aws partner network

Advanced
Consulting
Partner

E-Book

DevSecOps Automation

A Game Changer for Product Security

www.ittstar.com

Table of Contents

Introduction: About this book 03

Chapter 1: What DevSecOps is and why organizations should care? 04

Chapter 2: Automating DevSecOps and Compliance 05

Chapter 3: How to defend against threats through Automated DevSecOps 07

Chapter 4: The DevSecOps Framework 08

Chapter 5: To Sum Up 10

Introduction:
About this book

Since everything is becoming fast-paced these days. Companies want software products to be developed quickly so they can be used for business purposes. With this comes the challenge of testing the software for security, reliability, and performance.

This eBook is intended for business owners and managers who want to implement the DevSecOps framework for their teams and don't know where to start.

What You'll Learn

- ✓ Know about DevSecOps
- ✓ Develop an understanding of its framework.
- ✓ How your business will benefit from its implementation
- ✓ Framework required for implementing DevSecOps and Compliance

Chapter 1:
What DevSecOps is and why organizations should care?

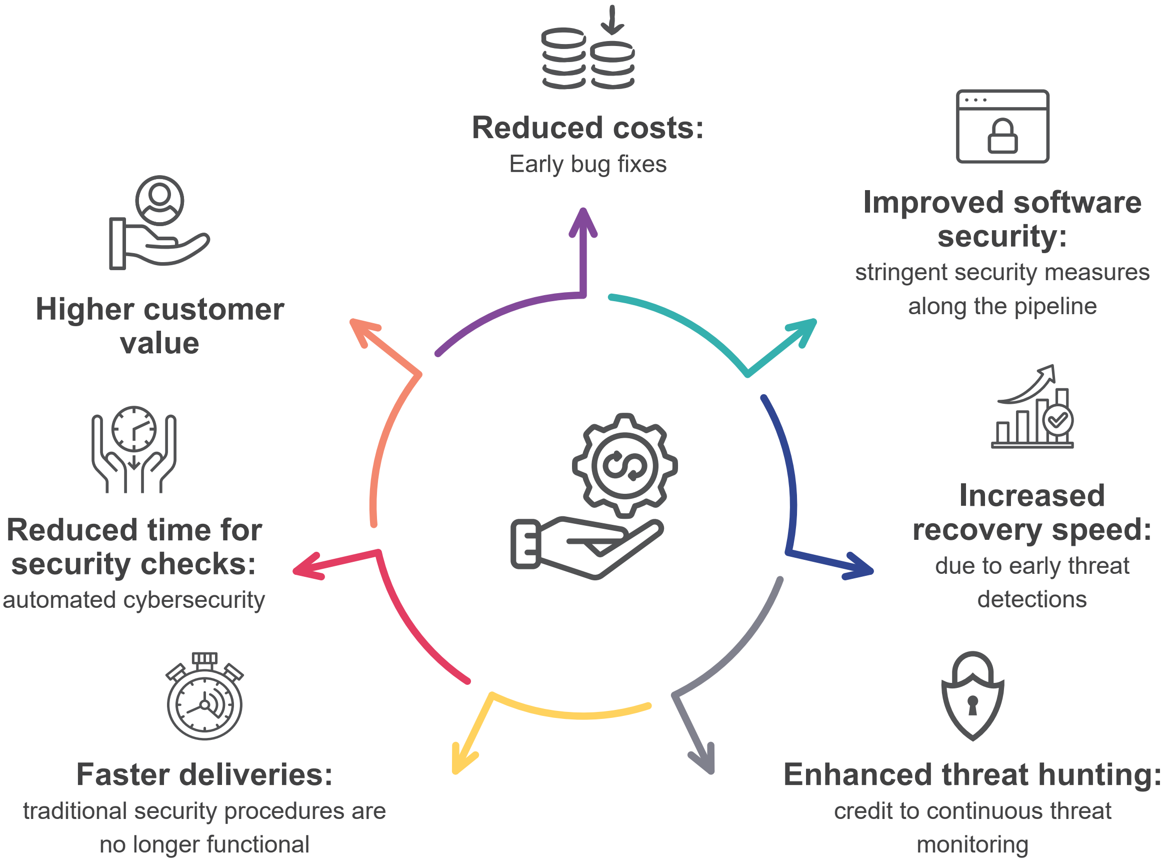
DevSecOps is an abbreviation for development, security, and operations. It is becoming an industry standard for implementing compliance and safety for newly developed software applications.

