Automating Security and Compliance in the world of Containers and Hybrid Cloud

Lucy Kerner

Senior Principal Security Global Technical Evangelist & Strategist

lkerner@redhat.com

Twitter: @LucyCloudBling

Let’s start with a related personal story …

LUCY KERNER

Security Global Technical Evangelist & Strategist

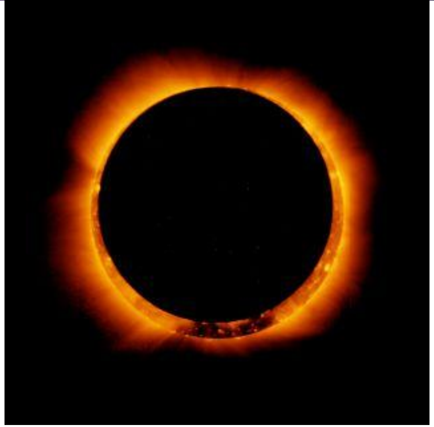
Based in Washington D.C. area

Carnegie Mellon University

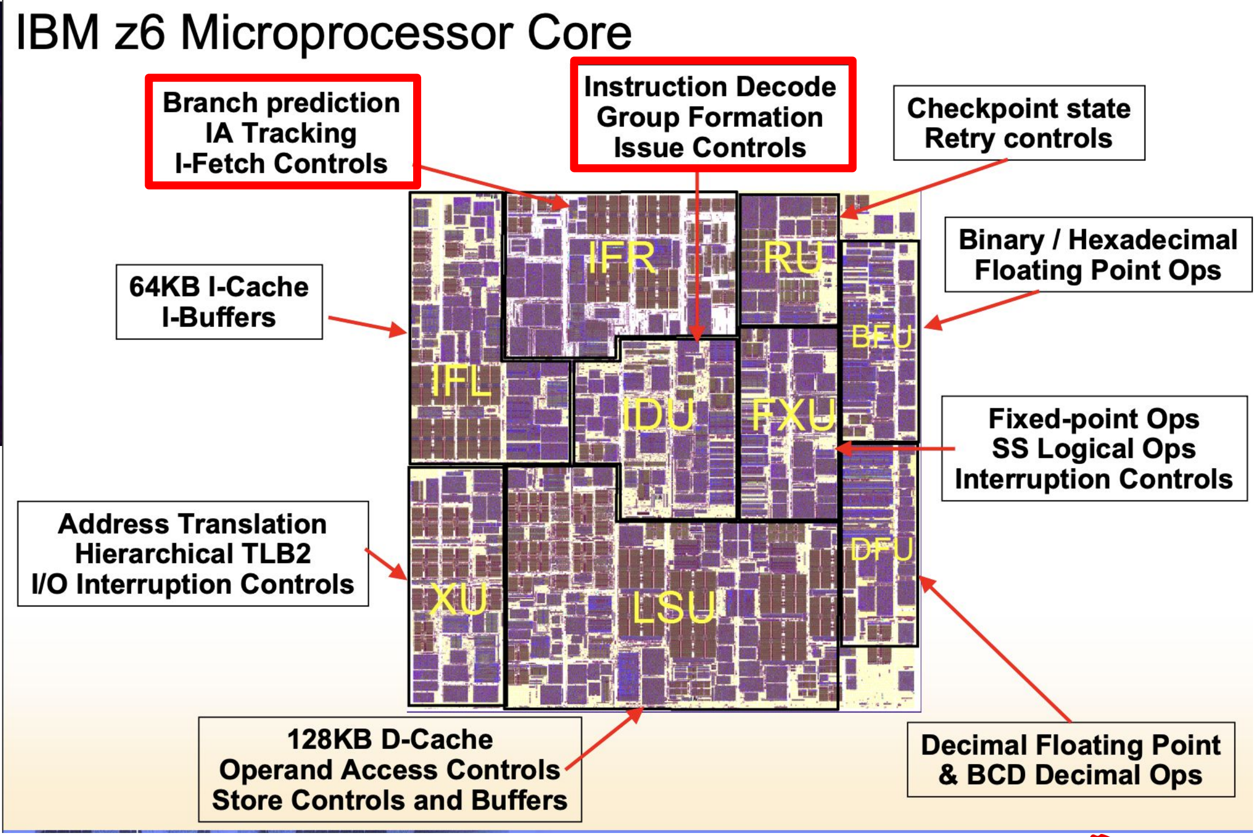
Electrical & Computer ENGINEERING

My first job after college

whoami



Project ECLipz



IBM z6 Microprocessor Core

Branch prediction
IA Tracking
I-Fetch Controls

Instruction Decode
Group Formation
Issue Controls

Checkpoint state
Retry controls

64KB I-Cache
I-Buffers

Binary / Hexadecimal
Floating Point Ops

Fixed-point Ops
SS Logical Ops
Interruption Controls

Address Translation
Hierarchical TLB2
I/O Interruption Controls

128KB D-Cache
Operand Access Controls
Store Controls and Buffers

Decimal Floating Point
& BCD Decimal Ops

CYBERSECURITY ATTACKS ARE CONTINUOUSLY EVOLVING

Meltdown and Spectre

Vulnerabilities in modern processors leak passwords and sensitive data.

THERE’S NO SUCH THING AS 100% SECURITY

- Only certain # hrs in a day
- Limited resources
- Can’t fix everything, so have to make risk decision
    - Implement preventative + responsive measures to manage risk
        - Have a consistent automation strategy

KEY LESSONS FROM RECENT BREACHES

2018 speech by David Hogue, a National Security Agency official, who said the NSA had not responded to an intrusion that exploited a zero-day vulnerability in over two years.

99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident[3]

81% of hacking-related breaches leveraged either stolen and/or weak passwords[1]

68% of breaches took months or longer to discover[2]

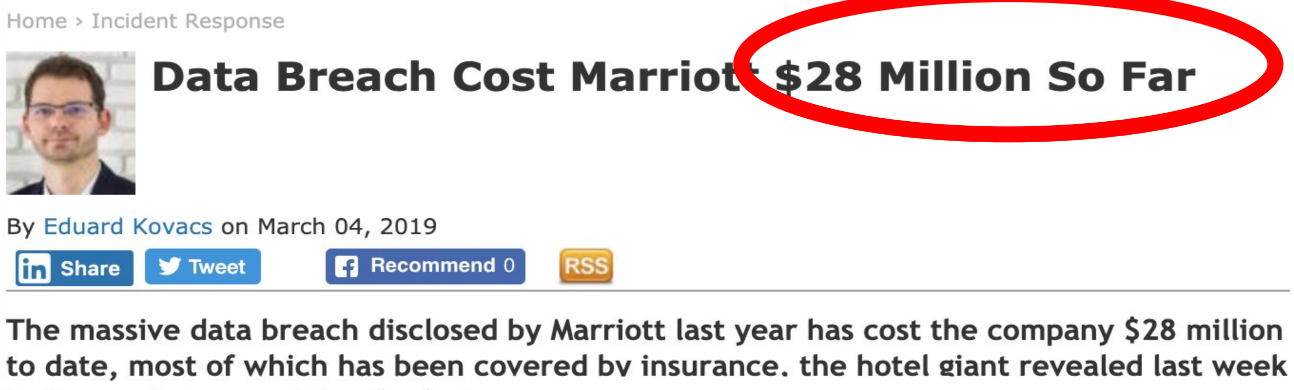
[1] 2017 Verizon Data Breach Investigations Report

[2] 2018 Verizon Data Breach Investigations Report

[3] Gartner, "Focus on the Biggest Security Threats, Not the Most Publicized," November, 2017

2018 Marriott Data Breach

- Exposed personal information of 500 million customers
- **Marriott did not know about the breach for 4 years**



Home › Incident Response

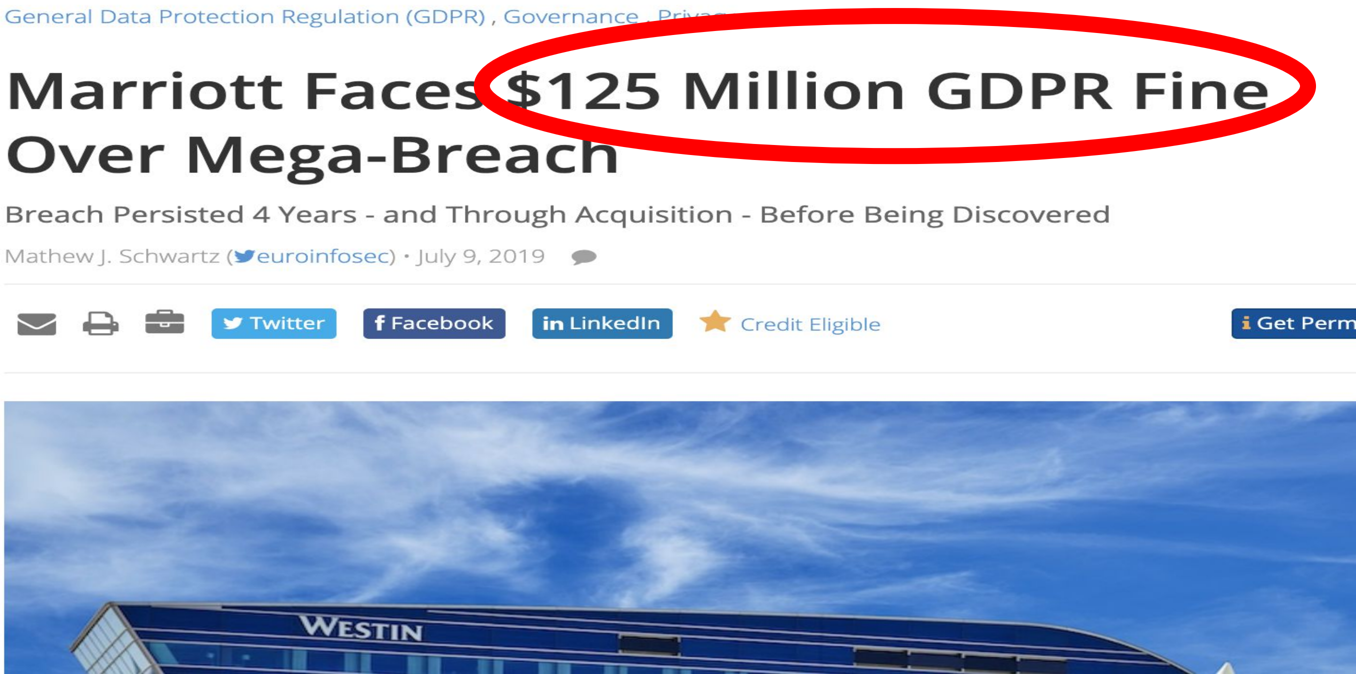
Data Breach Cost Marriott $28 Million So Far

By Eduard Kovacs on March 04, 2019

The massive data breach disclosed by Marriott last year has cost the company $28 million to date, most of which has been covered by insurance, the hotel giant revealed last week in its earnings report for the last

According to Marriott, $25 million security incident has been covered

During an earnings call, Arne Sore been any RevPAR (revenue per ava appear that customer loyalty has b received by Marriott's dedicated c less than 3,000 in February.



General Data Protection Regulation (GDPR) , Governance , Priva

Marriott Faces $125 Million GDPR Fine Over Mega-Breach

Breach Persisted 4 Years - and Through Acquisition - Before Being Discovered

Mathew J. Schwartz (euroinfosec) • July 9, 2019

Lessons Learned from **Wyndham Hotels** Data Breach

- Federal Trade Commission (FTC) claimed that Wyndham violated the FTC’s standards for data security:
    - failed to use readily available security measures, such as firewalls
    - **stored credit card information in clear text**
    - failed to implement reasonable information security procedures prior to connecting local computer networks to corporate-level networks
    - **failed to address known security vulnerabilities on servers**
    - **used default user names and passwords for access to servers**
    - **failed to require employees to use complex user IDs and passwords to access company servers**
    - failed to inventory computers to appropriately manage the network
    - **failed to maintain reasonable security measures to monitor unauthorized access + unauthorized, suspicious changes**
    - failed to conduct security investigations
    - failed to reasonably limit third-party access to company networks and computers

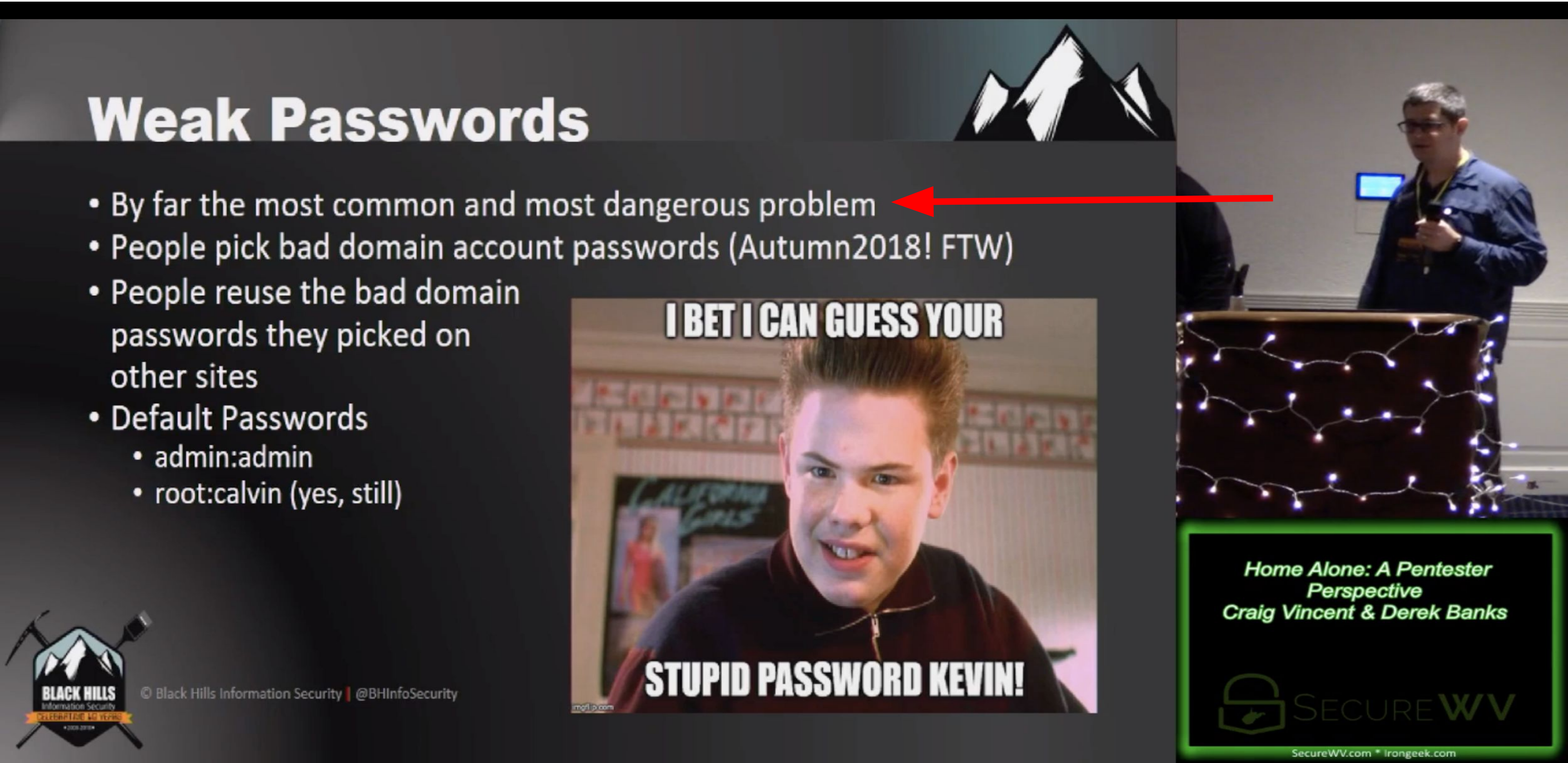
“Any company that does not address these requirements is likely to experience a breach.”

Source: https://www.hospitalitynet.org/opinion/4073687.html

Red Hat

2018 Hack3rCon/SecureWV Talk on:

Defending your organization against attackers



Weak Passwords

- By far the most common and most dangerous problem
- People pick bad domain account passwords (Autumn2018! FTW)
- People reuse the bad domain passwords they picked on other sites
- Default Passwords
  - admin:admin
  - root:calvin (yes, still)

© Black Hills Information Security | @BHInfoSecurity

Home Alone: A Pentester Perspective
Craig Vincent & Derek Banks

SecureWV.com * Irongeek.com

2018 Hack3rCon/SecureWV Talk on:
Defending your organization against attackers

- **Unpatched software last for a reason**
  - Patching is important , but more likely that authentication or configuration attacks will be used

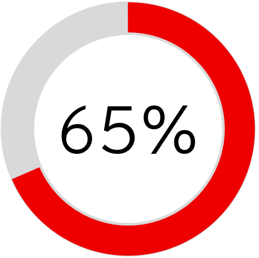
Unpatched Software

- Saved for last for a reason
- Patching is important, but more likely that authentication or configuration attacks will be used
- Sign up for USCERT email lists and email lists for the vendors of products you use to get notifications when vulns are realeased
- Run your own vulnerability scans
  - OPEN VAS is free
  - Nessus is not free, but not too expense

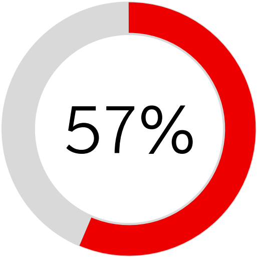
Not If. When.*(and how resilient will you be)*

Agenda
Upcoming Sessions (next 2 hours)
FND207-R1 – [REPEAT 1] Building a well-engaged and secure AWS account access management
8:45AM–10:45AM
LEVEL 2, ROOM 259A
GRC342 – Scalable encryption: A key to public sector compliance
9:30AM–10:30AM
LEVEL 0, HALL B2, BLUE
SEP321 – Innovating FIPS validation in the Cloud
9:30AM–10:30AM
LEVEL 0, HALL B2, GREEN
GRC206 – Technology compliance
9:30AM–10:30AM
LEVEL 0, HALL B2, PURPLE
Not if. When
Download the mobile app to get informati

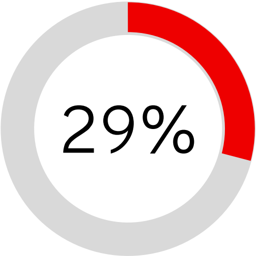
The Security Challenge is not Getting Easier In the World of Containers & Hybrid Cloud



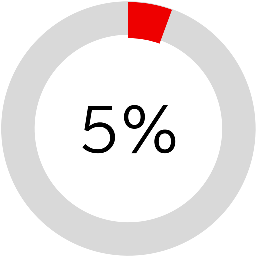
Reported increased Severity of attacks



Said the time to resolve an incident has grown



Have their ideal security-skilled staffing level, making it the #2 barrier to Cyber resilience

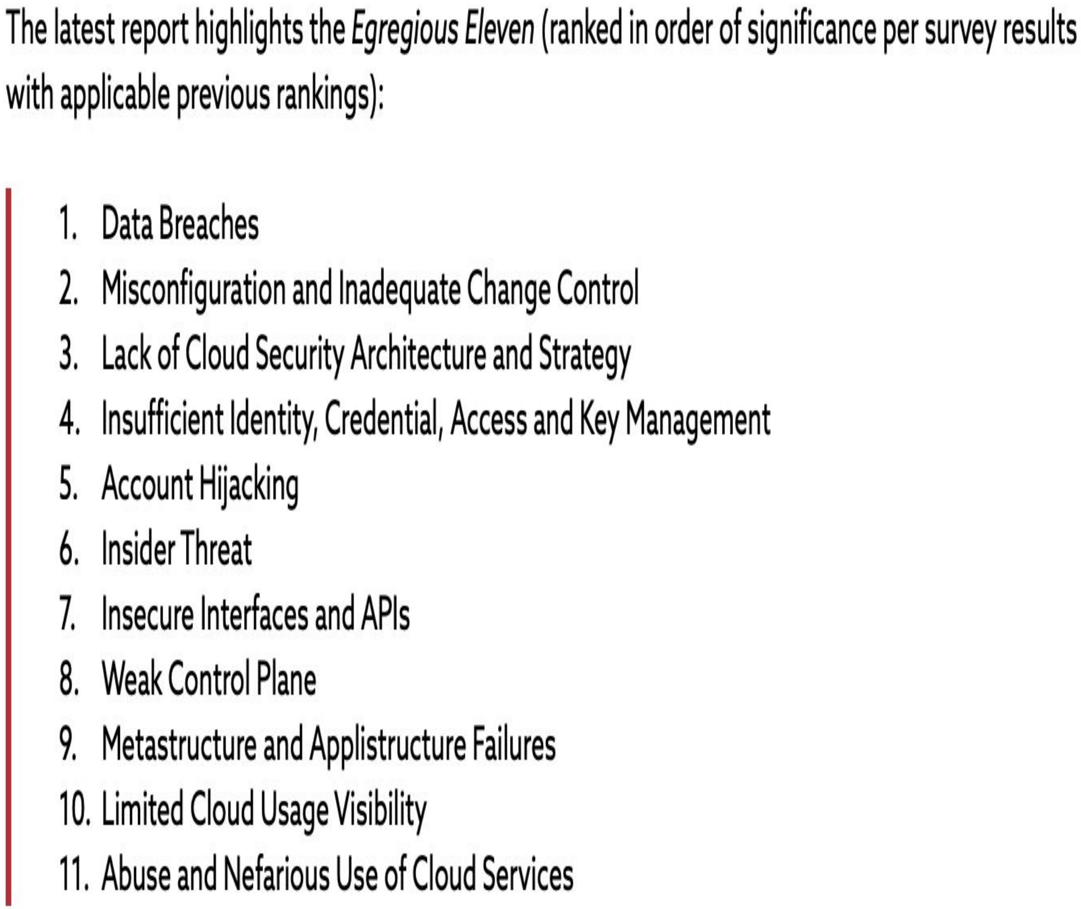


Portion of alerts coming in that the average security team examines every day

Source:

1 The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)

2 https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/


The latest report highlights the *Egregious Eleven* (ranked in order of significance per survey results with applicable previous rankings):

1. Data Breaches
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces and APIs
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services

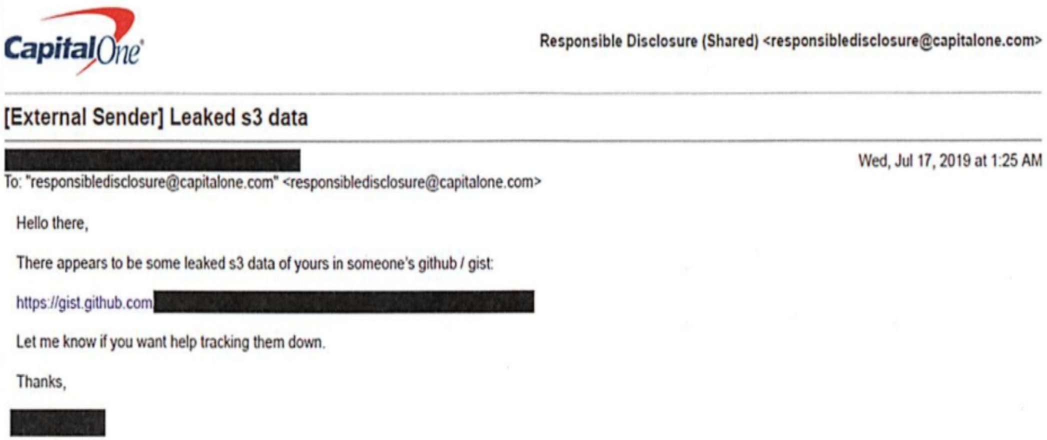
https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven

> ***“Traditional perimeter-based network security does not work in the cloud. Identity is the new perimeter.”***

Stephen Schmidt
Chief Information Security Officer, AWS

Capital One • Pixabay

Capital One Data Theft Impacts 106M People



Capital One

Responsible Disclosure (Shared) <responsibledisclosure@capitalone.com>

[External Sender] Leaked s3 data

[redacted]

Wed, Jul 17, 2019 at 1:25 AM

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

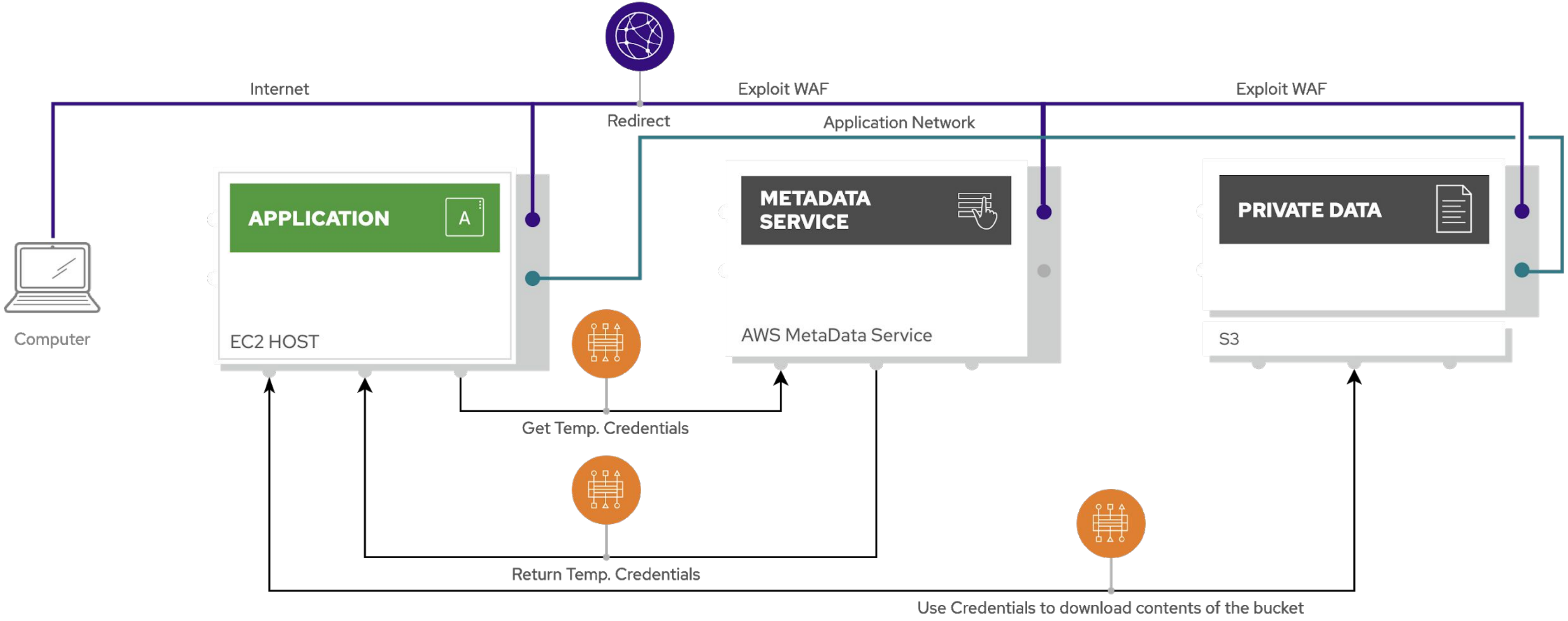
The tip that alerted Capital One to its data breach.

Former AWS engineer arrested for Capital One data breach

https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/

https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/

Looking Deeper into the Capital One Breach



"Server Side Request Forgery (SSRF) has become the most serious vulnerability facing organizations that use public clouds."

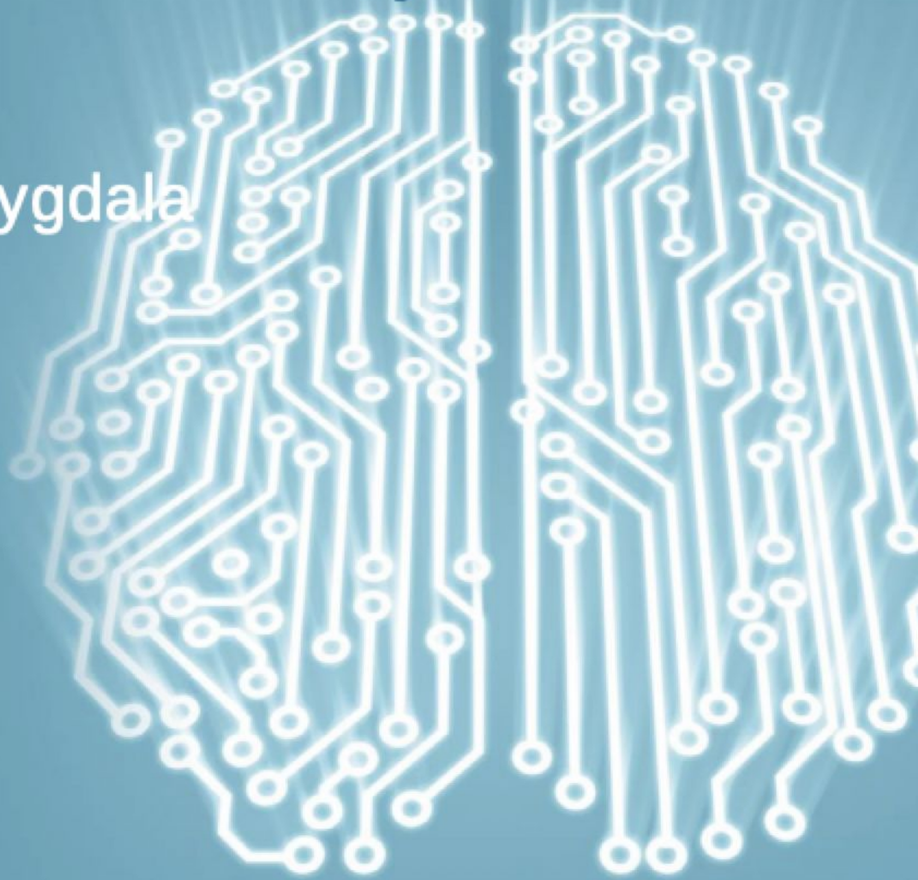
https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/

https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/

Why humans are bad at security

The neocortex versus the amygdala

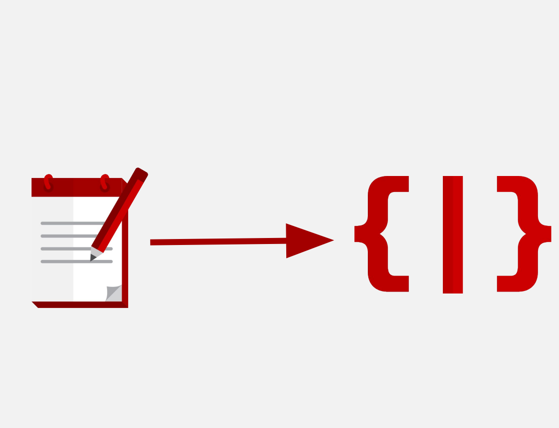
- Devaluing long term risk
- Motivated by catalyzing events
- Fighting fires first

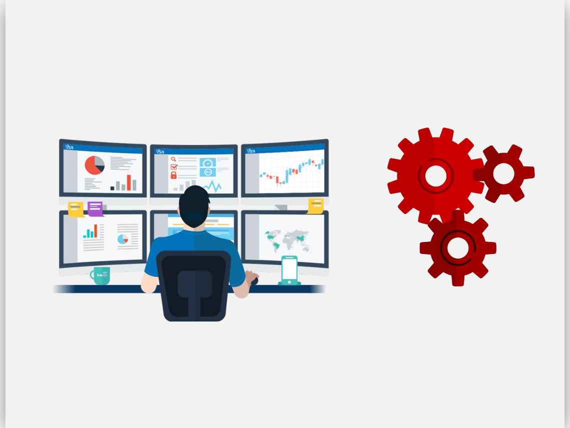


Some prescriptive steps to tackle security in this new world of containers and hybrid cloud

Implement a consistent automation strategy for the infrastructure operations, application, and security operations center

Automation for Improved Security and Compliance





Bake Security into Dev & Ops

Infrastructure, Security, and Compliance as Code =
Repeatable, Shareable, Verifiable

Continuous Monitoring & Automated Controlled Remediations

Red Hat

At Cloud Scale, You Have No Choice But to Automate

“Manually monitoring & managing systems for security and compliance becomes IMPOSSIBLE”
(Chris Gardner - Forrester)

“The Bad Guys use Automation - Fight Fire with Fire”[1]

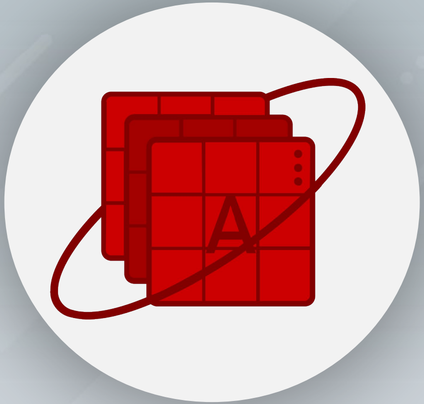
“Automate anything you can as this reduces the human error associated with many breaches we see.” [2]

Sources:

1:: Reduce Risk and Improve Security Through Infrastructure Automation (Forrester, June 2018)

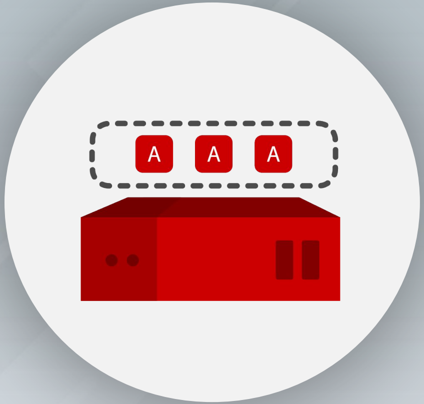
2:: 2019 and 2018 Verizon Data Breach Investigations Report

Automated Security and Compliance with Red Hat



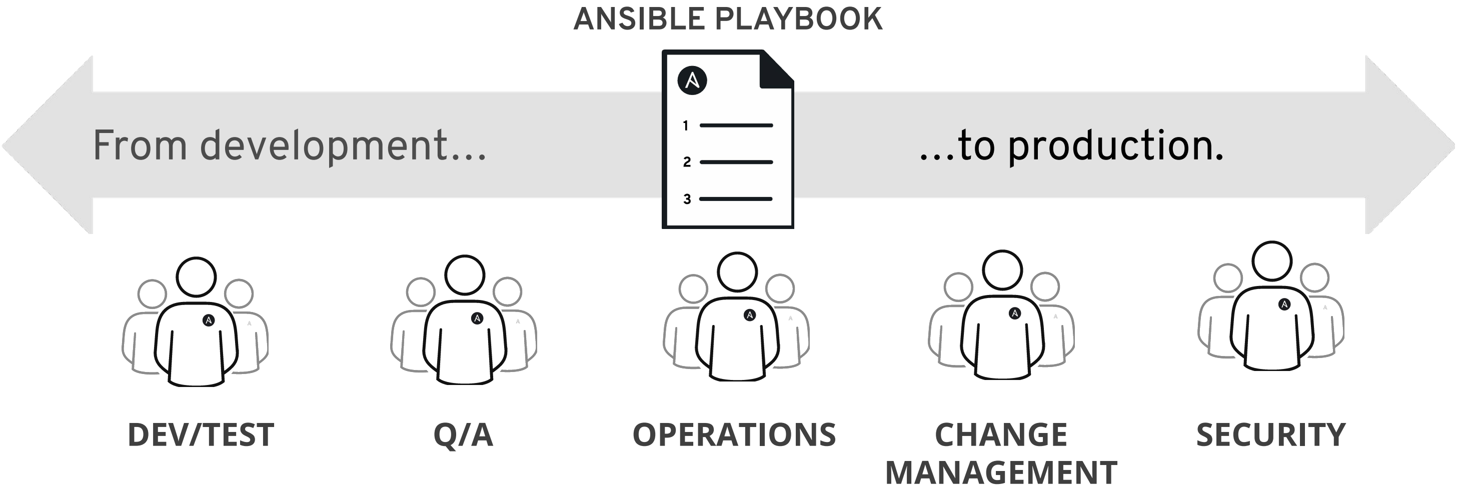
Applications

Security Operations



Infrastructure

Use Ansible as the **common language**



ANSIBLE PLAYBOOK

From development...

...to production.

DEV/TEST

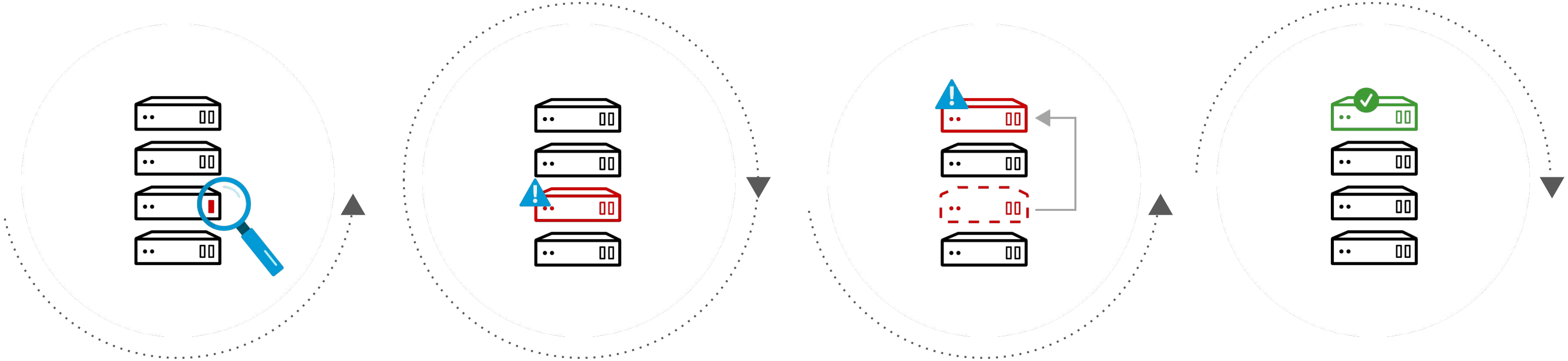
Q/A

OPERATIONS

CHANGE MANAGEMENT

SECURITY

Red Hat Automated Security & Compliance for Infrastructure Operations



Vulnerability & Compliance scanning

Host hardening

Enforcing automated compliance

Automated Patching of hosts

Automation & Analytics are the key to effective Security & Compliance

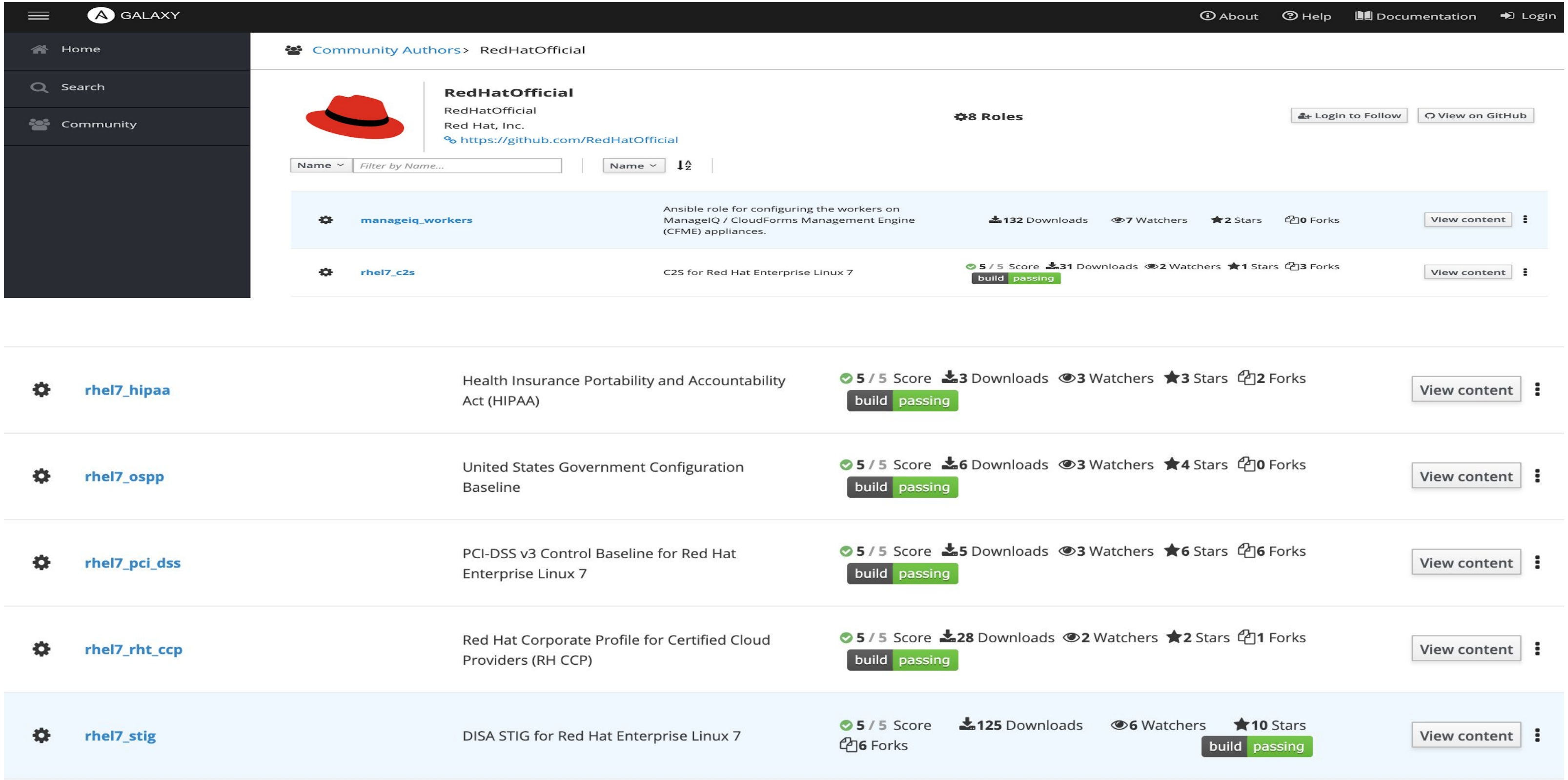
More details here:
https://red.ht/securitylabs

