Pivotal

Transform your Security Team with DevOps

Paul Czarkowski
@pczarkowski

Pivotal

Transform your DevOps Practice with Security

Paul Czarkowski
@pczarkowski


HEY THERE
I'M A DEVELOPER ADVOCATE
memegenerator.net

Agenda

- Who I Am
- Compliance
- DevOps
- DevOps + Compliance
- Q+A

Pivotal

Pivotal

What is Compliance ?

Self Imposed

- CIS Controls / Benchmarks
- Security Technical Implementation Guide (STIG)
- Allowed opensource licenses

Regulatory

- PCI (US)
- HIPAA (US)
- Sarbanes-Oxley (US)
- EU GDPR
- NZ Information Security Manual (NZISM)

Compliance

Specifications

Documentation of requirements that need to be met in order to be compliant.

- PDFs
- Verbose

Controls

Checklists

Practice, Policy or Procedure established to meet compliance requirements.

- Spreadsheets
- Checklists
- Sharepoint Pages

Audit

Verification

Validation of compliance based on Controls in place.

- Checklists
- External Auditors

Example of Compliance Specifications

The SSH daemon must be configured to use only the SSHv2 protocol.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-38607	RHEL-06-000227	SV-50408r1_rule		High

Description

SSH protocol version 1 suffers from design flaws that result in security vulnerabilities and should not be used.

STIG	Date
Red Hat Enterprise Linux 6 Security Technical Implementation Guide	2017-03-01

Details

Check Text (C-46165r1_chk)

To check which SSH protocol version is allowed, run the following command:

grep Protocol /etc/ssh/sshd_config

If configured properly, output should be

Protocol 2

If it is not, this is a finding.

Fix Text (F-43555r1_fix)

Only SSH protocol version 2 connections should be permitted. The default setting in "/etc/ssh/sshd_config" is correct, and can be verified by ensuring that the following line appears:

Protocol 2

Example of Compliance Specifications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

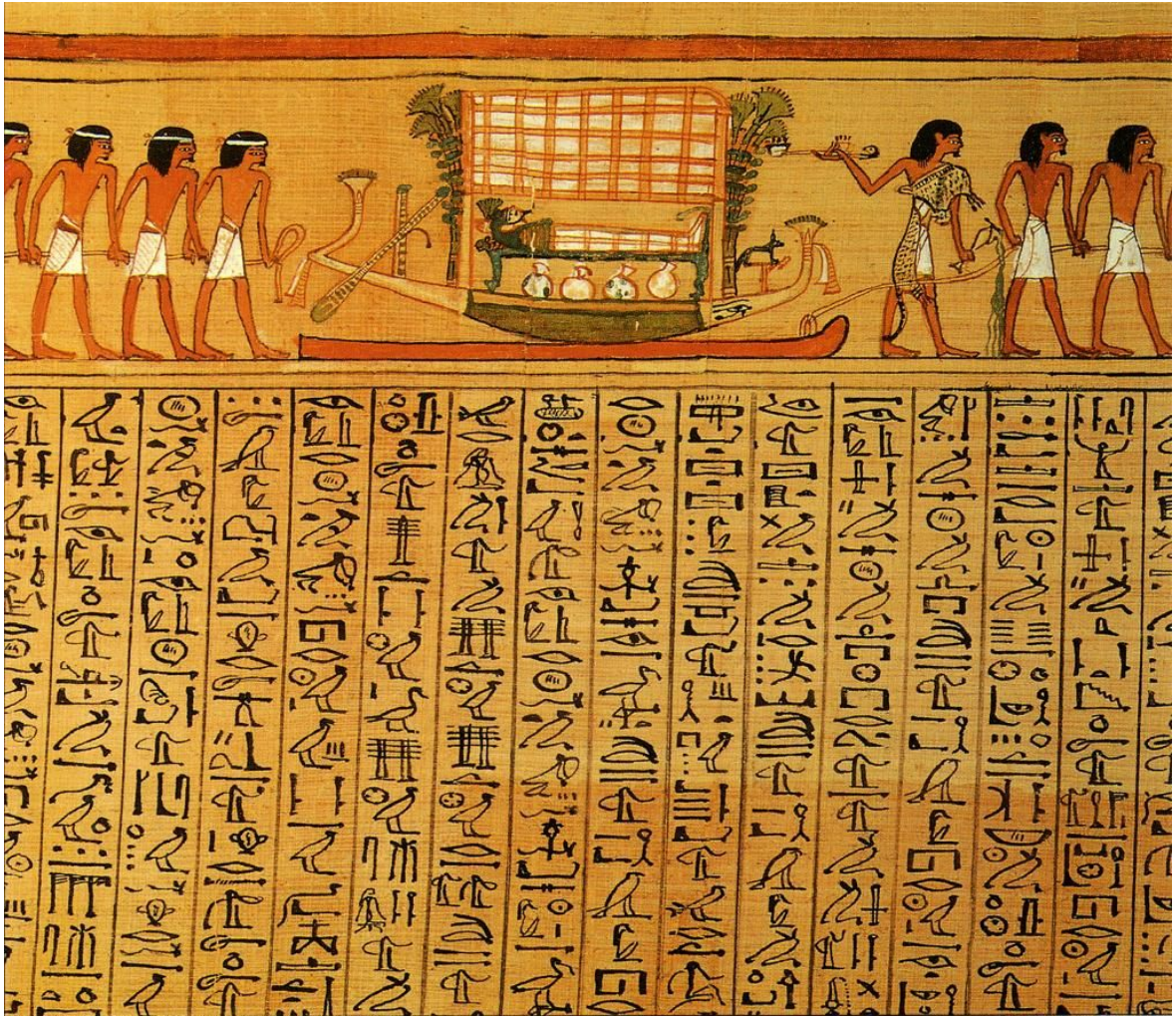
To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

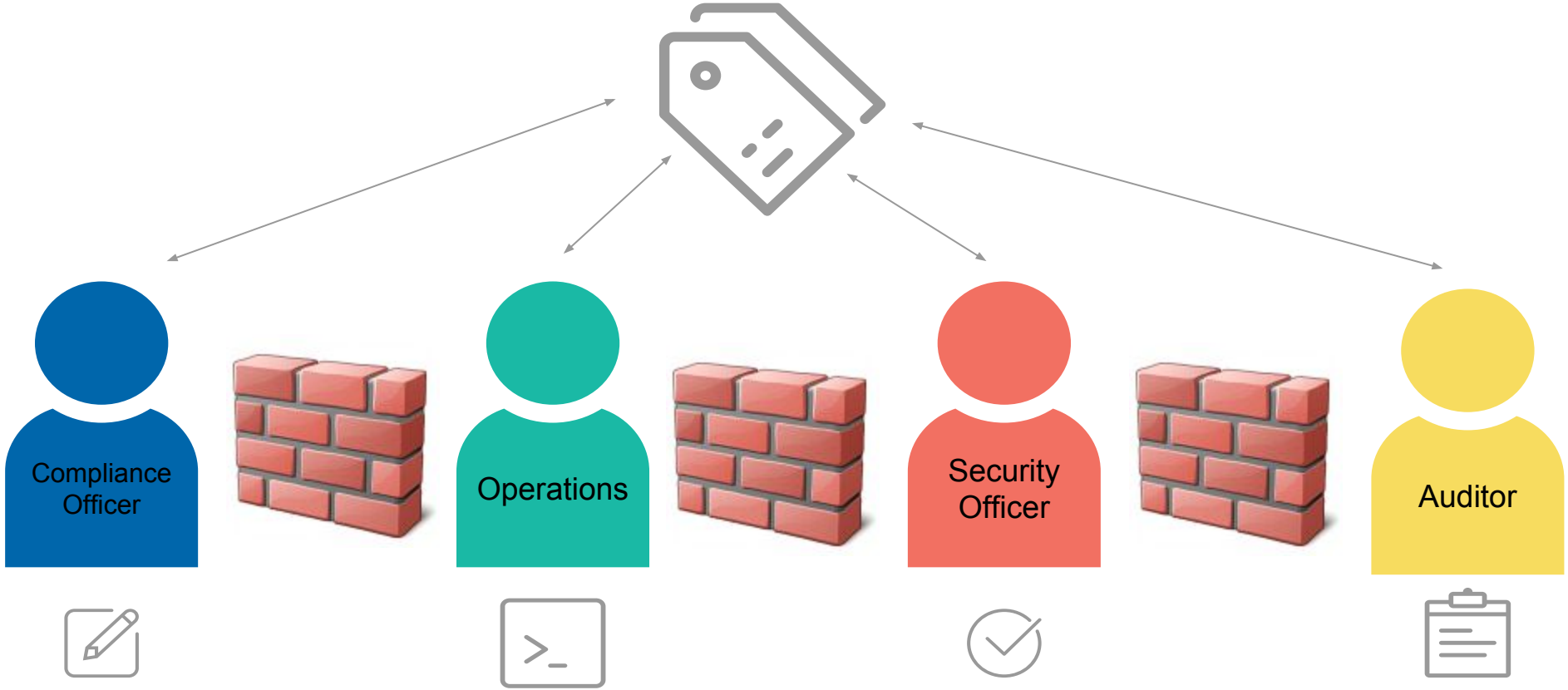
PCI DSS Requirements	Testing Procedures	Guidance
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	**7.1** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	**7.1.1** Select a sample of roles and verify access needs for each role are defined and include: • System components and data resources that each role needs to access for their job function • Identification of privilege necessary for each role to perform their job function.	In order to limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	**7.1.2.a** Interview personnel responsible for assigning access to verify that access to privileged user IDs is: • Assigned only to roles that specifically require such privileged access • Restricted to least privileges necessary to perform job responsibilities.	When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the "least privileges"). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator.

(Continued on next page)

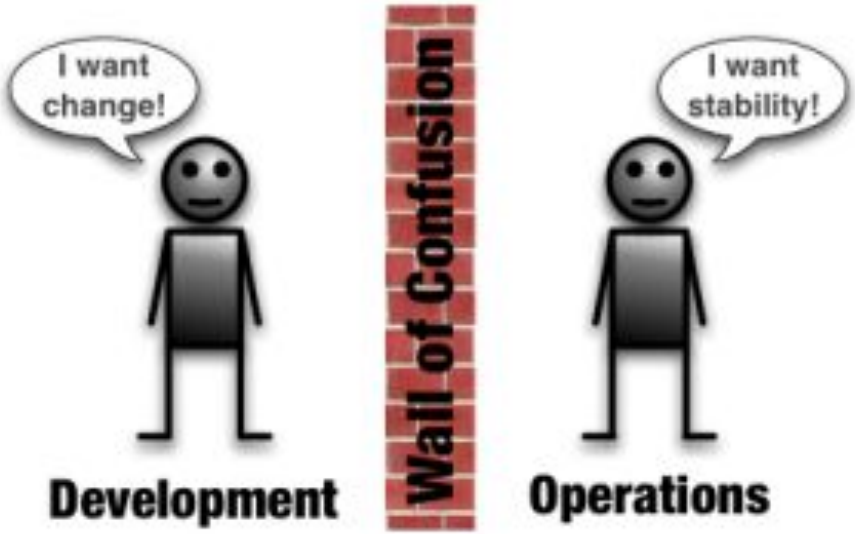
Pivotal



Pivotal


Compliance Officer
Operations
Security Officer
Auditor

Pivotal


I want change!
Wall of Confusion
I want stability!
Development
Operations

Pivotal

The conference that brings development and operations together.

