RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: CRWD-T10

Using Team Structure as Defense in Depth

William (Bil) Harmer III, CISSP, CISM, CIPP

CSO
GoodData Inc
@wilharm3

#RSAC
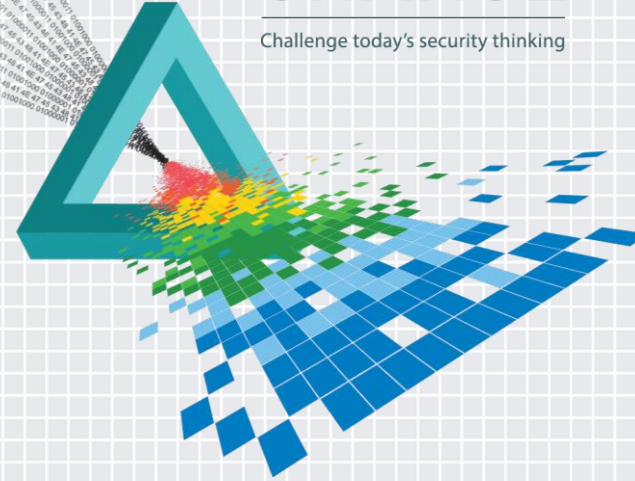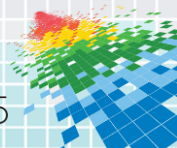
"Stuff" gets thrown over the fence

