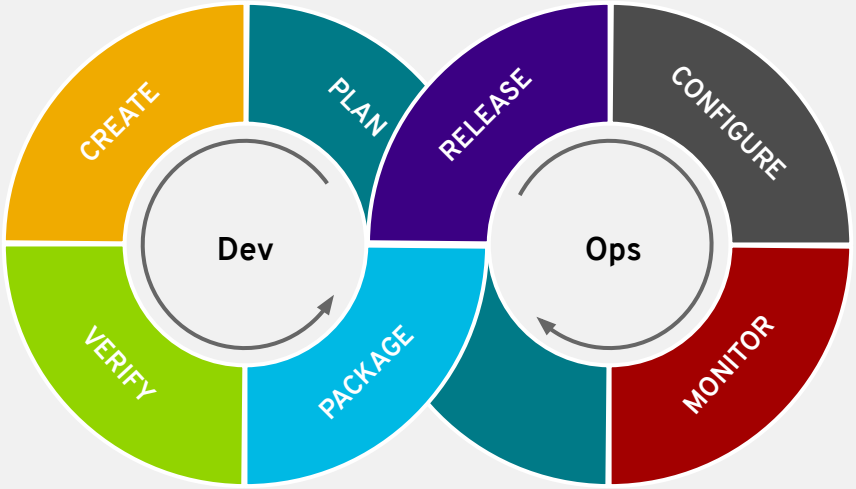
Security in a DevSecOps World

Rich Lucente
Principal Solutions Architect

THE DevOps MODEL



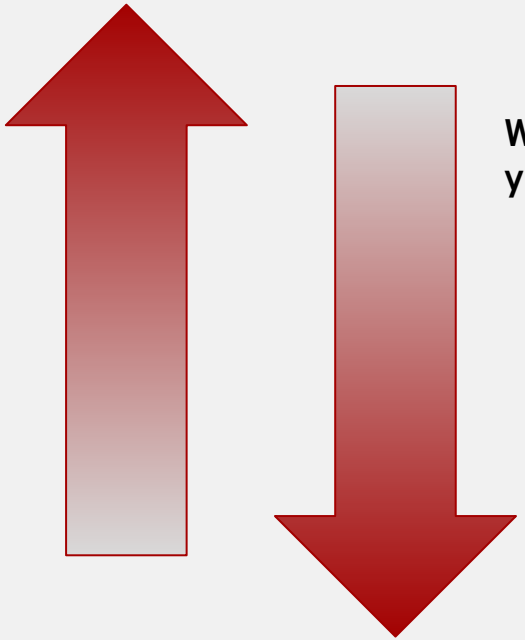
THE DIGITAL WORLD:
THE COST OF SECURITY BREACHES

Total average costs are increasing:

2016 $4.0 million

2015 $3.8 million

2014 $3.5 million

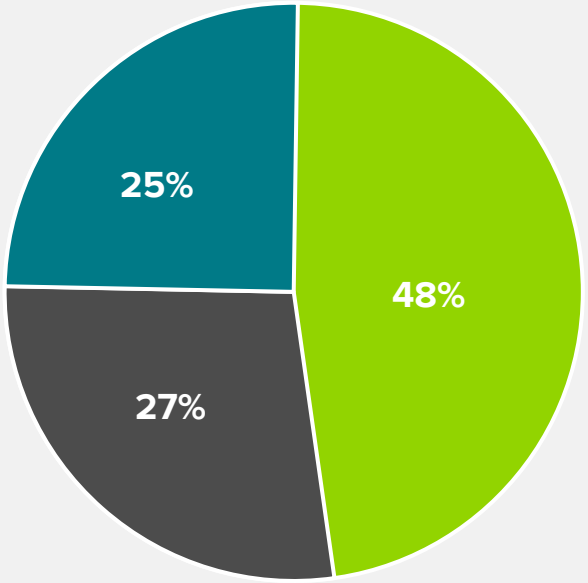


While “soft” costs are impacting your business

- Disruption
- Loss of public trust
- Brand erosion
- etc

2016 Cost of Data Breach Study: Global, June, 2016. Ponemon Institute LLC© Research Report

THE DIGITAL WORLD: MULTIPLE SOURCES OF RISKS



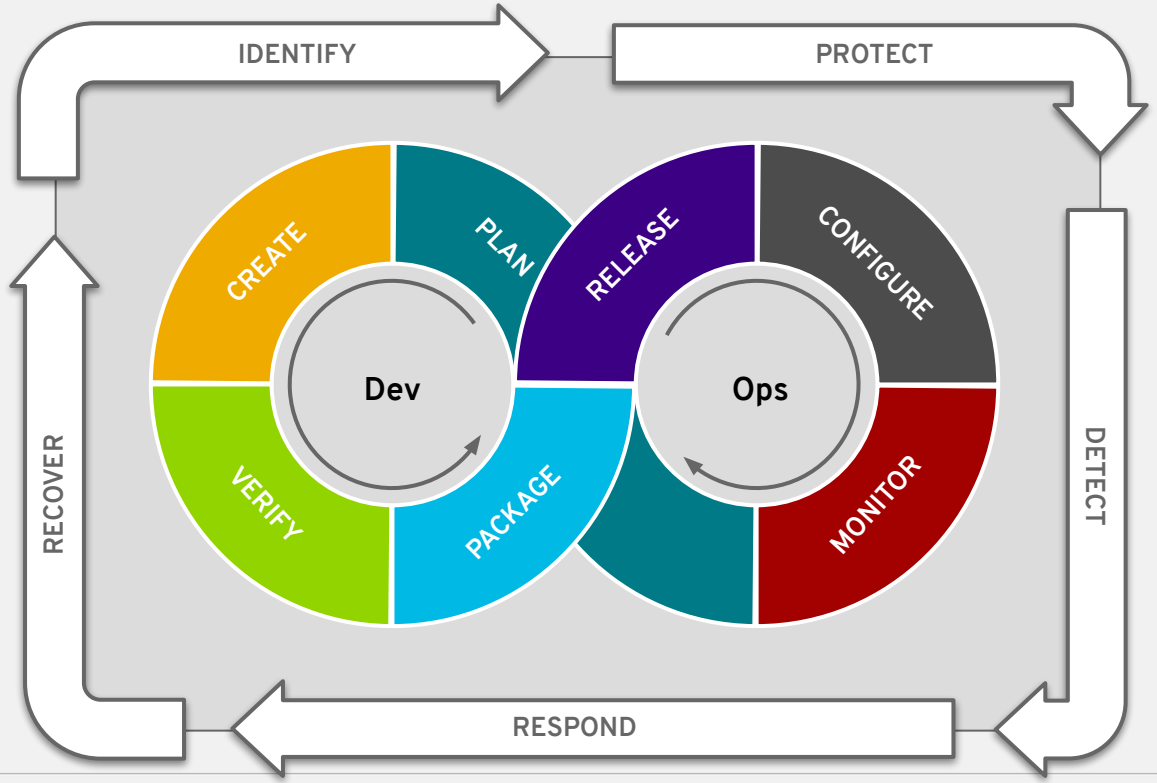
Cyber criminals and hackers are more:

- Dangerous
- Sophisticated
- Global
- Profit-oriented
- Nation state sponsored

Human error System glitch Malicious or criminal attack

2016 Cost of Data Breach Study: Global, June, 2016. Ponemon Institute LLC© Research Report

THE DevSecOps MODEL



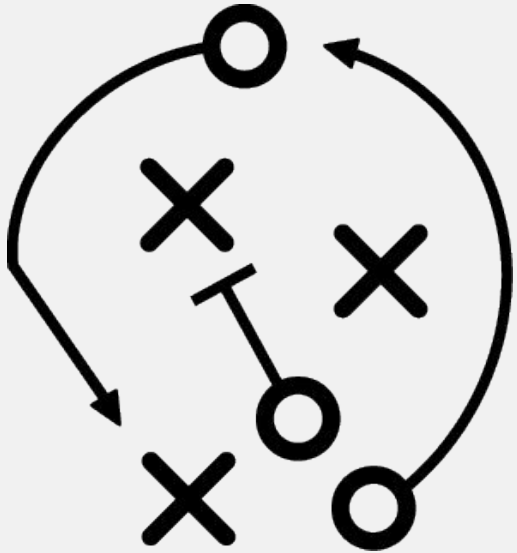
CHALLENGES IN THE DIGITAL WORLD

For Developers

- Developers must ensure security is baked-in
- Accepting that sometimes “Worse is better” [1]
- Must adapt to new development models