Red Hat

ANSIBLE ROLES FOR SECURITY COMPLIANCE

Compliance to industry standard or custom security baselines

https://galaxy.ansible.com/RedHatOfficial



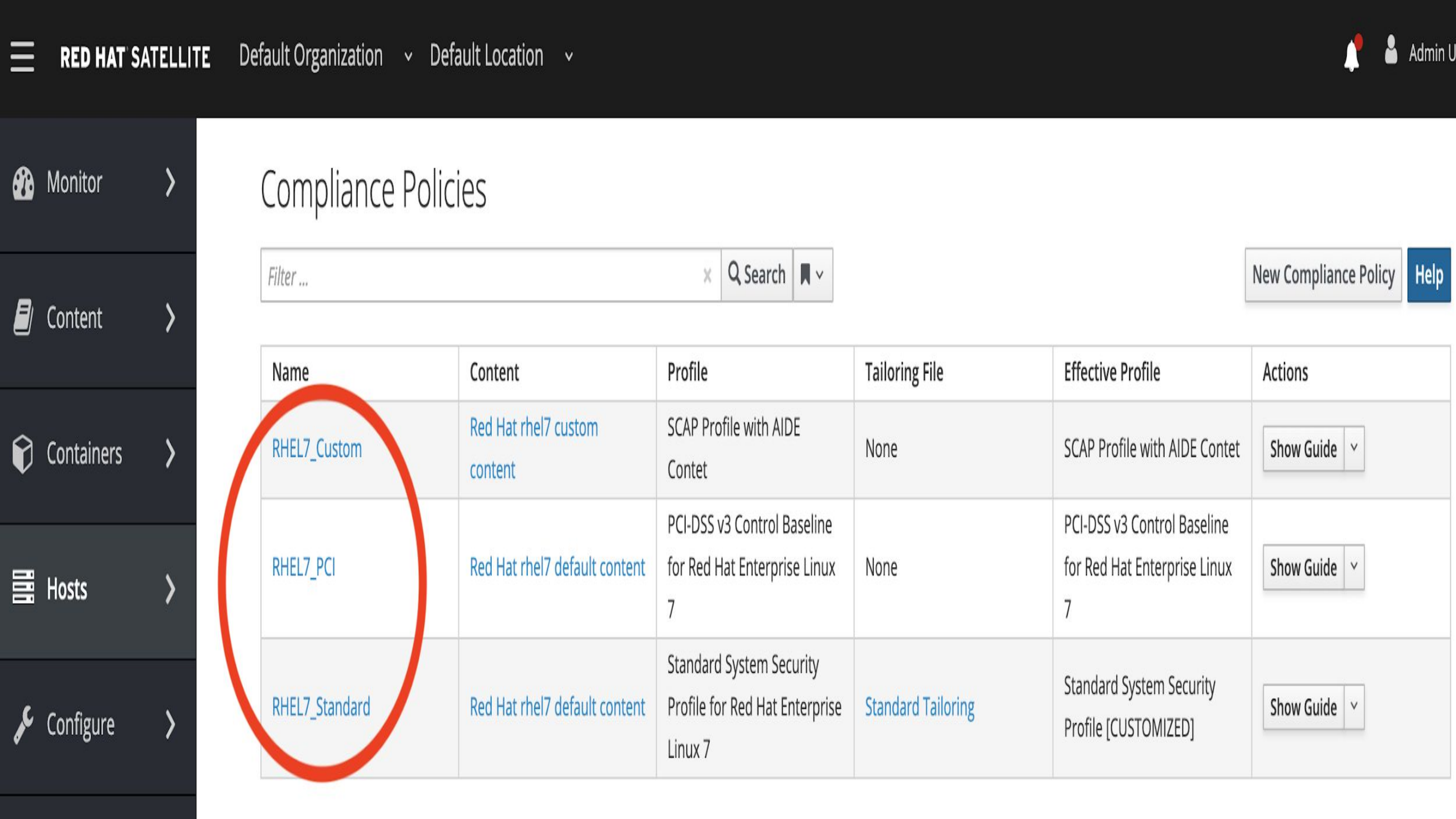
RedHatOfficial
RedHatOfficial
Red Hat, Inc.
https://github.com/RedHatOfficial

8 Roles

manageiq_workers	Ansible role for configuring the workers on ManageIQ / CloudForms Management Engine (CFME) appliances.	132 Downloads 7 Watchers 2 Stars 0 Forks	View content
rhel7_c2s	C2S for Red Hat Enterprise Linux 7	5 / 5 Score 31 Downloads 2 Watchers 1 Stars 3 Forks build passing	View content
rhel7_hipaa	Health Insurance Portability and Accountability Act (HIPAA)	5 / 5 Score 3 Downloads 3 Watchers 3 Stars 2 Forks build passing	View content
rhel7_ospp	United States Government Configuration Baseline	5 / 5 Score 6 Downloads 3 Watchers 4 Stars 0 Forks build passing	View content
rhel7_pci_dss	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	5 / 5 Score 5 Downloads 3 Watchers 6 Stars 6 Forks build passing	View content
rhel7_rht_ccp	Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	5 / 5 Score 28 Downloads 2 Watchers 2 Stars 1 Forks build passing	View content
rhel7_stig	DISA STIG for Red Hat Enterprise Linux 7	5 / 5 Score 125 Downloads 6 Watchers 10 Stars 6 Forks build passing	View content

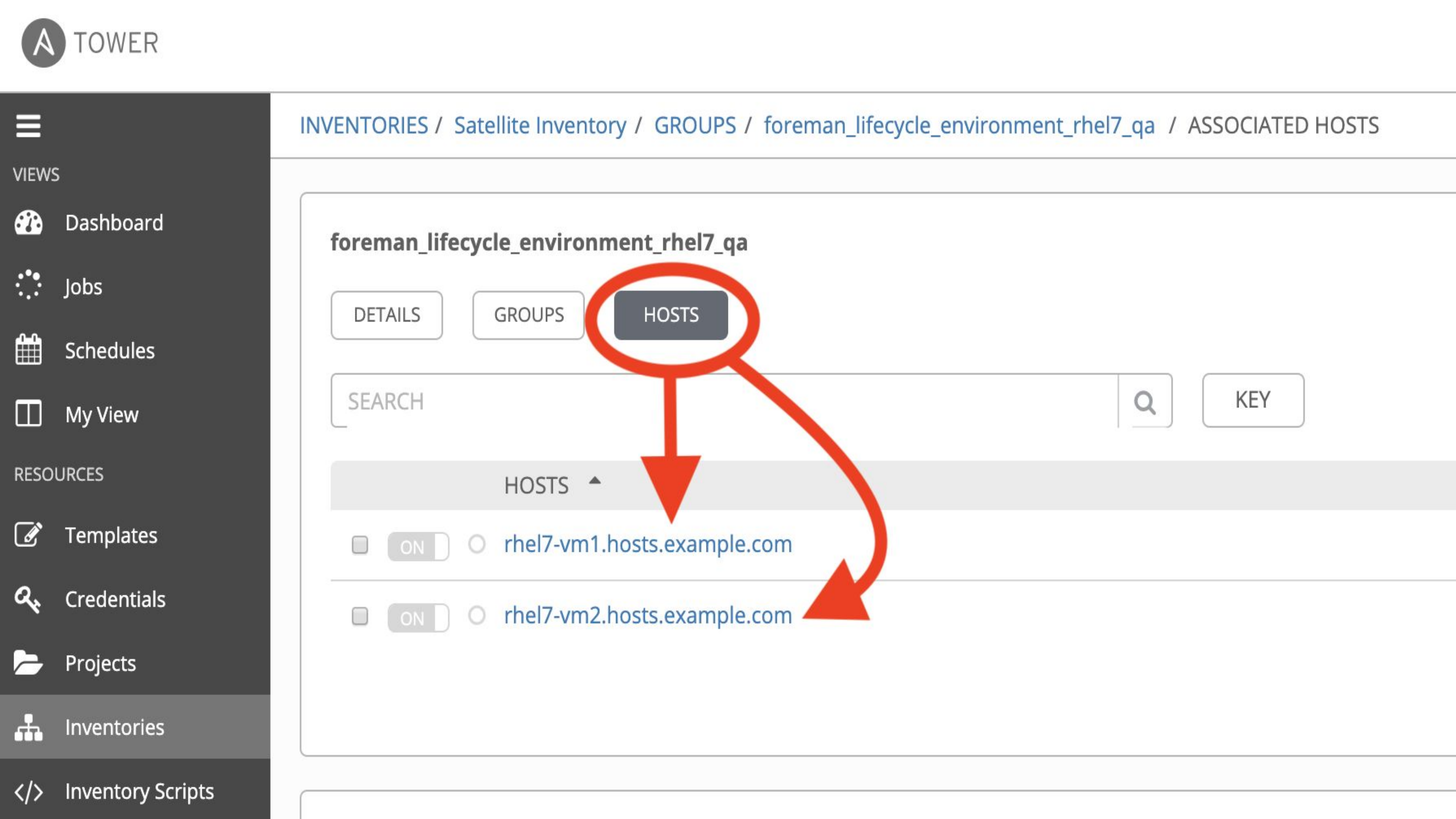
Vulnerability & Compliance Scanning + Remediations on Hosts at Scale with Red Hat Ansible Tower + Satellite

Red Hat



Compliance Policies

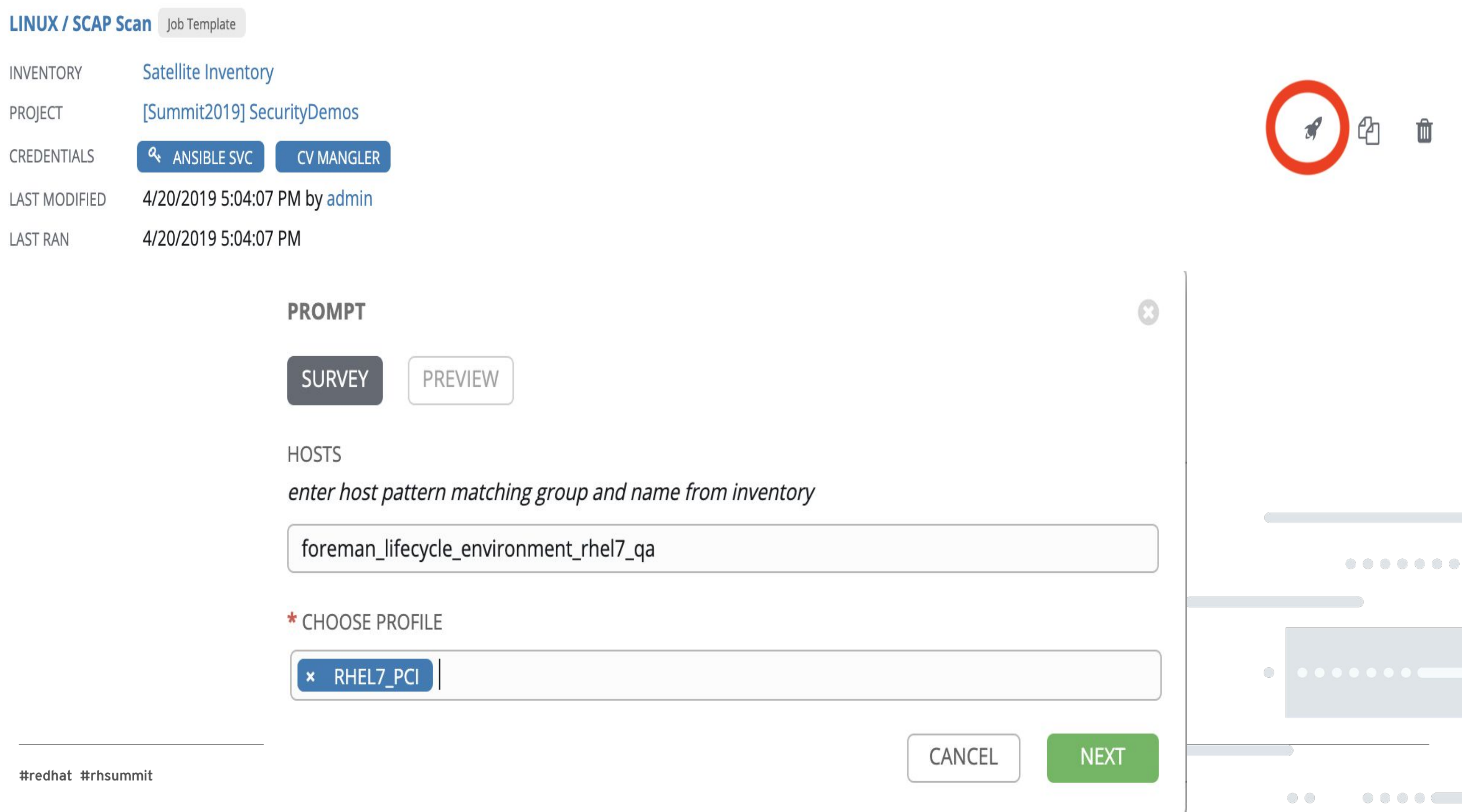
Name	Content	Profile	Tailoring File	Effective Profile	Actions
RHEL7_Custom	Red Hat rhel7 custom content	SCAP Profile with AIDE Contet	None	SCAP Profile with AIDE Contet	Show Guide
RHEL7_PCI	Red Hat rhel7 default content	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	None	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	Show Guide
RHEL7_Standard	Red Hat rhel7 default content	Standard System Security Profile for Red Hat Enterprise Linux 7	Standard Tailoring	Standard System Security Profile [CUSTOMIZED]	Show Guide



INVENTORIES / Satellite Inventory / GROUPS / foreman_lifecycle_environment_rhel7_qa / ASSOCIATED HOSTS

foreman_lifecycle_environment_rhel7_qa

HOSTS
rhel7-vm1.hosts.example.com
rhel7-vm2.hosts.example.com



LINUX / SCAP Scan Job Template

INVENTORY Satellite Inventory

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC CV MANGLER

LAST MODIFIED 4/20/2019 5:04:07 PM by admin

LAST RAN 4/20/2019 5:04:07 PM

PROMPT

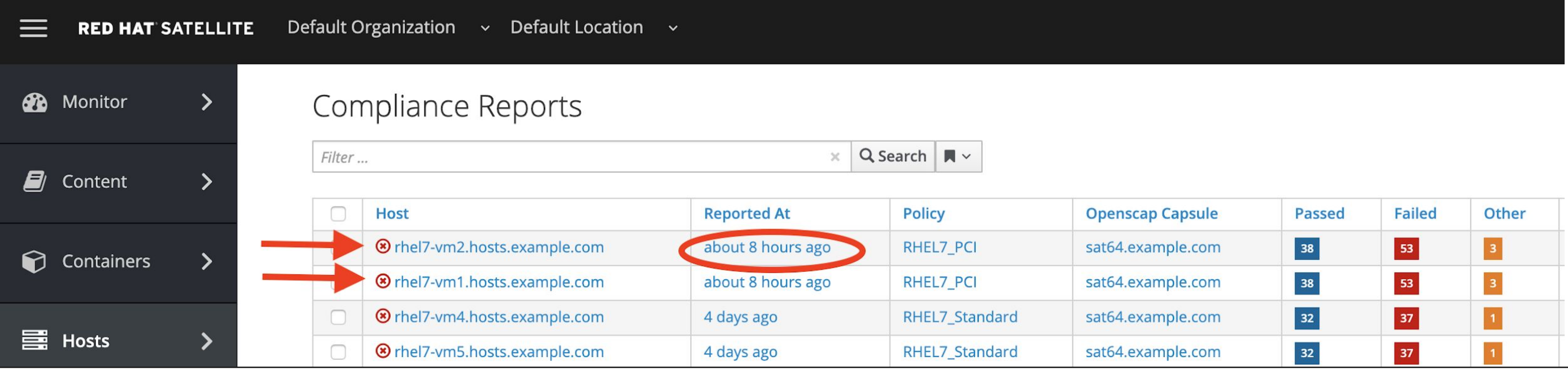
HOSTS

enter host pattern matching group and name from inventory

foreman_lifecycle_environment_rhel7_qa

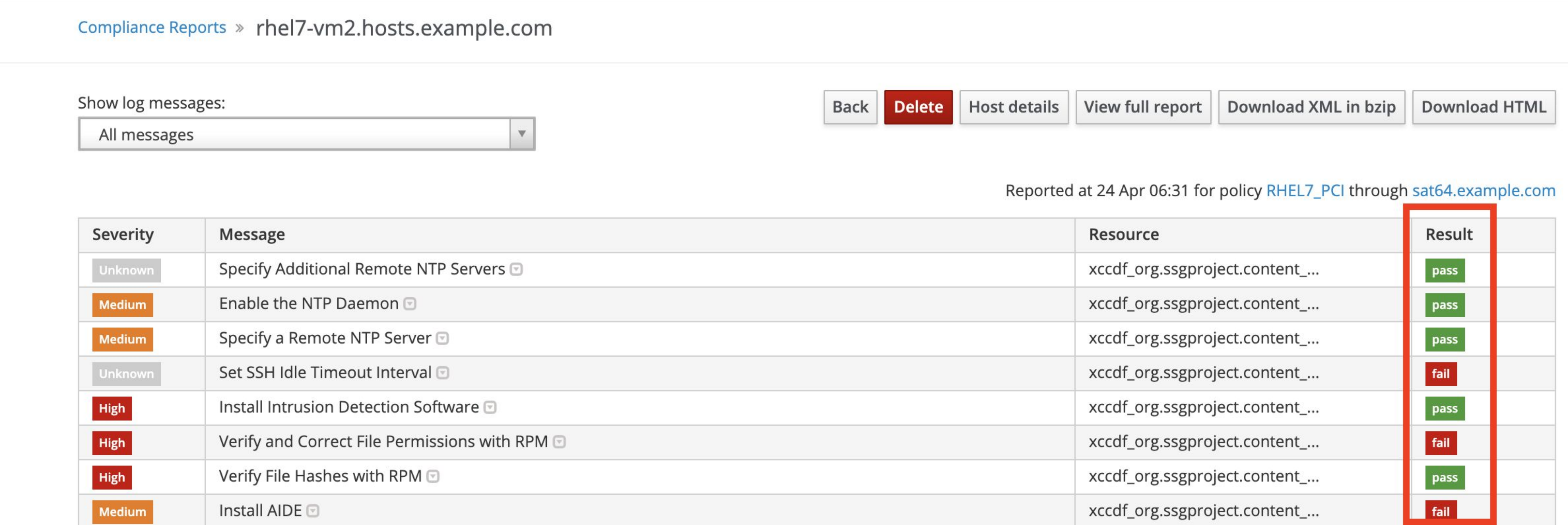
* CHOOSE PROFILE

× RHEL7_PCI



Compliance Reports

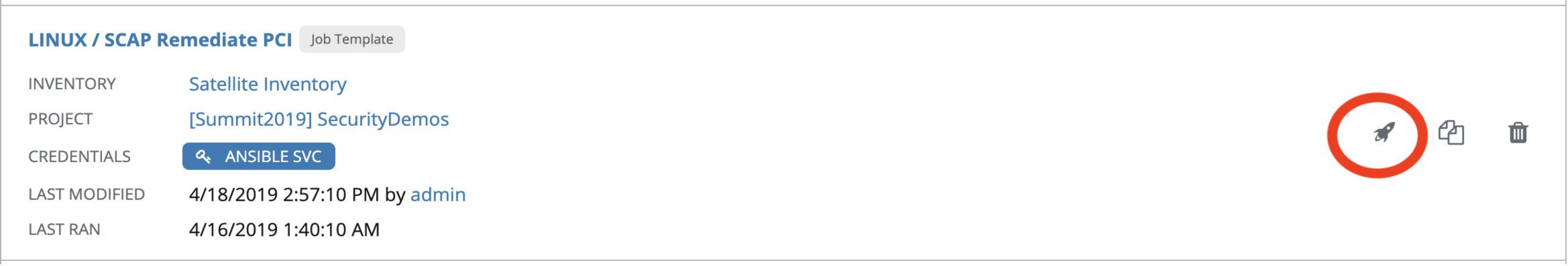
Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other
rhel7-vm2.hosts.example.com	about 8 hours ago	RHEL7_PCI	sat64.example.com	38	53	3
rhel7-vm1.hosts.example.com	about 8 hours ago	RHEL7_PCI	sat64.example.com	38	53	3
rhel7-vm4.hosts.example.com	4 days ago	RHEL7_Standard	sat64.example.com	32	37	1
rhel7-vm5.hosts.example.com	4 days ago	RHEL7_Standard	sat64.example.com	32	37	1



Show log messages: All messages

Reported at 24 Apr 06:31 for policy RHEL7_PCI through sat64.example.com

Severity	Message	Resource	Result
Unknown	Specify Additional Remote NTP Servers	xccdf_org.ssgproject.content_...	pass
Medium	Enable the NTP Daemon	xccdf_org.ssgproject.content_...	pass
Medium	Specify a Remote NTP Server	xccdf_org.ssgproject.content_...	pass
Unknown	Set SSH Idle Timeout Interval	xccdf_org.ssgproject.content_...	fail
High	Install Intrusion Detection Software	xccdf_org.ssgproject.content_...	pass
High	Verify and Correct File Permissions with RPM	xccdf_org.ssgproject.content_...	fail
High	Verify File Hashes with RPM	xccdf_org.ssgproject.content_...	pass
Medium	Install AIDE	xccdf_org.ssgproject.content_...	fail