GoodData

RSAConference2015
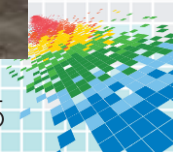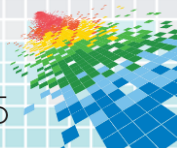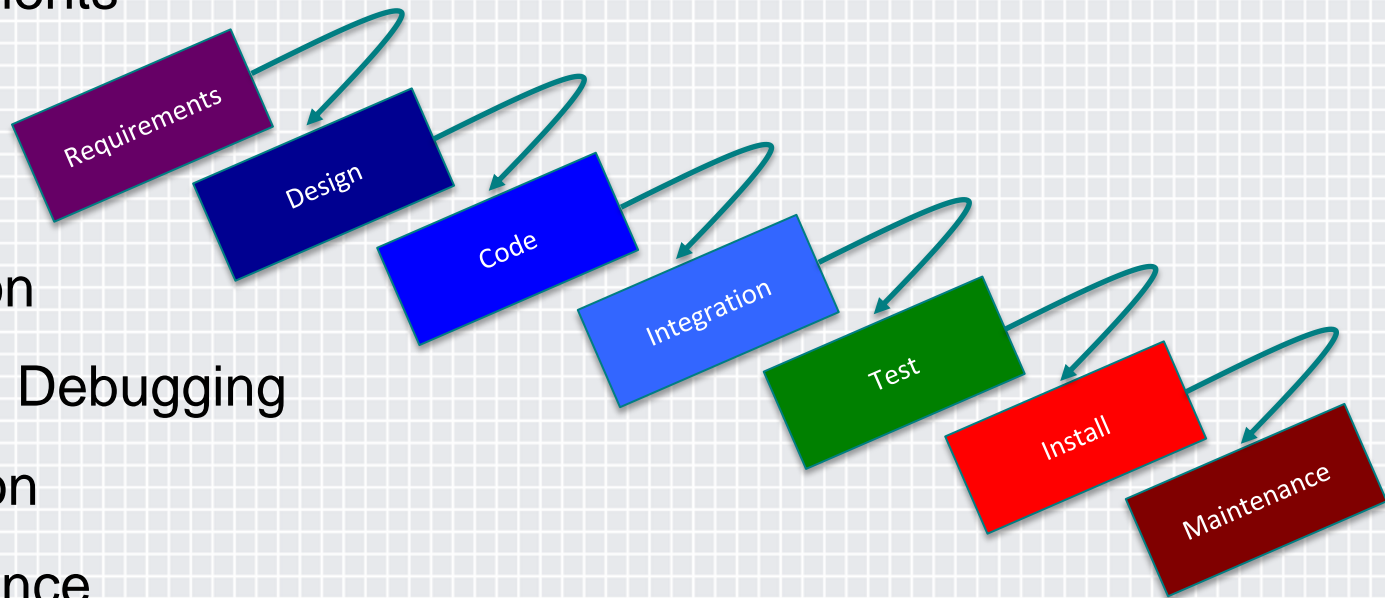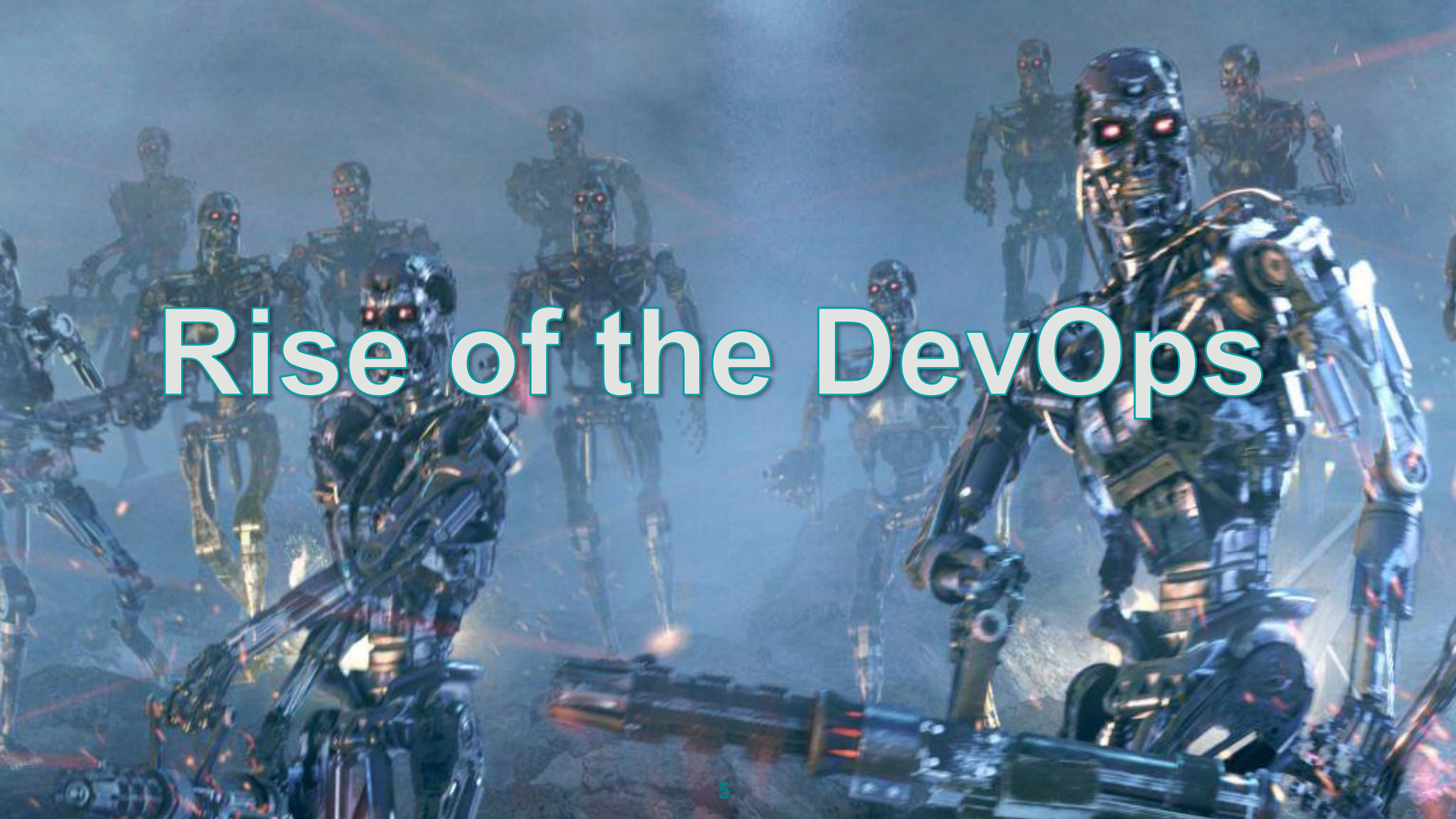
So Where Did All This Start?