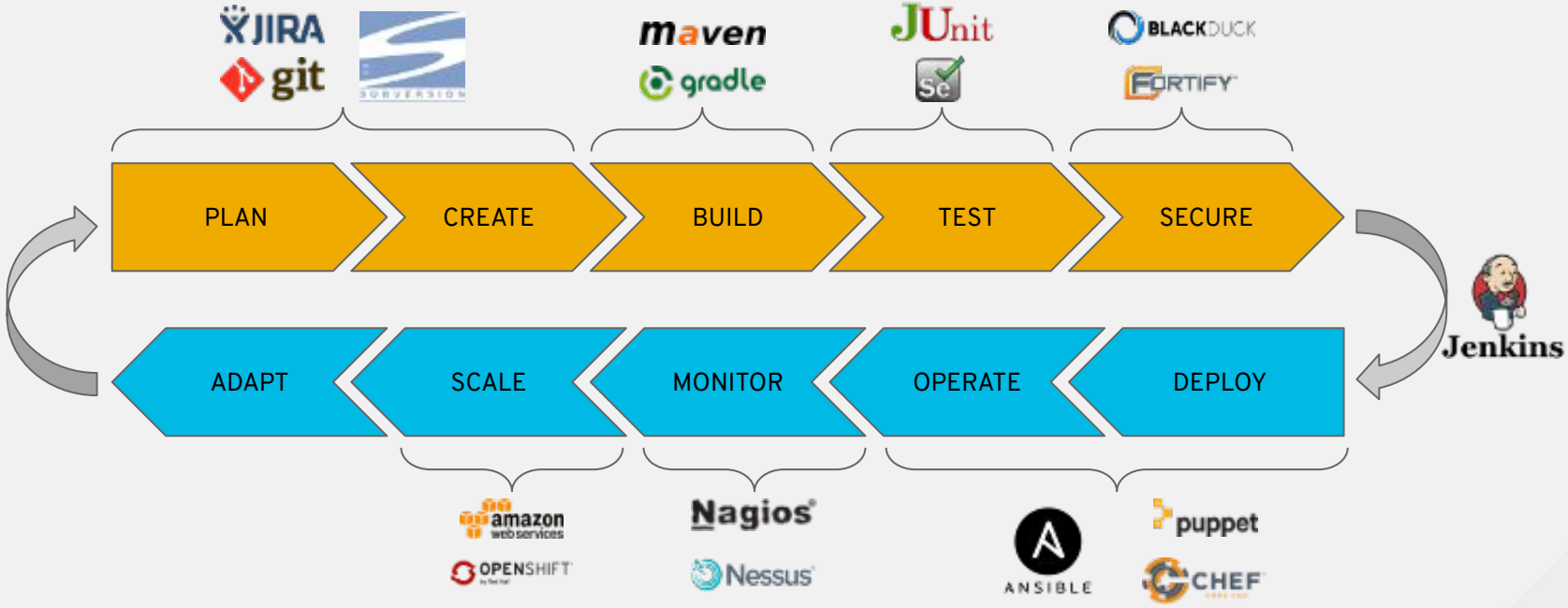
For IT Operations and IT Security

- I.T. Operations and Security must adapt to DevOps
- Security cannot be an afterthought
- Increasing use of automation



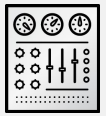
[1] https://en.wikipedia.org/wiki/Worse_is_better

AUTOMATION: THE KEY TO DevSecOps



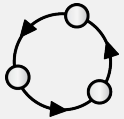
THE ULTIMATE GOAL: ACCELERATED ATOs

Three capabilities to help meet the objective



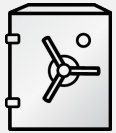
CONFIGURATION MANAGEMENT:

- Maintaining consistency for security and performance



AUTOMATION:

- Interconnect systems so that they self-regulate
- Provide repeatable processes that reduce errors and save time



SECURITY CONTENT AUTOMATION PROTOCOL (SCAP):

- Standardized expression and reporting

CONFIGURATION MANAGEMENT

Knowledge of the information assurance baseline

- AKA Security Configuration Management (SCM)
- Maintains the security features and changes made to software and hardware including documentation for the lifecycle of a system
- Determines the appropriate security configuration to apply to ensure a secure configuration state
- Ensures that the configuration baseline is documented and maintained

ANSIBLE

CHEF™

AUTOMATION

Repeatable it tasks across the entire network without human error

Do this...

Orchestration	Configuration Management	Application Deployment	Provisioning	Continuous Delivery	Security and Compliance

On these...