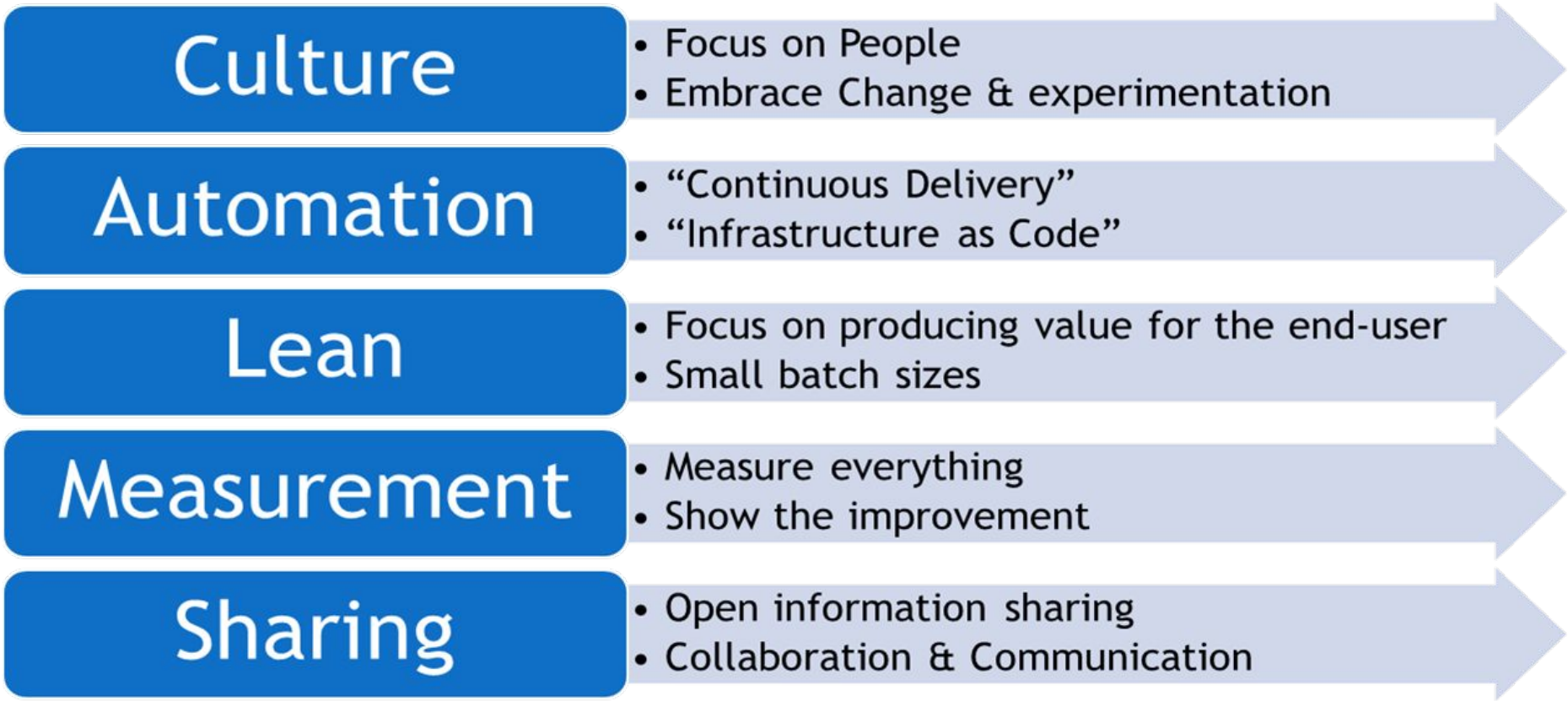
Ghent 2009 program

Tweets from devopsdays events

Intro video - devopsdays video stream

Non-Functional Requirements: do user stories help? [PDF][Video] Rachel Davies

Cucumber-nagios [slideshare][Video] **Flapjack ... rethinking monitoring for the cloud** [slideshare][Video] Lindsay Holmwood


Culture
• Focus on People
• Embrace Change & experimentation
Automation
• “Continuous Delivery”
• “Infrastructure as Code”
Lean
• Focus on producing value for the end-user
• Small batch sizes
Measurement
• Measure everything
• Show the improvement
Sharing
• Open information sharing
• Collaboration & Communication


OBSERVE
ORIENT
the
OODA
LOOP
DECIDE
ACT

chetan conikee
@conikeec

Follow

Congrats Mark Miller (@EUSP) and John Willis (@botchagalupe) on launch of devsecopsdays.com #DevSecOps #devops #RSAC2018

5:08 PM - 15 Apr 2018

10 Retweets **6** Likes

10 6

Pivotal

http://blog.d2-si.fr/2016/02/22/devopsconnection/

You Had One Job
@YouHadOneJ0B

Follow

Nobody gets in, nobody gets out

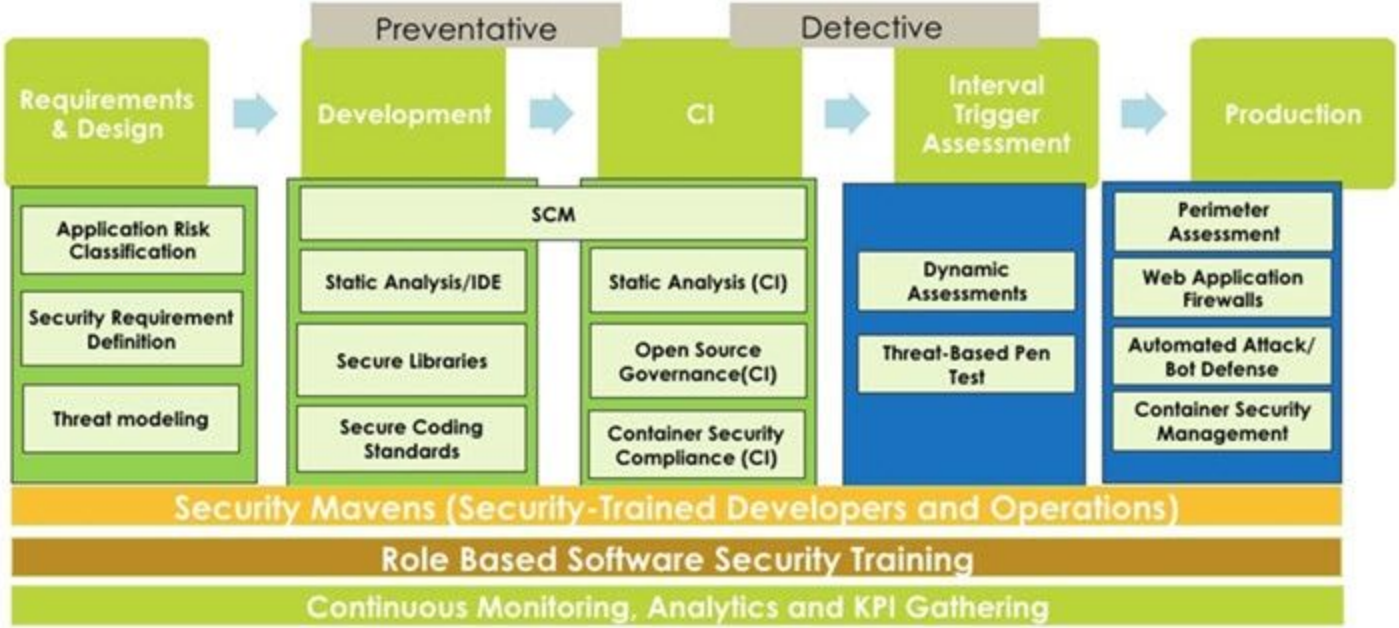
Rugged DevOps

DevSecOps

Secure DevOps

Pivotal

Implementing DevOps in a Regulated Environment



https://www.devsecopsdays.com/articles/its-just-a-name

chetan conikee
@conikeec

Follow

Congrats Mark Miller (@EUSP) and John Willis (@botchagalupe) on launch of devsecopsdays.com #DevSecOps #devops #RSAC2018

