

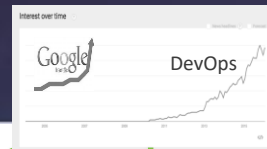


OWASP  
AppSec EU  
**Belfast**  
8-12 May, 2017

# What is a DevSecOps Engineer?

Helen Beal, DevOpsologist

# A Short History of DevOps



Patrick Debois  
Google  
Agile System Administrator Group



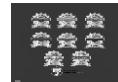
DevOps Days Belgium  
#devops  
JUJU



Mike Gualateri, Forrester  
– 'NoOps'



DevOps Days Belgium  
5 Year anniversary Ghent



2007

2009

2011

2013

2015

2017

2008



Andrew Shafer  
Agile Conference, Toronto



John Allspaw & Paul Hammond  
FlickrR



2010



'Gartner Explores DevOps'  
Cameron Haight



ranger4

2012



Ronnie Colville of Gartner: 'ARA is a Key to DevOps'



2014

2016



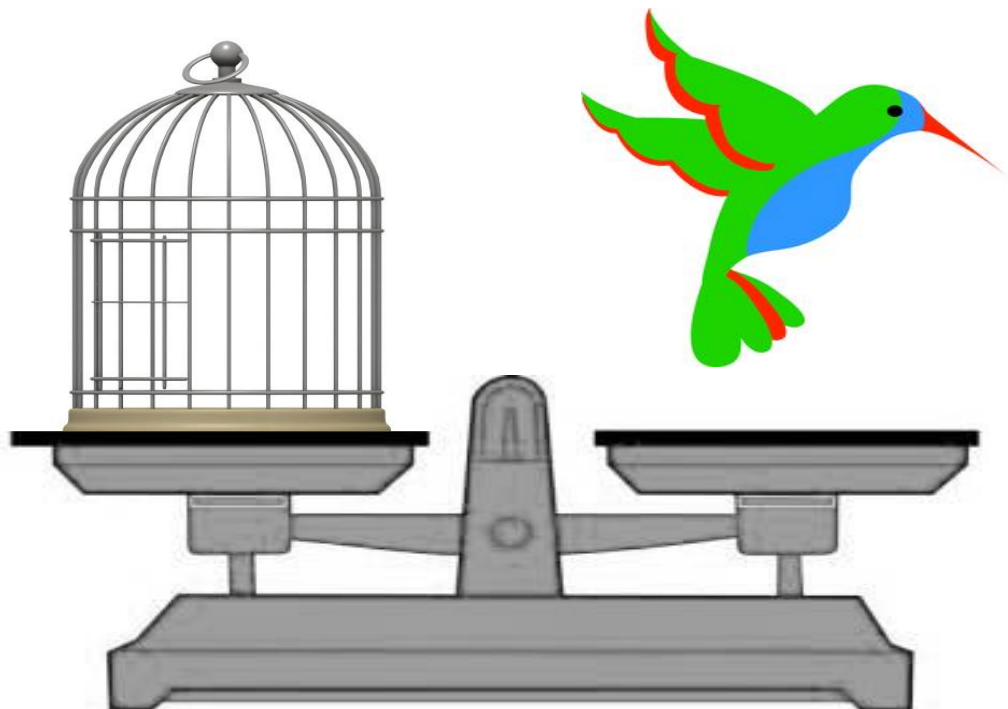
The Phoenix Project GAME





“DevOps, in a sense, is about setting up a value delivery factory - a streamlined, waste-free pipeline through which value can be delivered to the business with a predictably fast cycle time.”

