Concepts and Practices of DevSecOps

Crack the DevSecOps interviews

Ashwini Kumar Rath

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55519-320

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

www.bpbonline.com

Dedicated to

My mother, the first architect of my words

About the Author

Ashwini Kumar Rath is an accomplished entrepreneur, prolific writer, and seasoned DevSecOps consultant with extensive computer programming experience. As the Director and CEO of Batoi, he has shaped its strategic vision and product development while extending his leadership to several tech companies he co-founded in India and internationally. Rath's educational background in theoretical physics and software management has fueled his successful transition into technology, culminating in the establishing of multiple tech startups. His academic interests encompass cloud computing, AI, and mathematical sciences, driving his contributions to numerous scholarly articles and business features in leading publications. As a frequent speaker at international forums, his expertise and insights are highly sought after. Committed to leveraging knowledge for socio-economic development, Rath also serves on various educational and business leadership boards.

About the Reviewers

- **Rakesh** is a seasoned technologist who has worked in the fast-paced technology field for 23 years. He gained expertise at Hewlett Packard, where he exhibited his passion for technology in positions like Technical Architect and Senior Software Engineer. Rakesh has been the Chief Technology Officer at In Time Tec for the past fifteen years, fulfilling his dream of helping clients worldwide overcome technology challenges. With a focus on IoT/Embedded Systems and Highly Scalable Cloud Solutions, his leadership experience ranges from creating low-level embedded software to creating high-performance cloud-based applications.

  Rakesh strongly believes in the power of effective communication, analytical thinking, and team-building. Outside the boardroom, he remains current on the most recent technological advancements and supports open-source initiatives, showcasing his commitment to creativity and lifelong learning. Rakesh is always eager to collaborate on worthwhile initiatives with like-minded enthusiasts, highlighting the positive impact of technology on our daily lives. His diverse technological background reflects a commitment to expanding the possibilities of technology.

- **Ankit** is a senior cloud data architect with Google and has over a decade of progressive work experience in Cloud, Data, AI, and ethical machine learning practices. He works with customers to develop scalable, reliable, and performant data and machine learning platforms and has worked across companies like Amazon, CVS, Deloitte, and Infosys. He is a technical reviewer for various books focused on data governance, ethical AI, AI governance, Data and AI platforms, Python for AI, and other material related to the promotion of AI ethically and responsibly in society. He earned his master's from the esteemed Kelley School of Business and serves as the advisory board member for the Institute of Business Analytics, Indiana University Bloomington.

Acknowledgement

My most profound appreciation goes out to my beloved family and steadfast friends, whose constant support and motivation served as my guiding star throughout the creation of this book. In particular, my wife, Mita, deserves a special mention for her unwavering encouragement and patience during my perpetual travels and work, gently nudging me to complete each chapter.

I owe a significant debt of gratitude to BPB Publications. Their expertise and professional guidance were pivotal in transforming the raw manuscript into this finished work. It has been an enriching journey, enriched further by the diligent reviewers, technical experts, and editors whose input significantly enhanced the content and structure of this book.

My time in the tech industry, filled with the teachings and insights from my esteemed colleagues and peers from industry and academics, has been instrumental in my growth and understanding. Their generous contributions have immeasurably shaped the narratives and perspectives within these pages.

Last but not least, my sincere thanks to you, the readers, whose interest and support fuel the purpose of this work. Your enthusiasm is the heart of this endeavor, and your encouragement has been priceless. Thank you for making this book a reality.

Preface

Welcome to **Concepts and Practices of DevSecOps**!

As we find ourselves in the midst of a digital revolution, one thing has become evident – the importance of integrating security into our development and operational practices. This has given rise to the practice of DevSecOps, a discipline that builds upon the principles of DevOps with a sharpened focus on security.

This book aims to demystify the DevSecOps field, from its foundational concepts to the advanced practices and technologies that define it today. This comprehensive guide has been designed to equip you with the knowledge you need to excel in DevSecOps roles and to confidently face interviews that test your understanding and application of these principles.