5:08 PM - 15 Apr 2018

10 Retweets **6** Likes

10 6

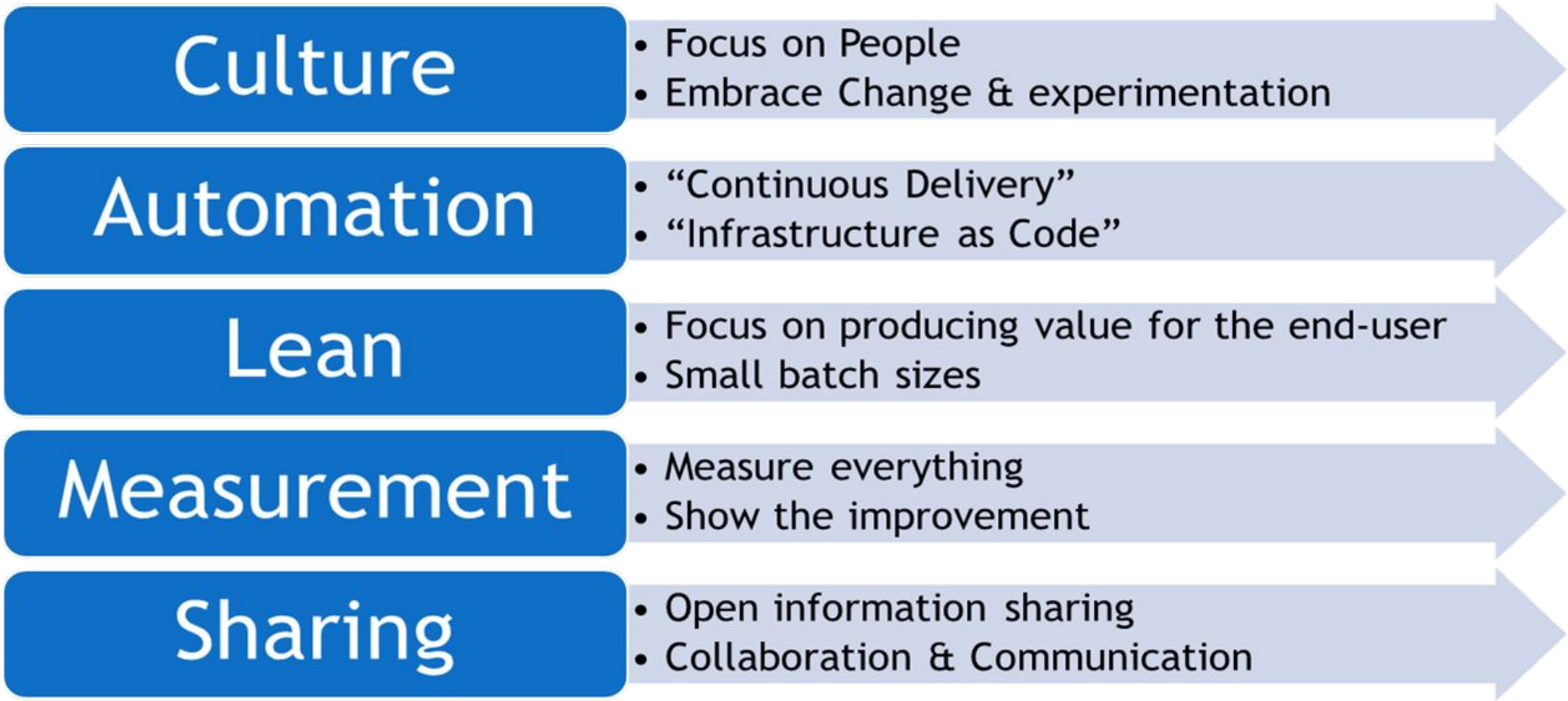
Tweet your reply

Czarcloudski @pczarkowski · now

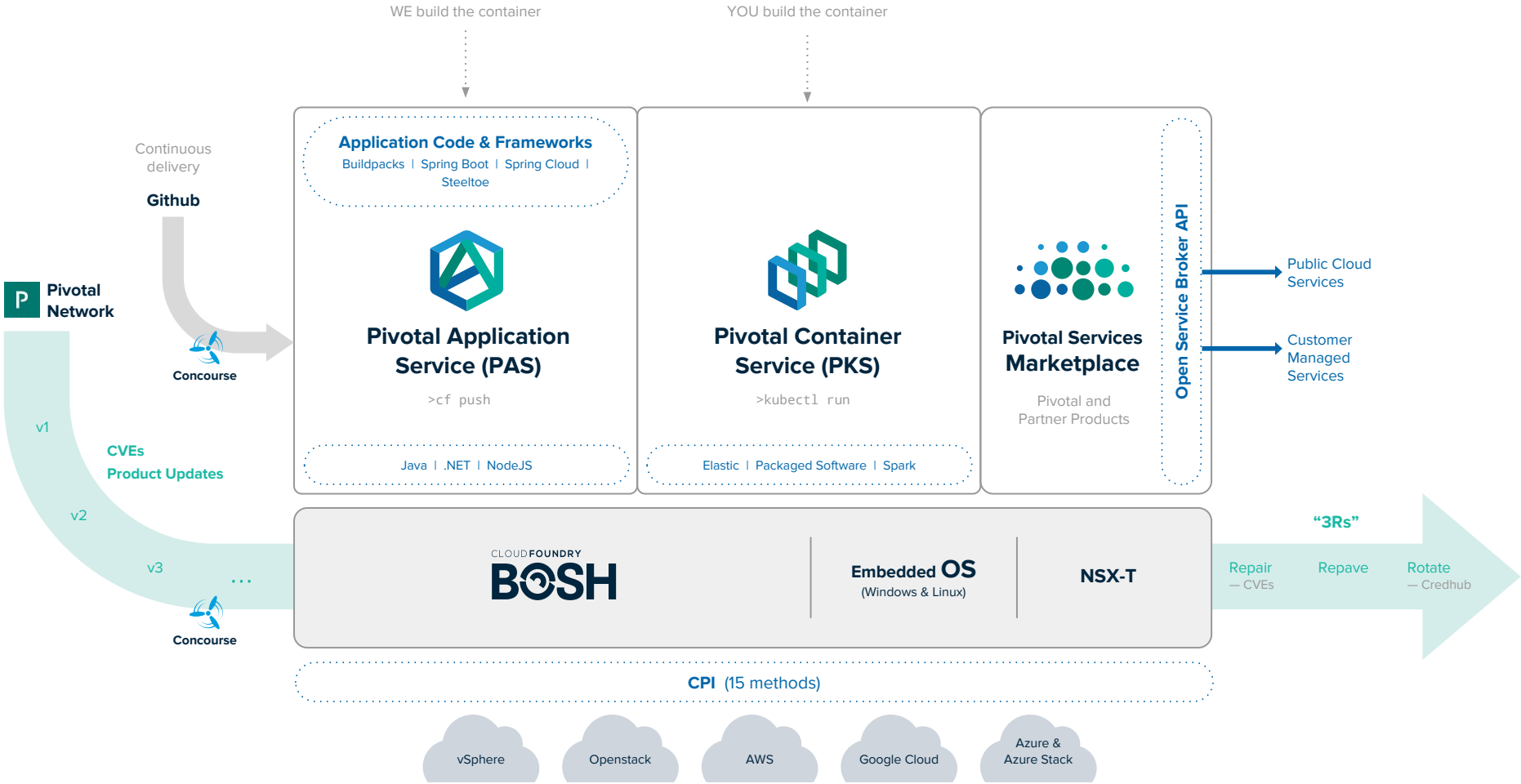
Replying to @conikeec @EUSP @botchagalupe

Awesome! It's about time we empower security to be part of the devops revolution instead of actively depriving them from doing their jobs.

Pivotal


Culture
• Focus on People
• Embrace Change & experimentation
Automation
• “Continuous Delivery”
• “Infrastructure as Code”
Lean
• Focus on producing value for the end-user
• Small batch sizes
Measurement
• Measure everything
• Show the improvement
Sharing
• Open information sharing
• Collaboration & Communication

Pivotal


WE build the container
YOU build the container
Continuous delivery
Github
Pivotal Network
Concourse
v1
CVEs
Product Updates
v2
v3
...
Concourse
Application Code & Frameworks
Buildpacks | Spring Boot | Spring Cloud | Steeltoe
Pivotal Application Service (PAS)
>cf push
Java | .NET | NodeJS
Pivotal Container Service (PKS)
>kubectl run
Elastic | Packaged Software | Spark
Pivotal Services Marketplace
Pivotal and Partner Products
Open Service Broker API
Public Cloud Services
Customer Managed Services
CLOUDFOUNDRY BOSH
Embedded OS (Windows & Linux)
NSX-T
"3Rs"
Repair — CVEs
Repave
Rotate — Credhub
CPI (15 methods)
vSphere
Openstack
AWS
Google Cloud
Azure & Azure Stack

Pivotal

PIVOTAL CLOUD FOUNDRY OPS

Powered by BOSH

× BOSH

BOSH is an open source tool for release engineering, deployment, lifecycle management, and monitoring of distributed systems.

- Packaging w/ embedded OS
- Server provisioning on any IaaS
- Software deployment across availability zones
- Health monitoring (server AND processes)
- Self-healing w/ Resurrector
- Storage management
- Rolling upgrades via canaries
- Easy scaling of clusters

PIVOTAL CLOUD FOUNDRY OPS

Powered by BOSH

× BOSH

BOSH is an open source tool for release engineering, deployment, lifecycle management, and monitoring of distributed systems.

- Packaging w/ embedded OS
- Server provisioning on any IaaS
- Software deployment across availability zones
- Health monitoring (server AND processes)
- Self-healing w/ Resurrector
- Storage management
- Rolling upgrades via canaries
- Easy scaling of clusters

