How Do I “DevSecOps”?  

Presented by ASMGi  

October 27, 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

- Introduction and Objectives
- Security at Every Level
- Perform a Security / Risk Assessment
- Automate
- Dashboards and Alerts for Continuous Monitoring
- Be in a Continuous State of Compliance
Introduction and Objectives

You’ve learned how to assess your current maturity in the DevSecOps model. So what’s next? How do you implement a mature DevSecOps program? This is what we mean by ‘How do I DevSecOps’!

- Discuss **Methods** to implement a DevSecOps Program
- Learn how to implement and integrate **Security Tools** and **Processes** throughout the SDLC
- The importance of **Automation** in every process possible
- The importance of **Continuous Monitoring**
- How to maintain **Continuous Compliance** through the DevSecOps model
DevSecOps – Security at Every Level

It Starts...and Ends with Security

- “You have to know where you’re at to know where your going”
- And it starts with SECURITY
- Security integrated into every phase of the DevOps Lifecycle
DevSecOps – Where to Begin???

Self-Assessment – It starts with Security

““You have to know where you’re at to know how to reach the destination”.

Complete an Assessment and determine what’s needed to create a successful DevSecOps Program.

With the Assessment complete it’s time to Prioritize and Remediate!
A Method to the Model

- Evaluate Roles, Processes, and Tools
- Does each Role, Process, and/or Tool serve a purpose and bring value?
- Are there any Bottlenecks?
- Are there any missing Roles, Processes, or Tools?
- Design for an outcome!
Choosing the Right [blank] for the Job

Choosing and Implementing Processes and Tooling

- Threat Modeling
- Penetration Testing
- Code Scans
- Code Review
- License Compliance
- Open Source Compliance
- Hardened Container/OS Image
- WAF and Service Mesh

- Listing Pros and Cons
- RACI Diagrams
- Cost Analysis
- Risk Analysis
Security is Everyone’s Responsibility

Empower developers to suggest critical security changes. Make everyone accountable for security empowering your teams with tools and expertise to respond to (and neutralize) threats before they become a major issue.

(Sumo Logic)
DevOps Program Methodologies
Not a One Size Fits All

◆ Figure out what DevOps model suits your organization or project need.

◆ DevSecOps Can be as broad as an organization or as granular as project based.

The goal for a "DevOps Team" should be to put itself out of business by enabling the rest of the org.

EricMinkk
Methods to Avoid

Anti-Type A: Dev and Ops Silos

Anti-Type B: DevOps Team Silo

Anti-Type C: Dev Don’t Need Ops

Anti-Type D: DevOps as Tools Team

Anti-Type E: Rebranded SysAdmin

Anti-Type F: Ops Embedded in Dev Team

Anti-Type G: Dev and DBA Silos
Tools to Enable Secure Code

- SCA → Open Source Compliance
- SCA → License Compliance
- SAST → Source Code Scan
- DAST → Web Security Scanning
- IAST → Interactive Security Scanning
- IDE Plug-Ins → Real-Time Code Scanning
- CI/CD → Automated Testing
Software Testing Methods

Types of Software Testing

- Unit Testing
- Integration Testing
- Smoke Testing
- System Testing
- Regression Testing
- Performance & Load Testing
- UAT
Test Automation for Secure Code and Secure Applications

- Why is automation important in software testing?

  Automated software testing can increase the depth and scope of tests to help improve software quality. Test automation can easily execute thousands of different complex test cases during every test run providing coverage that is impossible with manual tests.

- Benefits of Automated Testing
  - Faster Feedback Cycle. Without test automation, feedback for newly developed features can take a while. ...
  - Team Saves Time. ...
  - Reduced Business Expenses. ...
  - Higher Test Coverage. ...
  - Reusability of Test Suite. ...
  - Faster Time to Market. ...
  - Better Insights. ...
  - Improved Accuracy
  - Automated Testing Provides More Features
  - Less Stress on QA Team
  - Quickly Determine the Stability of Your Build
  - Eliminate Human Error
Continuous Monitoring, Alerting, & Dashboards

- Effective Monitoring
  - Systems
  - Application
  - Infrastructure
  - Security

- Meaningful Alerts
- Accurate Reporting
- Risk Assessment
Continuous Compliance

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.

(Graphic: Business Wire)
...What’s Next

Join us for the next session to apply priorities identified through a DevSecOps Assessment...

- SAST - Static Application Security Testing
- SCA - Software Composition Analysis
- DAST - Dynamic Application Security Testing
Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com