LINUX / SCAP Remediate PCI

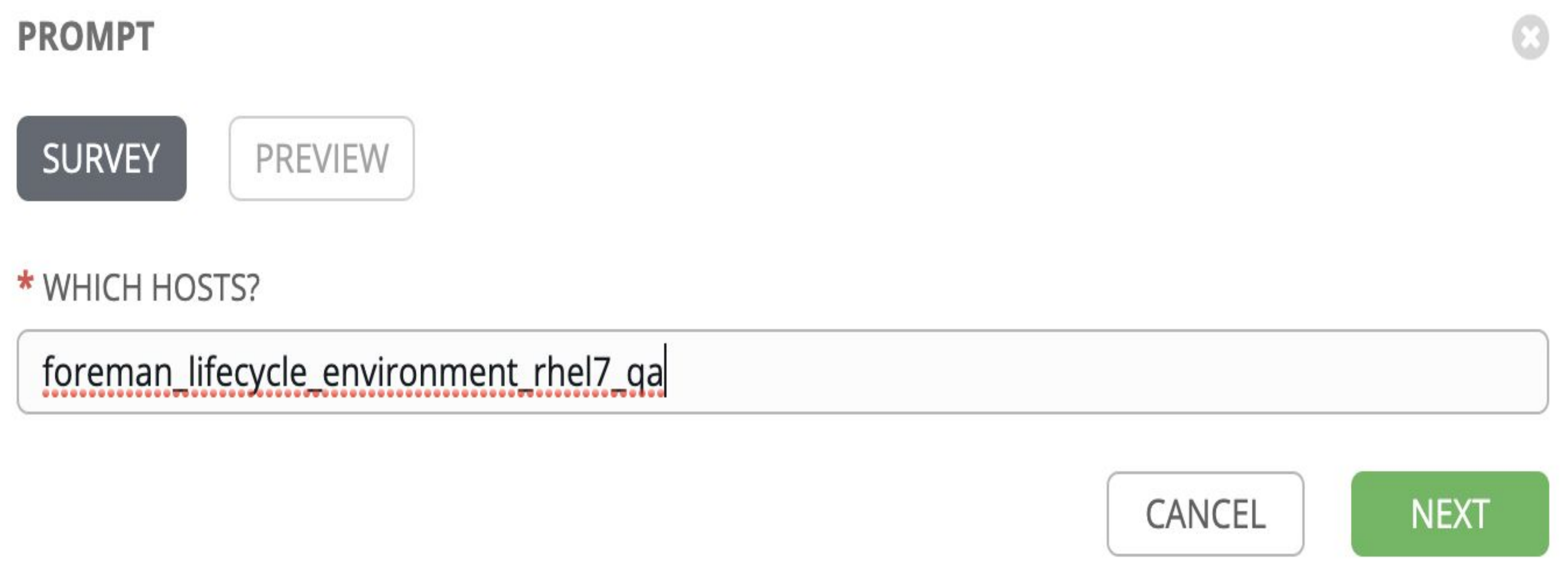
INVENTORY Satellite Inventory

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC

LAST MODIFIED 4/18/2019 2:57:10 PM by admin

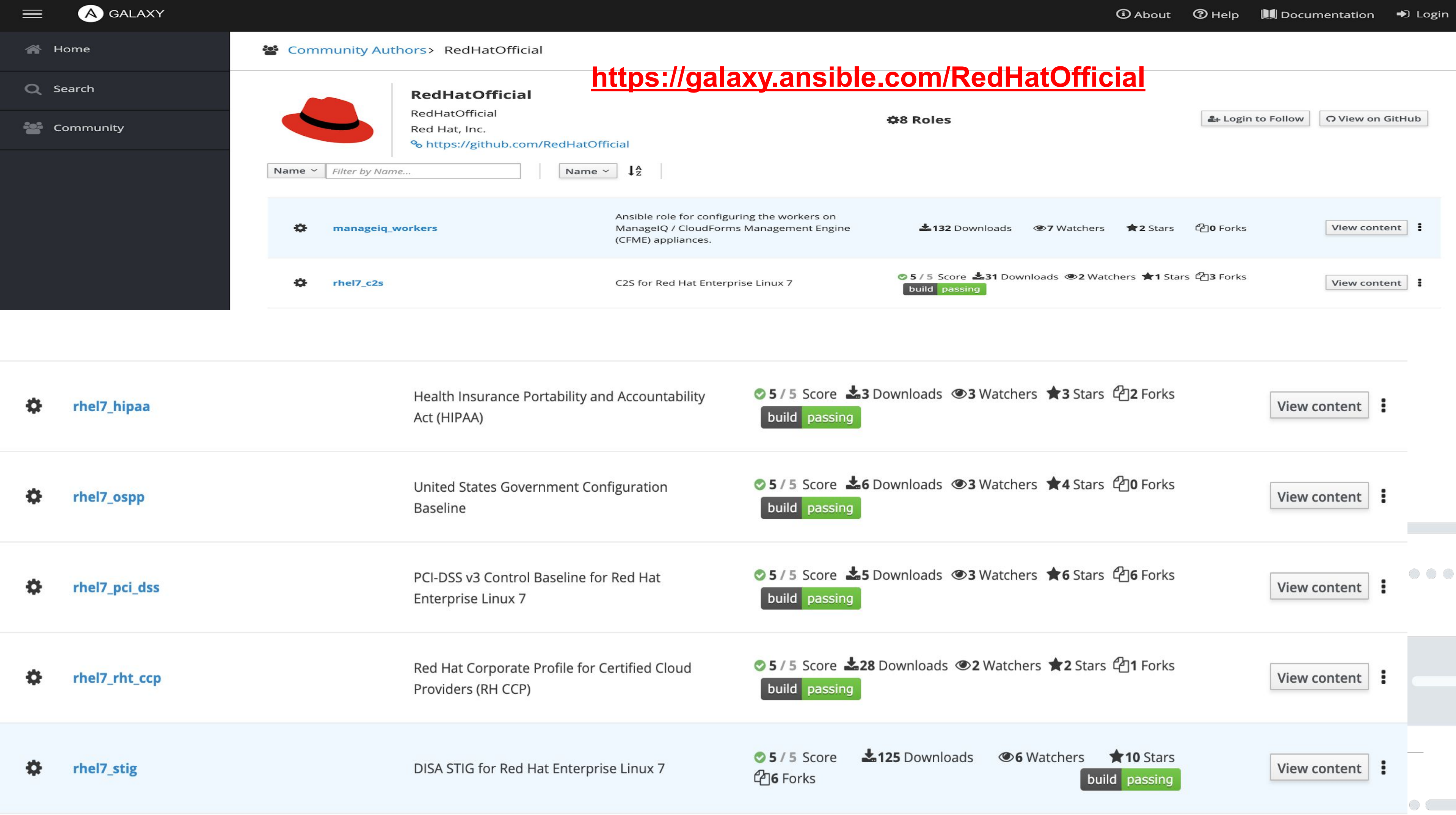
LAST RAN 4/16/2019 1:40:10 AM



PROMPT

* WHICH HOSTS?

foreman_lifecycle_environment_rhel7_qa



https://galaxy.ansible.com/RedHatOfficial

Community Authors > RedHatOfficial

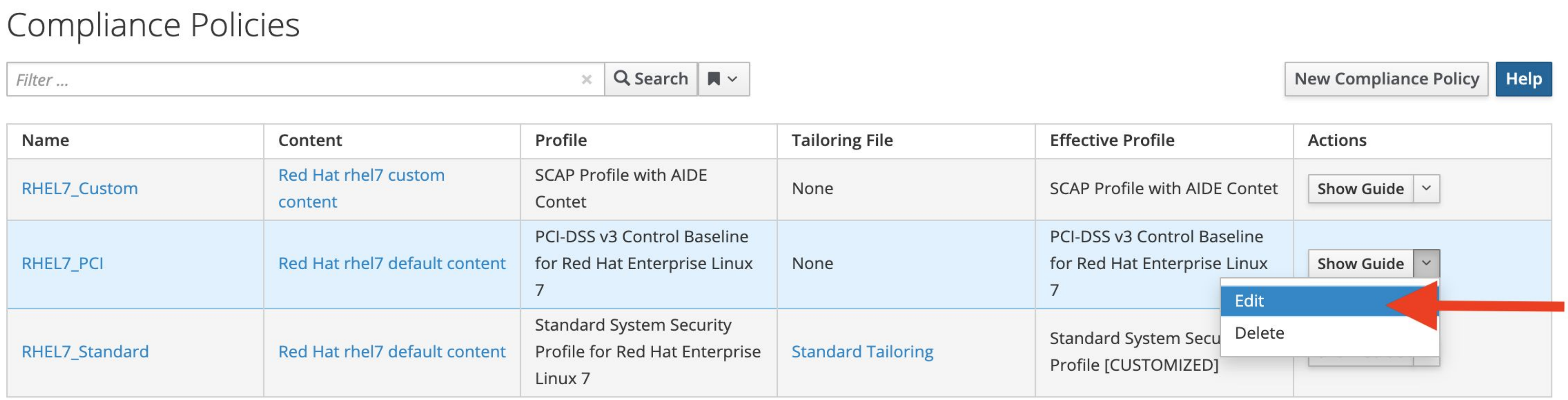
RedHatOfficial
RedHatOfficial
Red Hat, Inc.
https://github.com/RedHatOfficial

8 Roles

Login to Follow | View on GitHub

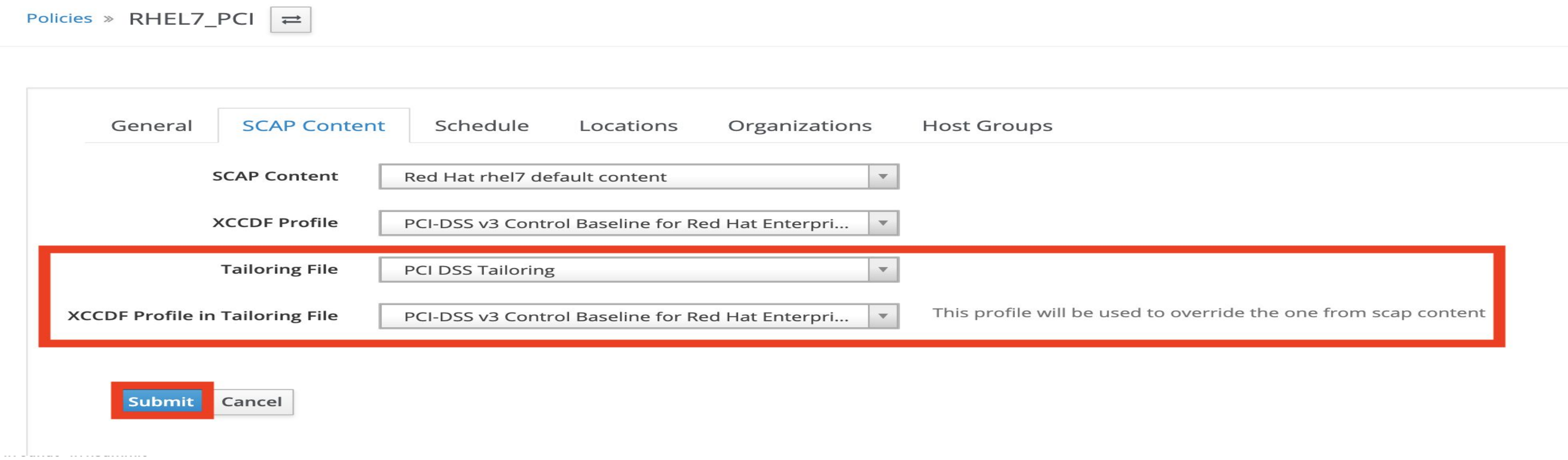
Name | Filter by Name... | Name

Role	Description	Stats	
manageiq_workers	Ansible role for configuring the workers on ManageIQ / CloudForms Management Engine (CFME) appliances.	132 Downloads 7 Watchers 2 Stars 0 Forks	View content
rhel7_c2s	C2S for Red Hat Enterprise Linux 7	5 / 5 Score 31 Downloads 2 Watchers 1 Stars 3 Forks build passing	View content
rhel7_hipaa	Health Insurance Portability and Accountability Act (HIPAA)	5 / 5 Score 3 Downloads 3 Watchers 3 Stars 2 Forks build passing	View content
rhel7_ospp	United States Government Configuration Baseline	5 / 5 Score 6 Downloads 3 Watchers 4 Stars 0 Forks build passing	View content
rhel7_pci_dss	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	5 / 5 Score 5 Downloads 3 Watchers 6 Stars 6 Forks build passing	View content
rhel7_rht_ccp	Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	5 / 5 Score 28 Downloads 2 Watchers 2 Stars 1 Forks build passing	View content
rhel7_stig	DISA STIG for Red Hat Enterprise Linux 7	5 / 5 Score 125 Downloads 6 Watchers 10 Stars 6 Forks build passing	View content



Compliance Policies

Name	Content	Profile	Tailoring File	Effective Profile	Actions
RHEL7_Custom	Red Hat rhel7 custom content	SCAP Profile with AIDE Contet	None	SCAP Profile with AIDE Contet	Show Guide
RHEL7_PCI	Red Hat rhel7 default content	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	None	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	Show Guide
RHEL7_Standard	Red Hat rhel7 default content	Standard System Security Profile for Red Hat Enterprise Linux 7	Standard Tailoring	Standard System Secu Profile [CUSTOMIZED]	



Policies » RHEL7_PCI

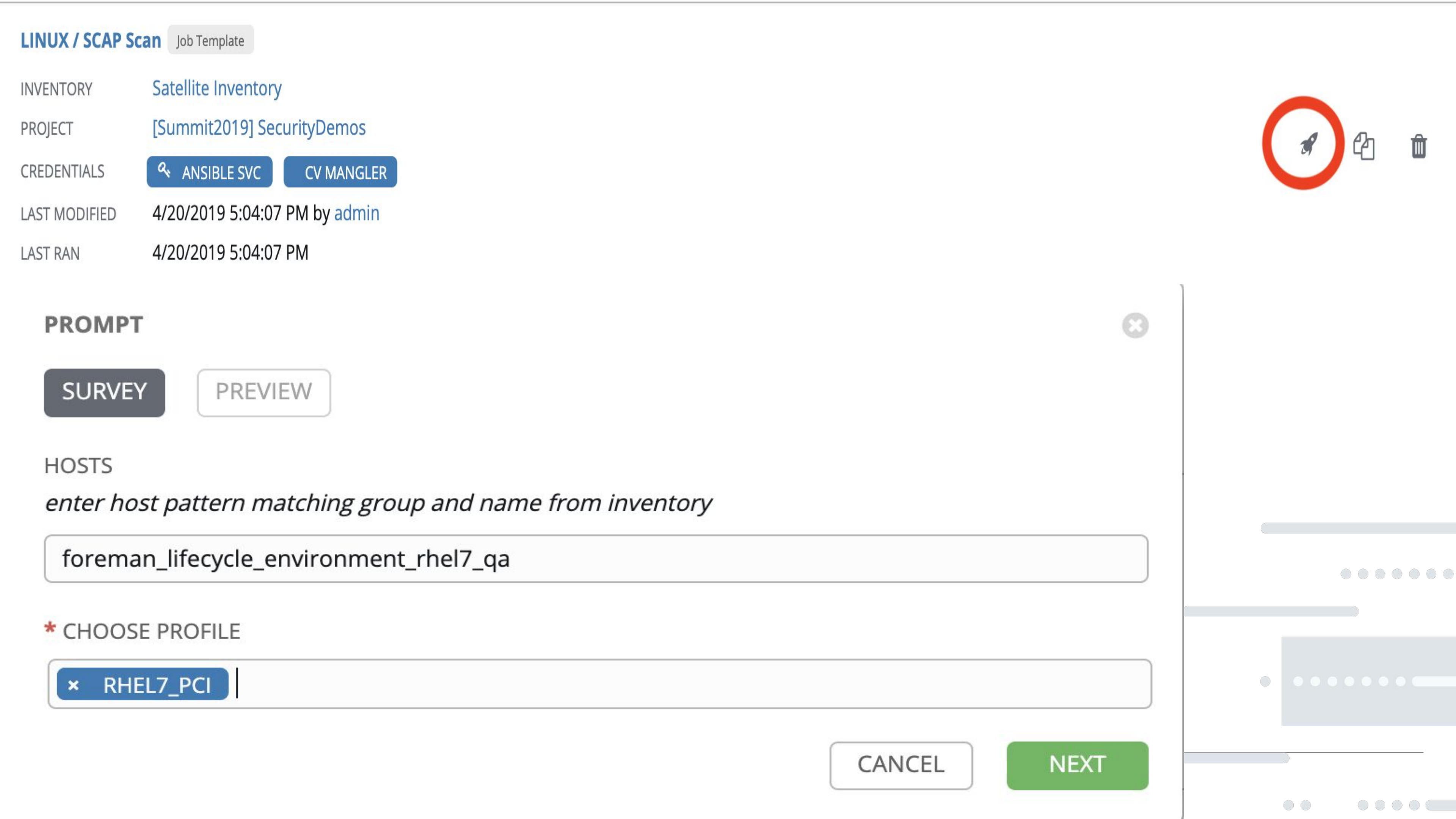
SCAP Content: Red Hat rhel7 default content

XCCDF Profile: PCI-DSS v3 Control Baseline for Red Hat Enterpri...

Tailoring File: PCI DSS Tailoring

XCCDF Profile in Tailoring File: PCI-DSS v3 Control Baseline for Red Hat Enterpri...