◆ The traditional development methodology is a sequential design process commonly referred to as "Waterfall"

◆ Originally created in the manufacturing and construction industries where changes in scope are not typically possible due to costs

◆ First documented in software development in 1970

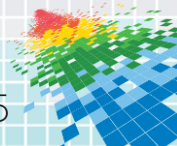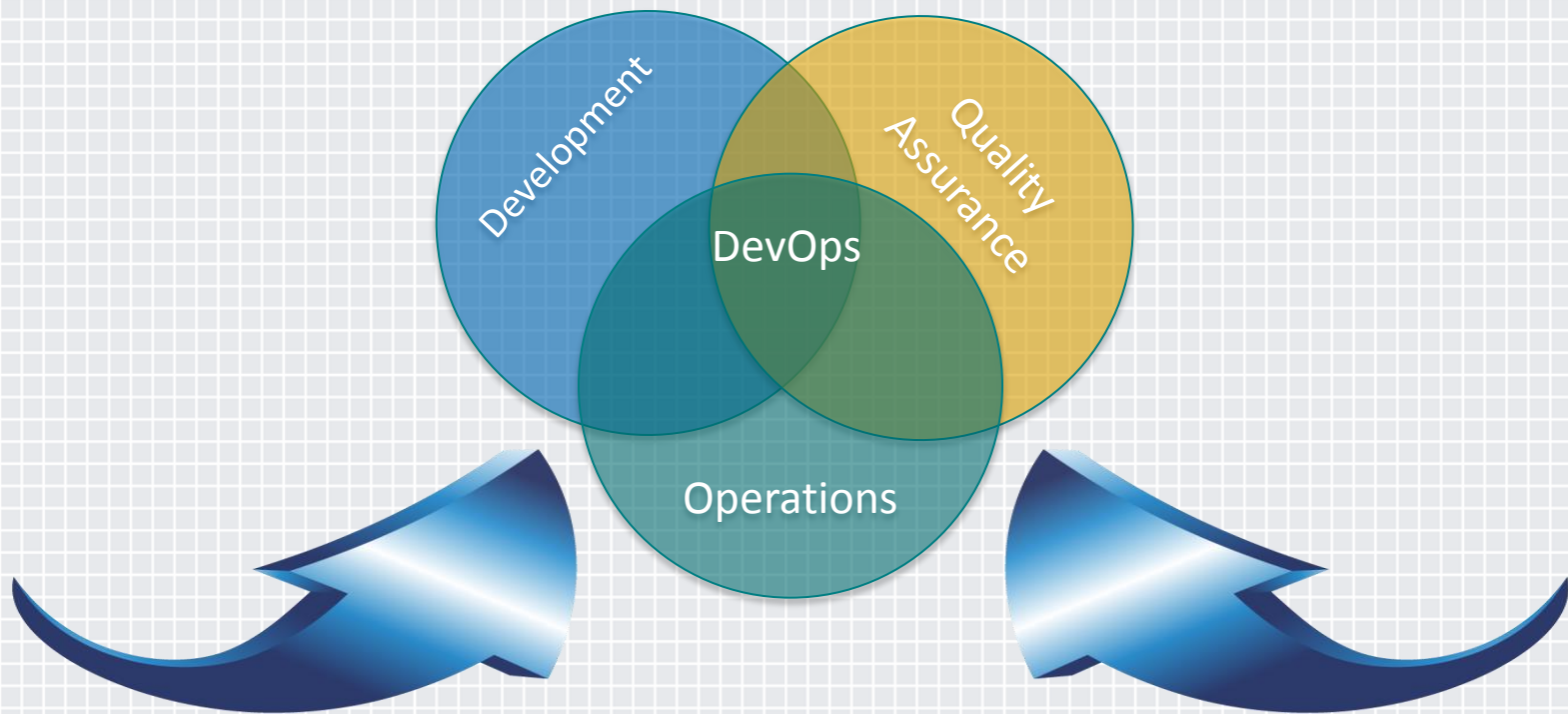◆ **For some software companies it's still in use today…**

GoodData

RSAConference2015

What's a Waterfall Look Like?

- Requirements
- Design
- Code
- Integration
- Testing & Debugging
- Installation
- Maintenance

GoodData

RSAConference2015

Rise of the DevOps

Rise of the DevOps

Development

Quality Assurance

DevOps

Operations

GoodData

RSAConference2015

Now That DevOps Rules....

