Things to know about DevSecOps

“The purpose and intent of DevSecOps is to build on the mindset that “everyone is responsible for security” with the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required”

– devsecops.org –

Watch this 4 minutes video

https://www.youtube.com/watch?v=d-WRcamtyVo&t=47s

DevSecOps stands for development, security, and operations. It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.

DevSecOps vs. DevOps

DevOps isn’t just about development and operations teams. If you want to take full advantage of the agility and responsiveness of a DevOps approach, **IT security** must also play an integrated role in the full life cycle of your apps.

Why? In the past, the role of security was isolated to a specific team in the final stage of development. That wasn’t as problematic when development cycles lasted months or even years, but those days are over. Effective DevOps ensures rapid and frequent development cycles (sometimes weeks or days), but outdated security practices can undo even the most efficient DevOps initiatives.

The goal is to meet the customer’s need quickly and DevOps delivers. How does the DevOps methodology achieve this?

- By building a high-trust, high-performance culture
- By viewing IT capabilities as strategic assets instead of overhead
- By creating cross-functional teams
- By creating a process that is highly automated
- By enabling continuous delivery of software

Role of BA in DevOps World

In the DevOps world, the Business Analysts are a part of the cross-functional team and have immediate and ongoing input regarding the needs and progress as development, testing, and operations all work together for the common goal of providing value quickly to the customer.

The DevSecOps Manifesto

- Leaning in over Always Saying, “No.”
- Data & Security Science over Fear, Uncertainty, and Doubt.
- Open Contribution & Collaboration over Security-Only Requirements.
- Relying on empowered development teams more than security specialists.
- Consumable Security Services with APIs over Mandated Security Controls & Paperwork.
- Business Driven Security Scores over Rubber Stamp Security.
- 24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident.
- Shared Threat Intelligence over Keeping Info to ourselves.
- Compliance Operations over Clipboards & Checklists.

Read this small CASE Study

https://www.slksoftware.com/wp-content/uploads/2022/08/Accelerating-Digital-Transformation-with-DevSecOps.pdf

DevSecOps Myths

It’s common for buzzwords to have anti-patterns, and DevSecOps is no exception. Let’s discuss some common misconceptions.

Myth 1: We Need “Super Developers” for DevSecOps!

Not really. If you think you need to recruit certain people with magical coding skills for DevSecOps, then you’re mistaken. Unless you can’t train your existing people effectively or your developers aren’t interested in making the DevSecOps shift, you

don’t have to put on your hiring cap just yet. DevSecOps aims to break down silos. Your development team, which is comprised of people with different skill sets, will receive training on DevSecOps processes and methodologies that should hold well throughout your delivery pipeline. So you’ll be bringing together existing teams—not hiring a new separate team.

Myth 2: DevSecOps Can Replace Agile

It can’t. DevSecOps complements agile, but it’s not a substitute for it. They must co-exist in order for organisations to maximize their business benefits. Agile fosters collaboration and constant feedback. But unlike DevSecOps, it doesn’t cover software delivery through testing, QA, and production. DevSecOps completes the picture by providing methodologies and tools to facilitate agile adjustments.

Myth 3: You Can Buy DevSecOps

Not exactly. You can only buy tools to use for the process, such as release management and CI/CD tools. You can’t buy the entire DevSecOps process because it’s a philosophy or a methodology. What really makes a difference to your business—the collaboration between teams and the focus on team responsibility and ownership—are things you can’t go out and buy.