This profile will be used to override the one from scap content



LINUX / SCAP Scan Job Template

INVENTORY Satellite Inventory

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC CV MANGLER

LAST MODIFIED 4/20/2019 5:04:07 PM by admin

LAST RAN 4/20/2019 5:04:07 PM

PROMPT

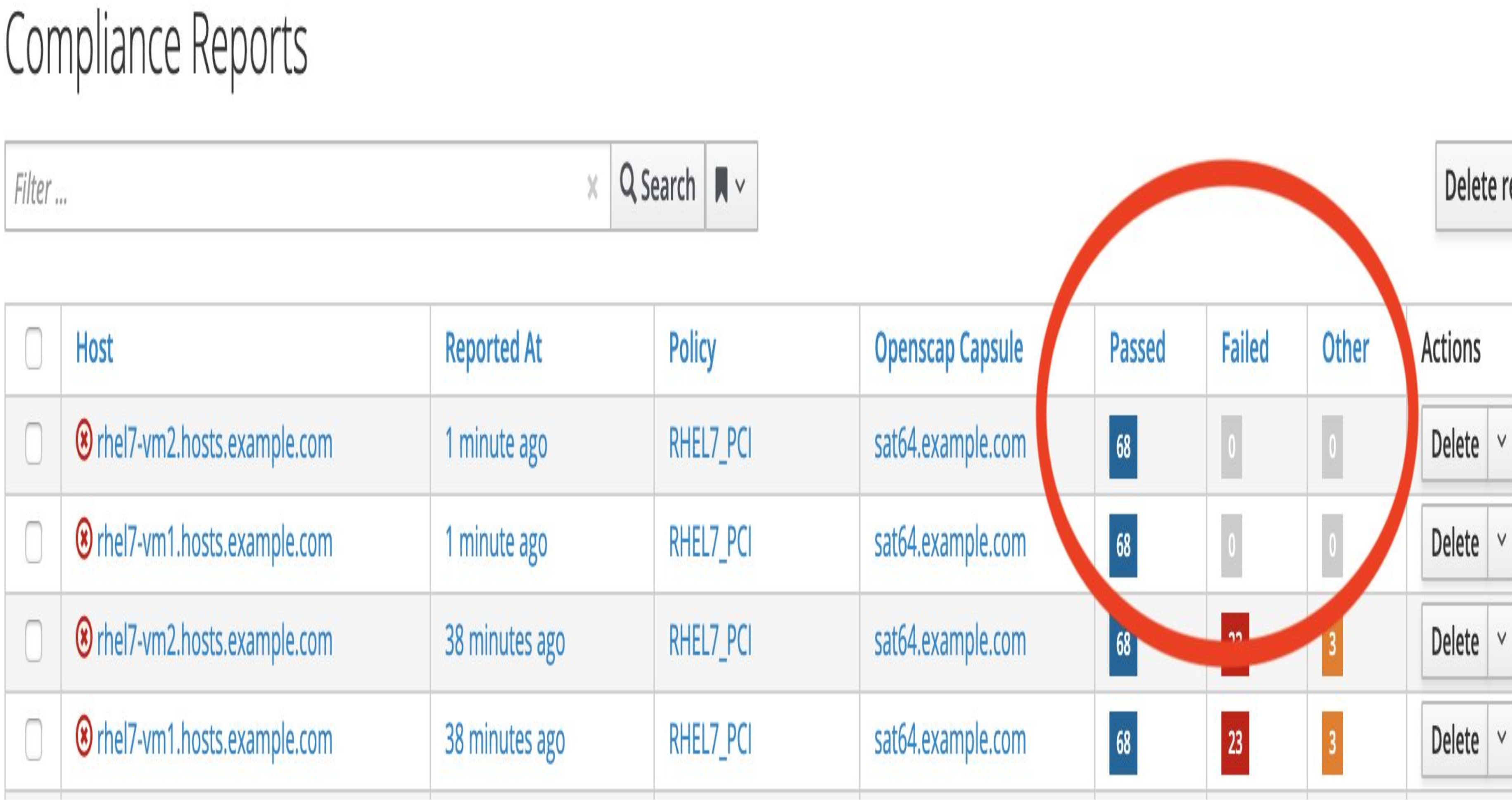
HOSTS

enter host pattern matching group and name from inventory

foreman_lifecycle_environment_rhel7_qa

* CHOOSE PROFILE

× RHEL7_PCI



Compliance Reports

Filter ... ✕ Search ∨

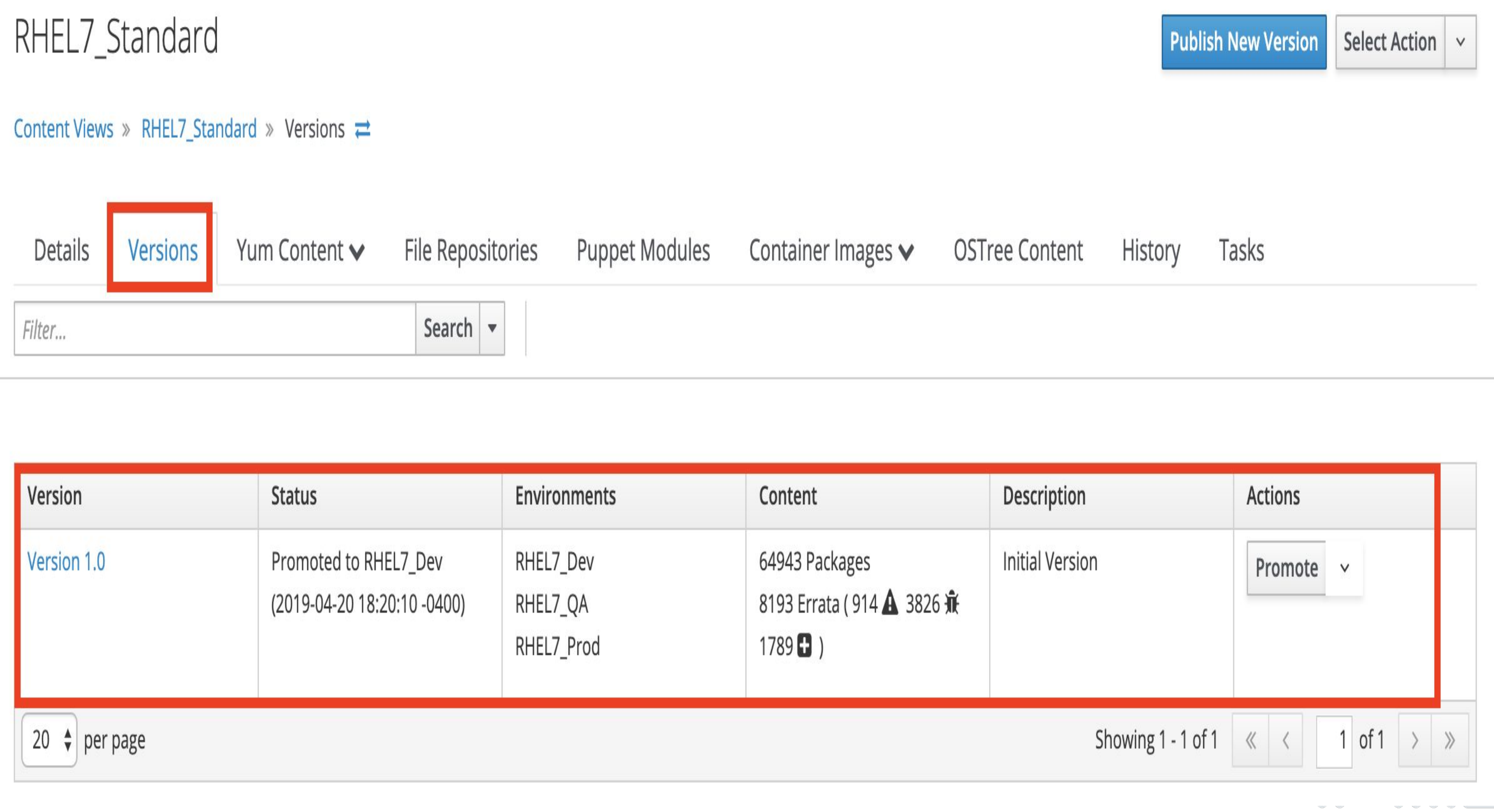
Delete r

□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other	Actions
□	⊗ rhel7-vm2.hosts.example.com	1 minute ago	RHEL7_PCI	sat64.example.com	68	0	0	Delete ∨
□	⊗ rhel7-vm1.hosts.example.com	1 minute ago	RHEL7_PCI	sat64.example.com	68	0	0	Delete ∨
□	⊗ rhel7-vm2.hosts.example.com	38 minutes ago	RHEL7_PCI	sat64.example.com	68	23	3	Delete ∨
□	⊗ rhel7-vm1.hosts.example.com	38 minutes ago	RHEL7_PCI	sat64.example.com	68	23	3	Delete ∨

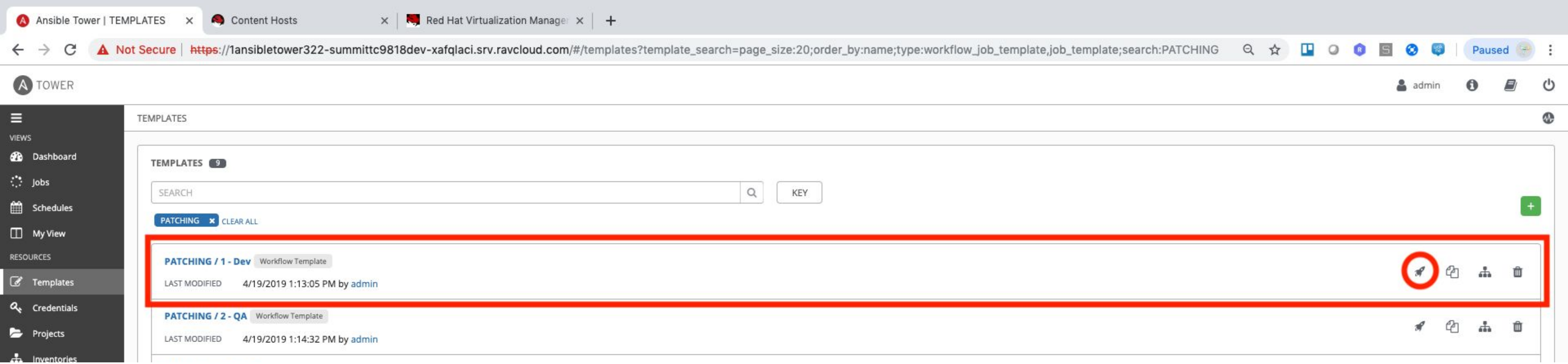
Automated Patching of Host Systems at Scale

AFTERNOON KEYNOTE
John Evans, Chief Information Security Officer (CISO)
MD Department Information Technology (DoIT)
CYBER//2019
HOWARD
COMMUNITY COLLEGE

“There is no such thing as 100% security. But, the majority of the time, you can stay secure if you do these three things (particularly patching). Yes, some bad actors have more resources but you will thwart 99% of them:
1) protect /lock down exposed network protocols (ssh, snmp, etc) to stop initial foothold - regular scans of network
2) ***regular patching - most important of three (stop lateral movement with patching)***
3) training of people “



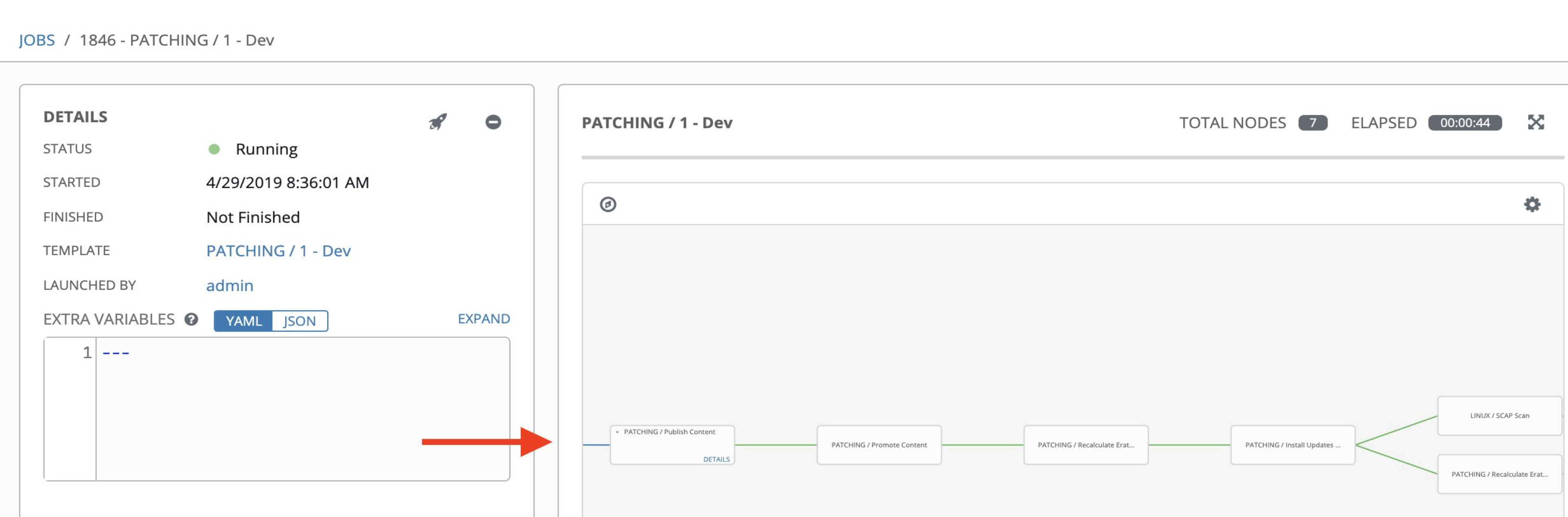
Version	Status	Environments	Content	Description	Actions
Version 1.0	Promoted to RHEL7_Dev (2019-04-20 18:20:10 -0400)	RHEL7_Dev RHEL7_QA RHEL7_Prod	64943 Packages 8193 Errata (914 ⚠ 3826 🐞 1789 ⊞)	Initial Version	Promote


Ansible Tower | TEMPLATES
Content Hosts
Red Hat Virtualization Manager
Not Secure
https://1ansibletower322-summittc9818dev-xafqlaci.srv.ravcloud.com/#/templates?template_search=page_size:20;order_by:name;type:workflow_job_template,job_template;search:PATCHING
Paused
TOWER
admin
VIEWS
Dashboard
Jobs
Schedules
My View
RESOURCES
Templates
Credentials
Projects
Inventories
TEMPLATES
SEARCH
KEY
CLEAR ALL

TEMPLATES 9

PATCHING ×

PATCHING / 1 - Dev	Workflow Template
LAST MODIFIED	4/19/2019 1:13:05 PM by admin
PATCHING / 2 - QA	Workflow Template
LAST MODIFIED	4/19/2019 1:14:32 PM by admin



JOBS / 1846 - PATCHING / 1 - Dev

DETAILS

STATUS	● Running
STARTED	4/29/2019 8:36:01 AM
FINISHED	Not Finished
TEMPLATE	PATCHING / 1 - Dev
LAUNCHED BY	admin

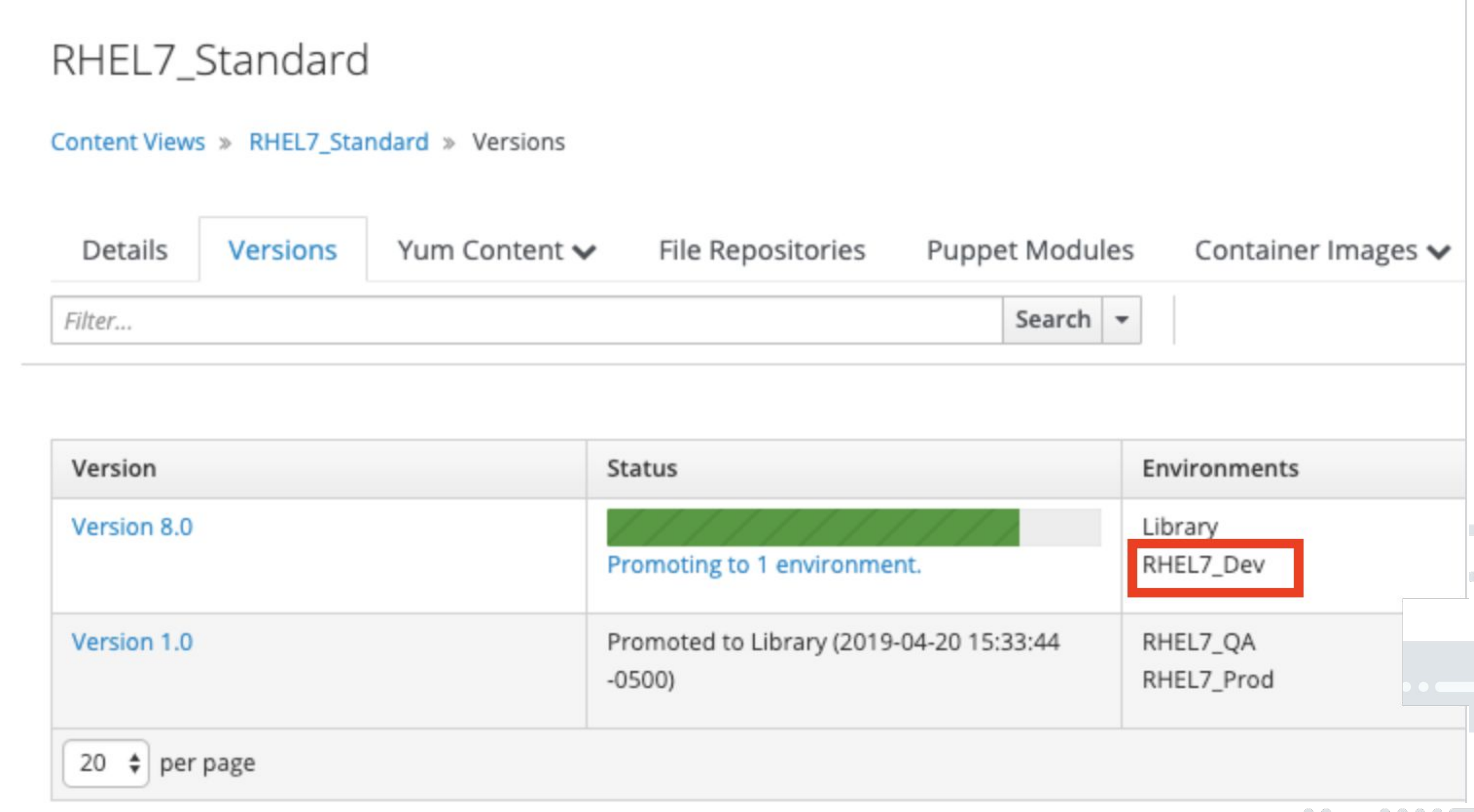
EXTRA VARIABLES

```
---
```

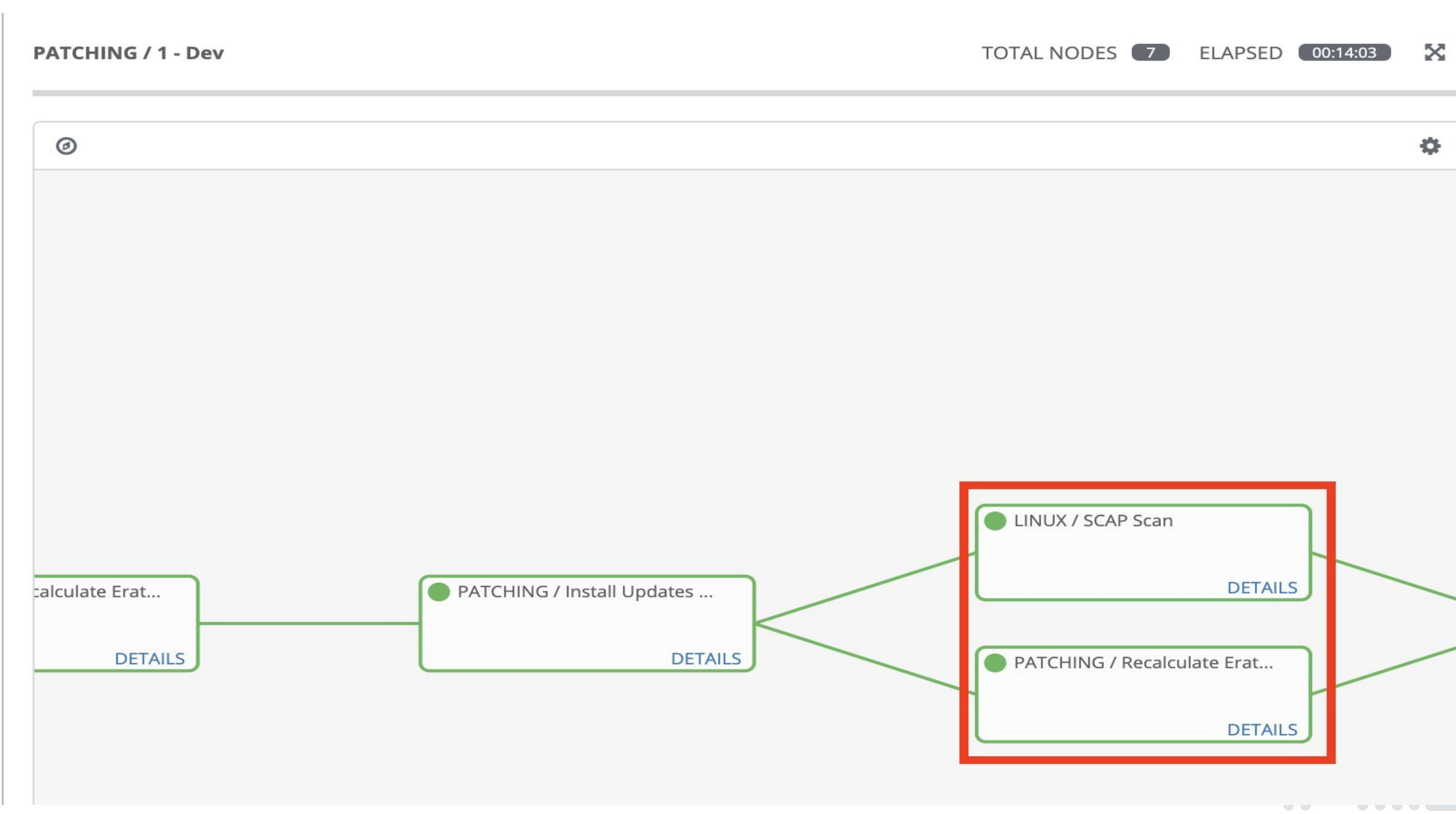
PATCHING / 1 - Dev

TOTAL NODES 7 ELAPSED 00:00:44

PATCHING / Publish Content
PATCHING / Promote Content
PATCHING / Recalculate Erat...
PATCHING / Install Updates ...
LINUX / SCAP Scan
PATCHING / Recalculate Erat...



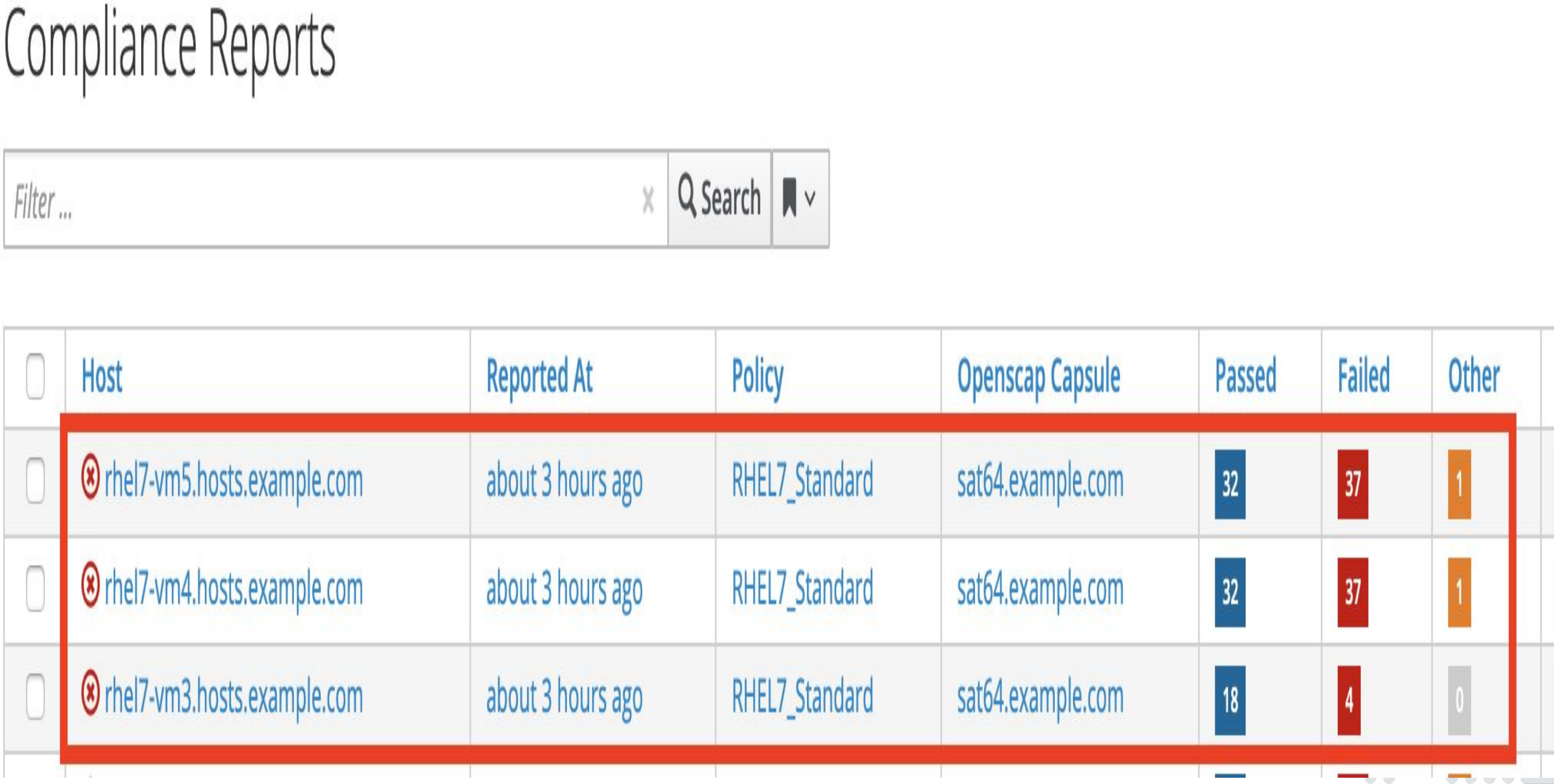
Version	Status	Environments
Version 8.0	Promoting to 1 environment.	Library RHEL7_Dev
Version 1.0	Promoted to Library (2019-04-20 15:33:44 -0500)	RHEL7_QA RHEL7_Prod



