Building_the_Coded_Enterprise

chef.io

Continuous Compliance in a DevSecOps World

Why Compliance as Code Matters

Presented By

Galen Emery
Lead Compliance Architect
Chef Software

Adam Montville
Chief Product Architect
Center for Internet Security

Center for Internet Security®

Toward Compliance Agility
Foundational Automation

Adam Montville, Chief Product Architect

2019-10-30

About CIS

- **Non-profit** using the power of a global community to develop best practices for securing IT systems and data
  - Founded in the year 2000
  - 200+ employees across the U.S.
- **Vision:** Leading the community to secure our connected world.
- **Mission:** Identify, develop, validate, promote, and sustain best practice solutions for cyber defense. Build and lead communities to enable an environment of trust in cyberspace.

Confidence in the Connected World

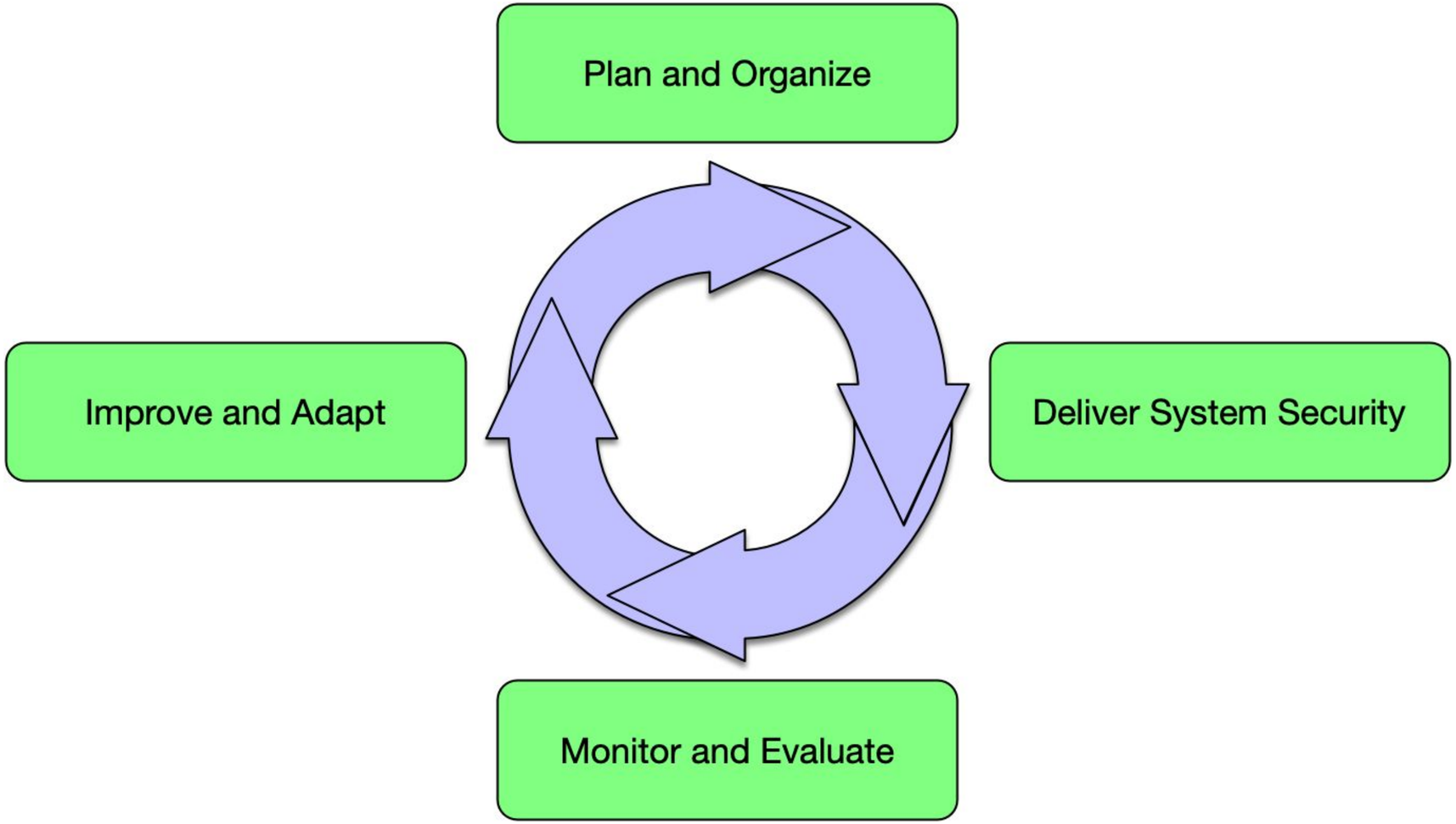
Start Secure. Stay Secure.®