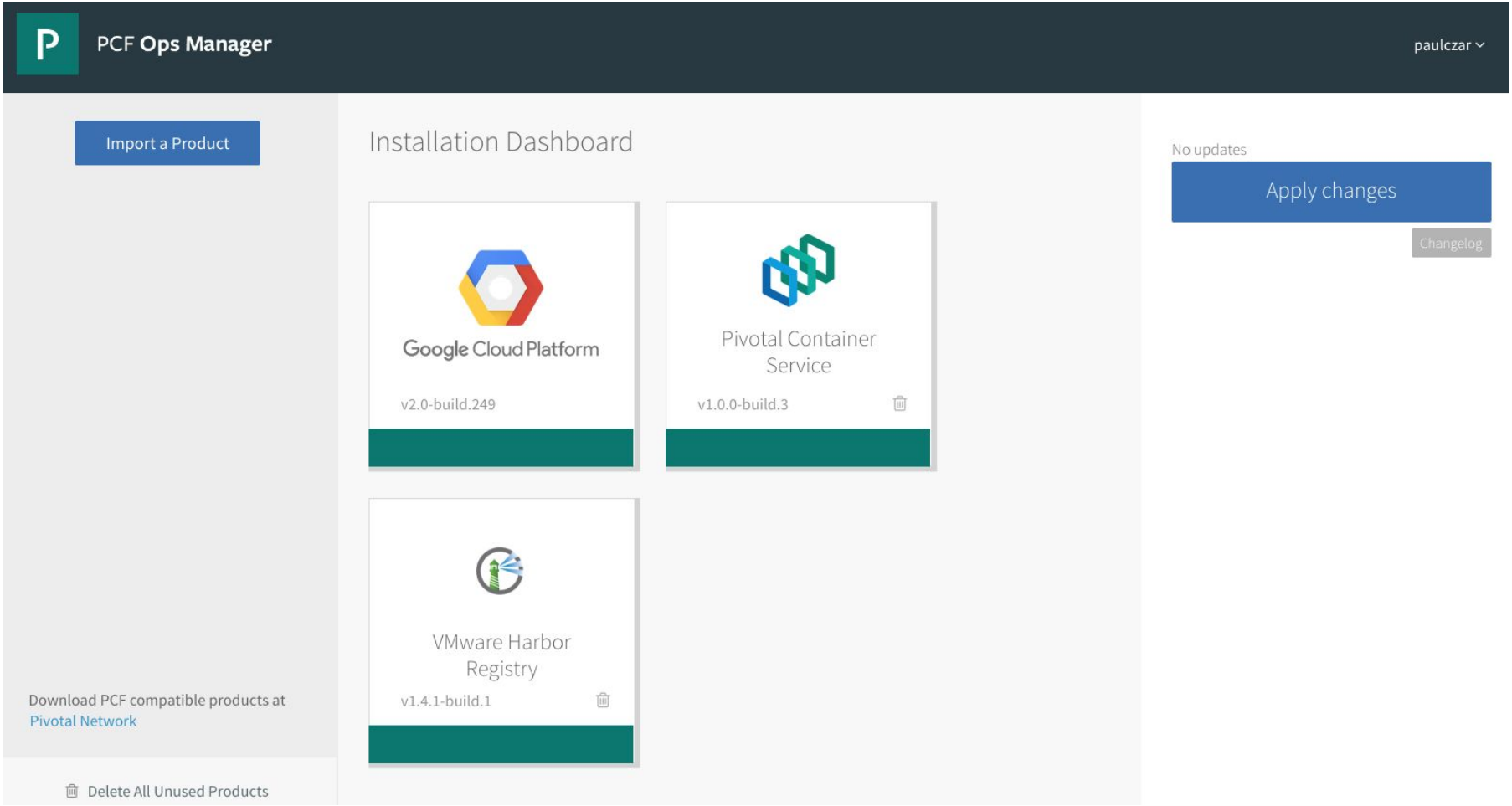
PIVOTAL CLOUD FOUNDRY OPS

Powered by BOSH

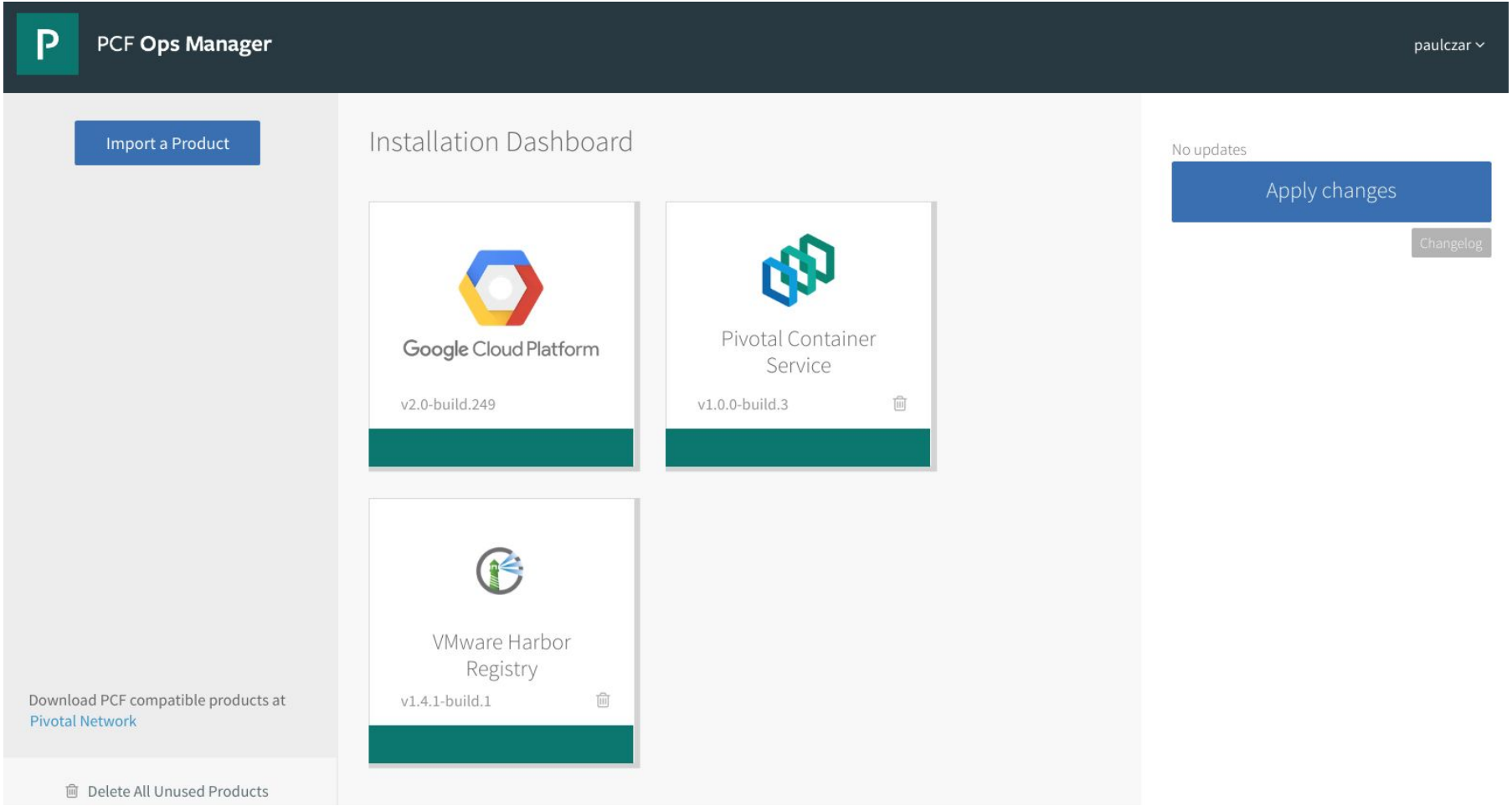
× BOSH

BOSH is an open source tool for release engineering, deployment, lifecycle management, and monitoring of distributed systems.

- Packaging w/ embedded OS
- Server provisioning on any IaaS
- Software deployment across availability zones
- Health monitoring (server AND processes)
- Self-healing w/ Resurrector
- Storage management
- Rolling upgrades via canaries
- Easy scaling of clusters


PCF Ops Manager
paulczar
Import a Product
Installation Dashboard
No updates
Apply changes
Changelog
Google Cloud Platform
v2.0-build.249
Pivotal Container Service
v1.0.0-build.3
VMware Harbor Registry
v1.4.1-build.1
Download PCF compatible products at
Pivotal Network
Delete All Unused Products

Pivotal


PCF Ops Manager
paulczar
Import a Product
Installation Dashboard
No updates
Apply changes
Changelog
Google Cloud Platform
v2.0-build.249
Pivotal Container Service
v1.0.0-build.3
VMware Harbor Registry
v1.4.1-build.1
Download PCF compatible products at
Pivotal Network
Delete All Unused Products

Pivotal

Daniel Jones
@EngineerBetter

Follow

Last week saw Pivotal Cloud Foundry doing 30-40 upgrades over 200 VMs. Took one pair a few days. Trad ops team would've taken 2 years.

Daniel Jones
@EngineerBetter

Follow

Last week saw Pivotal Cloud Foundry doing 30-40 upgrades over 200 VMs. Took one pair a few days. Trad ops team would've taken 2 years.

Repair

Repair vulnerable software as soon as updates are available.

Repave

Repave servers and applications from a known good state. Do this often.

Rotate

Rotate user credentials frequently, so they are only useful for short periods of time.

Repair

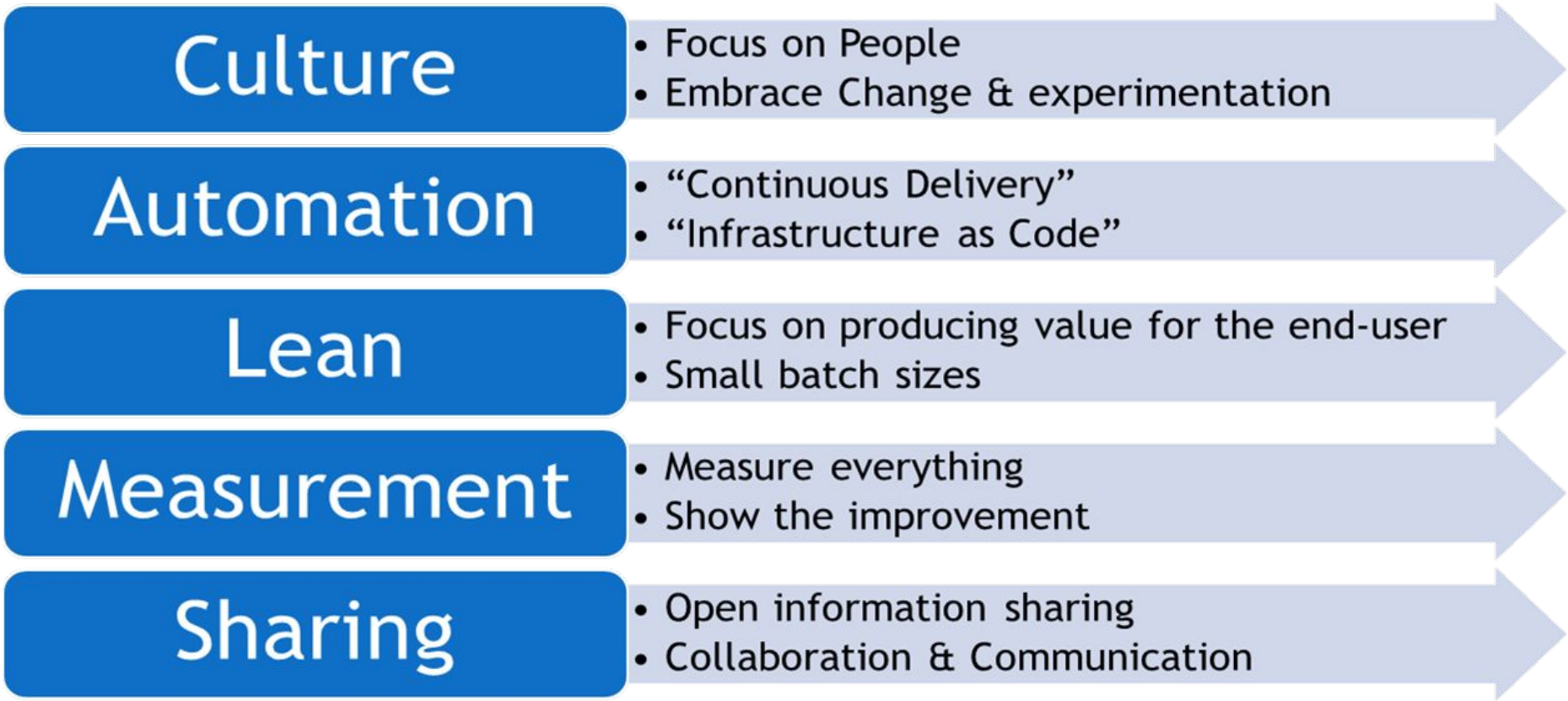
Repair vulnerable software as soon as updates are available.