*Mark Schwartz*  
*‘The Art of Business Value’*





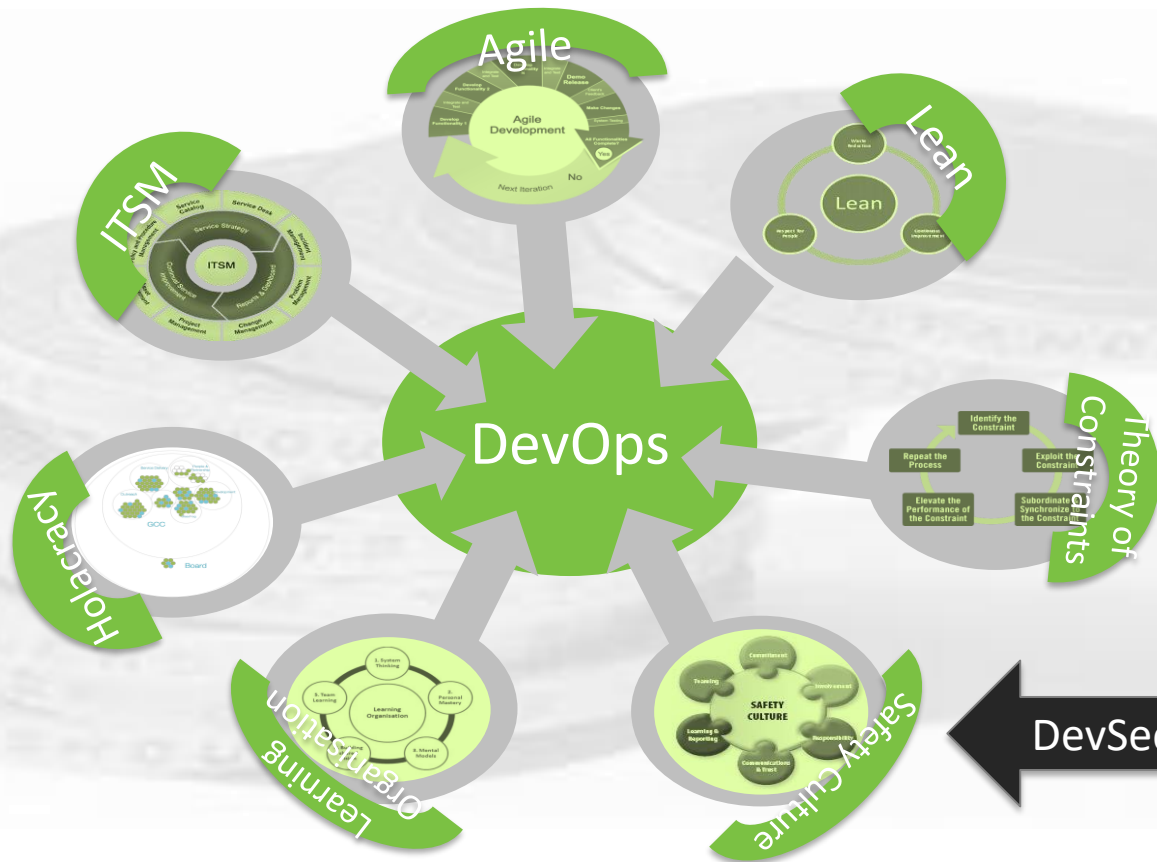
**C**ULTURE

**A**UTOMATION

**M**EASUREMENT

**S**HARING

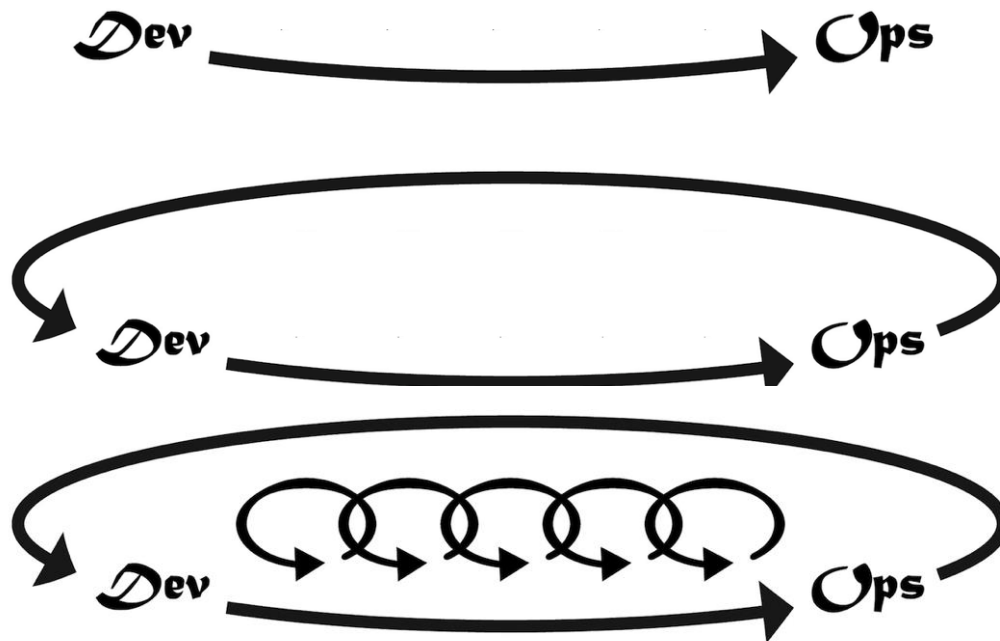
# The DevOps Superpattern



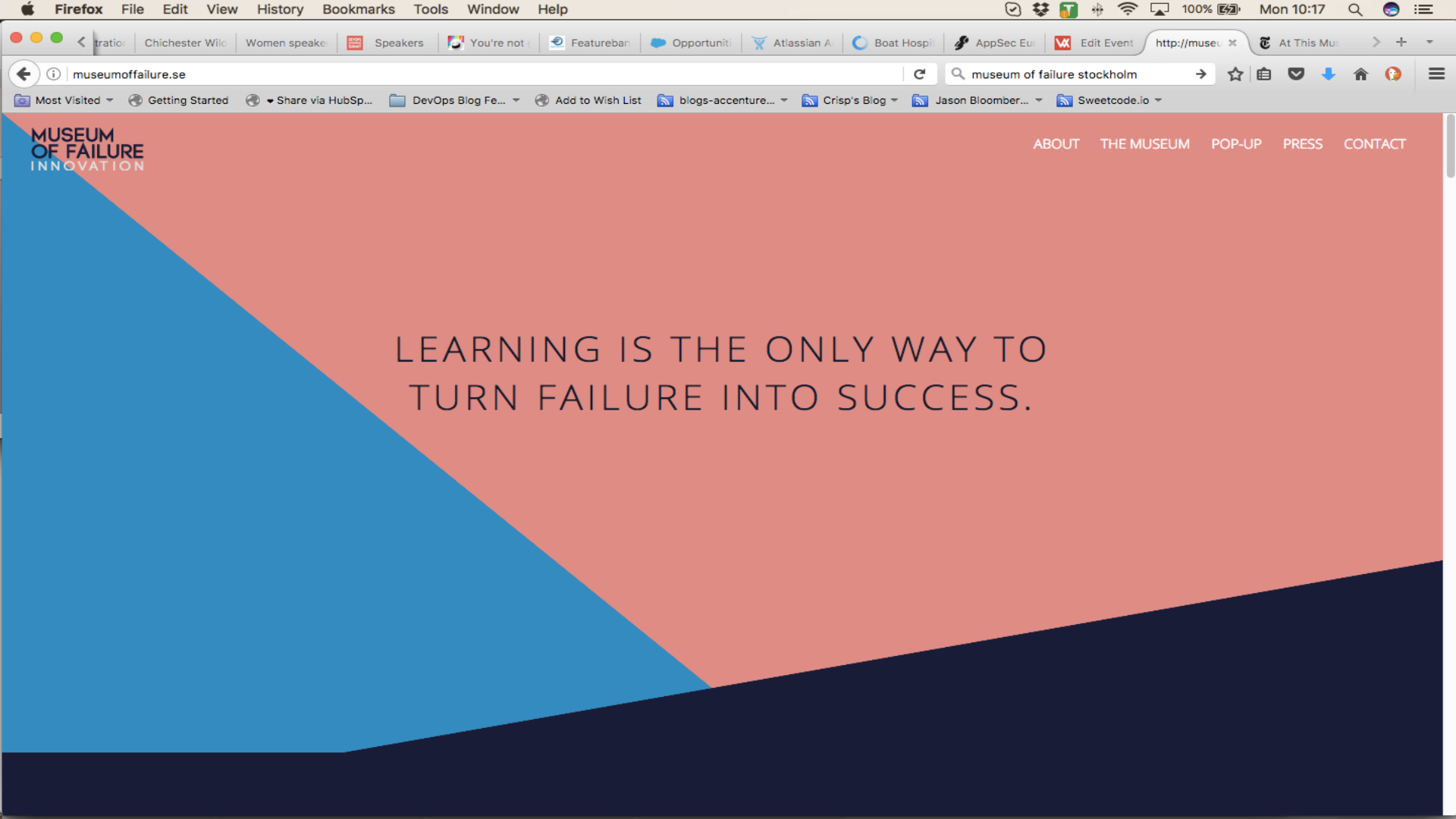


Discipline	Culture	Automation	Measurement	Sharing
Agile	The customer is elevated. Support and trust are key. Teams self organise. The importance of motivating individuals is recognised. Behaviour is adjusted as an output of reflection.	The 1st principle of the Agile Manifesto is the continuous delivery of value. This is best optimised through automation.	Focus on velocity via sprint burndown charts. Also ideally measuring value to the customer. Working software is the primary measure of progress.	Daily collaboration between business and tech is emphasised. Face to face interaction is preferred. The team reflects together.
