IBM Security

DevSecOps Workshop

Today's DevOps isn't just about development and operations teams. If you want to take full advantage of the agility and responsiveness of DevOps approach, IT security must also play an integrated role in the full development lifecycle of your applications. DevSecOps practices mean more than just selecting automation tools that continuously integrate security into DevOps workflow – it builds on the cultural changes of DevOps to bring security teams early in the development cycle.

As part of IBM Application Security Services portfolio, DevSecOps Workshop is designed help unify your DevOps and Security for best DevSecOps practices across people, process and technology. The workshop assesses the DevSecOps maturity level and transforms DevSecOps best practices to help securely build, deploy and iterate applications.

Solution Value

IBM Security DevSecOps Workshop provides deliverables and insights defining DevSecOps, best starting point for the client, analysis of clients' current and target state, and best practices. As part of these deliverables, IBM Security DevSecOps experts will recommend culture practices, security tooling, and process techniques to ensure clients' success in DevSecOps implementation.

- Provides DevSecOps expertise
- Analyzes current state
- Develops DevSecOps processes
- Recommends DevSecOps tooling
- Helps implement target state
- Enables DevSecOps culture

Why IBM Security

IBM Security is the industry leader in delivering consultation, service integration, managed security services for DevSecOps.

IBM Security DevSecOps offerings are rooted in experience around cloud, application, and SDLC security best practices.

How we deliver the DevSecOps Workshop

Phase 1

Workshop preparation

Develops business and technology objectives, schedules workshop, evaluates data and determines high-level current state around people, process, and technology.

Key deliverables & artifacts:

- Current state documents
  - Architectures
  - CI/CD pipelines
  - Current tools & processes
- Current state observations

Phase 2

Workshop

Identifies and evaluates DevSecOps models, designs the high-level architecture, discusses best DevSecOps practices, and validates all findings with client.

Key deliverables & artifacts:

- Current DevSecOps model validation
- Maturity model rating identification
- Gap analysis findings and recommendations
- Target state conceptual views and model

Phase 3

Finalize deliverables

Provides recommendation of portfolio dispositions and prioritization, finalizes benefits case, develops cloud strategy and enables roadmap.

Final deliverables:

- DevSecOps maturity ratings
- Current state and target state best practices
- High-level DevSecOps roadmap
- Next steps