Security Best Practices

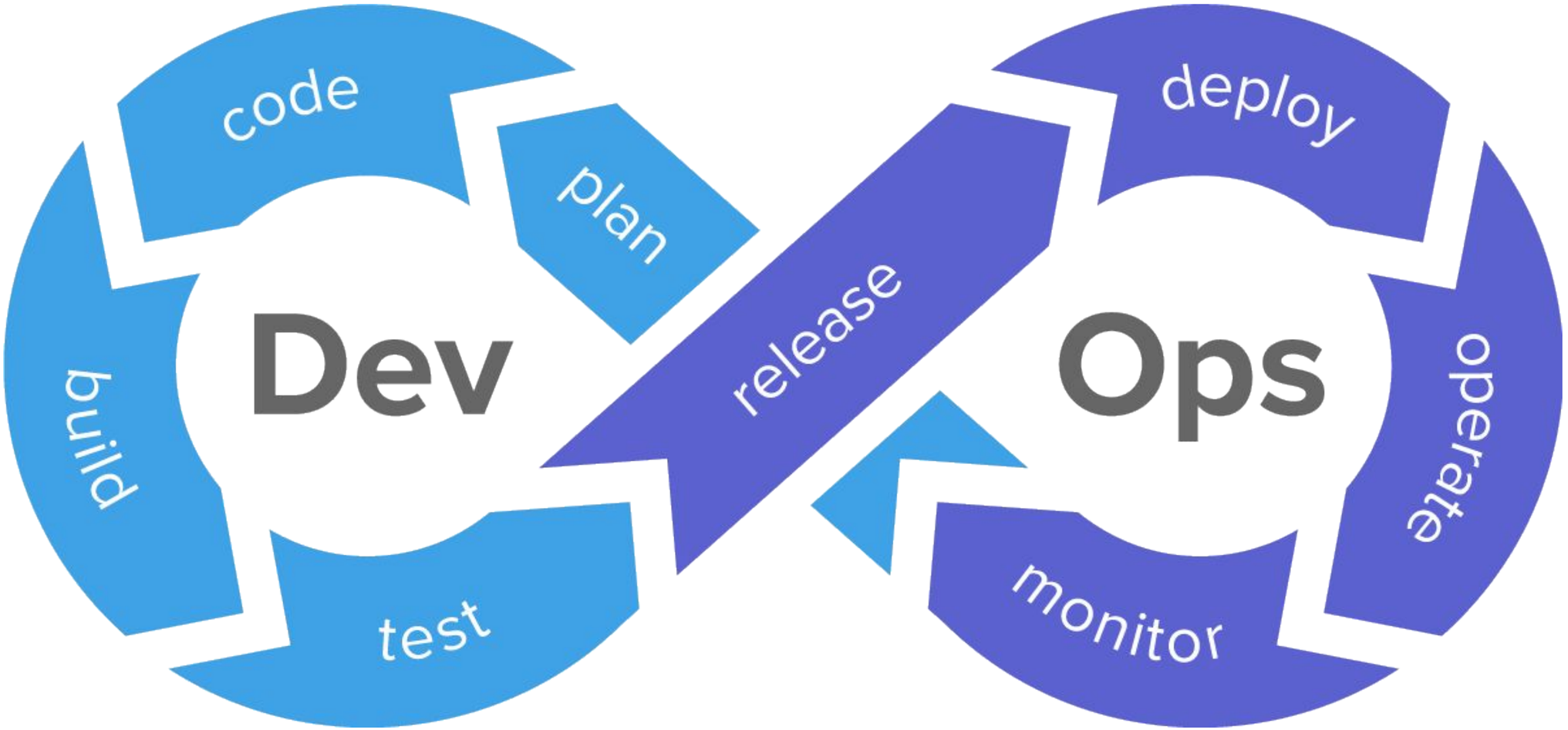
CIS Controls

CIS Benchmarks

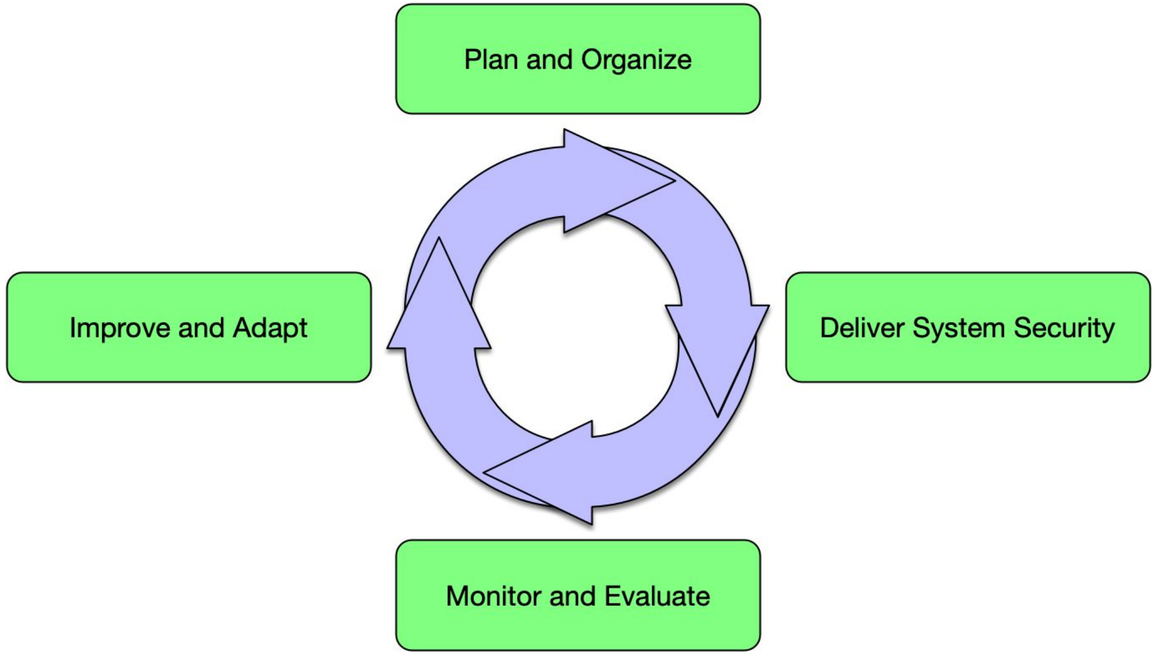
Traditional Compliance Paradigm

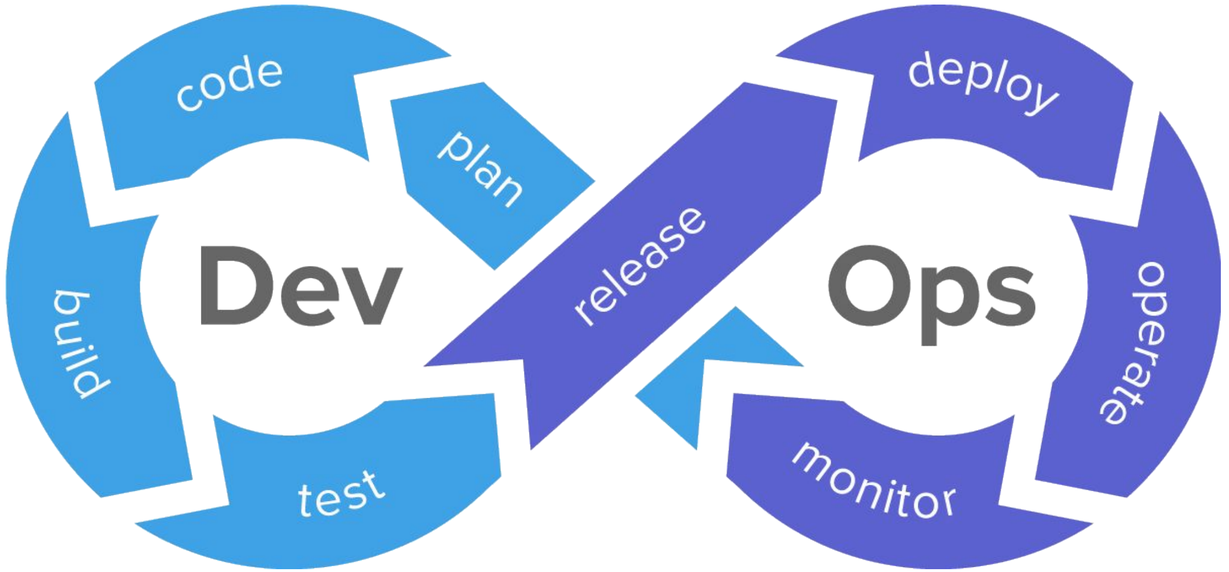


Devops Paradigm



What are the real differences?





How can Security Programs become DevSecOps?

- Articulate security requirements in code-friendly ways
- Empower your product/service teams
- Think iteratively
- Maximize CI/CD