Firewalls	Load Balancers	Applications	Containers	Clouds
Servers	Infrastructure	Storage	Network Devices	**And more...**

Result: known configurations with repeatable tasks that can quickly change the security posture

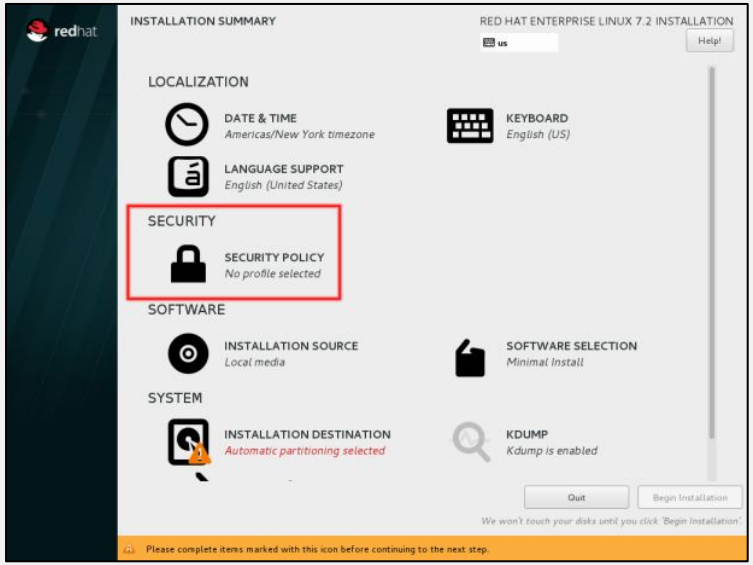
SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

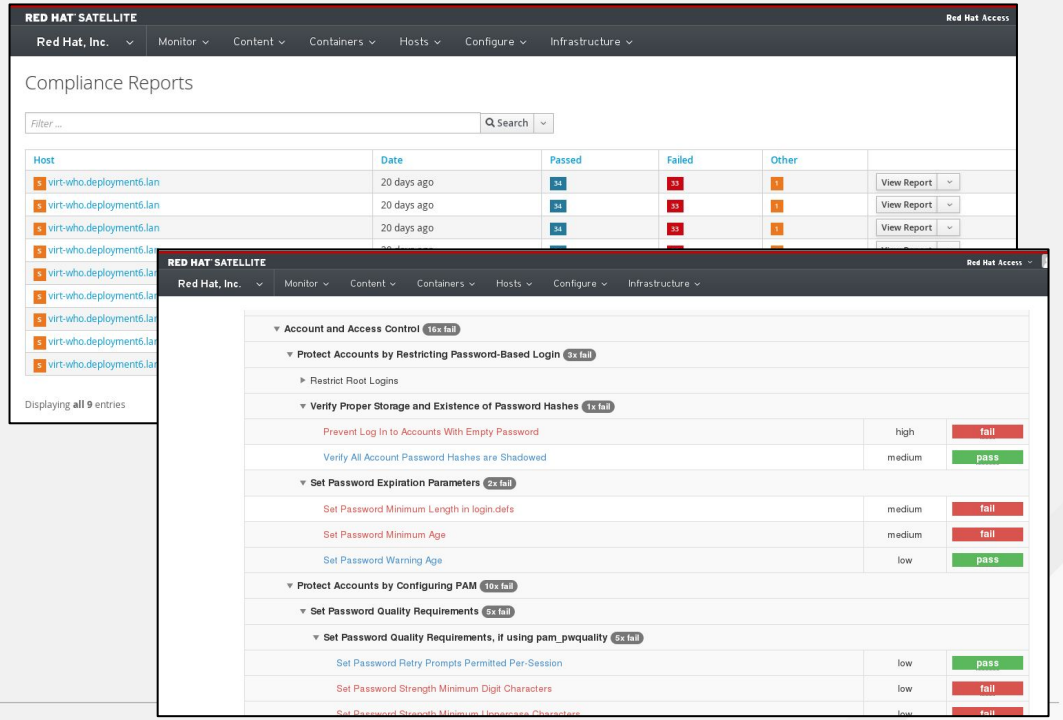
Maintaining proactive security configuration

- **Determine** the specific security baseline to achieve compliance
- **Obtain** a security checklist suitable for machine processing
- **Quickly identify the current state** of the computer infrastructure
- **Remediate** – perform **corrective operations** for items that did not meet the requirements
- **Automated approach** – perform compliance analysis and corrective operations (remedial actions) in a **machine-controlled, unattended way** on a **regular** basis
- **Utilize** proper software tools to carry out these tasks with **minimal effort**, and at the same time attempt to reduce any required **outage periods** related to these tasks to a minimum.

SCAP INTEGRATION

Maintaining compliance via scanning and remediation is everyone's job



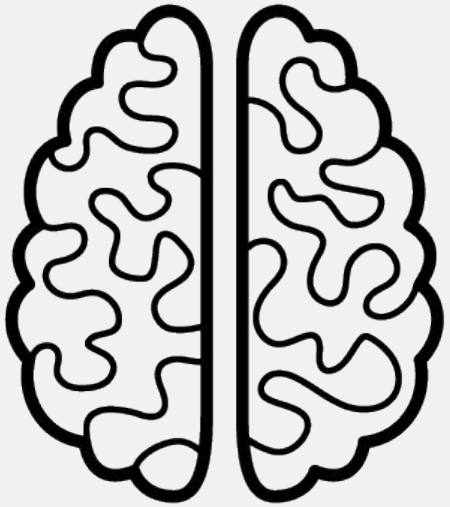


redhat.