Security is an essential component as the software applications often store sensitive data of the employees, clients, or customers of the businesses. With the increasing demand for newly developed products competing for consumer attention and loyalty, security breaches can hinder the performance and growth of any organization.

Adopting and implementing the DevSecOps framework within the organization requires a shift in the working pattern of the teams. It brings development, security, and operations teams together to work in collaboration. It also brings about a cultural shift within the teams.

DevSecOps seamlessly integrates with the existing processes and tools. It also addresses security issues as they emerge. This makes rectification of the code easier, faster, and less expensive because constant changes are implemented to the software code before production.

The overall SDLC (Software Development Life Cycle) process also becomes smooth and the organizations can deliver software that are tested for security and performance.



Reduced costs: Early bug fixes

Improved software security: stringent security measures along the pipeline

Increased recovery speed: due to early threat detections

Enhanced threat hunting: credit to continuous threat monitoring

Faster deliveries: traditional security procedures are no longer functional

Reduced time for security checks: automated cybersecurity

Higher customer value

Chapter 2: Automating DevSecOps and Compliance

The rise in malicious activities and cybersecurity attacks has forced companies to shift their efforts from a preventive to a diagnostic approach. It is essential for the teams to integrate security practices into the software development process to ensure safety, efficiency, and fast software delivery.

There are certain advantages of implementing the DevSecOps framework for the software development process. They are as follows:

- **Faster and cost-effective software delivery**

  When software is developed in a non-DevSecOps environment, rectifying issues related to security can be costly and time-consuming. Whereas, implementing the DevSecOps process takes care of all the aspects. Several automation tools are used to test the software application for security issues that may arise in the future.

  Testing before deployment and delivery minimizes the chances of re-work, making the process rapid and cost-effective.

- **Efficient**

  DevSecOps ensure that the software is tested for cybersecurity issues from the very beginning as security is kept at the center of the software development process. Fixing security issues before deployment costs less, and makes the process more efficient at the early stage.

  Moreover, the collaborative efforts of development, security, and operation teams improve the organizations' response toward compliance and incident management.

- **Reliable, consistent, and transparent operations**

  Implementing DevSecOps within the teams minimizes the communication silos within the teams. This helps each team take equal responsibility for the project, resulting in forming a system that is reliable, consistent, and transparent.

Accurate output

The automation tools used for application security testing combine static, dynamic, and interactive security testing to provide highly accurate results for your company's security vulnerabilities and compliance.

The automation tools provide results after testing the software for several parameters. The continuous integration and continuous deployment (CI/ CD) process help developers quickly implement changes to the code. Early identification of the flaws makes implementation or integration of new features easier.

This ensures that correct and tested code reaches the deployment and you get a product that is tested for all parameters including security, efficiency, and reliability.

CI/CD is an essential part of DevSecOps as it helps your organization automate the entire process from code development to product deployment.

Chapter 3:
How to defend against threats through Automated DevSecOps

Most of the processes consider security checks after the deployment. The number of cyber threats and data security issues has led organizations to rethink about building software that is secure.

The organizations that build their software solutions around DevSecOps are able to mitigate the risks at a much higher rate.