My (Boring?) Parting Thoughts

2010

- Overall Membership: < 300
- Vendor Members: ~10

2019

- Overall Membership: 10,000+
- Vendor Members: 50+

2018

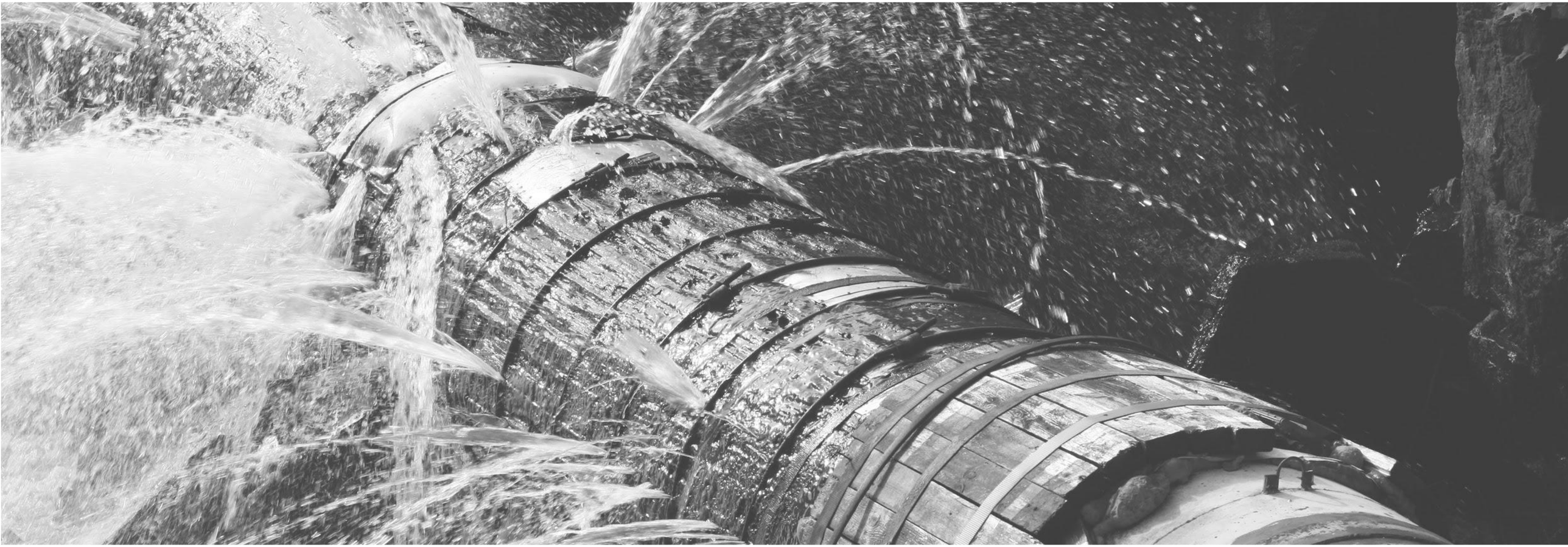
Benchmark Downloads: 1M+

Compliance as Code

Why does it matter?

Plugging Security Holes

It never ends



The Delicate Balance

Security & Compliance: The Challenge

Security & Compliance are non-negotiable, but too often impede velocity and create inefficiencies.

- Security reviews at the end of the dev process block progress
- Audit time commitments distract staff from high value work
- Limited visibility and collaboration create undue risk

PERCEPTION

81%

Among IT professionals, 81% believe InfoSec policies inhibit agility and speed.[1]

77%

Information Security professionals agree that their policies inhibit agility and speed.[1]