Repave

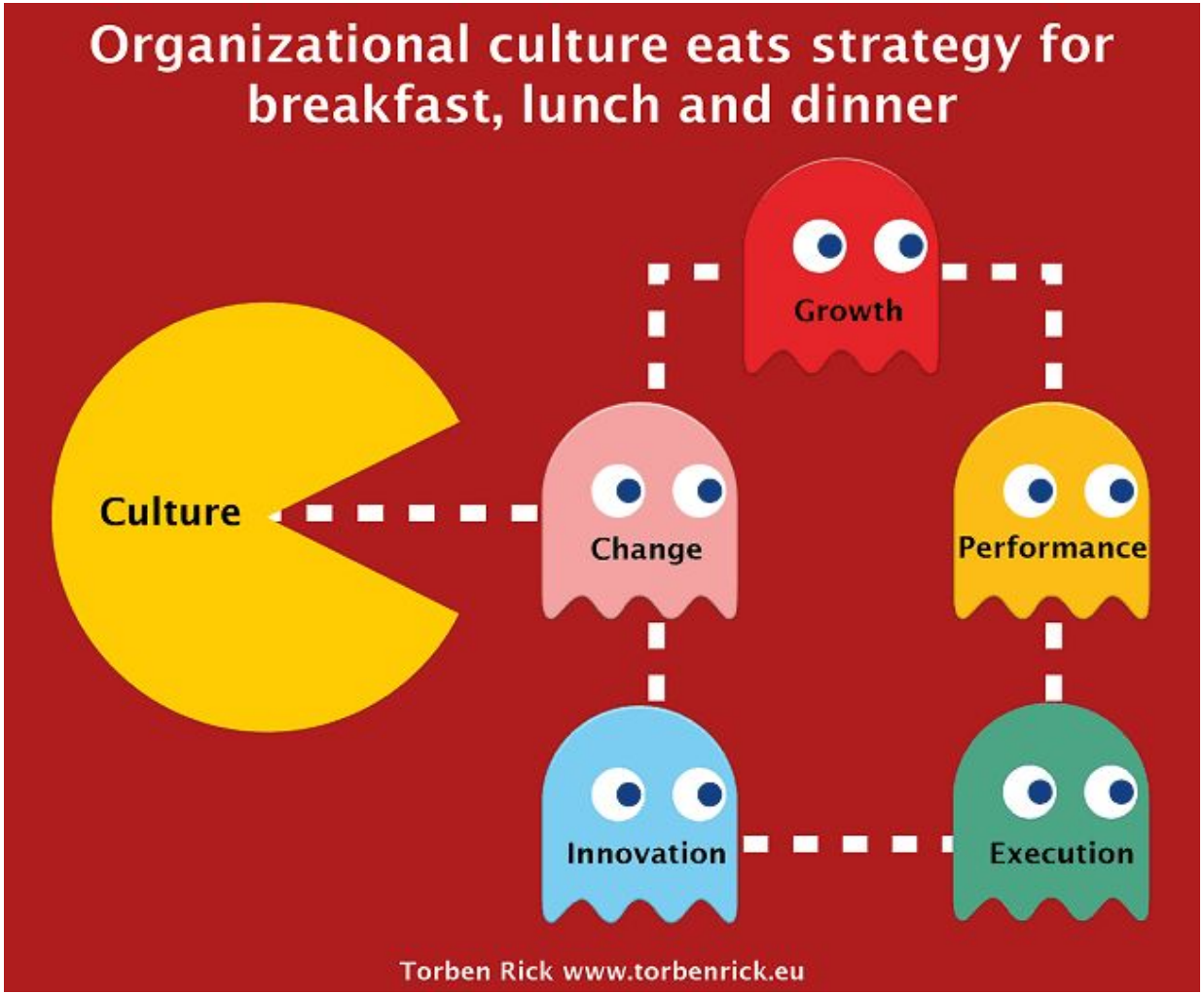
Repave servers and applications from a known good state. Do this often.

Rotate

Rotate user credentials frequently, so they are only useful for short periods of time.


Culture
• Focus on People
• Embrace Change & experimentation
Automation
• “Continuous Delivery”
• “Infrastructure as Code”
Lean
• Focus on producing value for the end-user
• Small batch sizes
Measurement
• Measure everything
• Show the improvement
Sharing
• Open information sharing
• Collaboration & Communication

Pivotal


Organizational culture eats strategy for breakfast, lunch and dinner
Growth
Culture
Change
Performance
Innovation
Execution
Torben Rick www.torbenrick.eu

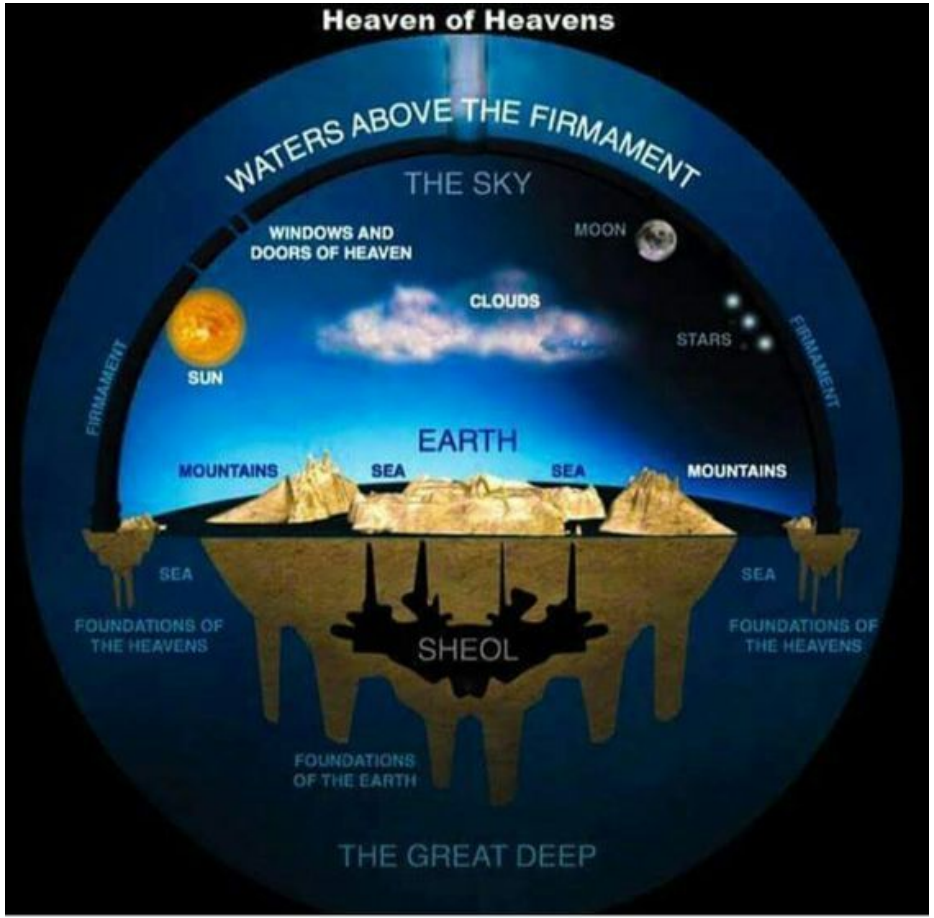
Adopting a DevOps culture

Despite varying approaches to describing high-performance teams there is a set of common characteristics that are recognised to lead to success.

- Participative leadership – using a democratic leadership style that involves and engages team members
- Effective decision-making – using a blend of rational and intuitive decision making methods, depending on that nature of the decision task
- Open and clear communication – ensuring that the team mutually constructs shared meaning, using effective communication methods and channels
- Valued diversity – valuing a diversity of experience and background in team, contributing to a diversity of viewpoints, leading to better decision making and solutions
- Mutual trust – trusting in other team members and trusting in the team as an entity
- Clear goals – goals that are developed using SMART criteria; also each goal must have personal meaning and resonance for each team member, building commitment and engagement
- Defined roles and responsibilities – each team member understands what they must do (and what they must not do) to demonstrate their commitment to the team and to support team success
- Positive atmosphere – an overall team culture that is open, transparent, positive, future-focused and able to deliver success

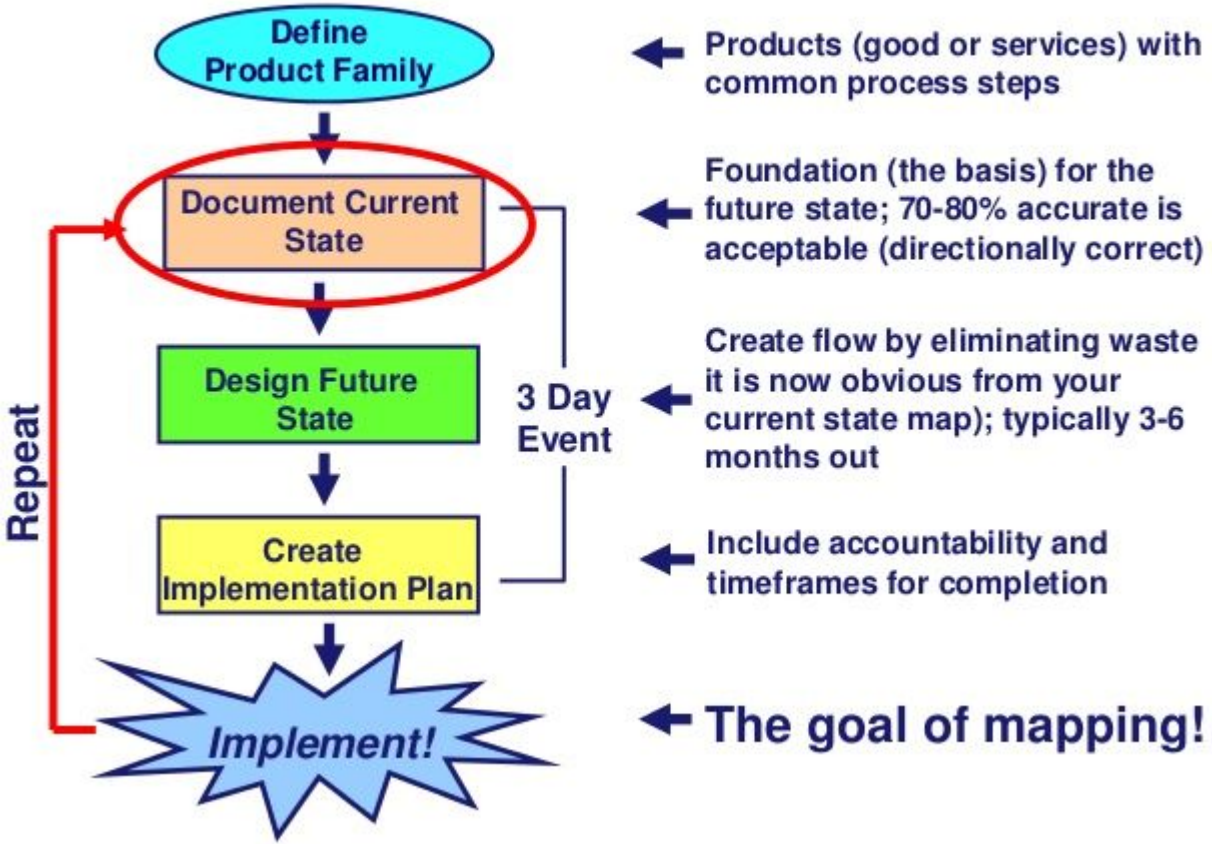
https://en.wikipedia.org/wiki/High-performance_teams

Pivotal



https://imgur.com/gallery/kMJWs

Value Stream Mapping Process



https://www.slideshare.net/KarenMartinGroup/value-stream-mapping-in-office-service-setttings