PATCHING / 1 - Dev

TOTAL NODES 7

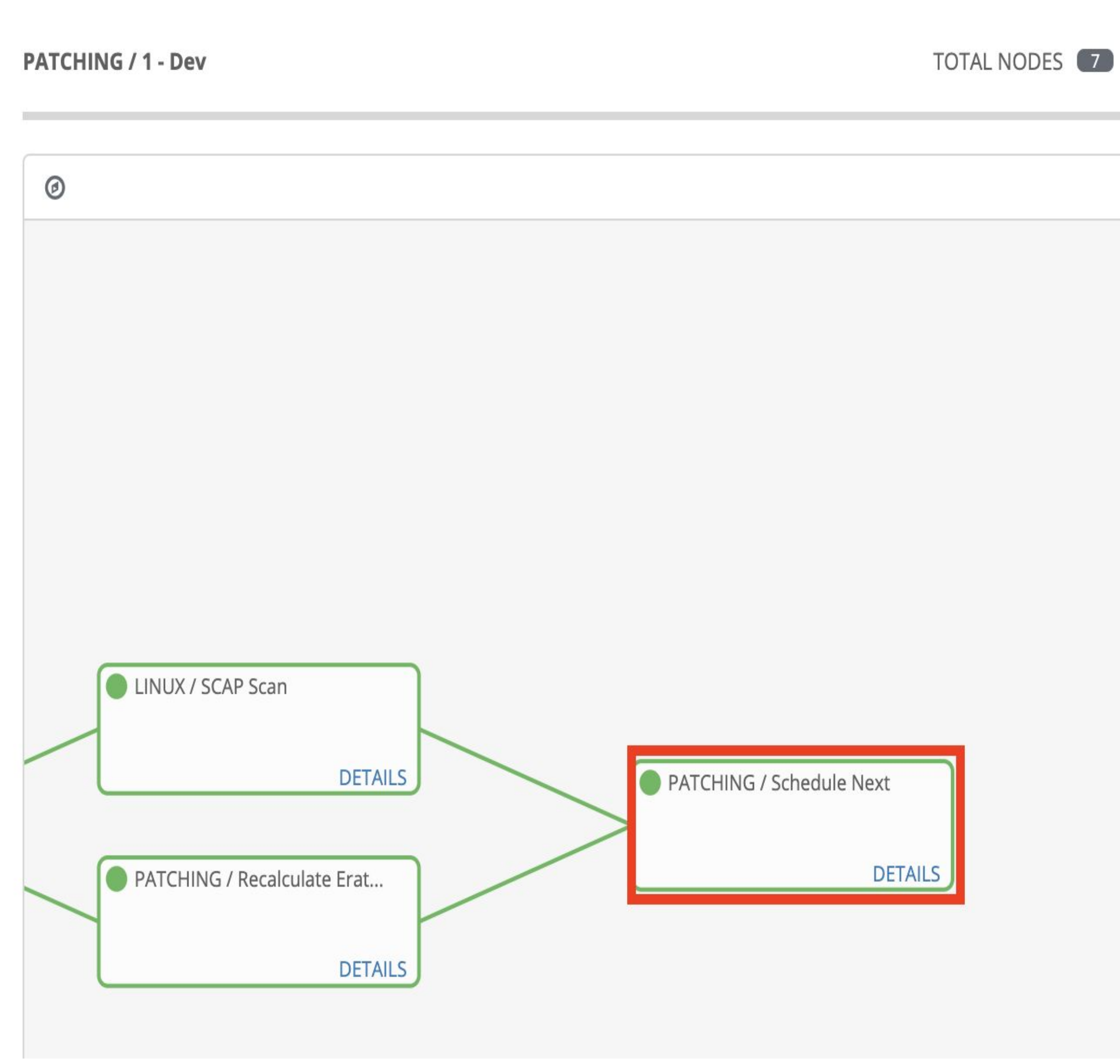
ELAPSED 00:14:03

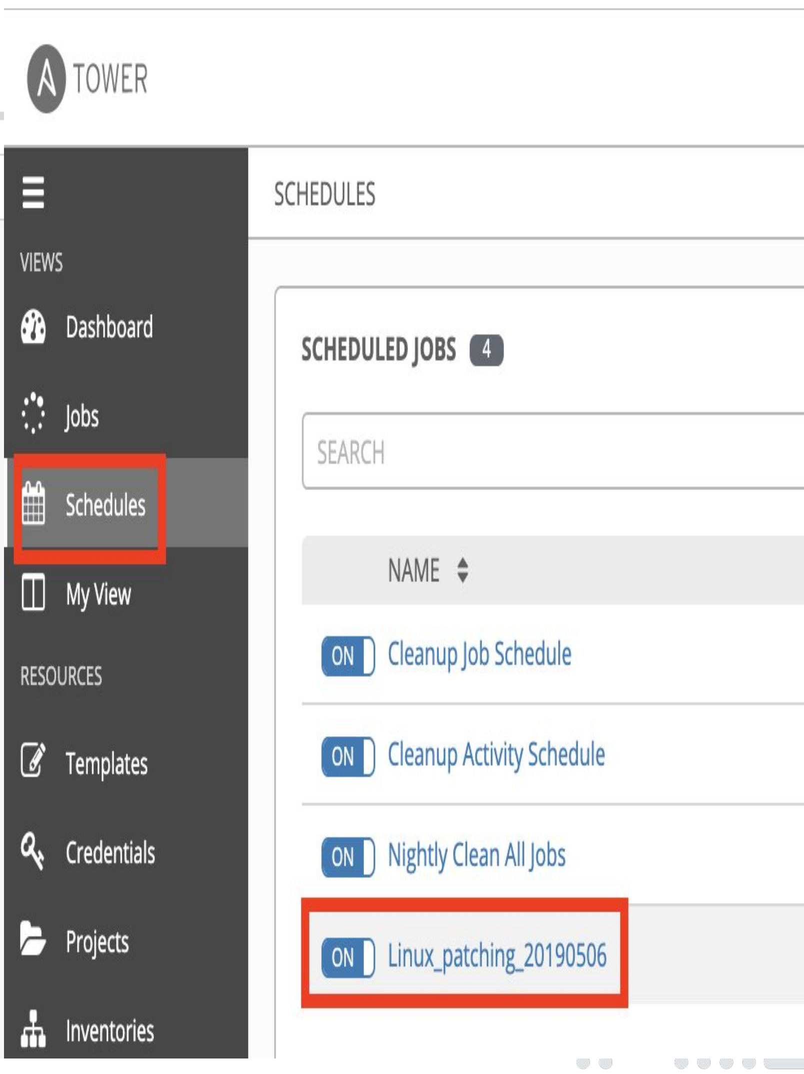


Compliance Reports

Filter ... ✕ Search

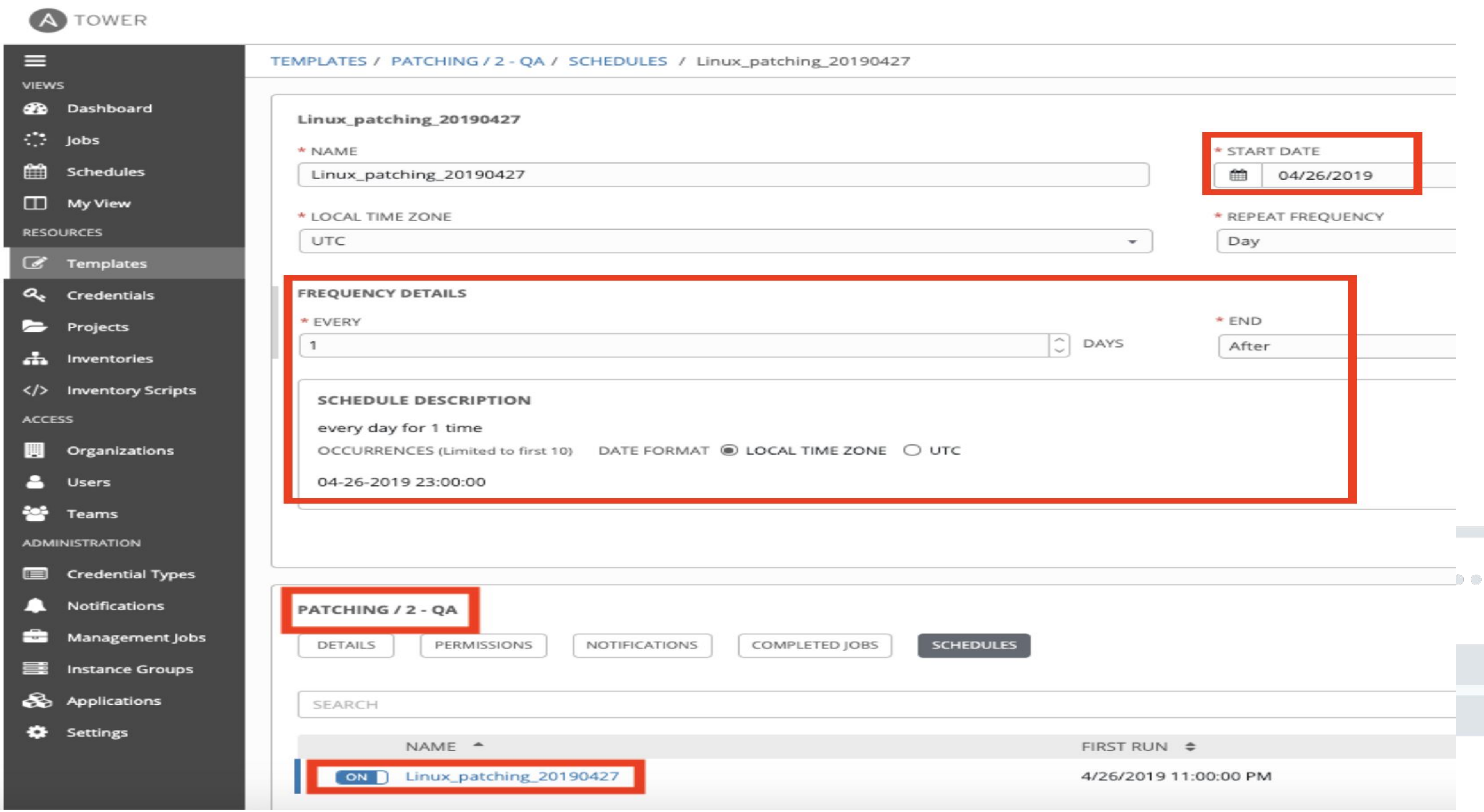
□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other
□	⊗ rhel7-vm5.hosts.example.com	about 3 hours ago	RHEL7_Standard	sat64.example.com	32	37	1
□	⊗ rhel7-vm4.hosts.example.com	about 3 hours ago	RHEL7_Standard	sat64.example.com	32	37	1
□	⊗ rhel7-vm3.hosts.example.com	about 3 hours ago	RHEL7_Standard	sat64.example.com	18	4	0





SCHEDULED JOBS 4

	NAME
ON	Cleanup Job Schedule
ON	Cleanup Activity Schedule
ON	Nightly Clean All Jobs
ON	Linux_patching_20190506



Linux_patching_20190427

* NAME: Linux_patching_20190427

* START DATE: 04/26/2019

* LOCAL TIME ZONE: UTC

* REPEAT FREQUENCY: Day

FREQUENCY DETAILS

* EVERY: 1 DAYS

* END: After

SCHEDULE DESCRIPTION

every day for 1 time

OCCURRENCES (Limited to first 10) DATE FORMAT ● LOCAL TIME ZONE ○ UTC

04-26-2019 23:00:00

PATCHING / 2 - QA

	NAME	FIRST RUN
ON	Linux_patching_20190427	4/26/2019 11:00:00 PM

Enabling Faster & Scalable DevSecOps with Red Hat OpenShift Container Platform

AUTOMATED BUILDS

CI/CD using Jenkins

Tekton

Source-2-Image

Buildah

CONTINUOUS BUILT-IN SECURITY

Automated analysis with SonarQube, OWASP Dependency Check, NPM Audit, OWASP Zed Attack Proxy, OpenSCAP, etc...

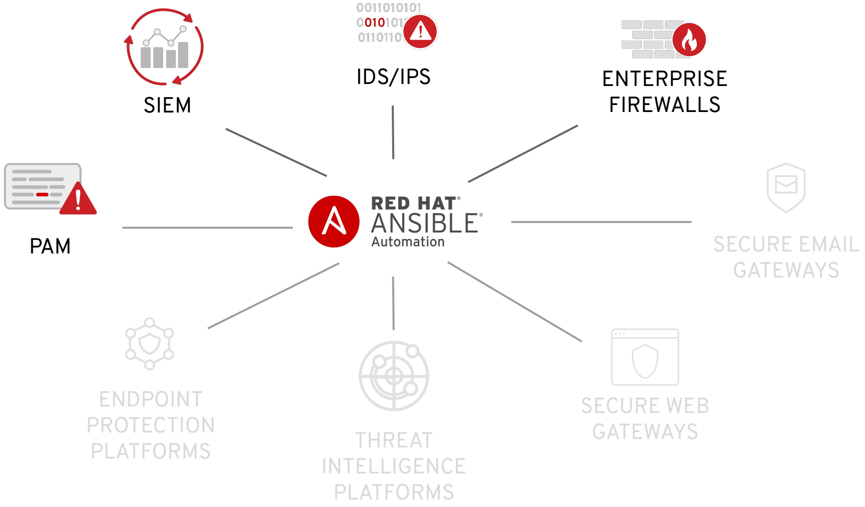
AUTOMATED OPERATIONS

RHEL CoreOS immutable OS, OpenShift Operators to monitor and respond to changing needs, load, threats, etc..

Automating the Security Operations Center with Ansible

DESIGNED TO ORCHESTRATE THREAT RESPONSE ACROSS SECURITY DOMAINS

- Expansion of Ansible as the Enterprise automation platform
- Integrates & orchestrates multiple classes of security solutions
- Provides modules, roles and playbooks to support security use cases across those solutions



WHO ARE OUR PARTNERS?

Security Information & Events Management

splunk>

IBM

Enterprise Firewalls

Check Point SOFTWARE TECHNOLOGIES LTD

CISCO

f5

FORTINET

Intrusion Detection & Prevention Systems

SNORT

Check Point SOFTWARE TECHNOLOGIES LTD

FORTINET

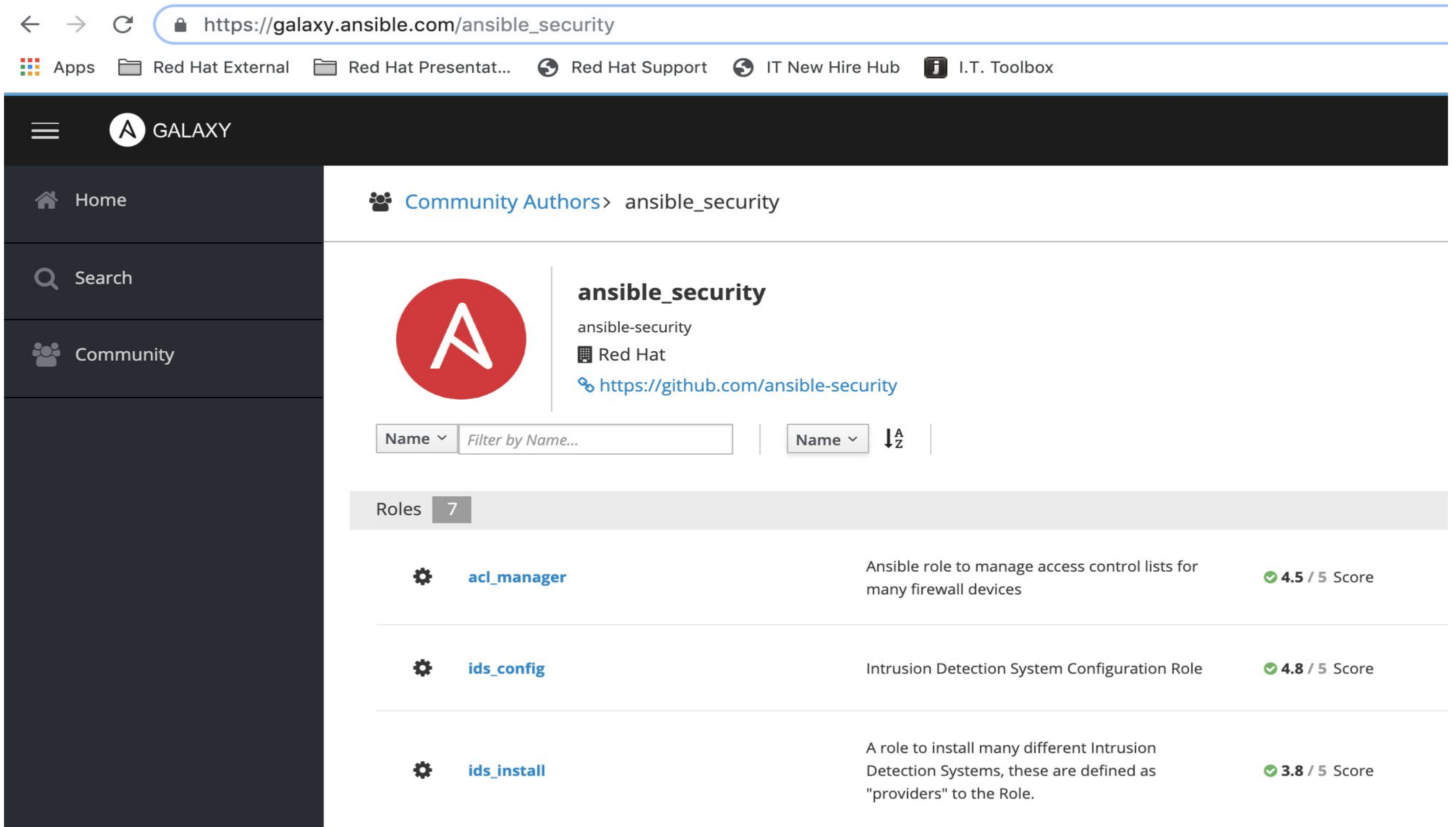
Privileged Access Management

CYBERARK

Syncope

ANSIBLE ROLES TO AUTOMATE SECURITY OPERATIONS

https://galaxy.ansible.com/ansible_security



https://galaxy.ansible.com/ansible_security

Community Authors › ansible_security

ansible_security

ansible-security

Red Hat

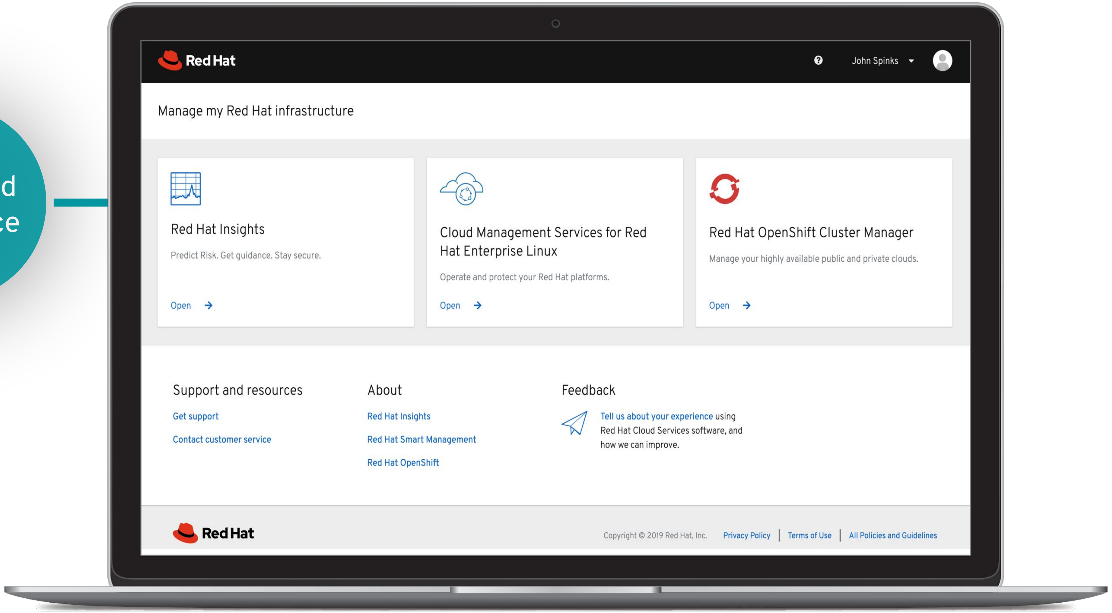
https://github.com/ansible-security

Roles 7

acl_manager	Ansible role to manage access control lists for many firewall devices	4.5 / 5 Score
ids_config	Intrusion Detection System Configuration Role	4.8 / 5 Score
ids_install	A role to install many different Intrusion Detection Systems, these are defined as "providers" to the Role.	3.8 / 5 Score

Scaling Security and Compliance with Cloud Services in cloud.redhat.com

Integrated experience



Red Hat

John Spinks

Manage my Red Hat infrastructure

Red Hat Insights

Predict Risk. Get guidance. Stay secure.

Open →

Cloud Management Services for Red Hat Enterprise Linux

Operate and protect your Red Hat platforms.

Open →

Red Hat OpenShift Cluster Manager

Manage your highly available public and private clouds.

Open →

Support and resources

Get support

Contact customer service

About

Red Hat Insights

Red Hat Smart Management

Red Hat OpenShift

Feedback

Tell us about your experience using Red Hat Cloud Services software, and how we can improve.