Here are some best practices that organizations can adopt:

- Organizations need to create an archive of the earlier threats and vulnerabilities that appeared in the past. This will help developers update the libraries so that new software developed is capable of handling them.
- A DevSecOps security strategy should automate traditional practices of security engineers, operations teams, and development teams so that developers can remediate the vulnerabilities at a faster pace without missing out on any.
- A single automated process cannot find all the bugs. Therefore several testing methods and automation techniques will help in the detection.
- Integration of DevSecOps in the existing framework will increase the security with which the software is developed and delivered.

Chapter 4:
The DevSecOps Framework

DevSecOps is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes.

While including security in the initial stages can make the development process slow as this cultural shift needs to be adopted by the entire team and accepting and implementing needs a complete understanding of the framework. Before completely integrating, you can also start by making low-friction changes to the code. Focus on changes that will have a positive effect on the development process

Planning

Typically companies work on agile methodology. Scrum is an agile process that involves planning before the start of each sprint. Introducing security during this phase should focus on threat modeling, IDE security plug-in for code checks in the development environment, and maintaining security coding standards during peer reviews.

Threat Modeling

This is the most essential part of the security practice. It is easy to implement and can be detailed and more technical according to the needs of the project. Threat modelling delivers immediate results and helps establish a security mindset in developers to improve security in all their future projects

Safeguarding the Repository for Safe Collaboration

Generally, developers submit code to the central repository. This facilitates version control for developers and also allows for easy collaboration. Since many users or collaborators share the same platform, this can lead to the risk of vulnerabilities. The development teams need to implement repository scanning tools to overcome this security threat. These tools will perform checks for any possible vulnerability and flag any items for remediation. This will protect the repository against any human error and risks.

Securing CI/CD Pipeline

Modern DevSecOps follow the Continuous Integration/ Continuous Development (CI/CD) pipeline as a part of the development cycle. Since these pipelines are an integral part of the development process, the development team should make sure that no malicious code runs through them. This can give attackers a window to steal the data. Implementing proper security controls will ensure the proper security of the CI/CD pipeline.