Mappable Processes that include Security / Compliance

Infrastructure Provisioning

- OS Hardening
- Firewalling
- User Management
- Remote logging and auditing
- Intrusion Detection
- Vulnerability Scanning

Application Release

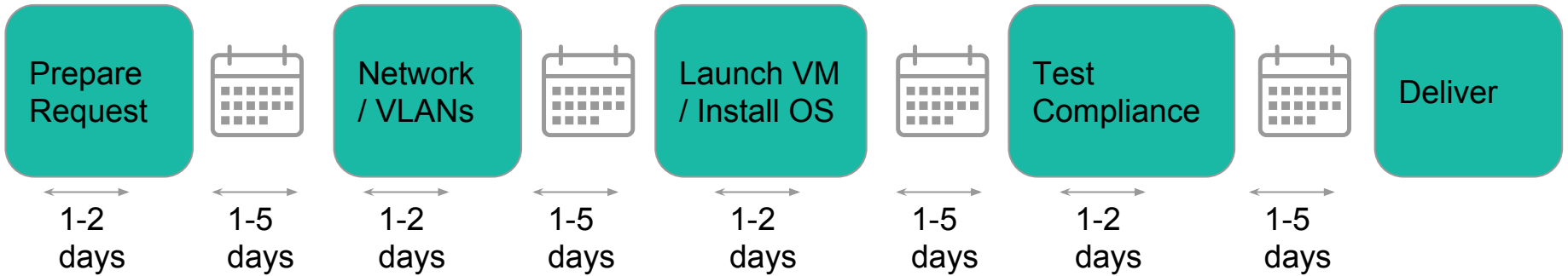
- Vulnerability Scanning
- Security Scanning (sql injection etc)
- License Scanning
- Attribution

Compliance Audits

- Vulnerability Scanning
- Security Scanning (sql injection etc)
- Package updates
- OS inspection

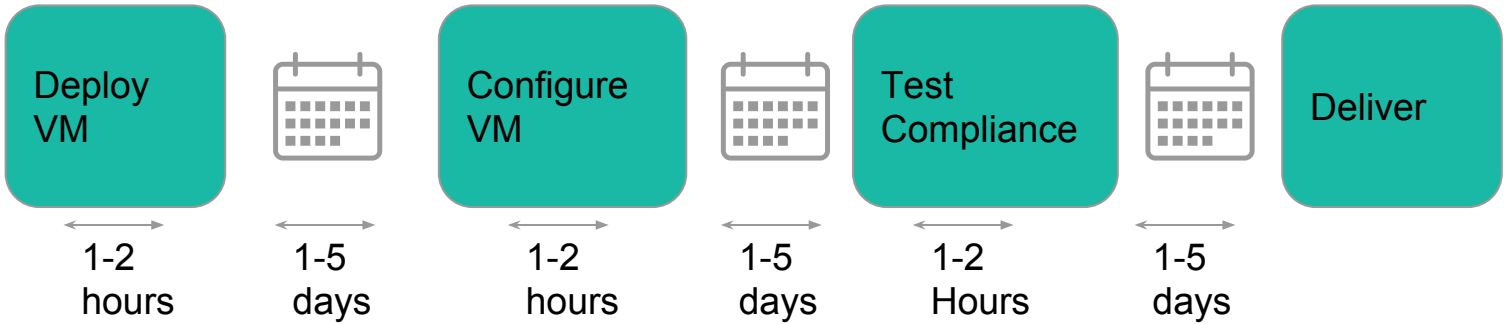
Value Stream map for Provisioning a New Server

Current State



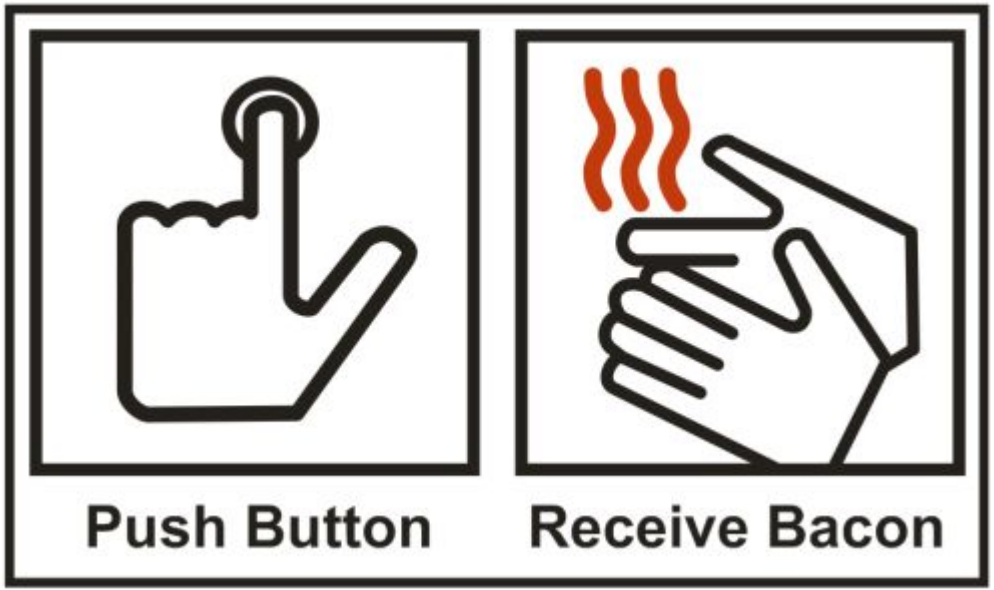
Value Stream map for Provisioning a New Server

