency. It can also include all in-house tech functionalities and also supply chain aspects and services.

a. Vulnerability and patch detection for cloud platforms

Selecting a cloud infrastructure that has automatic security vulnerabilities and patch management streamlines the team's workflow and secures the public cloud. IBM for instance manages and installs upgrades and fixes to IBM Cloud Platform, Runtime, and Utilities. IBM Cloud solutions use predefined, routine maintenance windows, that often enable the services will become unavailable [9]. On the IBM Cloud status list, IBM communicates broadcasts of the updates scheduled for every maintenance window. Besides, IBM is working with the user to plan security changes for the IBM Cloud service. IBM uses IBM Endpoint Manager to simplify IBM Cloud patch control. This eliminates the trial and error like whether to execute patch control procedures. IBM offers operational control of IBM Cloud physical resources and facilities (networks and servers hosted in this setting) while the users are instrumental in the creation, configuration, security, and production processes of the IBM Cloud hosting workflow [9]. The functions and duties for controlling and maintaining the protection of the different systems of the infrastructure. For cloud-based virtualization, IBM Cloud takes a role in managing the existing (physical) server and hypervisor, like initialization and patch management. This involves hypervisor hardening and patching, both planned and emergency. IBM Cloud offers local maintenance copies on private networks, meaning servers still have the new security updates and enhancements on their operating system. This enables users to start and deploy patches and upgrades on-demand with no-cost, unrestricted bandwidth.

b. Vulnerability and patch detection for cloud runtime and utilities

IBM regularly evaluates all its cloud services to identify security risks against security preparedness requirements due to security policies. IBM identifies security sections from each cloud service and ensures that the service complies with security and enforcement requirements. Operating systems or cloud frameworks and middleware have to be patched periodically to defend from recently identified bugs or to provide extra features [10]. IBM Cloud makes the new runtime and midway resources accessible via buildpack updates.

c. *Vulnerability Advisor for containers*

IBM Cloud services involve Vulnerability Advisor, the ability of IBM Containers to detect bugs and enforcement policy issues in container images hosted in IBM Cloud. With a Vulnerability Advisor, developers can create stable apps with little to no effort. The Vulnerability Advisor interacts with the DevOps lifecycle to enable IBM Container Service customers to identify critical bugs in their containerized systems without needing any agents. When they upload an image to the personal IBM Cloud registry, the Vulnerability Advisor immediately compares every one of the components in the image to the guidelines set by the company manager and the archive of documented problems [10]. One may check the effects of the vulnerability manager (pass or fail status) for all photos.

d. Vulnerability and patch detection in cloud systems

Vulnerabilities in a cloud program pose a major danger to consumers. Threat modeling to detect relevant application-related vulnerabilities and attack trends and to ensure a safe architecture helps to minimize these risks. Secure coding manuals and methods to avoid vulnerabilities are available. Security monitoring addresses bugs before the program is implemented and validates that the software is free from established security vulnerabilities. IBM Data Protection on Cloud helps protect the organization's software by identifying hundreds of today's most common security flaws [10]. Even so, it helps to extract bugs from the software before they are put into development and deployed.

III. Separation of duties

Separation of tasks means that consumers only have links to the work they need to do. Developers must ensure that tasks and duties are separated so that only users with the right roles have access to unique sections of the cloud design and implementation network. IBM Cloud meets the separation of duties rules for assigning granular access rights to users and ensuring that clients have only the access that is available to do their work per the concept of least privilege.

IV. *Availability and business continuity management*

Availability and business continuity maintenance guarantee that the infrastructure, application elements, and valued experiences are highly available. IBM Cloud is an on-going innovation network and numerous fail-safe mechanisms to ensure that the orgs, rooms, and applications are still open. Deployment of applications to several geographic regions allows consistent availability that prevents unplanned failure of several hardware or software dimensions or the disruption of an entire facility [11]. Because of this, and in the case of a natural catastrophe at a single geographic area, the IBM Cloud application can be spread in alternative geographic locations. IBM Cloud distinguishes those elements that monitor the state of interaction (stateful) from those that do not (stateless). This separation helps IBM Cloud to switch applications flexibly if necessary, to achieve scalability and agility. IBM Cloud is a dynamically accessible platform. IBM maintains availability, disaster recovery, and business continuity. Usually, this ensures that you have deployed the workflow across at least two pods and preferably across two geographically dispersed data centers. Due to IBM Cloud's vast global reach, two data center approaches to high availability, disaster recovery, and business continuity can be developed in most locations, including those with strict data locality criteria.

