DEVSECOPS UNPLUGGED

Why a Focus on Development and Operations Leaves a Massive Gap for Security
# OUTLINE

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Confluence of Events</td>
</tr>
<tr>
<td>2</td>
<td>Antipatterns</td>
</tr>
<tr>
<td>3</td>
<td>Industry Challenges</td>
</tr>
<tr>
<td>4</td>
<td>Role Challenges</td>
</tr>
<tr>
<td>5</td>
<td>Best Practices</td>
</tr>
<tr>
<td>6</td>
<td>Addressing the Collaboration Gap</td>
</tr>
<tr>
<td>7</td>
<td>Future Research</td>
</tr>
</tbody>
</table>
RESEARCH METHODOLOGY

**Research Questions**

1. What do we know about current best practices in DevSecOps?
2. What do we know about antipatterns in DevSecOps?
3. What do we know is missing in the DevSecOps discussion?
CONFLUENCE OF EVENTS

1. The strict controls used previously haven’t all migrated into the DevOps workflow.
   – Traditionally, we have used DevOps in failure tolerant systems.
   – DevOps is now being adopted in operating systems, routers, government communications, and critical infrastructure.

2. Traditional security is getting in the way of DevOps
   – Developers don’t have access to production or SecOps data.
   – Security testing is too slow.
   – Pressure to release quickly leads to missed security reviews.
ANTIPATTERNS

- Use of immature automated deployment tools
- Incorrect metrics
- Lack of controlled collaboration
- Disregard for quality
- Lack of centralized coordination
- Poor communication
- Emphasis on speed of feature releases
- Lack of audit and control points

- Lack of security throughout the process
- Vulnerabilities in the deployment pipeline
- Lack of sufficient third party library testing
LEADERSHIP PRESSURE TO TRANSFORM

50% of the CIOs that have not transformed their capabilities will be displaced from the digital leadership team.

WHEN SOFTWARE IS EVERYWHERE...

• Telecommunications
  – Distributed Denial of Service

• Financial
  – Flash Crash

• Medical
  – Electrical Medical Record distribution

• Transportation
  – Logistics security

• Software
  – Malware
ROLE CHALLENGES (NO LONGER JUST A DEV AND OPS ISSUE)

• Business
  – Technical masquerading

• Project Manager
  – Justifying technical debt for poor practices

• Quality Assurance
  – Lack of proof for bug free software

• Customer
  – Don’t know what to ask for around security

• Developer
  – Best practices are insufficient
Application Security Drivers
(n=28)

- General Risk Management: 78.57%
- Compliance Requirements: 50.00%
- Customer Demand: 35.71%
- Breaches/incidents at own or other organizations: 21.43%
- Competitive Need: 7.14%
- Privacy of Client Data: 3.57%
- Board Demand: 3.57%
- Business Model Transformation: 3.57%

THE RISK AND COMPLIANCE GAP

Who is responsible for triggering the discussion on functional and non-functional requirements around software security?

- **Security**: 48%
- **IT**: 45%
- **Compliance**: 4%
- **Risk**: 3%


n=29
# BEST PRACTICES (YES, GAPS EXIST!)

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>AUTOMATION</th>
<th>SECURITY</th>
<th>COMPLIANCE</th>
<th>RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Security requirements analysis</td>
<td></td>
<td>Risk analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defining security policies</td>
<td></td>
<td>Continuous planning</td>
</tr>
<tr>
<td>DESIGN</td>
<td></td>
<td>Data flow analysis</td>
<td></td>
<td>Design review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Untrusted boundaries</td>
<td></td>
<td>Threat modeling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Developer training</td>
<td></td>
<td>Supply chain</td>
</tr>
<tr>
<td>DEVELOP</td>
<td>Automated code review</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Input validation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Isolation of untrusted inputs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Code scanning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous integration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST</td>
<td>Functional testing</td>
<td></td>
<td>Penetration testing</td>
<td>Compliance testing</td>
</tr>
<tr>
<td>DEPLOY</td>
<td>Automated deployment</td>
<td></td>
<td>Configuring security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software defined firewall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automated performance monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous deployment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous delivery</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrated change management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Infrastructure as code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAINTAIN</td>
<td>Automated monitoring</td>
<td></td>
<td>Short lived access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous monitoring</td>
<td></td>
<td>Explicit authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rapidly fixing errors in production</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Compass

Copyright © 2018 Security Compass. All rights reserved.
WHERE IS RISK & COMPLIANCE IN THE DEVOPS DISCUSSION?