1—Gartner, How to Seamlessly Integrate Security Into DevOps (2016)

Is Security Slowing Digital Transformation?

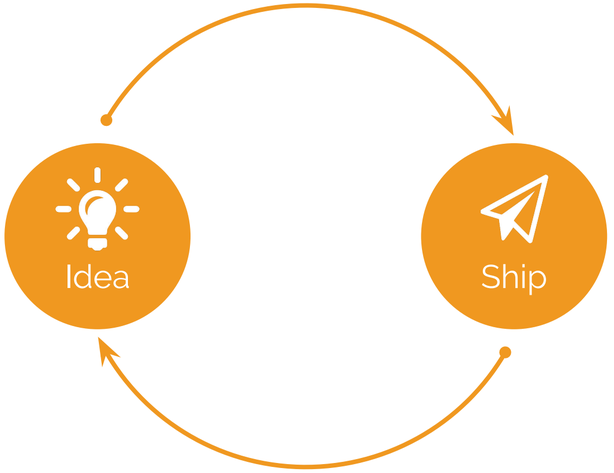
Shipping apps and experiences quickly is key to business growth

Problem

Information Security teams aren't set up to act rapidly

- 71% of IT orgs adopt DevOps[1]
- DevOps teams work fast
- Continuous delivery of change
- Slow response from InfoSec
- Vulnerabilities and risk

Requirement



PERCEPTION

81%

Among IT professionals, 81% believe InfoSec policies inhibit agility and speed.[1]

77%

Information Security professionals agree that their policies inhibit agility and speed.[2]

1—Rightscale, State of the Cloud 2017
2—Gartner, How to Seamlessly Integrate Security Into DevOps (2016)

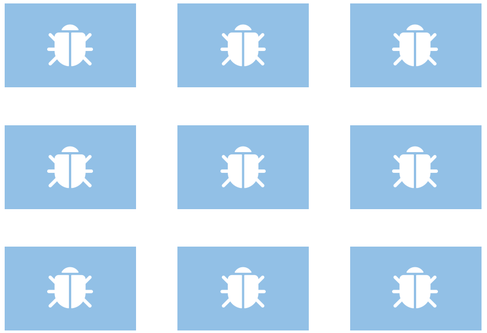
Disrupt or be disrupted. Outperform the competition with digital transformation.

