DevSecOps
Embedded Security Within the
Hyper Agile Speed of DevOps

Mark G. Moore, Managing Director, Deloitte and Touche LLP
Antonio L. Bovoso, Senior Manager, Deloitte and Touche LLP
**What is DevSecOps?**

A transformational shift which incorporates secure culture, practices, and tools to drive visibility, collaboration, and agility of security into each phase of the DevOps pipeline.

<table>
<thead>
<tr>
<th>Governance</th>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish security ‘guardrails’ and monitor results</td>
<td>Break down silos between security and DevOps teams and instill cyber awareness</td>
<td>Orchestrate an integrated process flow and drive ‘in-line’ risk rationalized feedback</td>
<td>Automate recurring security tasks and harden the development pipeline</td>
</tr>
<tr>
<td>- Redesign the operational &amp; compliance framework</td>
<td>- Incorporate security staff in DevOps teams</td>
<td>- Asset inventory and risk awareness</td>
<td>- Automate secure application development</td>
</tr>
<tr>
<td>- Establish shared metrics to evaluate progress</td>
<td>- Have security teams brief dev and ops teams on current threats / exploits/breaches</td>
<td>- Integrated backlog and pipeline</td>
<td>- Protect the toolchain and infrastructure</td>
</tr>
</tbody>
</table>

**Continuous improvement and added value**

- **Improve security and quality**
  - Increase deployment success rate
  - Reduce meantime to resolve incidents
  - Reduce number of open security defects

- **Improve time to market**
  - Increase production deployment frequency
  - Greater speed of deployment

- **Improve compliance feedback**
  - Reduction in open compliance findings
  - Decrease time from audit request to evidence delivery

- **Improve productivity**
  - More story points per sprint
  - Increase pipeline velocity
  - Controlled production access
From DevOps to DevSecOps

**What is DevOps?**
A set of practices that automates the processes between development and operation teams to build, test, and release software quickly and reliably

**Why security in DevOps?**
- The ability to deploy applications has improved in both scale and speed while security considerations are often overlooked in favor of meeting business demands quickly
- Given the reliance of applications to keep operations running; security in the development process cannot be an afterthought
- Application security must speed up to keep pace with operations

**How can we bring security into DevOps?**
- Tightly integrate security tools and processes throughout the DevOps pipeline
- Automate core security tasks by embedding security controls early on in the software development lifecycle
- Continuous monitoring and remediation of security defects across the application lifecycle including development and maintenance

---

**Key Benefits**

**Enhanced compliance**
In DevSecOps, security auditing, monitoring, and notification systems are automated and continuously monitored, which facilitates enhanced compliance

**Increased efficiency & product quality**
In DevSecOps, security auditing, monitoring, and notification systems are automated and continuously monitored, which increases the speed of delivery and enhances quality

**Continuous security**
DevSecOps implements the ‘secure by design’ principle by using automated security review of code and automated application security testing

**Increased collaboration**
By integrating development, security and operations, DevSecOps fosters a culture of openness and transparency from the earliest stages of development

---

Copyright © 2018 Deloitte Development LLC. All rights reserved.
Common myths and misconceptions

Perceived challenges and piece-meal integration often hinder organizations from realizing the value of incorporating security into DevOps

- DevSecOps is only “Security as Code” or Automation
- Security team does not require development knowledge
- DevSecOps just means code scanning
- DevSecOps prevents organizations from meeting their business objectives
- DevSecOps is incompatible with my compliance requirements
- DevSecOps requires developers to be security experts
- DevSecOps requires significant tool investment
The DevSecOps transformation is achieved through following pillars:

<table>
<thead>
<tr>
<th>Strategic Goals</th>
<th>Architecture and Operations</th>
<th>Program Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategy:</strong></td>
<td><strong>Design:</strong> Design a DevSecOps operating model that includes designing data flows, developing standards, and mapping technologies and processes to core security operations</td>
<td><strong>Monitor:</strong> Ensure processes are followed, maintained, reviewed and updated regularly</td>
</tr>
<tr>
<td>• Establish strategic drivers for DevOps teams to meet changing business requirements without excluding security and compliance needs</td>
<td><strong>Execution:</strong> Implement new tools and processes to enable security in DevOps environment</td>
<td>• Implement processes to perform lessons learned and evaluate policies and enhance training</td>
</tr>
<tr>
<td><strong>Cultural transformation:</strong> Continuous enablement to initiate culture change to foster collaboration between developers, security teams, and operations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Strategic Goals</strong></td>
<td><strong>Architecture and Operations</strong></td>
<td><strong>Program Evaluation</strong></td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td><strong>People</strong></td>
<td><strong>Technology</strong></td>
</tr>
<tr>
<td>Establish security ‘guardrails’ and monitor results</td>
<td>Staff against business priorities and disseminate security know-how</td>
<td>Automate recurring security tasks and harden the development pipeline</td>
</tr>
<tr>
<td><strong>Continuous Process Improvement</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Drive scalable governance for DevSecOps
The approach to develop a sustainable governance model is through enabling security services that are business aligned, agile, self-service and risk based.

- **DevSecOps Roles and Responsibilities**
  - Establishing well defined roles and responsibilities is imperative in the cross functional DevOps teams. It leads to efficient operations for a product.

- **Establish Policies and Procedures**
  - Introducing DevSecOps specific policies and procedures will enable organizations to keep up with the pace of application development in a DevOps environment.

- **Enable Security Automation**
  - Automated security tools in the DevSecOps pipeline improves overall security by reducing vulnerabilities and security flaws due to human error.

- **Automated Audit Evidence Collection**
  - Security monitoring and notification systems in DevSecOps creates an automated audit trail throughout the software development lifecycle, which facilitates compliance reporting.

- **Monitor Security Metrics for Continuous Feedback**
  - Continuously monitoring security metrics allows DevOps teams to consistently improve their security decisions and stay on top of the game.
DevSecOps success criteria

Open collaboration to shared objectives
- Set shared expectations and metrics for measuring success
- Align security architects and focus activities based on business priorities

Security at the source
- Create consumable, self-service security capabilities
- Establish security ‘guardrails’ and monitor results/provide targeted feedback

Reinforce and elevate through automation
- Orchestrate integrated process flow by automating recurring tasks
- Embed preventative operational controls and audit trails

Risk-oriented operations and actionable insights
- Utilize operational insights and threat intelligence to drive process flow, prioritization and remediation recommendations
- Don’t just rely on scans; take risk-based approach to testing

Holistic approach to security objectives
- Integrate framework to secure both the pipeline and application
- End-to-end security implementation
- Provide defense-in-depth with production environment

Proactive monitoring and recursive feedback
- Continuous testing to identify problems before they become issues
- Leverage logging/telemetry to drive learning and innovation
This presentation contains general information only and Deloitte Risk and Financial Advisory is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte Risk and Financial Advisory shall not be responsible for any loss sustained by any person who relies on this presentation.