Holacracy	An Agile organisational management system driven to distribute authority through self-organising teams preferring coaching over management. Focus on personal freedom and responsibility.	Uses Glassfrog to manage circles and GitHub.	Everyone's a sensor. No sales targets, no budgets.	Heavily focussed on using peer-review processes. Has its background in Agile thinking. Relies on collective intelligence.
ASM	Just enough governance to deliver the best service to the customer. Encourages a continuous learning environment.	Using service desk tools and monitoring to streamline processes. Using Cloud and release/environment orchestration to deliver faster.	SLA driven - focus traditionally on stability or uptime.	Promotes better collaboration by cross-pollinating vocabulary and methods.
Lean	Focus on delivering value to the customer with minimal waste.	Types of waste Lean seeks to eliminate are errors and duplication - both of which automation helps to tackle.	Use Kanban to measure velocity and Value Stream Mapping to expose waste and measure improvement.	Use Value Stream Mapping to understand the handoffs between processes and human interactions.
Learning Organisation	Decentralising the role of leadership. Putting long term sustainability ahead of short term fixes - avoidance of cultural debt.	Automate rote tasks to release time for learning and experimentation. Use Knowledge Management tools.		Exposing personal mental patterns and thinking for inspection and influence from others. Team learning is one of the 5 disciplines. Shared vision of the future.
Safety Culture	It's got culture in the name! In a highly experimental, innovative environment, we need to build safety in.	Fail safe, fast, smart - testing and auditing early in the release cycle and pre-emptive monitoring.	MTTR but measuring failure in terms of real business value is most effective.	Accountability is key and ensuring all understand their role in procedures.

# The Three Ways







LEARNING IS THE ONLY WAY TO  
TURN FAILURE INTO SUCCESS.





On / Off

Touch

Capture



**Colgate®**

**Beef  
Lasagne**

MUSEUM  
OF FAILURE  
INNOVATION

KEEP FROZEN

**Colgate®**

**Beef  
Lasagne**

NET WT. 14 OZ

DevOps  
is not one person's  
job - it's  
everyone's job.

