Using **Balanced Development Automation** to address security in a DevOps environment

Ehsan Foroughi

VP, Product
A bit of history

- Embedded QA! We learned that there is no QA team in Agile!
- QA starts with development and finishes with development!
- But wait! Isn’t security a type of quality?
- Why are we so late to the party?
Key Market Challenge

Simultaneously addressing the need for greater **speed** and the need to sustain adequate cyber **security and compliance**

- Proactive security processes are costly and very time consuming
- Coding errors and design flaws in applications remain a common source of incidents
- Uncertainty persists about effective compliance and control selection
- Developers have limited or no knowledge of secure coding
First Option: Fast and Risky

Reactive Processes
- Compliance Audit
- Penetration Testing
- Code Scanning

Fix & Delay
OR
Risk & Release

Go to Market
Second Option: **Slow and Safe**

**Proactive Processes**
- Threat Modeling
- Risk Assessments
- Secure Coding / Deployment Standards
- Privacy by Design
- Security Training

**Reactive Processes**
- Compliance Audit
- Penetration Testing
- Code Scanning

Go to Market

Software Development (Agile)
Common Steps in Proactive Processes

Proactive Processes

- Threat Modeling
- Risk Assessments
- Secure Coding / Deployment Standards
- Privacy by Design

Information Gathering

Expert Assessment

Recommendations

Validation and Reports

Start Project

Go to Market
Common Steps in **Proactive Processes**

- **Threat Modeling**
  - Manual
  - Expensive
- **Risk Assessments**
  - Slow
  - Inconsistent
- **Secure Coding / Deployment Standards**
  - Manual
- **Privacy by Design**
  - Siloed

---

**Reactive Processes**

- Accept risks in other apps
- Start Project
- Go to Market

---

**Proactive Processes**

- Internal Audit
- Pen Testing
- Code Scanning
- Software Development (Agile)

---

**Security Compass**
The Developer’s Dilemma:

Fast and Risky OR Slow and Safe

How do you make that impossible choice?
The Third Option...

Fast and Safe

BALANCED DEVELOPMENT
Third Option: Go Fast, Stay Safe

Proactive Processes
- Threat Modeling
- Risk Assessments
- Secure Coding / Deployment Standards
- Privacy by Design
- Security Training

Reactive Processes
- Compliance Audit
- Penetration Testing
- Code Scanning

Balanced Development Automation

Go to Market
Automating Key Parts of Proactive Processes

MANUAL STEPS

Information Gathering  Expert Assessment  Recommendations  Validation and Reports

PROFILER  DECISION ENGINE  TASK ORCHESTRATOR  VALIDATION ENGINE

BALANCED DEVELOPMENT AUTOMATION

Knowledge Base

POLICY  EXPERT KNOWLEDGE
Go fast. Stay safe.
Thank You!

Security Compass

www.securitycompass.com

Copyright © 2020 Security Compass. All rights reserved.