GoodData

RSAConference2015

The New Waterfall

Development

Quality Assurance

DevOps

Operations

Security

GoodData

RSAConference2015
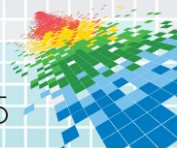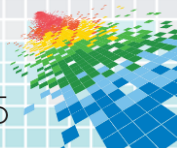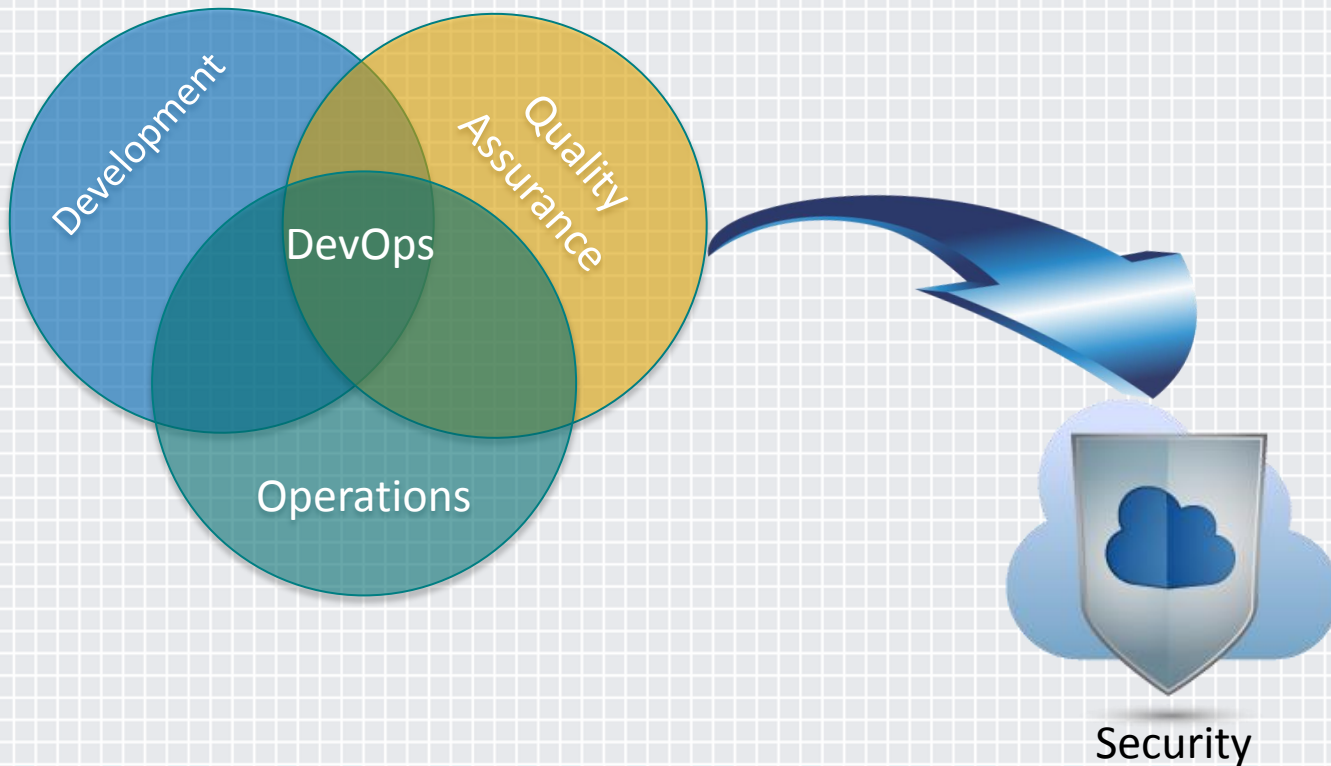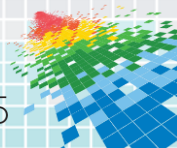
It's all about the mergers

If merging Development with Operations was so successful, why not include Security?