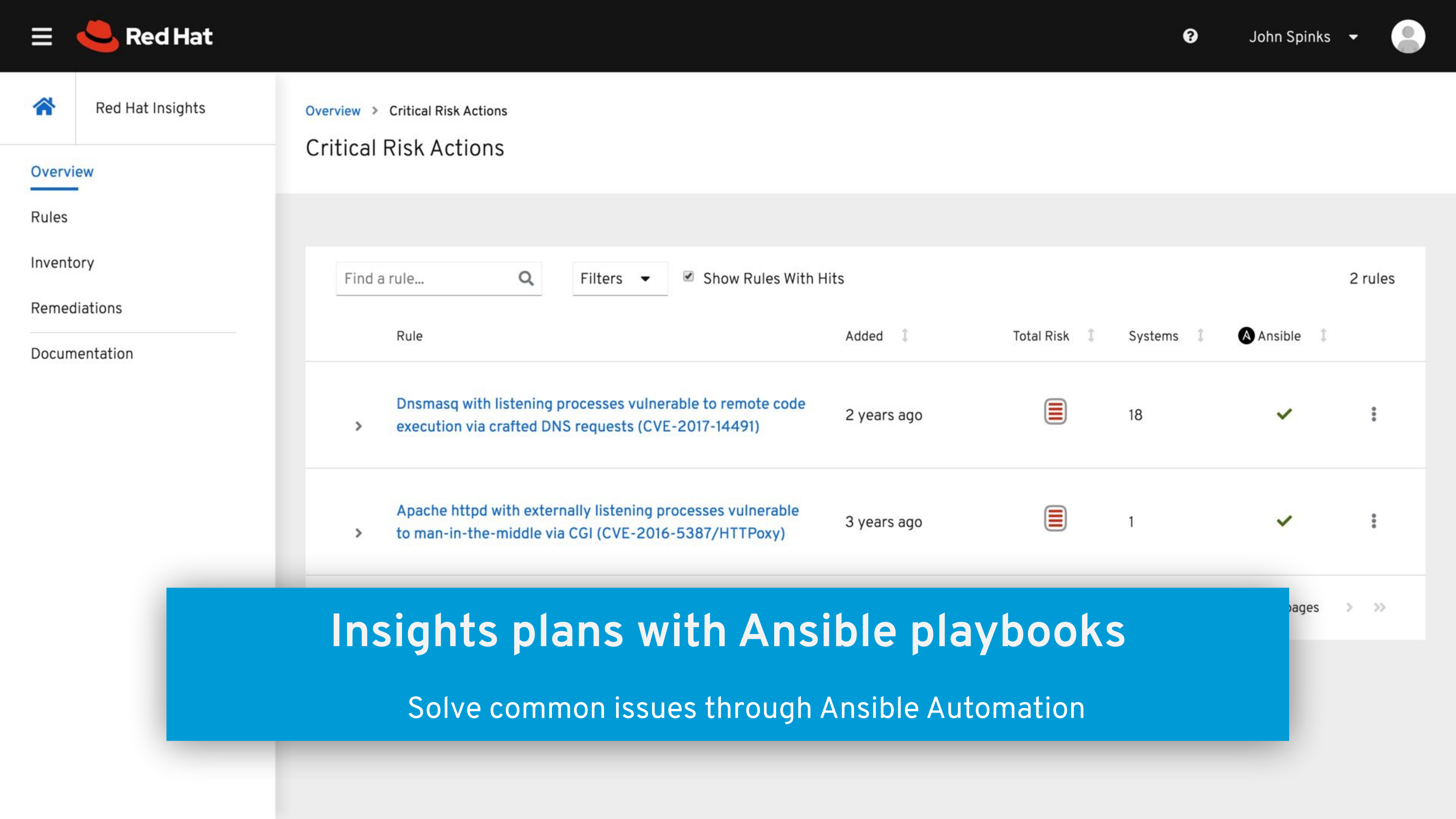
Red Hat

Copyright © 2019 Red Hat, Inc. Privacy Policy | Terms of Use | All Policies and Guidelines

Red Hat Insights

Now included with all Red Hat Enterprise Linux subscriptions

Buy	Get
Red Hat Enterprise Linux	Red Hat Insights

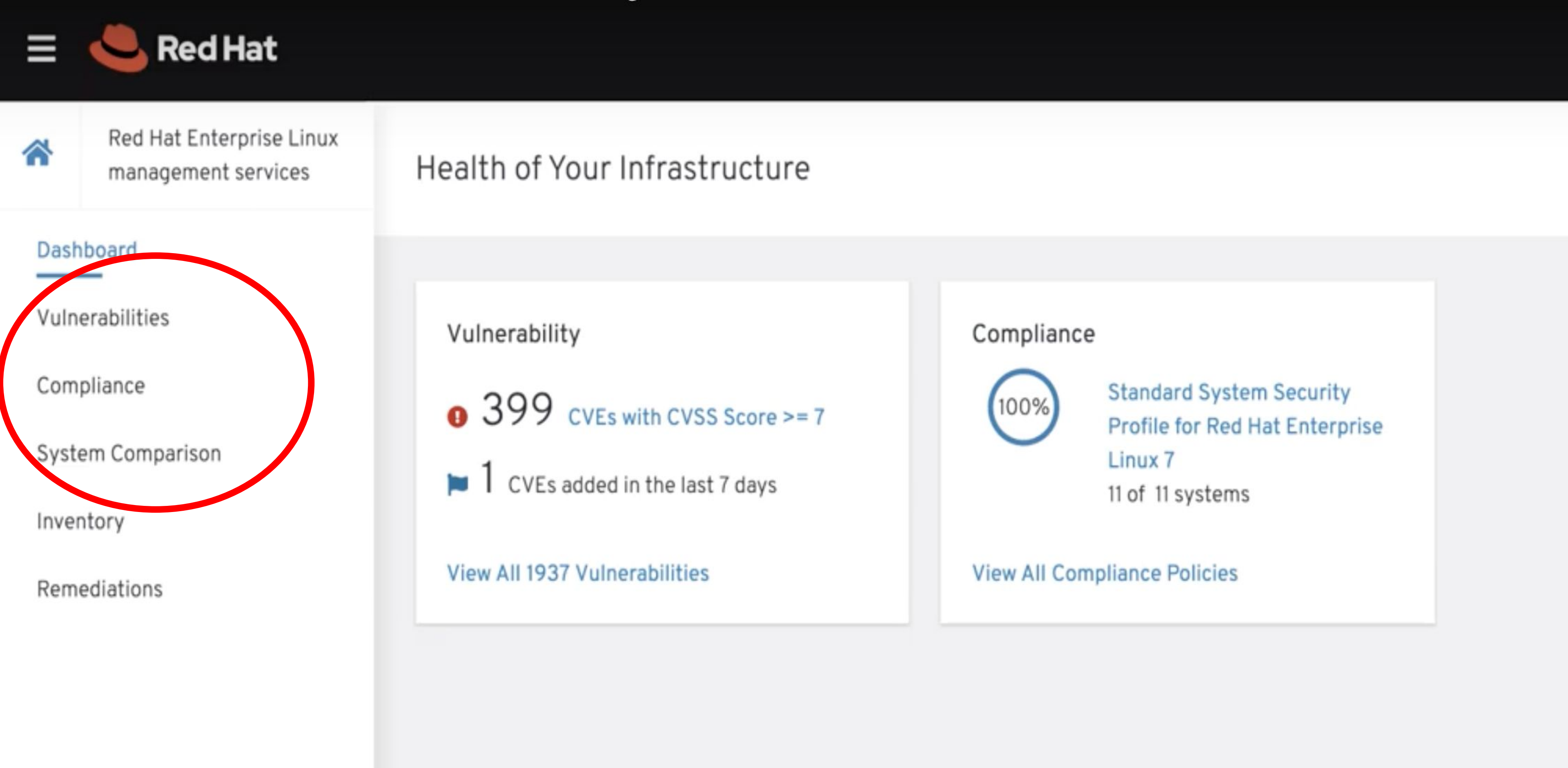


Critical Risk Actions

Rule	Added	Total Risk	Systems	Ansible
Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)	2 years ago	▤	18	✓
Apache httpd with externally listening processes vulnerable to man-in-the-middle via CGI (CVE-2016-5387/HTTPoxy)	3 years ago	▤	1	✓

Insights plans with Ansible playbooks

Solve common issues through Ansible Automation



Red Hat

Red Hat Enterprise Linux management services

Dashboard

Vulnerabilities

Compliance

System Comparison

Inventory

Remediations

Health of Your Infrastructure

Vulnerability

399 CVEs with CVSS Score >= 7

1 CVEs added in the last 7 days

View All 1937 Vulnerabilities

Compliance

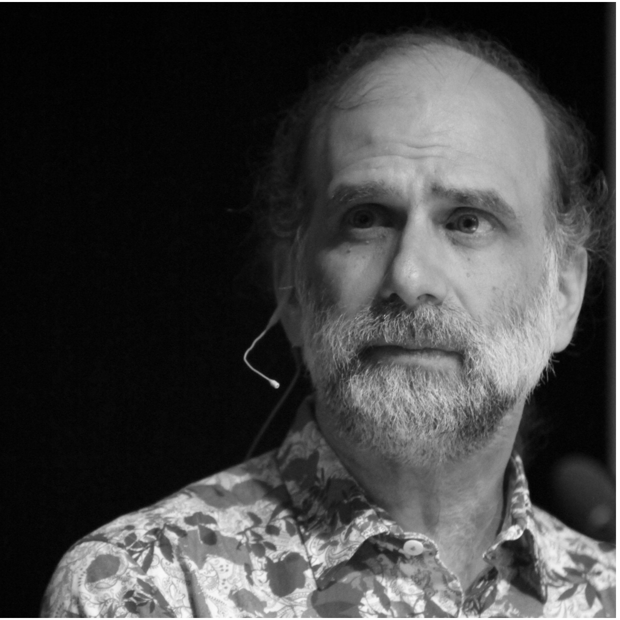
100% Standard System Security Profile for Red Hat Enterprise Linux 7

11 of 11 systems

View All Compliance Policies

There is no silver bullet solution or product for security

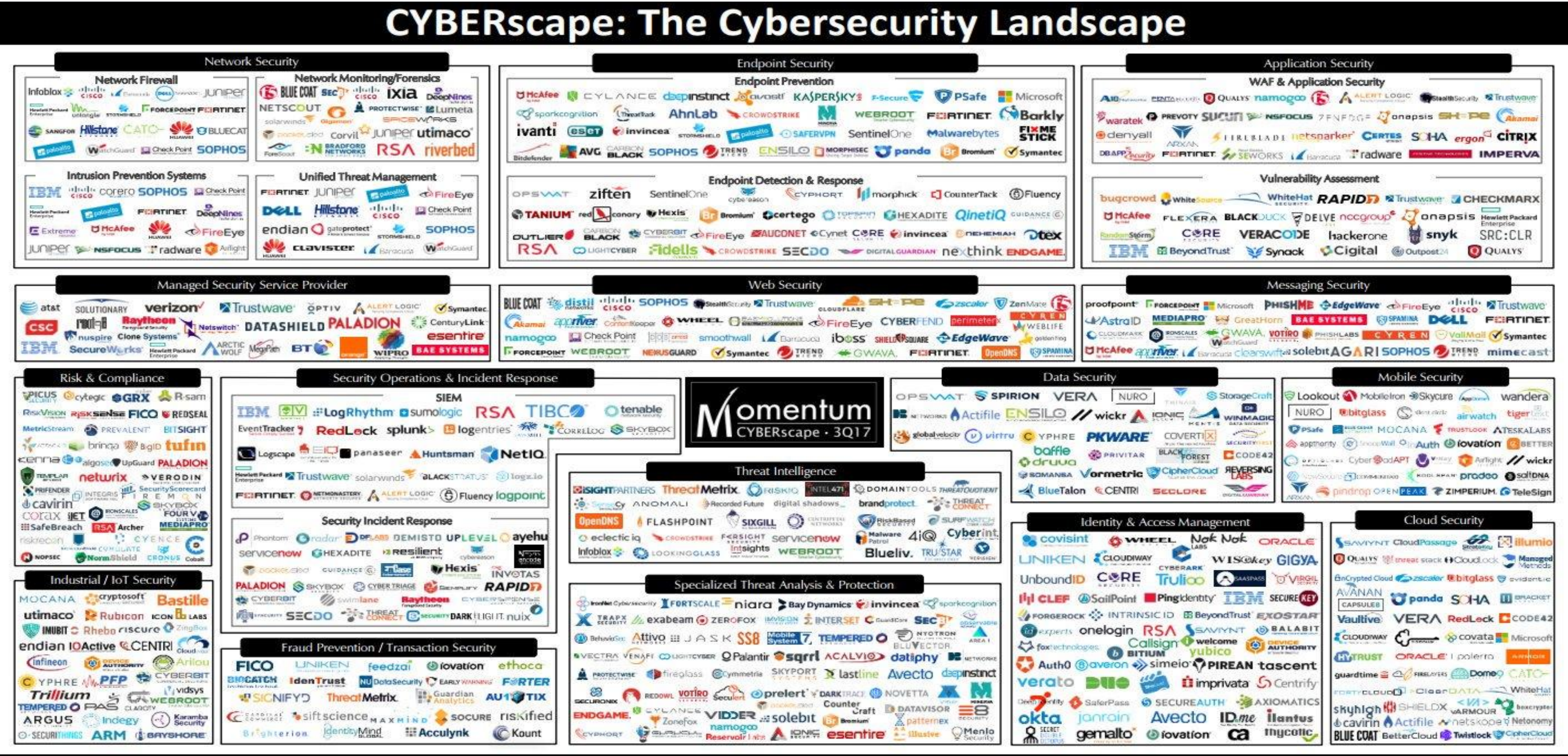
Don’t take a whack-a-mole approach to security



Security is a ***process***, NOT a product.

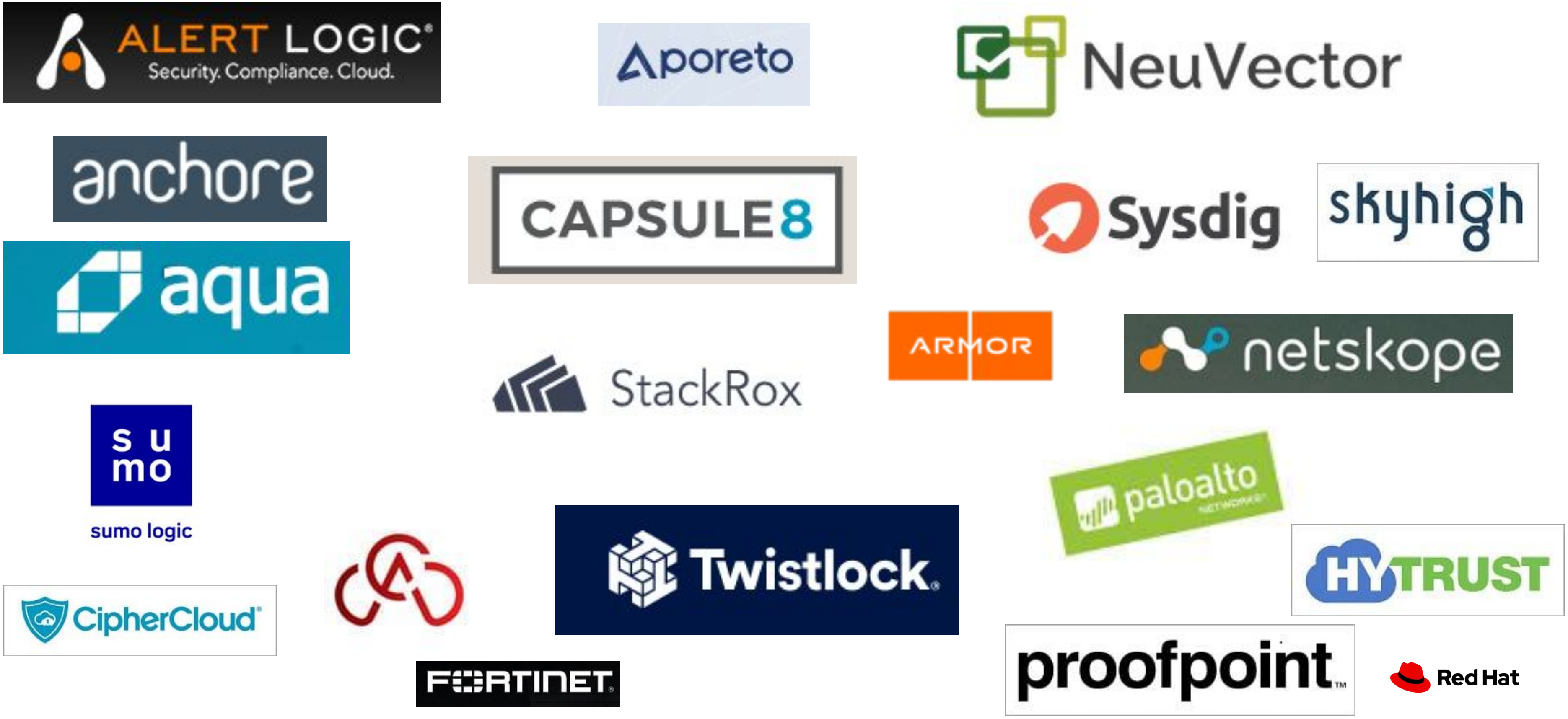
Bruce Schneier
Cryptographer, security blogger and author

Welcome to the Vast World of Cybersecurity Tools


CYBERscape: The Cybersecurity Landscape

Source: Momentum Partners

Growing # of cloud and container security vendors



Evolution of Traditional Security Vendors

"Prisma: Complete Cloud Security"

"Qualys Cloud Platform"

"Securing the Cloud Generation"

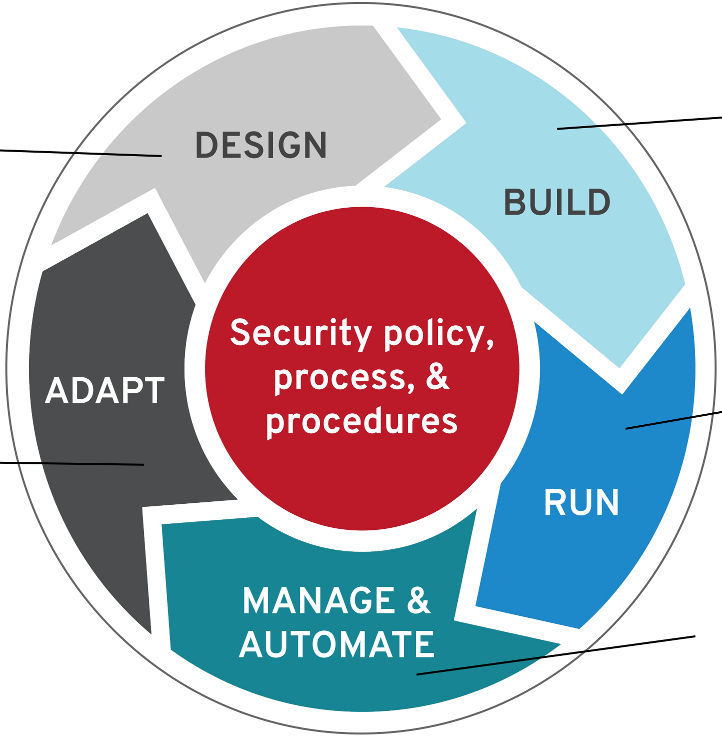
SECURITY PRACTICES, POLICIES, AND TOOLS HAVEN'T FULLY CAUGHT UP WITH CLOUD TECHNOLOGIES

> *"According to analyst firm McKinsey, a full 78 percent of more than 100 firms recently surveyed are NOT reconfiguring their security tools when migrating to the cloud"*

Source: B. Cameron Gain for thenewstack.io, *Microservices Security: Probably Not What You Think It Is*, Mar 2018
https://thenewstack.io/microservices-security-probably-not-what-you-think-it-is/