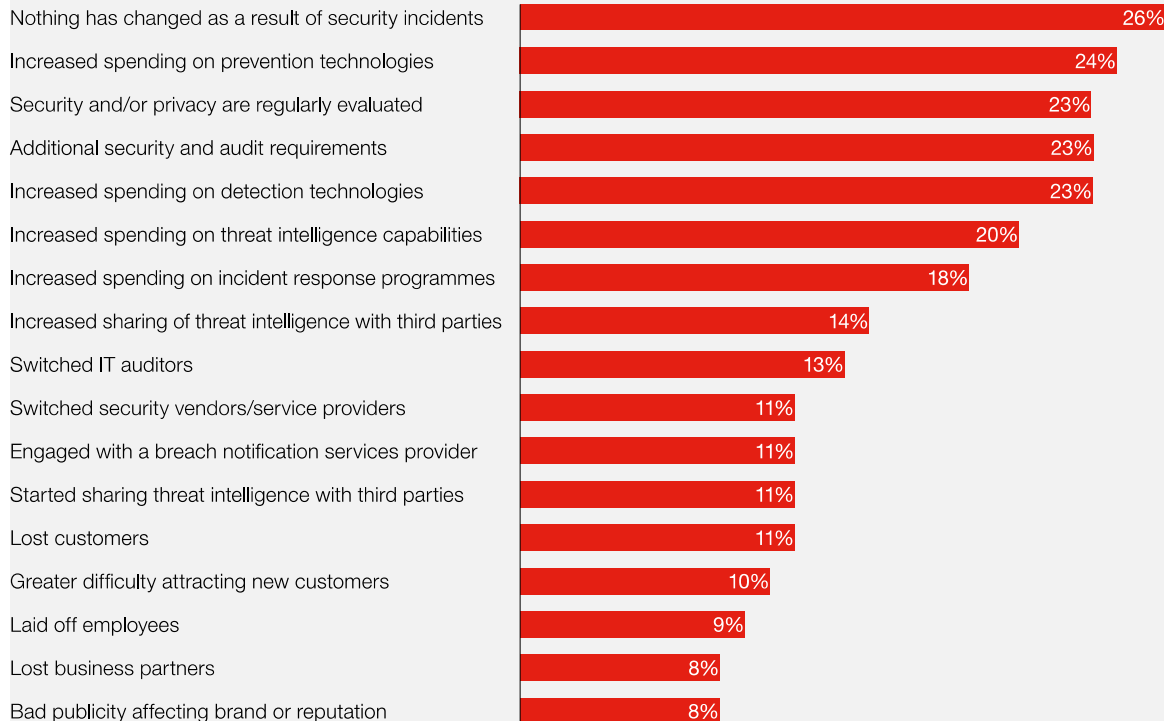


Security  
is not one person's  
job - it's  
everyone's job.

# Organisational response to security incidents

## Organisational response to security incidents

What has changed in the last 12 months



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

# Metrics & The Second Way

## Experts more likely to track metrics

Those who strongly agree and agree

■ Cyber novice ■ Cyber opportunist ■ Cyber expert

I am aware of the security metrics available in my organisation



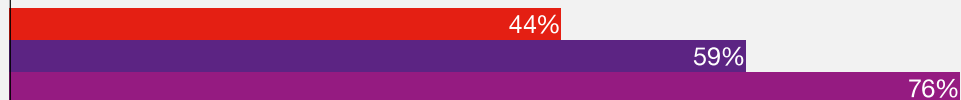
We use alerts/metrics from security equipment to make decisions