Source: Twitter search using #DevOps over a 7 day period ending 2018-02-22 11:06 AM.
WHERE IS RISK & COMPLIANCE IN THE DEVSECOPS DISCUSSION?

Source: Twitter search using #DevSecOps over a 7 day period ending 2018-02-19 11:24 AM.
WHERE IS DEVSECOPS IN THE RISK & COMPLIANCE DISCUSSION?

Source: Twitter search using #GRC over a 7 day period ending 2018-02-22 1:45 PM.
COLLABORATION

Development

Security

Operations

Challenges:

- Skills
- Regulations
- Culture

Moderate

Moderate /High

Highest

Challenges:

- Data volume
- Analytics


Copyright © 2018 Security Compass. All rights reserved.
THE MYTH THAT ALL DEVELOPERS KNOW ABOUT SECURITY

How broad is the adoption of developer security awareness training at your organization?

Finance (n=13)

ISV (n=6)

Energy/Utility (n=3)

RESPONSE RANGE: 1 = NO TRAINING TO 5 = ALL DEVELOPERS ARE TRAINED

On a scale from 1 to 5, how confident are you in measuring your cyber-security risk across your business environment?

THE RISK GAP

Are you 100% confident in your current cybersecurity posture?

- Yes: 15%
- No: 85%


n=27
ADDRESSING THE COLLABORATION GAP

Office of CIO
- Agile & DevOps
- Legacy & Waterfall Applications
- Cloud, On Premises, and Hybrid Environments

L.T. TASKS & PROCEDURES
- ITIL
- COBIT
- ISO 27001
- PCI-DSS
- GLBA
- CWE
- RISK

Security
- App Sec
- Op Sec
- Vendor Risk
- Threat Monitoring
- Awareness & Training

Risk & Compliance
- Privacy & Compliance
- Audit
- Policy

Copyright © 2018 Security Compass. All rights reserved.
ADDRESSING THE COLLABORATION GAP

PROACTIVE COMPLIANCE IN A DEVOPS WORLD

DEEP TRIBAL KNOWLEDGE

Questionnaire  Controls Selection  Workflow, Training & ALM/Bug Tracking Integration  Testing Integration & Correlation  Reporting: Audit & Compliance

Identify  Implement  Validate  Audit

HORIZONTAL DIVERSITY ACROSS THE SECURITY LIFECYCLE
CASE STUDY: PAYPAL

- Agile transformation to over 400 scrum teams across the world
- Seamless plugin to quarterly release plan
- Less than 15 minutes for product developer to complete survey
- Usage of dynamic / in-context security requirements (security stories) along with other controls in the continuous integration pipeline
- Wide adoption across product development organization
- Automated dashboard makes metrics transparent to product development leadership

Source: https://www.youtube.com/watch?v=_rFVui0dWnI
FUTURE RESEARCH

• What are the top challenges that you face with your application security program?

- Security skills and awareness gaps: 6
- Alignment and collaboration between teams (development, IT, business units, security, risk, compliance): 2
- Budget constraints and/or vulnerability remediation costs: 1
- Efficiency in fitting security into Agile/DevOps: 1
- Other: 19

n=29


• How are organizations addressing the Policy to Procedure gap?
SOURCES

• John Michener et al, 2016. “Mitigating an Oxymoron: Compliance in a DevOps environment”.
• Nicole Forsgren et al, 2017. “DevOps Metrics”.
• Theo Schlossnagle, 2017. “Monitoring in a DevOps World”.
• Twitter, 2018. Various #DevOps, #DevSecOps, #GRC.
• Vishnavi Mohan et al, 2016. “SecDevOps: Is It a Marketing Buzzword?”.
THANK YOU

EMAIL US AT:
info@securitycompass.com

SIGN UP TO TAKE OUR FREE COURSE ON SECURITY WITH AGILITY:
https://www.securitycompass.com/devsecops

JOIN THE DEVSECOPS DISCUSSION:
https://www.linkedin.com/groups/13551214