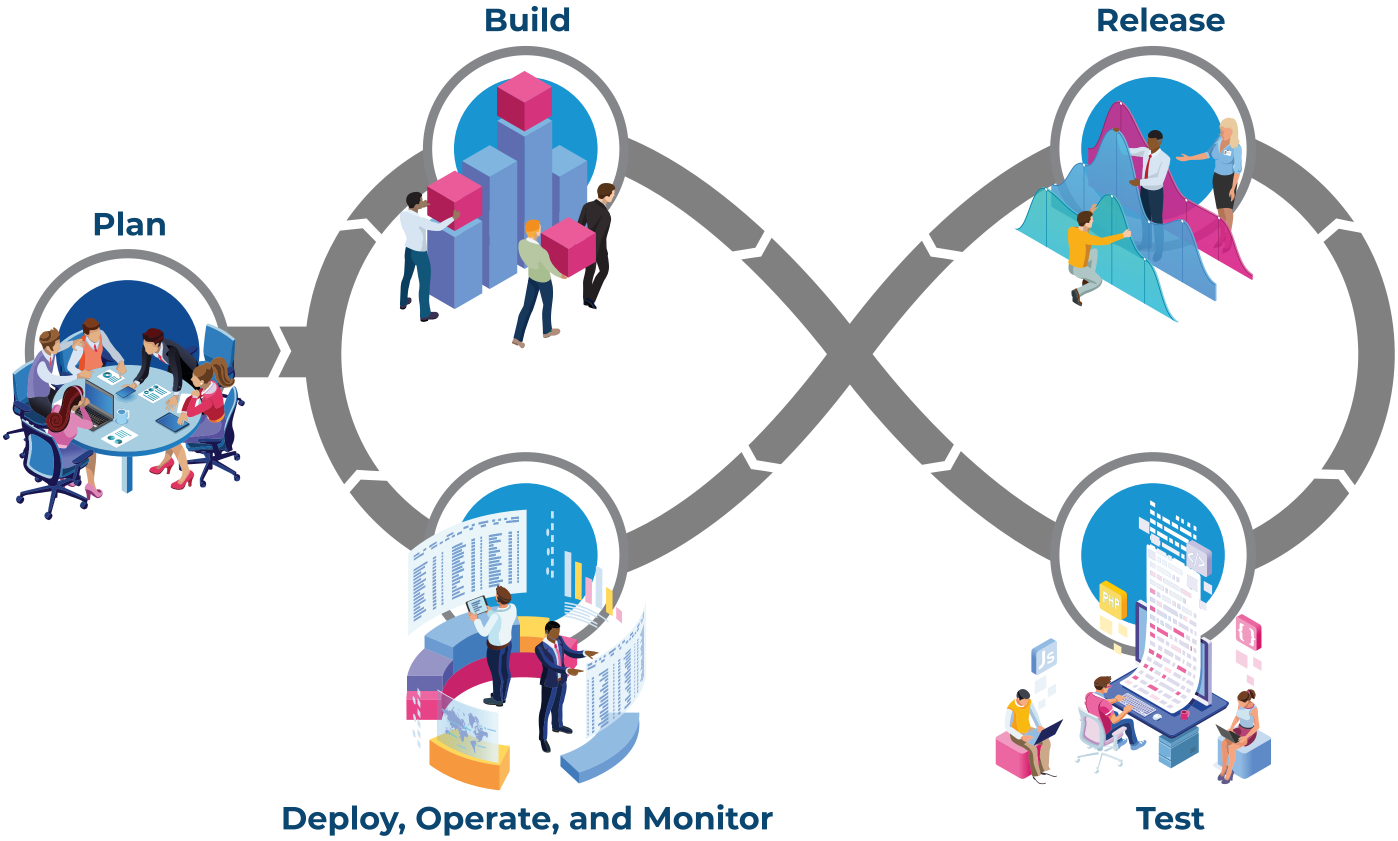
Dynamic Security Testing

To ensure safety around the software application, organizations need to automate and standardize the process of building and deploying the code. Some of the popular security testing approaches include penetration testing, vulnerability scanning, security scanning, risk assessment, security audit and review, ethical hacking, posture assessment, and authentication.

These approaches let the team look into the mindset of the hacker and make them take necessary action keeping in view the security aspect.

Building a Secure Deployment Environment

While creating secure systems and pipelines, also make sure the environments used for deploying are also secure. Such environments also open the scope for any experimentation. With cloud infrastructure, containerization is a popular approach, that teams take in application architecture decisions. Some container repositories scan for vulnerabilities. There are several open-source and commercial security tools that integrate with the CD process. Security tools help teams adopt infrastructure DevSecOps as code, especially in learning how to use containers.



To Sum Up

The methodologies discussed in this eBook are presented with a view to present a holistic security model for DevSecOps practices for the teams engaged with the software application production. Using this framework, organizations can implement DevSecOps within their teams seamlessly. This will help organizations build a secure environment and also promote innovation and experimentation for upcoming projects with peace of mind.

These processes will help your organization to adopt the DevSecOps process seamlessly and help teams identify, evaluate, and resolve potential risks.

Implementing DevSecOps also eliminates communication silos and helps teams to work in a structured manner where the code runs through several automated tests for safety, reliability, and speed.

The methodologies used in DevSecOps also allow for continuous changes during the development phase. The security and operations teams share their feedback and return to the development team for the remediation task.

This process provides developers with an effective way to solve problems within standard workflows such as development, testing, deployment, and delivery.

Get In Touch

Head Office

ITTStar Consulting, LLC

11175 Cicero Drive, Suite 100, Alpharetta, GA-30022, USA
Phone Number: 770-510-3456
inquiries@ittstar.com

Global Delivery Center

ITTStar Global Services Private Limited

Site #32, 4th "A" Cross Road, Bhuvaneshwari Nagar,
Dasarahalli Main Road, Hebbal Post, Bangalore - 560024
Phone Number: 080-4302 4523
inquiries@ittstar.com

We are always live on

www.ittstar.com