The security metrics we use directly support decision making

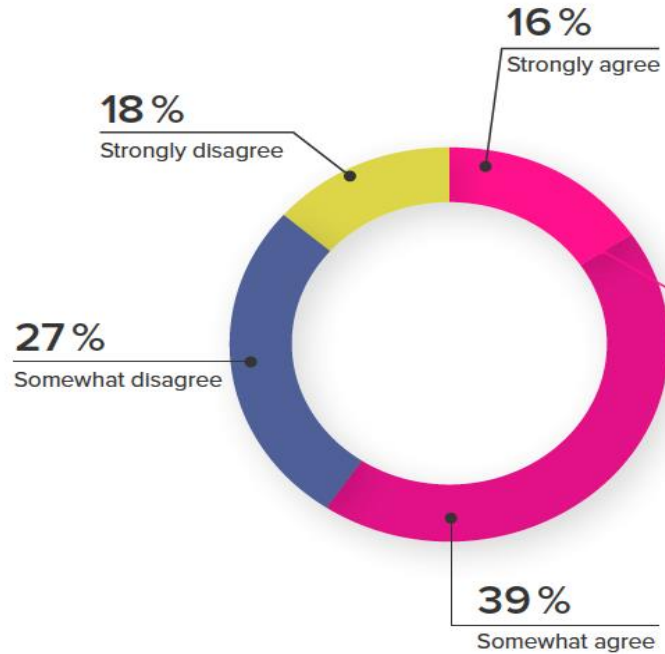


Security metrics form a graphical dashboard available in real-time

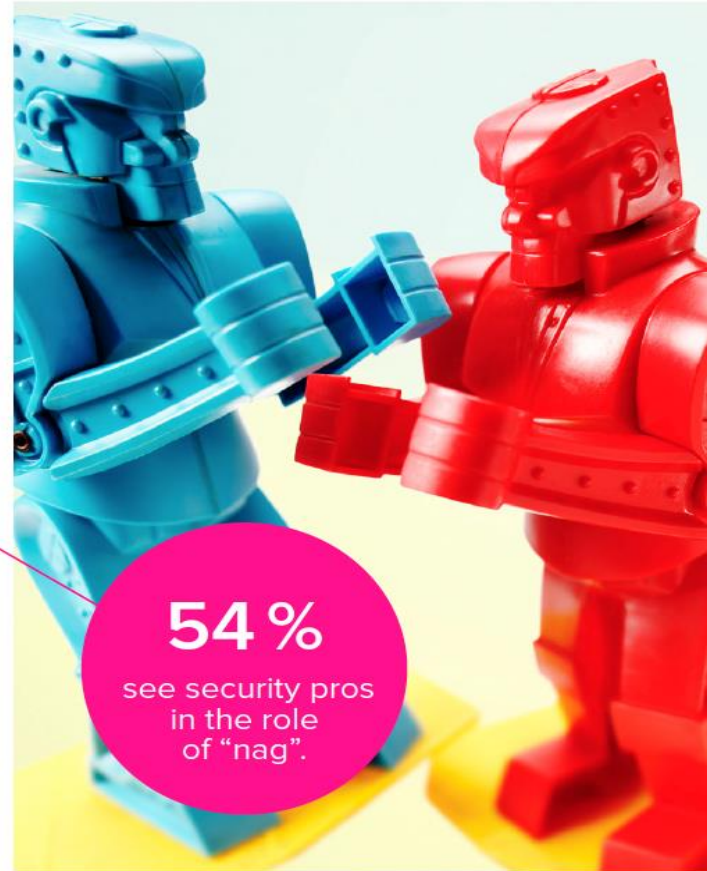


Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Our current approach to application security puts security pros in the role of nags who only point out vulnerabilities but who can't resolve them.



n = 1,775



FAIL

SAFE



FAIL

FAST

FAIL

OFTEN

FAIL

SMART

“One way to enable market-oriented outcomes is for Operations to create a set of centralized platforms and tooling services that any Dev team can use to become more productive... a platform that provides a shared version control repository with **pre-blessed security libraries**, a deployment pipeline that automatically runs **code quality and security scanning tools**, which deploys our applications into known, good environments that already have production monitoring tools installed on them.”

*The DevOps Handbook*

# The DevOps Handbook

HOW TO CREATE WORLD-CLASS  
AGILITY, RELIABILITY, & SECURITY  
IN TECHNOLOGY ORGANIZATIONS




GENE KIM,  
JEZ HUMBLE,  
PATRICK DEBOIS,  
& JOHN WILLIS

FOREWORD BY JOHN ALLSPAUGH

TAKE THE DORA DEVOPS X-RAY ASSESSMENT AND SEE WHERE YOU STAND.



A man with short dark hair and black-rimmed glasses, wearing a black t-shirt, is sitting at a desk in a cluttered office. He is looking slightly to his right with a thoughtful expression. The background is filled with shelves containing various items, including a large speaker, a mask, and many papers. A desk lamp is visible on the right side of the frame.

“Information security is a team sport. Everyone needs to play, or we all lose.”