The chapters in this book walk you through different aspects of DevSecOps, including Application Security, Infrastructure as Code, Containers and Security, Automation and Integration, and the Frameworks and Best Practices underpinning the discipline. As we journey into the world of DevSecOps together, we will explore how it plays a pivotal role in the current era of Digital Transformation.

Whether you are a DevOps engineer, project manager, product manager, software developer, or any professional seeking to fortify your understanding of DevSecOps, this book is a crucial resource. With a working knowledge of DevOps, you will find the content accessible and enlightening, helping you to contribute to or lead a DevSecOps team effectively.

Each chapter is structured to answer the pressing questions surrounding each topic, supplemented with practical use cases that bring the theoretical concepts to life. I have also included resources for further reading at the end of each section, allowing you to delve deeper into the subjects that interest you the most.

The world of DevSecOps is as fascinating as it is intricate. This book prepares you for your career progress in this field and ignites a passion for security's vital role in our ever-evolving digital landscape.

May this book serve as your compass, guiding you through the complex terrain of DevSecOps and helping you become an influential team member as you work together to build secure, efficient, and innovative solutions.

Chapter 1: Security in DevOps – It delves into the interweaving of security within DevOps culture, providing insights into the transformation of security measures within software systems management. It establishes a comprehensive framework for understanding DevSecOps, laying a foundation for the forthcoming chapters.

Chapter 2: Application Security – It offers an in-depth exploration of application security, discussing the intricate details of various application architectures and their inherent security aspects. Readers will gain a firm grasp of the tools and technologies that fortify applications, accompanied by a practical case study on constructing and sustaining an enterprise application.

Chapter 3: Infrastructure as Code – It acquaints the reader with different cloud platforms and essential infrastructure management tools instrumental in executing successful DevSecOps projects. Covering several leading vendors, it offers insights into tool selection for specific scenarios while focusing on scalability and change management for contemporary IT systems.

Chapter 4: Containers and Security – It offers a thorough understanding of security measures surrounding popular container technologies, emphasizing an understanding of various vulnerabilities. It examines solutions and processes for vulnerability management and discusses the optimal tools and techniques available.

Chapter 5: Automation and Integration – It introduces platforms and tools for comprehensive security management, particularly crucial in managing enterprise systems and large-scale software with substantial attack surfaces. It discusses a range of cloud security solutions, including CWPP, CSPM, CASB, and CNAPP, supplemented with a practical use case to demonstrate the substantial benefits of integration.

Chapter 6: Frameworks and Best Practices – It provides a detailed view of leading security frameworks and their management in the DevSecOps process, including audit, compliance, reporting, visualization, and threat modeling.

Chapter 7: Digital Transformation and DevSecOps – It discusses a lean approach to digital transformation projects with a spotlight on DevSecOps management. It touches upon cultural aspects, skills, roles, and responsibilities, managing technical liabilities, and establishing secure development practices.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/4c8758

The code bundle for the book is also hosted on GitHub at **https://github.com/bpbpublications/Concepts-and-Practices-of-DevSecOps**. In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Security in DevOps

Introduction

While DevOps promises a great deal to different stakeholders, security has long been an exclusive focus for any software development team. Traditionally, companies outsource the security audit to an external agency or keep the stuff separate for a group of security experts. Moreover, all security management functions start after a software version is deployed into production. Such a scenario experiences a few to and fro exchanges that include tool-based scanning and manual testing by the security team on the one hand and the resulting effort of troubleshooting by the software or IT team on the other. Consequently, it significantly increases the time of a DevOps cycle and nullifies the fundamental purpose of DevOps, which commits to faster software delivery.

Let us dive into the first chapter.