V. Security evaluation and learning

Compliance assessment and learning processes ensure the security features and assets in the code and services provided are preserved as risks develop and security problems emerge. Security assessment and learning are taking place at different stages. When a user wants to purchase, deploy, upgrade, run and manage computer systems in the organization, they need to make sure that development, operational processes teams have maximum insight on security issues across all levels of the technology stack. These teams should be able to influence the improvements needed to adjust the protection of

applications, devices, and facilities to emerging challenges and newly found vulnerabilities. IBM Controlled Security Systems and X-Force Command Centers will help the organization and the teams assess security and gain knowledge from security incidents. IBM monitors the security and reliability of its cloud customers and discusses them within our networks, networks, and facilities via the use of IBM X-Force Command Centers and also the Network Operations Centers and personnel. Users always need insight on security problems with the software installed in the IBM Cloud, the data stored in the IBM Cloud, the business continuity questions, and also the administration of security resources for the staff and end-users, like identity and access [11].

B. Cloud security opportunities

i. Serverless computing

With the development of cloud solutions in various industries, it is up to the individual cloud service providers to handle security for the service they offer to cut down the overall number of places the organization's security teams need to manage. Firms can best use the 'Infrastructure as a Service (IaaS) and 'Platform as a Service (PaaS) approaches when they free themselves from handling their hardware and software complexities [12]. The main purpose of serverless computing is to enable users to concentrate on the creation and deployment of code. This significantly reduces the network threat in data centers, virtual servers, databases, and network configuration. For instance, the KPMG Digital Risks Model largely uses serverless components, lowering costs significantly when it comes to patching and managing the server [13].

ii. Infrastructure as code

This is the principle that guides the management and provisioning hardware and software setup via machine-readable parameters, instead of manual and immersive error-prone configuration tools. Infrastructure as a code can be used by both platform and infrastructure modules. Both major cloud vendors are embracing this process. Another benefit is that the meanings (changes to) can be viewed as code [14]. This makes it easier to handle improvements to the infrastructure, in the same manner, using the same tools as handling changes to the standard (application) code, using well-known software methodologies for the design, delivery, and execution of the application infrastructure. Deployments are thus less prone to errors, the system is more homogeneous and protection configurations could be handled as part of the normal, secure development cycle [15].

iii. Security centralization

Cloud architectures allow unified security features, like encryption, identity management, key management, auditability, and security checks [16]. While companies tend to see this as an inherent problem, it offers greater exposure, prospects for automation, and convenience. Building on the economies of scale, any security requirements carried in by another cloud user will increase the overall security of the cloud provider, as they offer a huge opportunity to make the cloud secure. Cloud centralization helps systems such as Azure DevOps, Gitlab, and Atlassian to quickly monitor progress, work on code and incorporate continuous deployment [17]. It dramatically enhances flexibility and encourages production and technical teams to concentrate on the standards of DevOps.

IV. SIGNIFICANCE OF THE RESEARCH TO THE U.S

The integration of DevOps to cloud solutions will be significant to U.S organizations and governments in reinforcing the security of their systems. Many policymakers are now using digital tools to meet changing demands and aspects of smart governance. They still have to hit the full potential. The US Government has been experiencing a similar situation, looking for more in-depth infrastructure upgrades to meet public demands amid the challenges faced. Federal entities are seeing this demand in the light of two crucial factors: security issues emerging from a remote working environment and a break-in point for their current technological networks due to crowded traffic. The US Air Force could gain reliability by agile DevOps activities by releasing at least 10-30 updates every day. Many federal agencies are now searching for scalable solutions and resources to achieve their mission [18]. DevOps CI/CD and DevSecOps ensure improved reliability, smooth implementation, and continuity of operation in a secure environment. DevOps technologies help to ensure consistency of defense, operations, and maintenance in a decentralized workforce setting. Many companies in the U.S are growing their digitization activities, effectively bringing their goods and technologies more efficiently to the consumer. Technology, consistency, and, in particular, protection functions are unable to keep up with the pace. Although traditional businesses have challenges bringing their heterogeneous IT environment to the cloud, less conventional technology-oriented corporations are struggling to embed protection as a mechanism in their life cycle of growth, as they see it hindering their precious time on the market. Rather than applying security as a stage-gate at the end of production and life-cycle activities, it ought to be a continuous process across the value-added stream. In the end, this can help to place the security feature as a business enabler. Using cloud computing and working into a DevOps framework go hand-in-hand [18]. Future cloud technologies utilizing serverless computing or Infrastructure as Code have will have an influence on the security environment of the enterprise in the same way that DevOps organization has blurred boundaries between application creation and application processes.