Cory Doctorow

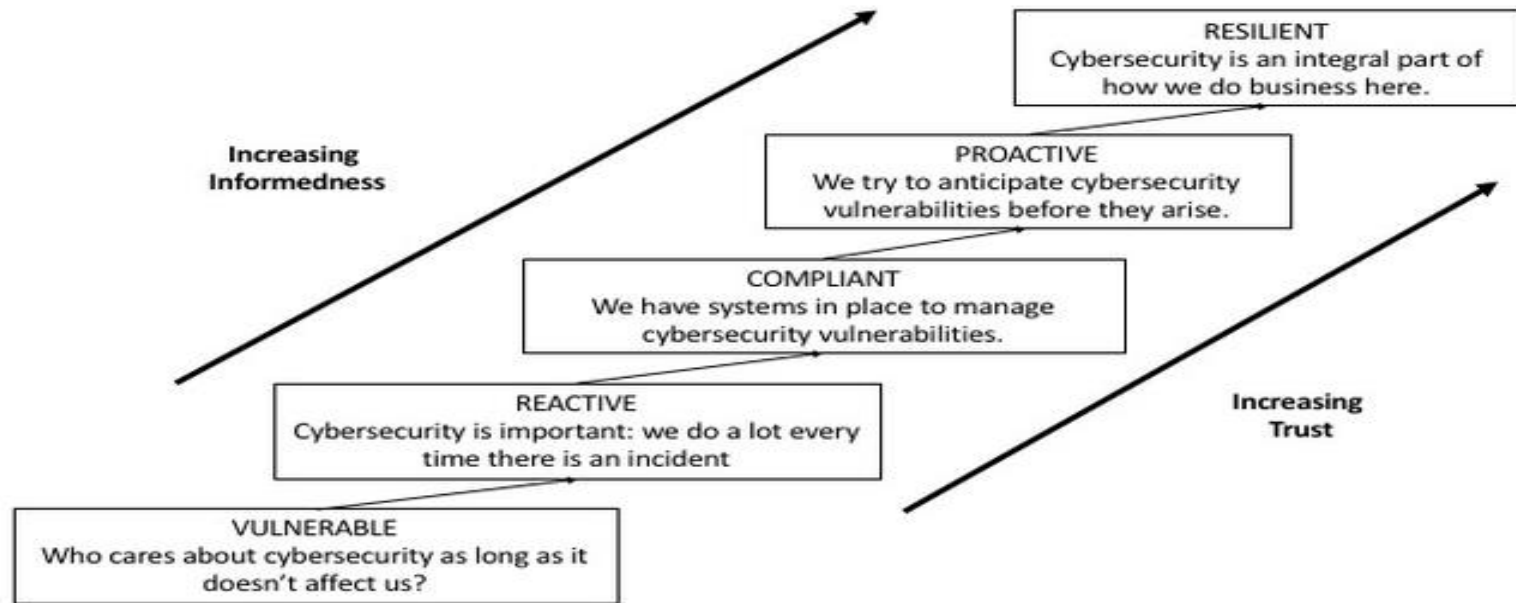
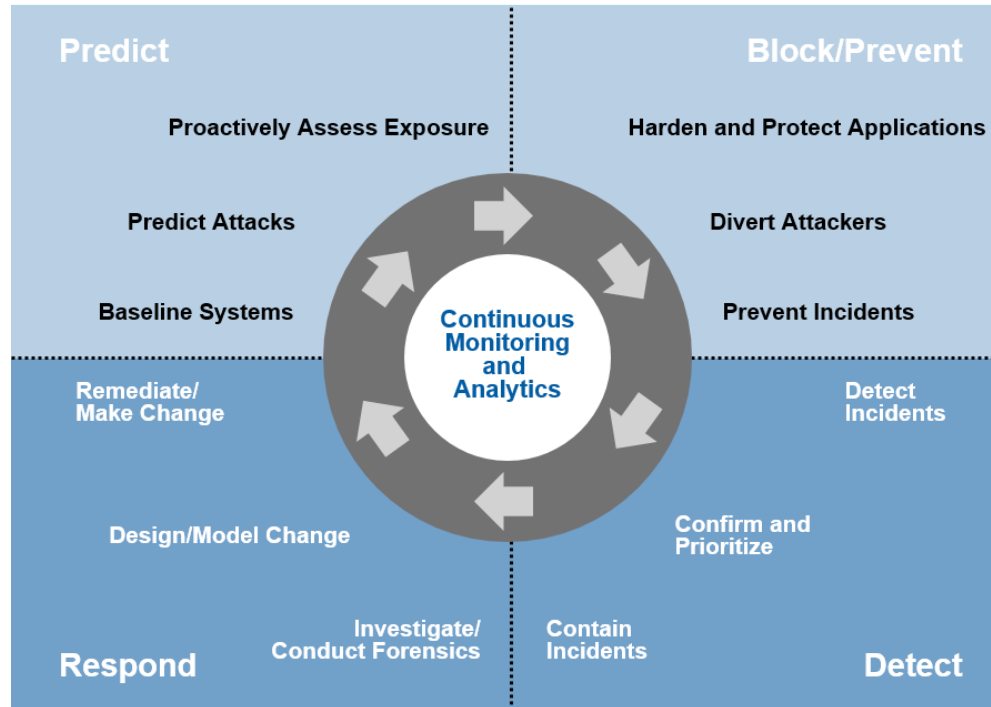