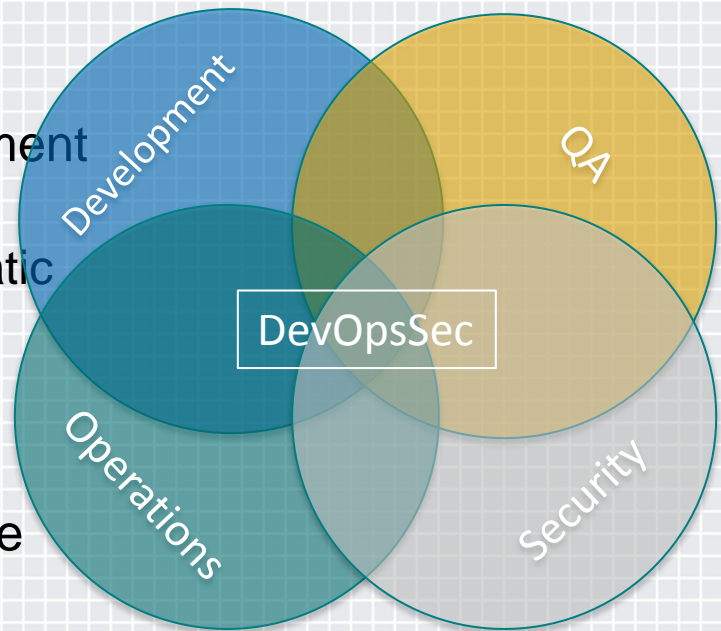"Nothing is so painful to the human mind as great and sudden change.
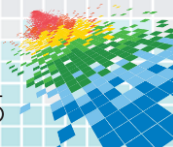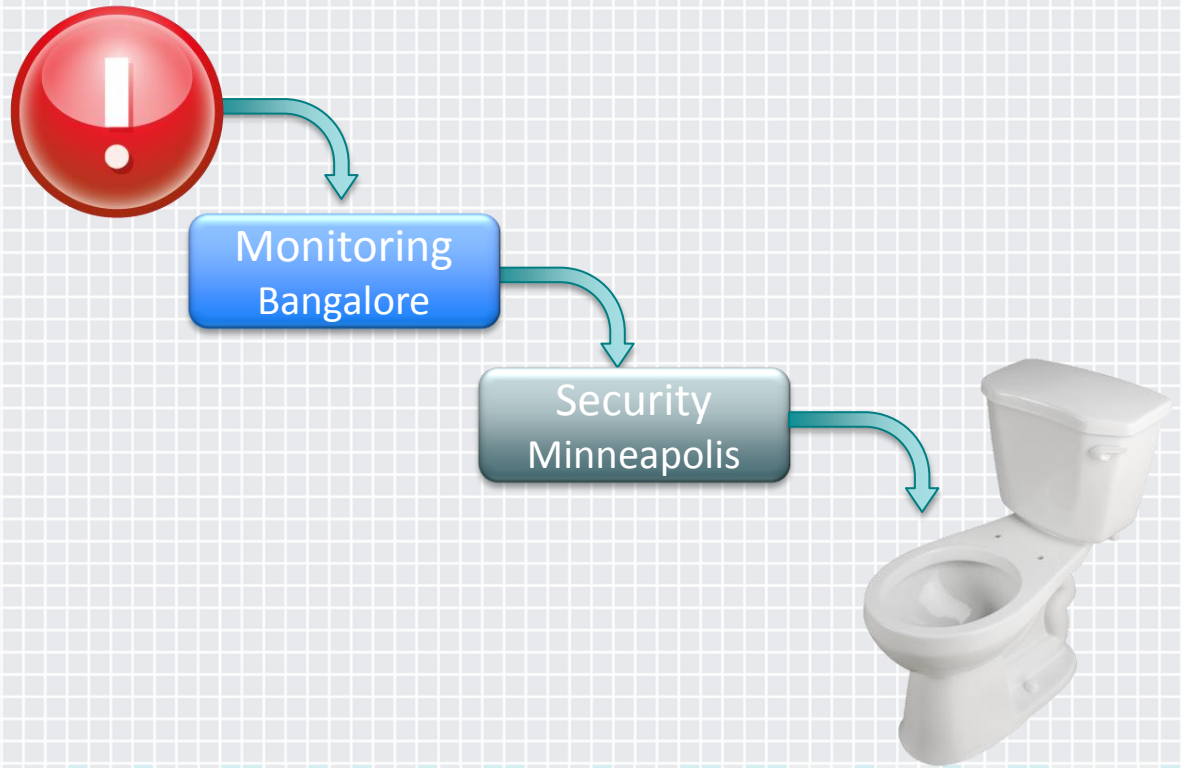
Mary Shelley, *Frankenstein*

GoodData

RSAConference2015

Along comes DevOpsSec
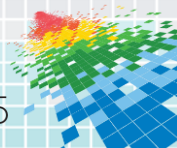
- Security is no longer at the end of the Waterfall
  - Application Security is part of the Development and tested in QA
    - Web App Testing, OWASP, PenTesting, Static Code analysis
  - Security Operations is part of Ops
    - Logging, Monitoring, IDS,
  - Infrastructure Security is part of Architecture
    - Firewalls, Proxies, IPS, Anti-virus, APT Detection