V. CONCLUSION

The paper looked at how DevOps plays a critical part in securing cloud resources. The key topics that can be drawn from the paper are the need for organizations should align security and budgetary initiatives with a business marketing and customer friendliness. Cloud transformations can help embed security concepts and solutions, particularly if they are applied by the DevOps principles. Shifting to the cloud is also a valuable way to incorporate security protocols into day-to-day operations so that companies get more 'secure by design.' I also addressed typical pitfalls in the deployment of cloud security technologies and presented security standards and activities that can be integrated into (agile) development processes. The main objective of the paper is to make DevOps engineers feel concerned about the security choices they make throughout development as well as provide them with the tools and the requirement to do so. This should allow companies to properly manage security and accessibility while ensuring an ever-increasing desire to provide value more quickly. The readiness to meet these obstacles for the implementation of DevOps would provide a productive direction for federal agencies. Appropriate professional support will help them to overcome key issues

and set out the ideal blueprint for the successful implementation of DevOps for securing cloud solutions.

References

[1] Snyder and B. Curtis, "Using Analytics to Guide Improvement during an Agile–DevOps Transformation", *IEEE Software*, vol. 35, no. 1, pp. 78-83, 2018. Available: 10.1109/ms.2017.4541032.

[2] D. Feng, M. Zhang, Y. Zhang, and Z. Xu, "Study on Cloud Computing Security", *Journal of Software*, vol. 22, no. 1, pp. 71-83, 2011. Available: 10.3724/sp.j.1001.2011.03958.

[3] R. Nord, "System and software architecture track third IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'97)", *ACM SIGSOFT Software Engineering Notes*, vol. 22, no. 2, p. 5, 1997. Available: 10.1145/251880.251886.

[4] M. Airaj, "Enable cloud DevOps approach for industry and higher education", *Concurrency and Computation: Practice and Experience*, vol. 29, no. 5, p. e3937, 2016. Available: 10.1002/cpe.3937.

[5] J. Morales, H. Yasar, and A. Volkmann, "Weaving Security into DevOps Practices in Highly Regulated Environments", *International Journal of Systems and Software Security and Protection*, vol. 9, no. 1, pp. 18-46, 2018. Available: 10.4018/ijsssp.2018010102.

[6] L. Bass, "The Software Architect and DevOps", *IEEE Software*, vol. 35, no. 1, pp. 8-10, 2018. Available: 10.1109/ms.2017.4541051.

[7] J. Verona, M. Duffy, and P. Swartout, Learning DevOps: continuously deliver better software: learn to use some of the most exciting and powerful tools to deliver world-class quality software with continuous delivery and DevOps: a course in three modules, 1st ed. Birmingham, England: Packt Publishing, 2016, pp. 800-815.

[8] V. Kumar, R. Kumar, and A. Sharma, "Applying Neuro-fuzzy Approach to build the Reusability Assessment Framework across Software Component Releases - An Empirical Evaluation", *International Journal of Computer Applications*, vol. 70, no. 15, pp. 41-47, 2013. Available: 10.5120/12041-8047.

[9] D. Ståhl, K. Hallén, and J. Bosch, "Achieving traceability in large scale continuous integration and delivery deployment, usage, and validation of the eiffel framework", *Empirical Software Engineering*, vol. 22, no. 3, pp. 967-995, 2016. Available: 10.1007/s10664-016-9457-1.

[10] M. Lovelace et al., *IBM Tivoli Storage Manager as a Data Protection Solution*, 1st ed. Poughkeepsie, NY: IBM Corp., International Technical Support Organization, 2014.

[11] L. Coyne et al., *IBM Private, Public, and Hybrid Cloud Storage Solutions*, 1st ed. New York: IBM Redbooks, 2018.

[12] G. Kim, K. Behr, and G. Spafford, *The Phoenix Project, 5th Anniversary Edition*, 1st ed. Portland, OR: IT Revolution Press, 2018.

[13] J. Vehent, *Securing DevOps: Security in the Cloud*. Shelter Island: Manning Publications, 2018.

[14] K. Jamsa, *Cloud computing*. Burlington: Jones & Bartlett Learning, 2013.

[15] S. Johann, "Kief Morris on Infrastructure as Code", *IEEE Software*, vol. 34, no. 1, pp. 117-120, 2017. Available: 10.1109/ms.2017.13.

[16] V. Gupta, P. Kapur and D. Kumar, "Modeling and measuring attributes influencing DevOps implementation in an enterprise using structural equation modeling", *Information and Software Technology*, vol. 92, pp. 75-91, 2017. Available: 10.1016/j.infsof.2017.07.010.

[17] N. Wilde et al., "Security for DevOps Deployment Processes: Defenses, Risks, Research Directions", *International Journal of Software Engineering & Applications*, vol. 7, no. 6, pp. 01-16, 2016. Available: 10.5121/ijsea.2016.7601.

[18] M. Soni, *Implementing DevOps with Microsoft Azure*, 1st ed. Birmingham, UK: Packt Publishing, 2017, pp. 262-318.