Figure 2: Cybersecurity culture maturity model levels (Lance and Bacic, 2016, based on Reason, 1997; Parker et al., 2006)

# Elements of an Adaptive Security Architecture



Source: Gartner (February 2016)



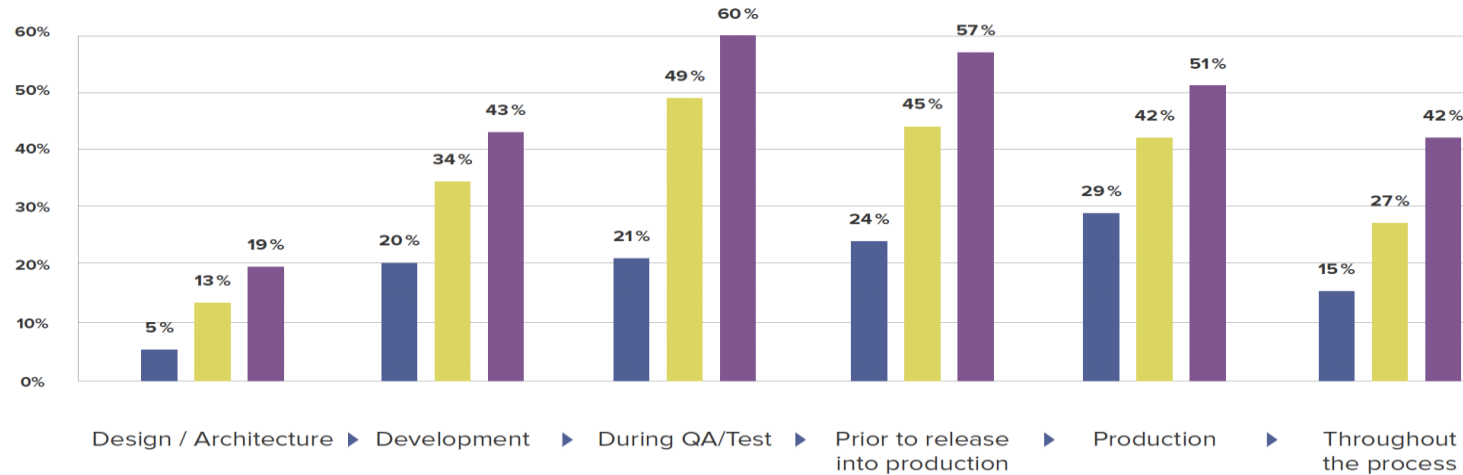
# Key Principles of DevSecOps



- Shifting Left
- Cooperation > Internal Competition
- Scaling Through Automation
- Measurable Outcomes
- Business Transformation

From the DevOps Institute DevSecOps Engineer Course

# Where is security being automated?



■ 2014 All responses

■ 2017 All responses

■ 2017 Mature DevOps Practices

From the Sonatype 2017 DevSecOps Survey



# The DevOps Loop™





# The Beal-Hedemark Golden Square



with DevOps you CAN have it all

Be DevOpstastic

# Thank You to Our Sponsors