...BUT IT IS **MORE** THAN AUTOMATION

A cultural shift is also needed

- It takes time to implement a new mindset
- Everyone is responsible for security
  - Security early and often (shift left)
  - Maintain quality, safety and privacy
- Helpful ideas
  - Integrate security processes into CI/CD pipeline
  - Build a security knowledge base
  - Coach developers on security
  - Open communication on security
  - Take full advantage of automation



COMPLIANCE AS CODE PROJECT

Bake security into the secret sauce

What it is:

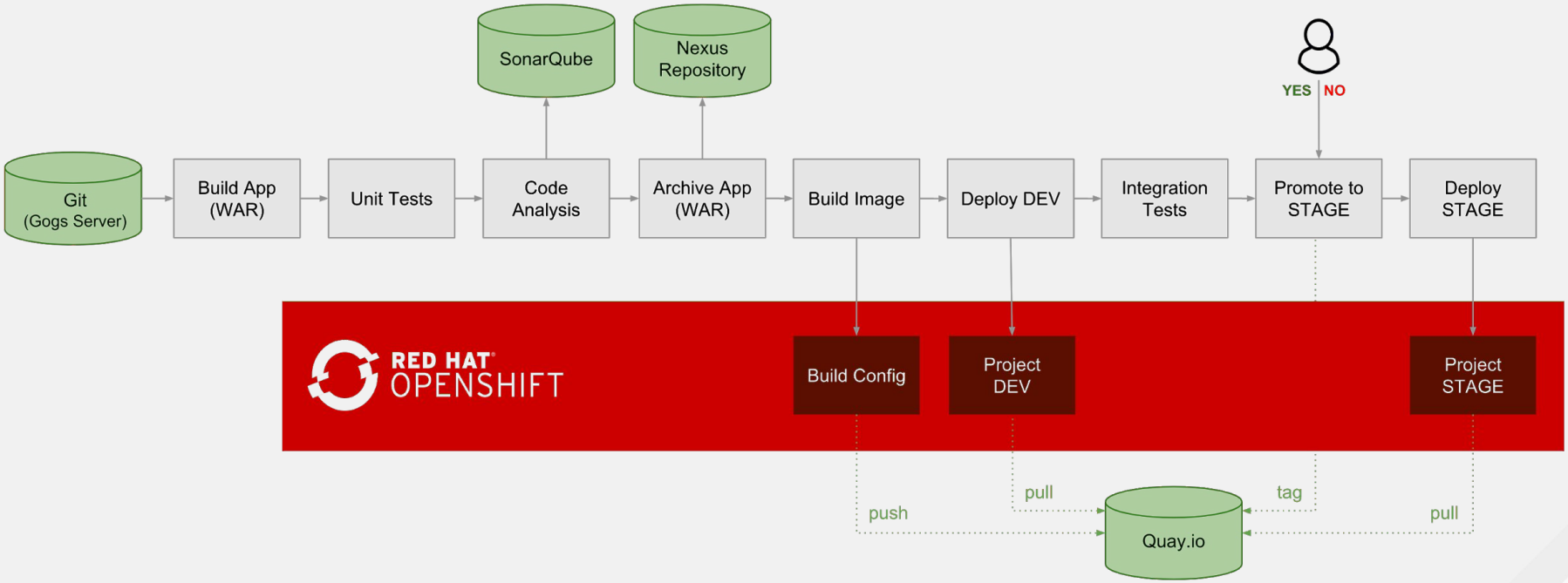
- Promotes risk reduction strategy via enforced compliance
- Process to consistently apply security policy
- Automate the generation of compliance artifacts
- A method for repeatable, shareable and verifiable results
- Easily Integrated into the CI/CD Pipeline and Operations

What it is not:

- The ultimate security solution

https://github.com/ComplianceAsCode

DevSecOps Demo


SonarQube
Nexus Repository
YES
NO
Git (Gogs Server)
Build App (WAR)
Unit Tests
Code Analysis
Archive App (WAR)
Build Image
Deploy DEV
Integration Tests
Promote to STAGE
Deploy STAGE
RED HAT OPENSHIFT
Build Config
Project DEV
Project STAGE
push
pull
tag
pull
Quay.io

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHat

youtube.com/user/RedHatVideos