Structure

In this chapter, we will discuss the following topics:

- Relooking at security operations
- Shifting security left
- Adopting DevSecOps: Key changes

- Security controls
- Documentation and security
- Threat modelling and security policies
- Infrastructure provisioning and security
- Code commit, release and security
- A use case: IoT application

Objectives

This chapter offers an insight into the security aspects of software systems and their management from the perspective of DevOps culture. We discuss the significant technological advancements, tools, and practices that have changed how we treat and incorporate security into the scheme of things. While the chapter serves as a solid introduction to DevSecOps, it also builds a broader framework for the later chapters.

Relooking at security operations

With the rapid adoption of cloud computing and remote working, the IT infrastructure is moving out of the cozy confines of office networks. Security has been more important than ever before. In this section, we shall relook at the **security operations** (**SecOps**) and how it fits into DevOps. Before we proceed further, let us review what a DevOps cycle looks like.

A DevOps cycle

It is famously illustrated with an infinity loop (*Figure 1.1*) broadly running over six stages:

- **Design:** You design new software, an improvement to existing software, or even a modification to the software to align with requirements.
- **Code:** The phase includes programming activities of coding, compiling (when needed) and testing the software units.
- **Integrate:** While different software developers work on different units, integration does the process of merging the changes into a codebase that will function as the designated software system.
- **Deploy:** After integration, the software system needs to be deployed at one or multiple server locations as per the deployment architecture.
- **Operate:** Users start using the system, they can be a selected user group (for doing a pilot) or the actual end users for whom the software is designed.
- **Monitor:** While the software is in use, its accuracy, usability, and performance must be monitored, and adequate feedback is gathered for the next cycle in the loop.

The ‘monitor’ stage of a cycle feeds the ‘design’ stage of the next loop cycle, thus creating an infinitely evolving software system's lifecycle. Every business owner or manager loves it, but they would expect the software to have minimal defects yet great security controls. They would also expect that each cycle should be as fast as possible to match the business goals and should lower the effective cost of software development and IT operation management.

It should be noted that different authors or practitioners describe the loop in slightly different ways. However, they fall broadly into the ones that we have described above.

The function of the DevOps infinite Loop is illustrated in *Figure 1.1*:

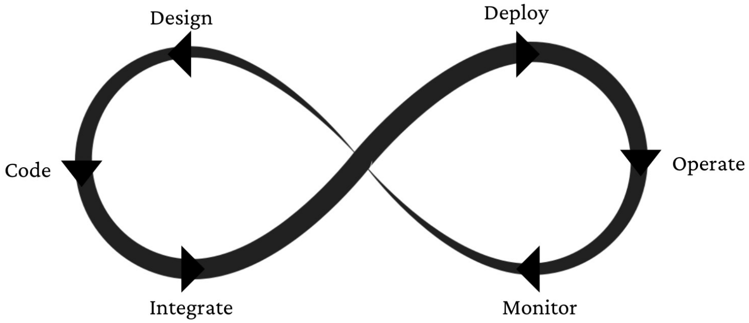

Figure 1.1*: DevOps infinite loop*

Conventional SecOps with DevOps

Let us cite an example to understand the traditional method of SecOps or security operations. Once, a software agency, which had recently adopted DevOps, was tasked with developing an application for its customer. The customer had their own chief security officer and chief risk officer. During one of the project review meetings, these two officers wanted to understand the software development cycle to eliminate process-related risks and have a transparent process for software development and management. The agency had automated the infrastructure provisioning on the Cloud and CI/CD pipeline. They could complete one DevOps cycle in less than a day. However, after each software release (software moving to production), they will refer to the security vendor, who will do a round of penetration testing and provide the list of findings (security issues observed) for the software development team to review and respond. The software team would do the following:

- If a finding is a false positive, they will ignore it.
- If a finding is of a high-risk category, they will fix it.
- If a finding refers to a low-risk category, they may fix or ignore it.

After the above tasks, the software team will respond to the security team. The security team will do another round of penetration testing. Here, the security team may add them