DevSecOps

Is It Really Possible to “DevSecOps”?

Presented by ASMGi

December 15, 2020
Today’s Presenters – *How Do I “DevSecOps”?*

**John Meyer**  
*Solutions Architect, ASMGi*  
jmeyer@asmgi.com

**Frank Yako**  
*CIO, Director of Strategic Initiatives*  
fyako@ asmgi.com
Agenda and Objectives

- Provide an Overview and Introduction to DevSecOps Concepts
- Discuss the Business Case and Correlation of DevSecOps to a Digital-First Strategy
- Demonstrate How to Assess DevSecOps Maturity in an Organization
- How to Align DevSecOps with Compliance and a Digital-First Strategy
- Questions and Closing Comments
What is the Meaning of DevSecOps?

DevSecOps, is short for development, security and operations. Its mantra is to make everyone accountable for security with the objective of implementing security decisions and actions at the same scale and speed as development and operations decisions and actions.

DevSecOps Defined
Security – Episodic vs Continuous

Back to the Drawing Board 😞

Keep it Moving!
DevSecOps is a Better Fit

◆ DevOps tends to have a narrow focus
  – Paired with Agile/Scrum

◆ DevSecOps can be more open
  – Can integrate into multiple SDLC models (SDLC agnostic)
What Does It Mean to Be Digital First

- Maximize Digital Interactions
- Access to Applications
- Cloud Accessible Data
- Automate Processes

A modern, digital-first organization has fully optimized their customer experience, operating model and employee experience for digital execution.

Employees have the tools, training, supporting leadership, culture and teamwork to work from anywhere, anytime.

- Larry English

((CENTRIC))
DevSecOps & Digital-First Better Together

- Enabling better collaboration
- Cloud focused
- Bringing applications closer to users
- Making security every user’s responsibility
- Making remote work easier
- Accelerating delivery of digital services

Cultural shift
Deploying Continuous Security: Building the Business Case for DevSecOps

Save time in a competitive market
When security is only done prior to deployment Engineers must debug and rework parts of a project from scratch all over again.

Consider security early and often in every phase of the SDLC
Security should be part of the design and planning discussions.

Distribute security throughout the SDLC
This is done through manual human intervention and automated processes through scripting and tooling.
Continuous Security Visualized

- Effective Monitoring
- Compliance & Reporting
- Code Security

1. PREVENT
   Compliance Rules:
   Establish boundaries to prevent non-compliance with cloud rules. Use our compliance jumpstarts, which consist of plug-and-play cloud rules, to enforce policy with minimal configuration.

2. DETECT
   Compliance Checks:
   Continuously monitor your cloud with customizable compliance checks. Apply these checks only where you need them, conducting scheduled and manual scans for 24/7 coverage. We provide many checks to get you started.

3. REPORT
   Compliance Dashboard:
   Keep eyes on the compliance gap with clear visual indicators on the dashboard. Track violations found and addressed and sort by compliance standard (such as NIST or CIS).

4. REMEDIATE
   Compliance Automation:
   Enable automatic remediation of issues to fix compliance findings without manual intervention. Gain the visual clarity to find and address other issues manually.
Assessing Your Organization

- List phases (9 phases)
- List requirements for each phase
- List processes & sub-processes to satisfy the requirement
- List organization roles needed to satisfy the requirement
- List the technology needs to carry out the processes
- Assess strengths, weaknesses, and risks, then prioritize!
## DevSecOps Maturity Assessment Tool - Sample

### Security Phase Requirements

<table>
<thead>
<tr>
<th>Phase</th>
<th>Security Phase Requirements</th>
<th>Process</th>
<th>Sub Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Perform constant secure code scans against code repositories</td>
<td>Secure code scan</td>
<td>Continuous code scanning on repositories</td>
</tr>
<tr>
<td>Plan</td>
<td>Data modeling; database selection; database deployment topology</td>
<td>Development</td>
<td>Database design</td>
</tr>
</tbody>
</table>