GoodData

RSAConference2015

Reduce Failures in Incident Response

Monitoring
Bangalore

Security
Minneapolis

GoodData

RSAConference2015

What Should Have Happened

GoodData

12

RSAConference2015
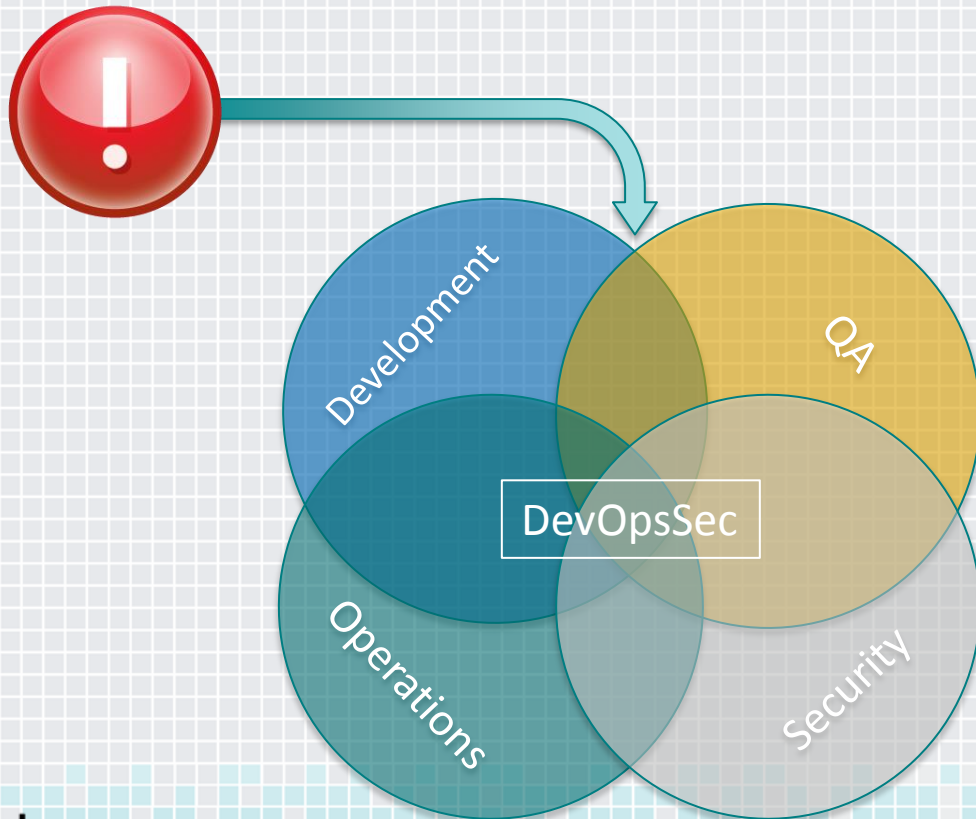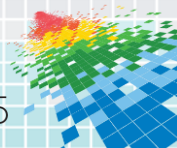
Personal Experience