The current state of information security

Despite velocity gains by other teams, InfoSec lags behind

⅔ of breaches took months or longer to discover [1]

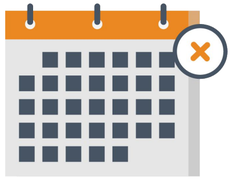
Since 2014, more than 90% of exploits observed use only nine known vulnerabilities



And after a compliance violation or security vulnerability is discovered:

1 in 2 teams need days or longer to remediate, 1 in 4 need weeks or months

30% need days



28% need weeks or months

Source: Verizon Data Breach Report 2018

Source: Chef Survey 2017

The continuous demand to increase speed potentially amplifies existing issues

Traditional Approaches Exacerbate Pain

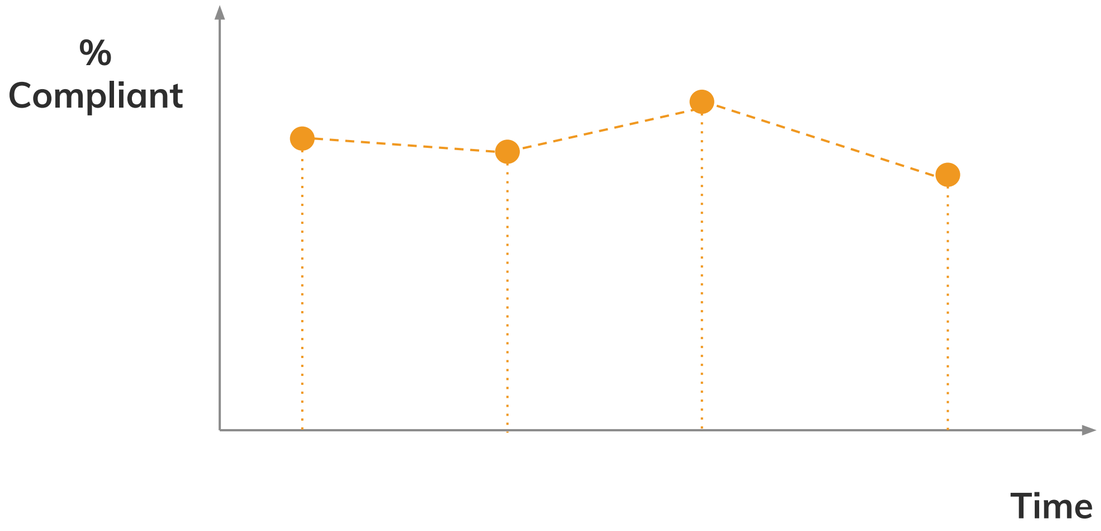
Security reviews:

- Are often manual (slow)
- Rely on scanning tools that generate too much data to effectively manage
- Catch problems too late in the development cycle to economically fix
- Don't manage exceptions appropriately

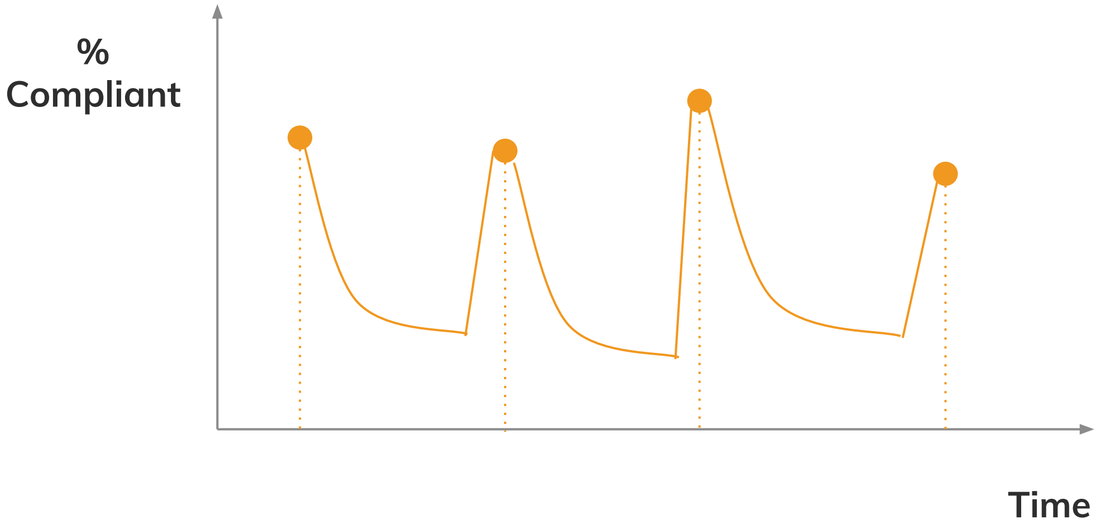
Periodic Audits Do Not Tell the Whole Story