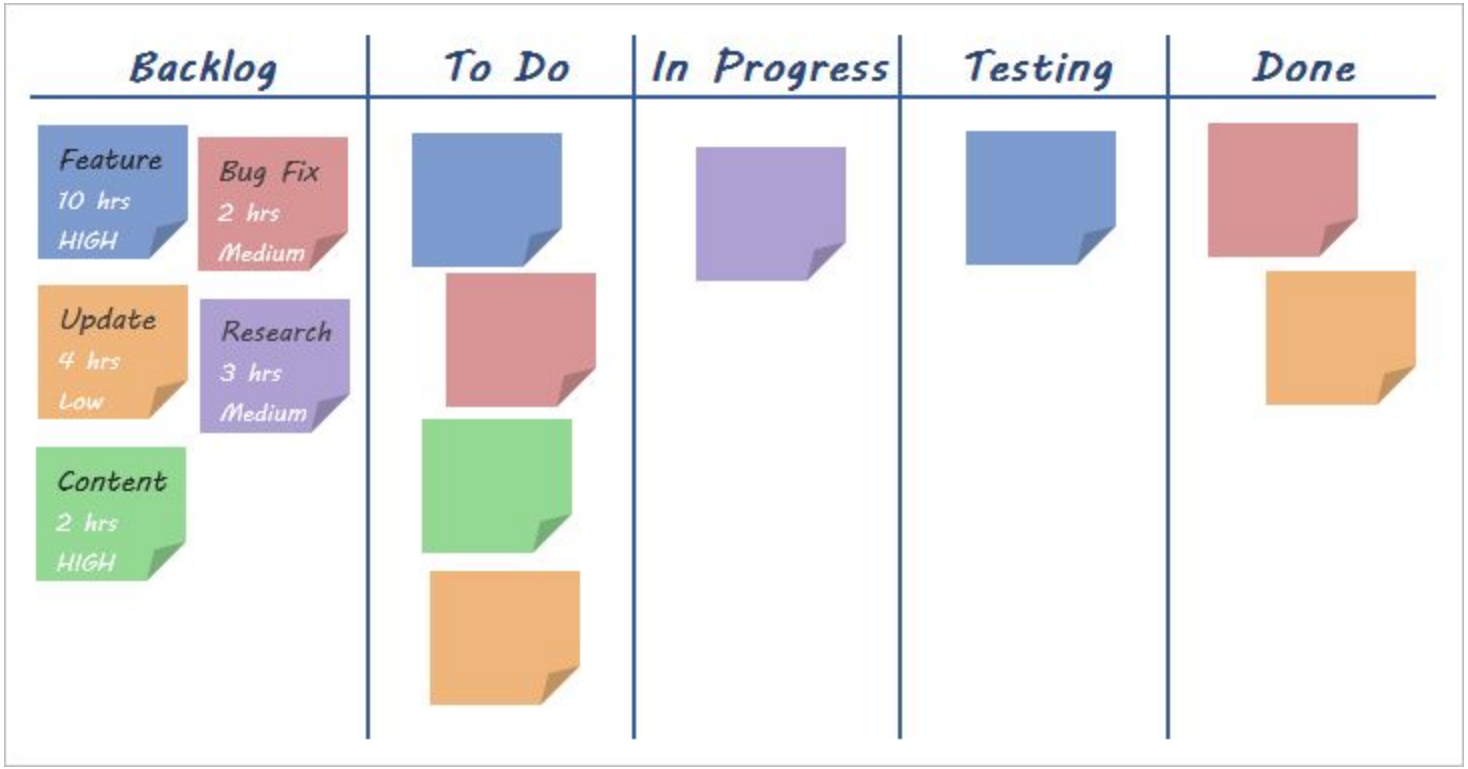
Future State

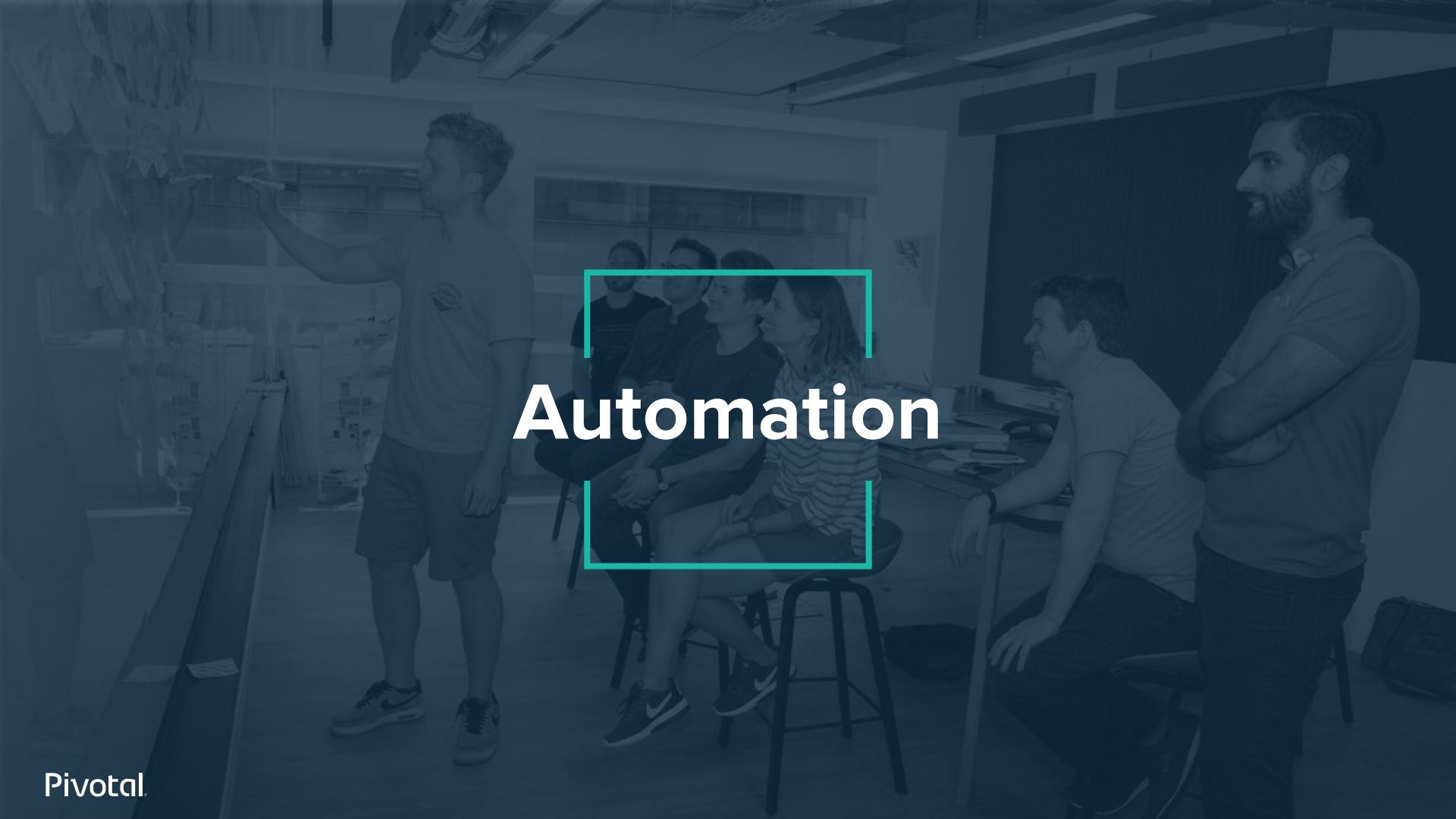


Value Stream map for Provisioning a New Server

Future State




Backlog
To Do
In Progress
Testing
Done
Feature
10 hrs
HIGH
Bug Fix
2 hrs
Medium
Update
4 hrs
Low
Research
3 hrs
Medium
Content
2 hrs
HIGH



Pivotal

requirement to B or S P=Process, Requirement, no requirement to B or S	Foundation (Y/N)	Section #	Section Heading	System Value/Parameter	Description	Recommended Value	Initial Value	Agreed to Value	BB Value	Change Date (YYYYMMDD)	"added" if this is a new parameter, "N" for "updated" if a value for an existing parameter has been changed)
I	Y	BBB.1.1.0	Password Requirements	No requirements in this category	No requirements in this category	No requirements in this category	None	No requirements in this category			

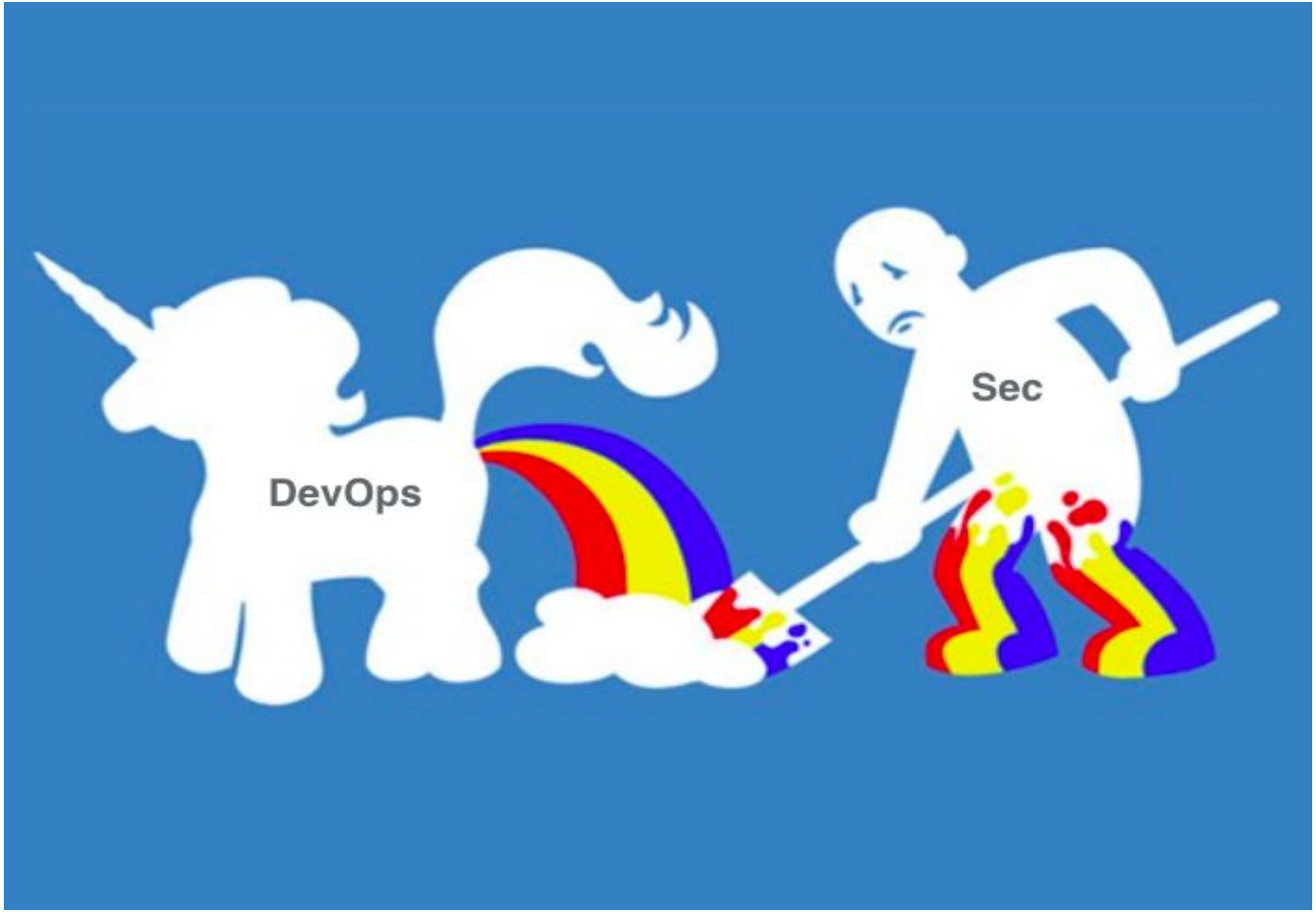
S	Y	BBB.1.2.1	Logging	logpath=<path> # log file path
				logappend=true # Set to true to add new entries to the end of the logfile rather than overwriting the content of the log when the process restarts.
					above two parameter should be in mongo DB's config file	logappend = true
						logpath = /var/log/mongo/mongod.log
							logappend = true
							logpath = /var/log/mongo/mongod.log
									root@qint-lon02-c1:~# cat /etc/mongod.conf | grep ^log
									logpath=/var/log/mongodb/mongod.log
									logappend=true		

I	Y	BBB.1.2.2	Logging	N/A	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	Y	BBB.1.2.3	Logging	N/A	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	N	BBB.1.2.4	Logging	N/A	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	Y	BBB.1.3.0	Anti Virus	No requirements in this category	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	N	BBB.1.4.0	System Settings	No requirements in this category	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	N	BBB.1.5.0	Network Settings	No requirements in this category	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	N	BBB.1.7.0	Identity and Authentication	No requirements in this category	No requirements in this category	No requirements in this category	None	No requirements in this category			
S	N	BBB.1.8.1	Protecting Resources ? OSRs	config file /etc/mongod.conf db file mount point: /var/lib/mongo/ encrpted db file as eCryptfs: /usr/mongo eCryptfs's passphrase_passwd_file:/var/lib/mongo/passwd_file.txt	1.config file para in mongo db start command., which contain config parameter for mongo db. 2. db file directory contain all mongo db related files and sub-directories 3. encryped db file as eCryptfs, will mount on db file directory 4. the passphrase_passwd_file for mount eCryptfs	config file: /etc/mongod.conf owner is root, 644 db file directory: /var/lib/mongo/ owner is mongod, directory is 755, related files is 600 (except mongod.lock file ,which is generated during mongod running, it has 755) eCryptfs related configuration data: Key type: passphrase Passphrase: passphrase_passwd_file:/var/lib/mongo/passwd_file.txt Cypher: ecryptfs_cipher:aes Key byte: ecryptfs_key_bytes:16 Plaintext passtrough: ecryptfs_passthrough:n Filename encryption: ecryptfs_enable_filename_crypto:n Add signature to cache: no_sig_cache:y ecryptfs_sig= the encrypted file will be under /usr/mongo directory	[root@par01cld002ccz056 ~]# ls -l /etc/mongod.conf -rw-r--r-- 1 root root 266 Dec 19 16:57 /etc/mongod.conf [root@par01cld002ccz056 ~]# ls -l /var/lib/ | grep mongo drwxr-xr-x. 4 mongod mongod 4096 Feb 3 09:11 mongo [root@par01cld002ccz056 ~]#		root@qint-lon02-c1:~# ll /etc/mongod.conf -rw-r--r-- 1 root root 1754 Sep 10 16:33 /etc/mongod.conf root@qint-lon02-c1:~# ll /var/lib/ | grep mongo drwxr-xr-x. 4 mongodb mongodb 4096 Sep 17 06:43 mongodb/		
I	N	BBB.2.0.0	Encryption	No requirements in this category	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	N	BBB.2.1.1	Encryption	N/A	No requirements in this category	No requirements in this category	None	No requirements in this category			
S	N	BBB.2.1.2	Encryption	database file encryption	database file encryption is needed since it contain financial related data	MongodB using an encrypted file system like eCryptfs to store confidential data	[root@par01cld002ccz056 ~]# cat /etc/fstab | grep mongo [root@par01cld002ccz056 ~]#				
I	N	BBB.2.1.3	Encryption	N/A	No requirements in this category	No requirements in this category	None	No requirements in this category			
I	Y	BBB.5.0.0	Privileged Authorization/Userids	Note	Description of privileged Ids : The rows in section 5 below describe the list of UserIDs or groups that have Privileged authority	No value to be set	No value to be set	No value to be set			
I	Y	BBB.5.0.1	Privileged Authorization/Userids	UserID: mongod group: mongod	No requirements in this category	No requirements in this category	None	No requirements in this category			

Pivotal

- Implements STIG controls via Ansible playbooks
- Opensource project started at Rackspace
- Plays well with existing config management
- Easily override problematic controls

- Extends RSPEC for Compliance testing
- Similar to Serverspec, but better.
- Easy to go from serverspec to inspec
- Inspec-STIG is all of STIG already written into inspec tests.