Using DevOpsSec

- Shellshock – 60 minutes

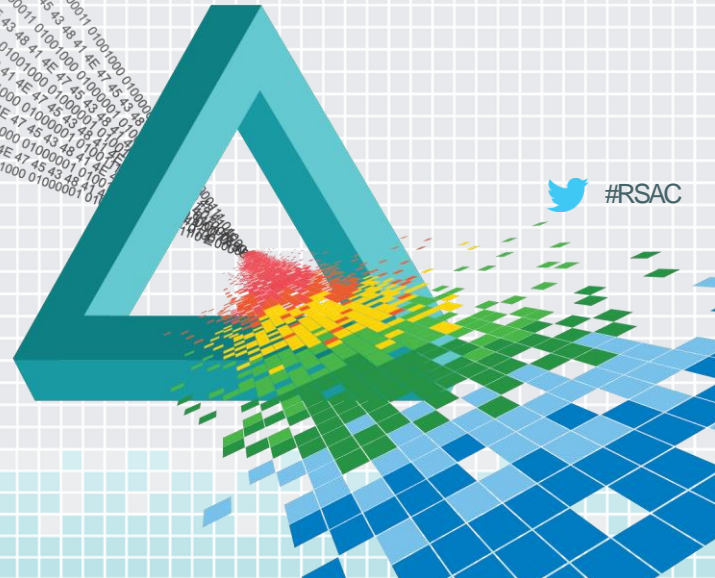- Poodle – 3 days

- Ghost – 3 days

Using traditional silos

- Shellshock – 8 weeks

- Poodle – 6 weeks

- Ghost – 8 weeks

GoodData

RSA Conference2015

COMPLIANCE is the new BLACK

GoodData

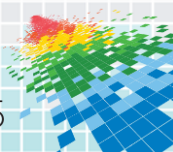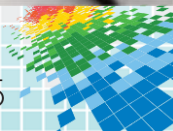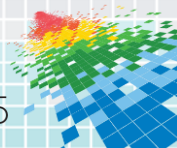RSAConference2015

Governance, Policies and Contracts…Oh My!

- **Privacy professional** – International compliance

- **Auditor** – Validate compliance

- **Documentation Specialist** – Document how to comply

- **Training** – Teach employees how to stay compliant

- **Legal** – Contractual compliance

GoodData

RSAConference2015

What Can They Do?

◆ Deliver Sprint like runs when dealing with:

   ◆ Contract negotiations to ensure they reflect what the company can delivery

   ◆ Document the requirements that come out of the contracts

   ◆ Build training programs that target subjects needed to ensure security and compliance based on the regulations they are operating in or based on the obligations in the contract

   ◆ Verify what the DevOpsSec teams are doing to provide transparency back to the customers

GoodData
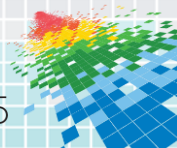
RSAConference2015
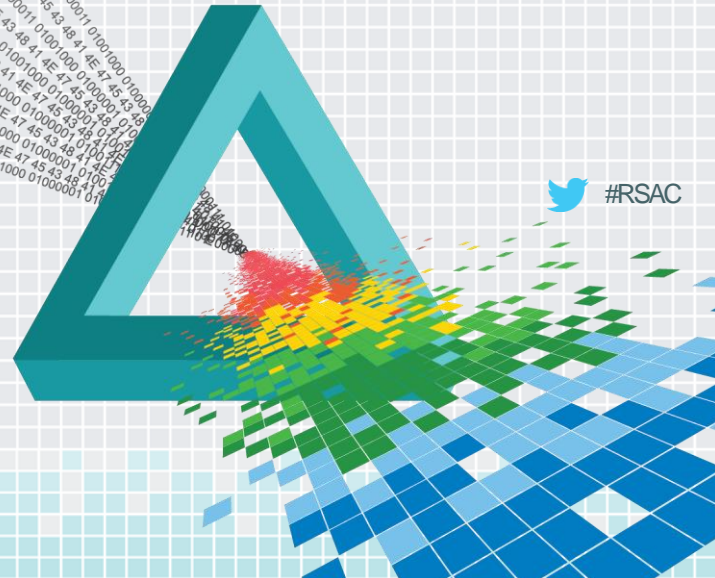
What About a Sales Team?

- **Sales Rep** – manage the sale
- **Compliance** – manage the security & privacy
- **Services** – manage the software requirements
- **Account Mgmt.** – manage the customer
- **Finance** – manage the terms
- **Legal** – manage the contract

GoodData

RSA Conference2015
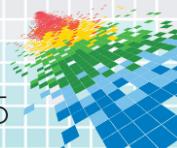
What can YOU do?

◆ Find an internal example of where you "waterfall" your process

◆ Create a scrum team using representatives from each of the layers of the waterfall

◆ Enable the team to operate and make decisions with autonomy

◆ Review the effectiveness of the autonomous team

◆ Find other places in the Org to make changes

GoodData

RSA Conference2015

Further Reading

- Security monitoring – Penetration testing meets monitoring
  - Gareth Rushgrove
  - https://speakerdeck.com/garethr/security-monitoring-penetration-testing-meets-monitoring

- DevOpsSec: Appling DevOps Principles to Security
  - Nick Galbreath
  - http://www.slideshare.net/nickgsuperstar/devopssec-apply-devops-principles-to-security/

GoodData

RSAConference2015

Thank You!

William (Bil) Harmer

William.harmer@gooddata.com

@wilharm3

GoodData

RSAConference2015