DevOps Institute

DevSecOps Practitioner℠

BLUEPRINT

DevSecOps Practitioner focuses on advanced practices, methods, techniques and tools to explore DevSecOps in your organization by looking at how people, process and technology can be combined to improve reliability and outcomes.

Advanced Basics

Understanding how to succeed, as highlighted by Malcolm Gladwell, depends on knowing not just the basics but understanding why and how those concepts matter. Exploring the fundamentals with Agile and Lean processes, learning about platforms, and knowing who to hire can make all the difference. Equally important to building teams, one must learn how to communicate among teams.

Applied Metrics

Everyone starts with basic metrics that can sometimes reach goals, but other times one needs a more concrete understanding of how to build appropriate metrics to succeed. Metrics can apply not just to production but to how one manages people and guides their process to improve success. Selecting the appropriate tools can help accelerate metrics collection and application.

Architecting & Planning for DevSecOps

Building a DevSecOps plan depends not just on espousing the right words, but having a solid plan on which one can build an effective architecture. Organizational metrics can be confusing and this area clearly builds on enterprise and API metrics across the architecture while including how to integrate effective security metrics.

Creating DevSecOps Infrastructure

Solid plans lead to solid infrastructure. Knowing how to transform an organization to cloud-native, lift and shift existing models, and integrate infrastructure as code can mean the difference between success and failure. The most effective parts of infrastructure can rely on securing gateways and end-points through analyzing how customer and internal traffic progresses securely through those areas.

Establishing a Pipeline

The key part in any good DevSecOps process relies on integrating a DevSecOps pipeline to support the overall value stream. Pipelines must not just be created by people, but then optimized for their success with good DevSecOps fundamentals using WIP across functional and non-functional areas of the pipeline. Effective pipelines contribute to secure repositories and create telemetry to feed back into the overall metric structure.

Observing DevSecOps Outcomes

The goal of DevSecOps is not just sooner and safer but establishing outcomes that contribute to organizational value. Shifting focus to create value depends on creating observability across all processes, to target metrics and build effective observational tools into the process. Different tools create different views and the observability tools one selects can affect overall outcomes.

Practical 3rd Way Applications

DevSecOps depends on not just flow and feedback but creating a continuous learning path to always improve. Knowing which areas can be improved relies on effectively collecting quantitative and qualitative data to support improvement efforts. At the same time, external events like hackathons and group sensing sessions can contribute to understanding learning effectiveness.

The Future of DevSecOps

As a cultural process, DevSecOps is here to stay. Keeping in line with DevSecOps means comprehending technical advancements such as quantum computing, bio-design and artificial intelligence. Each of these may contribute to future pipelines, but only if one applies sound innovation practices into continual learning cycles.