They leave open windows of risk

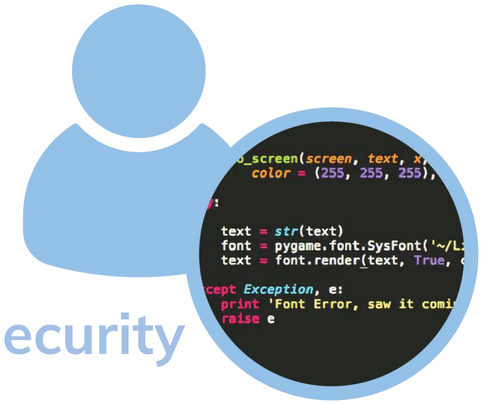
Assumed Compliance Levels



Actual Compliance Levels



Different Teams Speak Different Languages

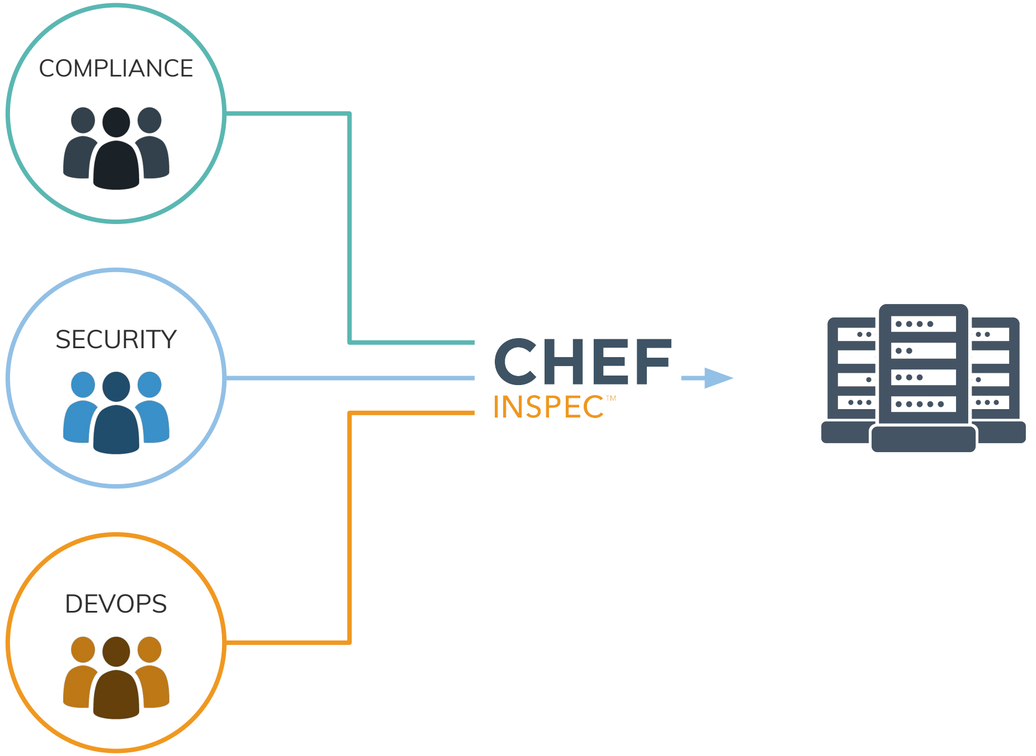


Bridging the Gap - Security Meets Operations

The Old Way
People working directly on machines

The Modern Way
People automating machines using code

The New Way
Shared tooling across organizations



Manage Security and Compliance as Code

Code enables continuous compliance

Collaborate

Code is an unambiguous common language

Enable scalability

Code scales across complexity sprawl

Shift left

Test throughout the software delivery process

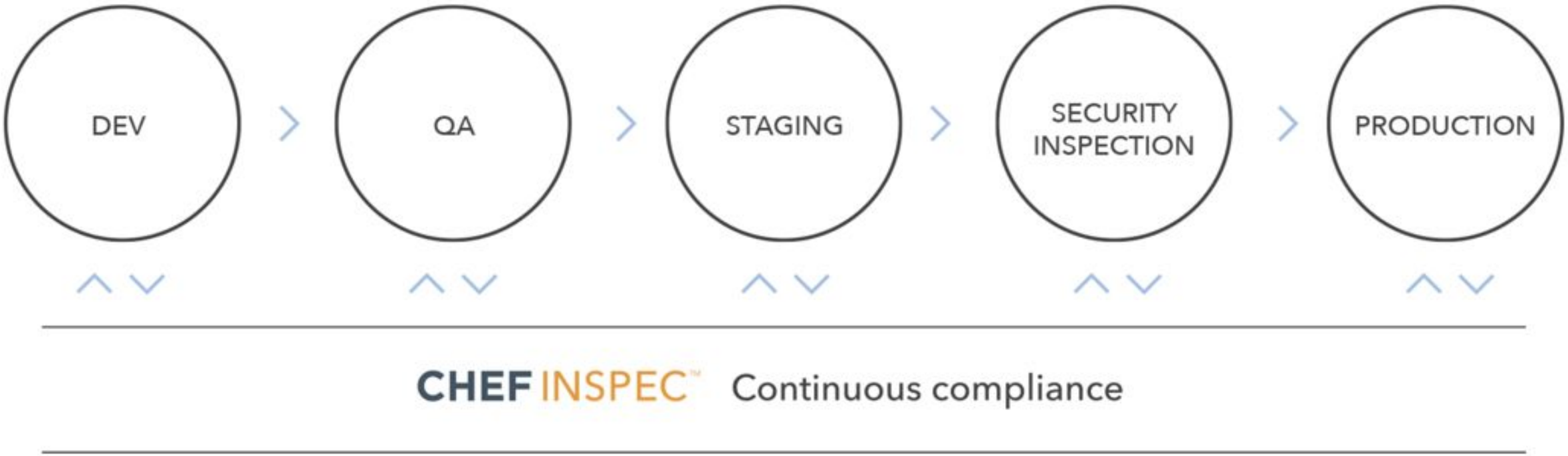
Continuous visibility

Monitor ongoing basis to eliminate windows of risk

```
control 'ssh-1234' do
  impact 1.0
  title 'Server: Set protocol version to SSHv2'
  desc "
    Set the SSH protocol version to 2. Don't use
legacy
    insecure SSHv1 connections anymore...
  "

  describe sshd_config do
   its('Protocol') { should cmp 2 }
  end
end
```

Continuous Compliance as Code



Customer Evidence - Compliance Automation

NOVARTIS

Every resource and app in HPC environment is **automatically qualified as compliant with FDA standards** before deployment; previously this was only checked four times per year

SCHOLASTIC

Remediated Shellshock security issues across entire cloud infrastructure in a single hour, a process that took more than a day for its smaller non-cloud infrastructure

Web & Media Giant

Can patch entire infrastructure of **250,000 nodes within 6 hours** of a patch being made available

Top 5 Global Bank

Eliminated $2M in security and network management software toolset costs while reducing remediation time across thousands of servers from weeks to one hour

CIS Security Software Certification for CIS Benchmark(s)

- CIS Benchmark for Amazon Web Services Foundations Benchmarks, Level 1
- CIS Benchmark for Amazon Web Services Foundations Benchmarks, Level 2
- CIS Benchmark for Google Cloud Platform Foundation, Level 1 Profile
- CIS Benchmark for Google Cloud Platform Foundation, Level 2 Profile
- CIS Benchmark for CIS Red Hat Enterprise Linux 7 Level 1 Server
- CIS Benchmark for CIS Red Hat Enterprise Linux 7 Level 2 Server
- CIS Benchmark for Microsoft Azure Foundations Level 1

CIS Center for Internet Security®

First CIS Partner Certified on AWS, Azure, and GCP

chef.io