Source: @petecheslock

Example of Compliance Specifications

The SSH daemon must be configured to use only the SSHv2 protocol.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-38607	RHEL-06-000227	SV-50408r1_rule		High

Description

SSH protocol version 1 suffers from design flaws that result in security vulnerabilities and should not be used.

STIG	Date
Red Hat Enterprise Linux 6 Security Technical Implementation Guide	2017-03-01

Details

Check Text (C-46165r1_chk)

To check which SSH protocol version is allowed, run the following command:

grep Protocol /etc/ssh/sshd_config

If configured properly, output should be

Protocol 2

If it is not, this is a finding.

Fix Text (F-43555r1_fix)

Only SSH protocol version 2 connections should be permitted. The default setting in "/etc/ssh/sshd_config" is correct, and can be verified by ensuring that the following line appears:

Protocol 2

```
title 'V-38607 - The SSH daemon must be configured to use only the SSHv2 protocol.'

control 'V-38607' do
  impact 1.0
  title 'The SSH daemon must be configured to use only the SSHv2 protocol.'
  desc 'SSH protocol version 1 suffers from design flaws that result in security vulr
  tag 'stig','V-38607'
  tag severity: 'high'
  tag fixtext: 'Only SSH protocol version 2 connections should be permitted. The defa
  tag checktext: 'To check which SSH protocol version is allowed, run the following c

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

end
```

```
control 'MYSQL005' do
  impact 1.0
  title 'Strict permissions for my.cnf to prevent unauthorized
  desc 'strict permissions(644) and ownership (root user and gr
  tag 'production','development'
  tag 'mysql'
  tag remediation: 'ansible-playbook site.yml --tags=MYSQL005'
  tag documentation: 'http://e.corp/MYSQL005'
    if File.file?('/etc/my.cnf')
      describe file("/etc/my.cnf") do
        its('mode') { should cmp '0644' }
        its('group') { should eq 'root' }
        its('owner') { should eq 'root'}
      end
    end
end
```

ANSIBLE

elastic

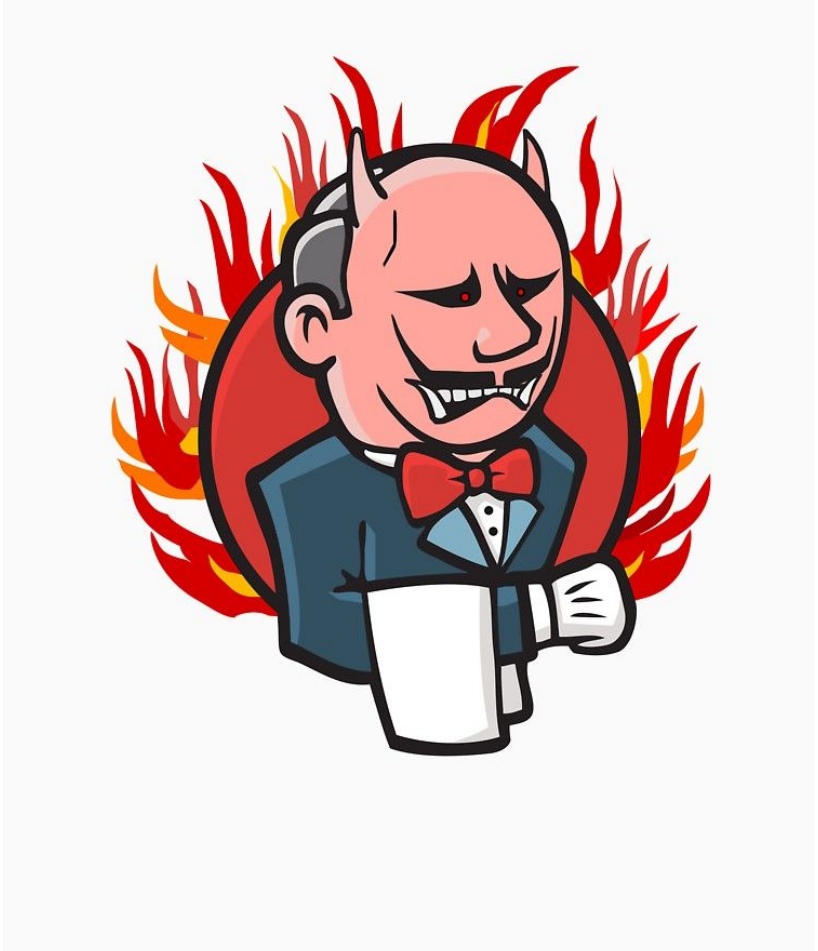
SERVERSPEC-CHECK

action	create
auto_resolve	true
command	sudo /etc/sensu/plugins/check-serverspec.rb -d /etc/serverspec -s warning
duration	4.744
executed	2016-10-14 15:22:20
handle	true
handlers	default
history	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1
interval	3600
issued	2016-10-14 15:22:20
name	serverspec-check
occurrences	1920
output	CheckServerspec WARNING: 286 examples, 1 failure FAILED: os_spec.rb:42, File /etc/adduser.conf should contain ^DIR_MODE=700
standalone	true
status	1
total_state_change	0
type	standard


kibana
Discover
Visualize
Dashboard
Settings
Last 15 minutes
serverspec
[logstash-]YYYY.MM.DD
58 hits
Selected Fields
_source
Available Fields
Popular
cluster_name
customer_id
host
message
@timestamp
@version
_id
_index
_score
October 14th 2016, 15:18:00.853 - October 14th 2016, 15:33:00.853 — by 30 seconds
Count
@timestamp per 30 seconds
Time
_source
October 14th 2016, 15:32:25.000
message: sensu : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/etc/sensu/plugins/check-serverspec.rb -d /etc/serverspec -s warning syslog_message: sensu : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/etc/sensu/plugins/check-serverspec.rb -d /etc/serverspec -s warning @version: 1 @timestamp: October 14th 2016, 15:32:25.000 type: syslog file: /var/log/auth.log host: ds0098 offset: 975711Z cluster_name: uat-sjc customer_id: 00001 tags: auth syslog_timestamp: Oct 14 20:32:25 syslog_hostname: ds0098 syslog_program: sudo received_at: 2016-10-14T20:32:26.624Z syslog_severity_code: 5 syslog_facility_code: 1 syslog_facility: user-level syslog_severity: INFO _id: AVfE5VYv7XmOdW3Ht5d8 _type: sys

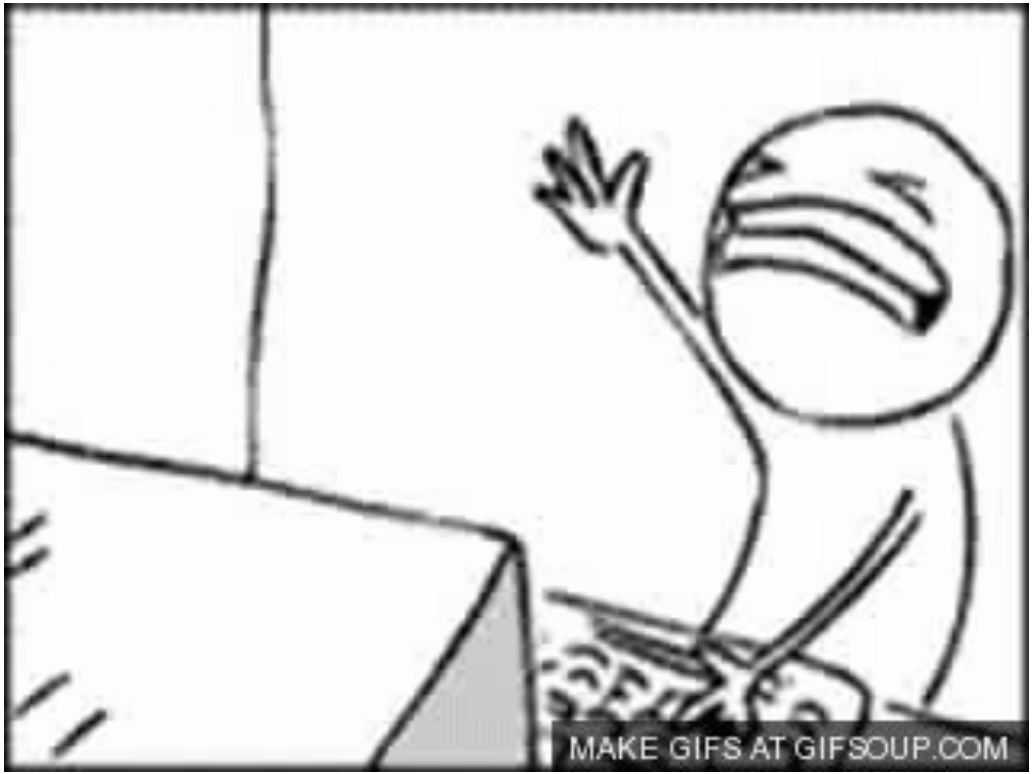
Pivotal

```
- name: Adjust ssh server configuration based on STIG requirements
  blockinfile:
    dest: /etc/ssh/sshd_config
    state: present
    marker: "# {mark} MANAGED BY ANSIBLE-HARDENING"
    insertbefore: "BOF"
    validate: '/usr/sbin/sshd -T -f %s'
    block: "{{ lookup('template', 'sshd_config_block.j2') }}"
  notify:
    - restart ssh
  tags:
    - high
    - sshd
    - V-38607
...
...
...
```



Pivotal

Pivotal


MAKE GIFS AT GIFSOUP.COM

SERVERSPEC-CHECK

action	create
auto_resolve	true
command	sudo /etc/sensu/plugins/check-serverspec.rb -d /etc/serverspec -s warning
duration	4.744
executed	2016-10-14 15:22:20
handle	true
handlers	default
history	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1
interval	3600
issued	2016-10-14 15:22:20
name	serverspec-check
occurrences	1920
output	CheckServerspec WARNING: 286 examples, 1 failure FAILED: os_spec.rb:42, File /etc/adduser.conf should contain ^DIR_MODE=700
standalone	true
status	1
total_state_change	0
type	standard

Pivotal

Pivotal

Pivotal

Other Security / Compliance tools

- Gauntlt (Security Testing Framework)
- Metasploit (Penetration Testing)
- Syntribos (API security testing)
- Pivotal LicenseFinder (Scanning licenses of dependencies)
- Snort (Intrusion Detection)
- Fossology (license compliance)
- OpenVAS (vulnerability scanning)
- OSSEC (Intrustion Detection)


Questions ?

Transforming How The World Builds Software