### Security and Compliance Engineer

<table>
<thead>
<tr>
<th>Type of Requirement (or Dependencies)</th>
<th>Process Yes/No</th>
<th>People Yes/No</th>
<th>Technology Yes/No</th>
<th>Tech Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security and Compliance Engineer</td>
<td>1</td>
<td>Team collaboration tools</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Project Manager</td>
<td>1</td>
<td>Team collaboration tools</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>Change Control Manager</td>
<td>0</td>
<td>Team collaboration tools; Issue tracking system</td>
<td>0</td>
</tr>
</tbody>
</table>

### DevSecOps Grading & Health Report

<table>
<thead>
<tr>
<th>Category</th>
<th>Score Value</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>DevSecOps Model Completion</td>
<td>120</td>
<td>51.28%</td>
</tr>
<tr>
<td>DevSecOps Risk Assessment</td>
<td>116</td>
<td>42.03%</td>
</tr>
<tr>
<td>DevSecOps Maturity</td>
<td>76</td>
<td>38.19%</td>
</tr>
</tbody>
</table>

### DevSecOps Health Scorecard

- **DevSecOps Model Completion**: 51.28%
- **DevSecOps Risk**: 42.03%
- **DevSecOps Maturity**: 38.19%
Defining a Path Forward to Achieve DevSecOps Success

- Understand “Why”. Make the Business justification!
- Assessment = Current State vs. Desired Future State
- Identify Gaps and Propose Solutions
- Build a Roadmap = Can’t Do “IT” all at Once!
- Incremental Change over Time
- Start Now
  - It will take 2 years whether you “Start Now” or start 2 years from now, so Start Now!
Goals and Alignment of DevSecOps & Digital-First Strategy

- Boost Productivity
- Improve efficiency
- **Reduce cost**
- Solve complex business challenges
- Encourage innovation

Digital transformation requires fundamental changes to how an organization approaches the use of technology. Establishing an integrated DevSecOps program becomes essential in protecting company IP and data while strengthening the existing cybersecurity strategy.
Incorporating the Requirements of Risk & Compliance

How does technology impact organizations and what is its role in a Digital-First strategy.

• Automate
• Collaborate
• Streamline workflows
• = Cost savings and reduced risk

Regulations and Contractual Obligations Under Which DevOps Practitioners Are Working

<table>
<thead>
<tr>
<th>Mean Number of Regulations</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Laws and Regulations, Differs by Region (for e.g., EU GDPR)</td>
<td>47%</td>
</tr>
<tr>
<td>ISO 27001: Information Security Management System</td>
<td>46%</td>
</tr>
<tr>
<td>Federal Information Security Management Act (FISMA)</td>
<td>41%</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>37%</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard (PCI-DSS)</td>
<td>30%</td>
</tr>
<tr>
<td>NIST Cybersecurity Framework (CSF)</td>
<td>29%</td>
</tr>
<tr>
<td>Family Educational Rights and Privacy Act (FERPA)</td>
<td>23%</td>
</tr>
<tr>
<td>Basel or Gramm-Leach-Bliley Act (GLBA)</td>
<td>22%</td>
</tr>
<tr>
<td>Sarbanes-Oxley Act</td>
<td>19%</td>
</tr>
<tr>
<td>Service Organization Control (SOC)2</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
<tr>
<td>Not Required to Comply With Any Regulations</td>
<td>2%</td>
</tr>
</tbody>
</table>

n = 208 All Respondents, Excluding Unsure

Source: Gartner

Note: Multiple responses allowed for mean number calculations excluding "We are not required to comply with any regulations."
Aligning Around a Successful DevSecOps Practice

- Find the right balance and distribution of roles
- Successful integration of security controls and tools throughout the SDLC
- Use DevSecOps practices and automation to substitute traditional controls
- Validate and measure success of DevSecOps compliance efforts by continually monitoring status of compliance
- Scale compliance practices across the organization by leveraging compliance-specific software
QUESTIONS
Call to Action!

- DevSecOps Primer Session
  - As a standalone activity ASMGi is offering a 2-hour DevSecOps Primer Session to begin the process of educating an Organization about DevSecOps including qualifying the organization for a DevSecOps Maturity Assessment.

Contact Info:

John Meyer
jmeyer@asmgi.com