SECURITY MUST BE CONTINUOUS + HOLISTIC

AND INTEGRATED THROUGHOUT THE I.T. LIFE CYCLE



Identify security requirements & governance models

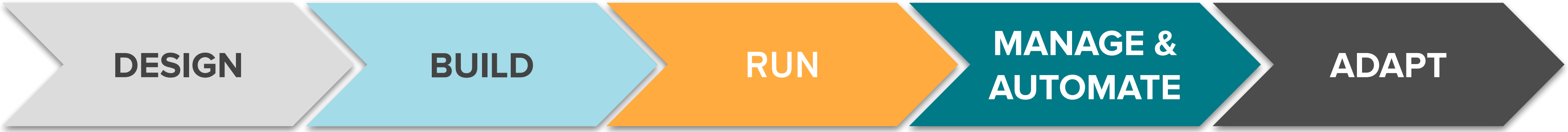
Built-in from the start; not bolted-on

Deploy to trusted platforms with enhanced security capabilities

Automate systems for security & compliance

Revise, update, remediate as the landscape changes

SECURITY THROUGHOUT THE STACK + LIFECYCLE

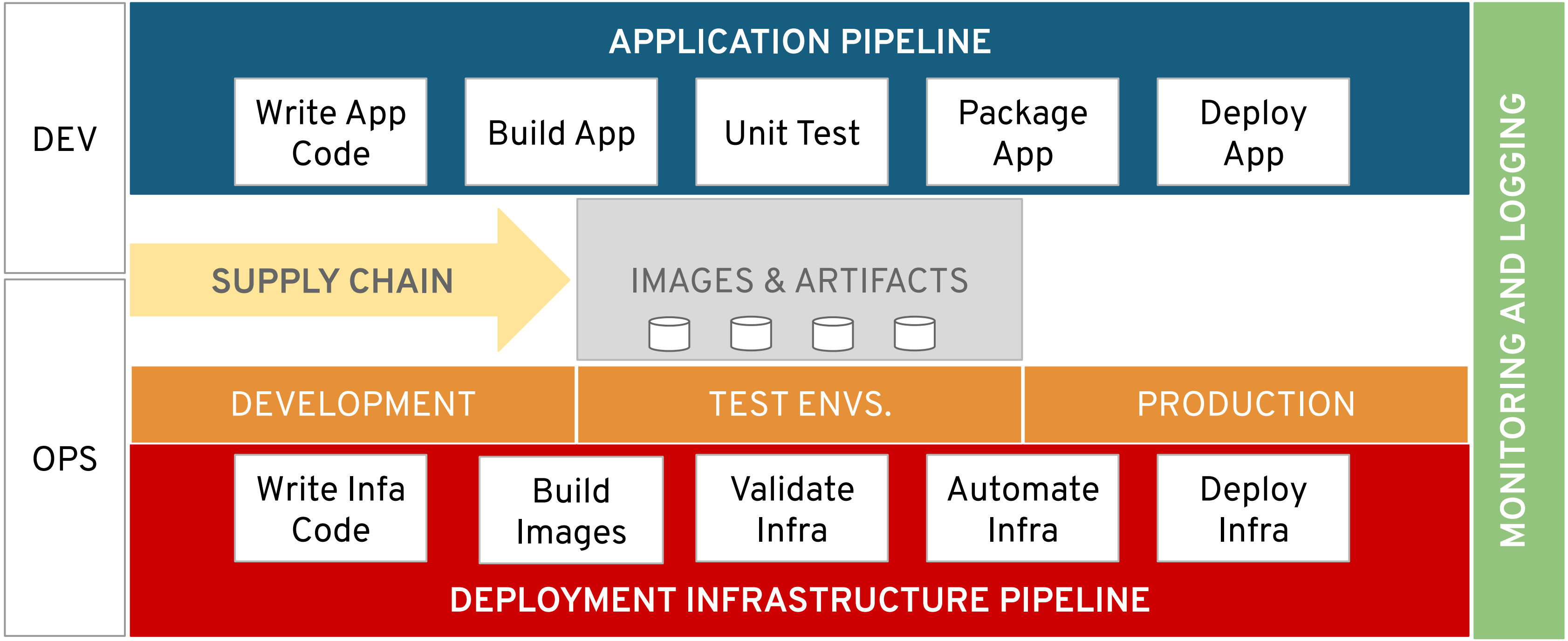


DESIGN	BUILD	RUN	MANAGE & AUTOMATE	ADAPT
Red Hat Consulting	**Red Hat** OpenShift Container Platform	**Red Hat** Enterprise Linux	**Red Hat** Ansible Automation Platform	**Red Hat** Insights
Red Hat Services	**Red Hat** Middleware	**Red Hat** Enterprise Linux CoreOS	**Red Hat** Satellite	**Red Hat** Security Advisories
Red Hat Training	**Red Hat** 3scale API Management	**Red Hat** Virtualization	**Red Hat** CloudForms	
		Red Hat OpenStack Platform		
		Red Hat Storage		

TESTED, CERTIFIED, STABLE, AND SUPPORTED OPEN SOURCE SOFTWARE

Holistic DevSecOps

It’s not just about the application CI/CD pipeline!



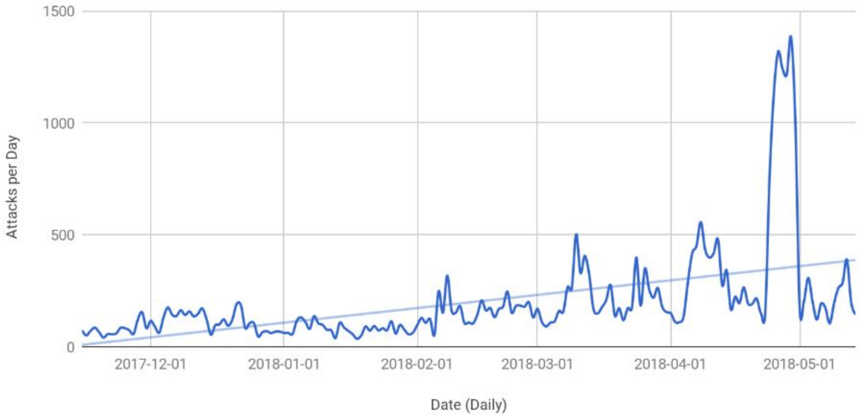
Understand the scope of open-source usage + ensure all open-source technologies are consumed securely

Red Hat

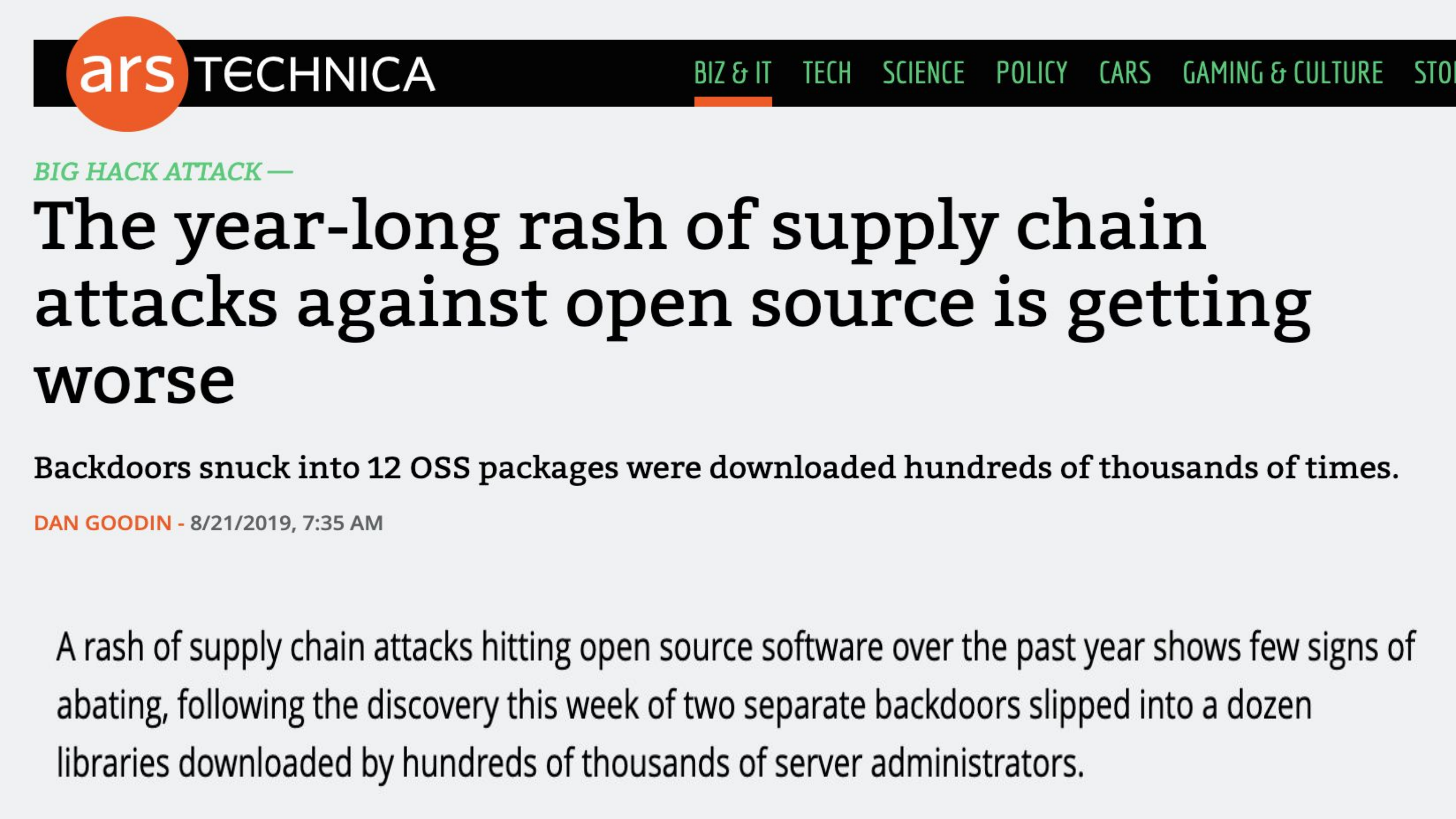
DEVELOPERS AREN'T SECURITY EXPERTS

L7 ATTACKS ON THE RISE

*"**The softest target in most organizations is the app layer and attackers know this**. In the last 6 months we have seen a large **upward trend of Layer 7 based DDoS attacks**… On average seeing around 160 attacks a day, with some days spiking up to over 1000 attacks."*



blog.cloudflare.com/rate-limiting-delivering-more-rules-and-greater-control/



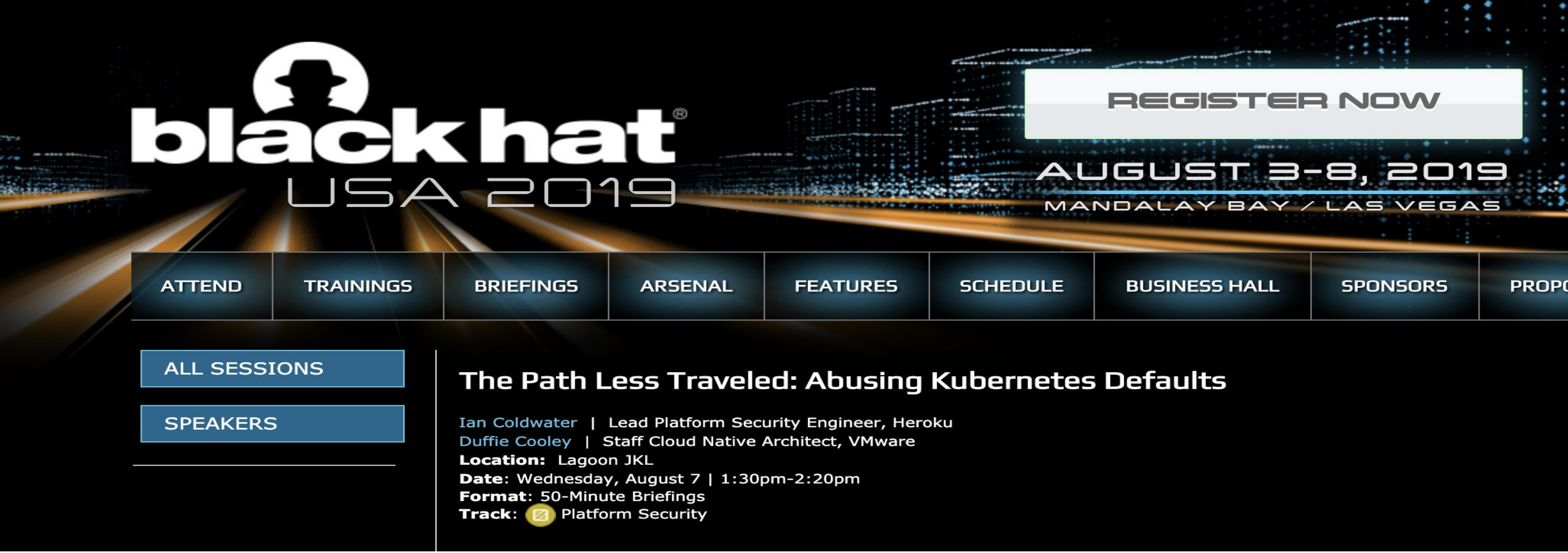
BIG HACK ATTACK —

The year-long rash of supply chain attacks against open source is getting worse

Backdoors snuck into 12 OSS packages were downloaded hundreds of thousands of times.

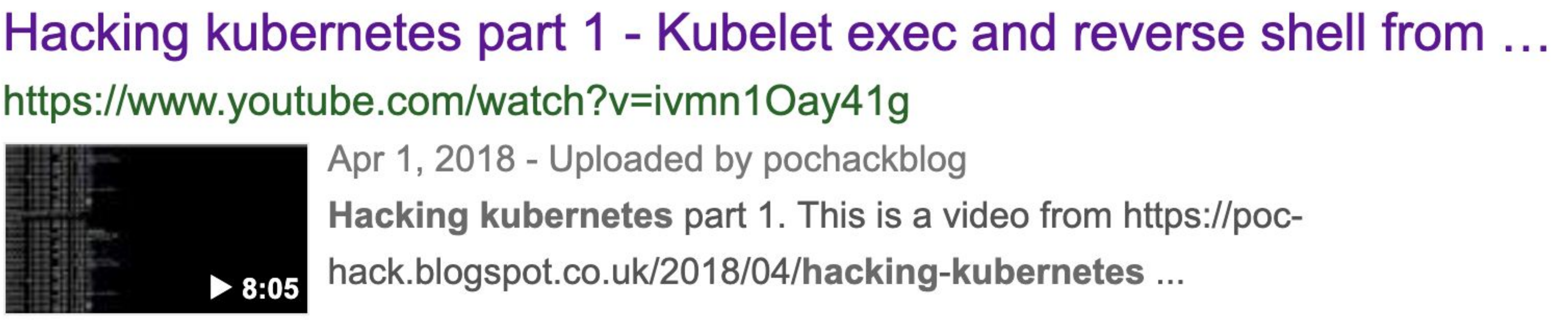
DAN GOODIN - 8/21/2019, 7:35 AM

A rash of supply chain attacks hitting open source software over the past year shows few signs of abating, following the discovery this week of two separate backdoors slipped into a dozen libraries downloaded by hundreds of thousands of server administrators.



The Path Less Traveled: Abusing Kubernetes Defaults

Ian Coldwater | Lead Platform Security Engineer, Heroku
Duffie Cooley | Staff Cloud Native Architect, VMware
Location: Lagoon JKL
Date: Wednesday, August 7 | 1:30pm-2:20pm
Format: 50-Minute Briefings
Track: Platform Security



Hacking kubernetes part 1 - Kubelet exec and reverse shell from ...

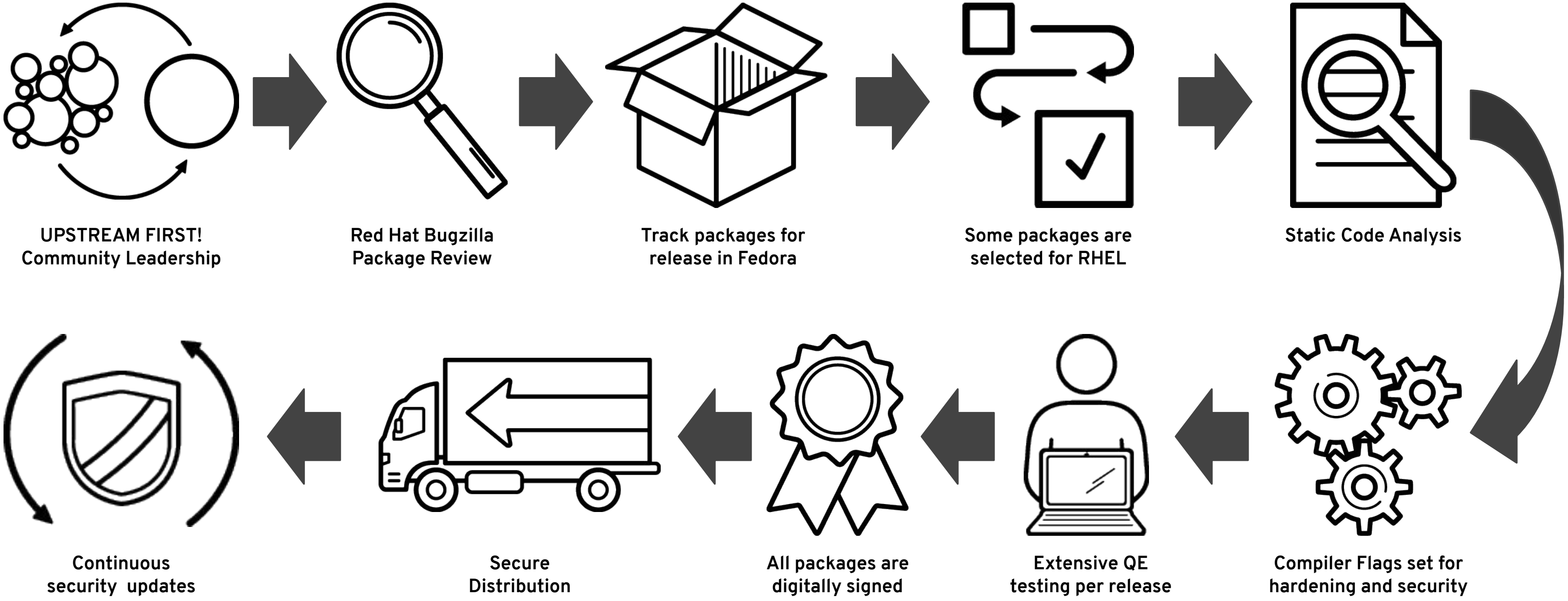
https://www.youtube.com/watch?v=ivmn1Oay41g

Apr 1, 2018 - Uploaded by pochackblog

Hacking kubernetes part 1. This is a video from https://poc-hack.blogspot.co.uk/2018/04/**hacking-kubernetes** ...

Red Hat Supply Chain Security

Reducing Risk and Making Open Source Consumable by the Enterprise



UPSTREAM FIRST!
Community Leadership

Red Hat Bugzilla
Package Review

Track packages for
release in Fedora

Some packages are
selected for RHEL

Static Code Analysis

Compiler Flags set for
hardening and security

Extensive QE
testing per release

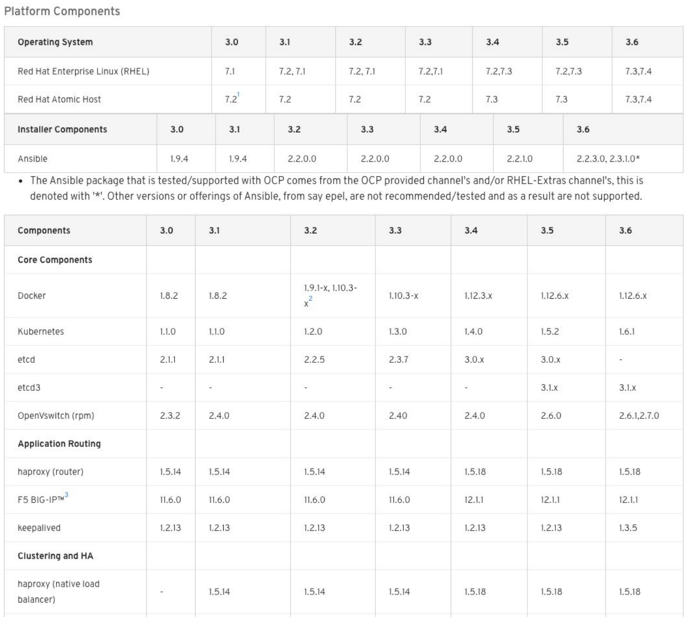
All packages are
digitally signed

Secure
Distribution

Continuous
security updates

Red Hat

REDUCING RISK WITH TESTED INTEGRATIONS



Platform Components

Operating System	3.0	3.1	3.2	3.3	3.4	3.5	3.6
Red Hat Enterprise Linux (RHEL)	7.1	7.2, 7.1	7.2, 7.1	7.2,7.1	7.2,7.3	7.2,7.3	7.3,7.4
Red Hat Atomic Host	7.2[1]	7.2	7.2	7.2	7.3	7.3	7.3,7.4

Installer Components	3.0	3.1	3.2	3.3	3.4	3.5	3.6
Ansible	1.9.4	1.9.4	2.2.0.0	2.2.0.0	2.2.0.0	2.2.1.0	2.2.3.0, 2.3.1.0*

- The Ansible package that is tested/supported with OCP comes from the OCP provided channel's and/or RHEL-Extras channel's, this is denoted with '*'. Other versions or offerings of Ansible, from say epel, are not recommended/tested and as a result are not supported.

Components	3.0	3.1	3.2	3.3	3.4	3.5	3.6
Core Components							
Docker	1.8.2	1.8.2	1.9.1-x, 1.10.3-x[2]	1.10.3-x	1.12.3.x	1.12.6.x	1.12.6.x
Kubernetes	1.1.0	1.1.0	1.2.0	1.3.0	1.4.0	1.5.2	1.6.1
etcd	2.1.1	2.1.1	2.2.5	2.3.7	3.0.x	3.0.x	-
etcd3	-	-	-	-	-	3.1.x	3.1.x
OpenVswitch (rpm)	2.3.2	2.4.0	2.4.0	2.40	2.4.0	2.6.0	2.6.1,2.7.0
Application Routing							
haproxy (router)	1.5.14	1.5.14	1.5.14	1.5.14	1.5.18	1.5.18	1.5.18
F5 BIG-IP™[3]	11.6.0	11.6.0	11.6.0	11.6.0	12.1.1	12.1.1	12.1.1
keepalived	1.2.13	1.2.13	1.2.13	1.2.13	1.2.13	1.2.13	1.3.5
Clustering and HA							
haproxy (native load balancer)	-	1.5.14	1.5.14	1.5.14	1.5.18	1.5.18	1.5.18

- 100+ defects fixed between every upstream Kubernetes and commercial OpenShift release
- 140+ combinations of common products tested with every *minor* OpenShift release, incl. Storage drivers, networking, database images, …
- Tested for performance & scalability, security and reliability

https://access.redhat.com/articles/2176281

Make security everyone's job

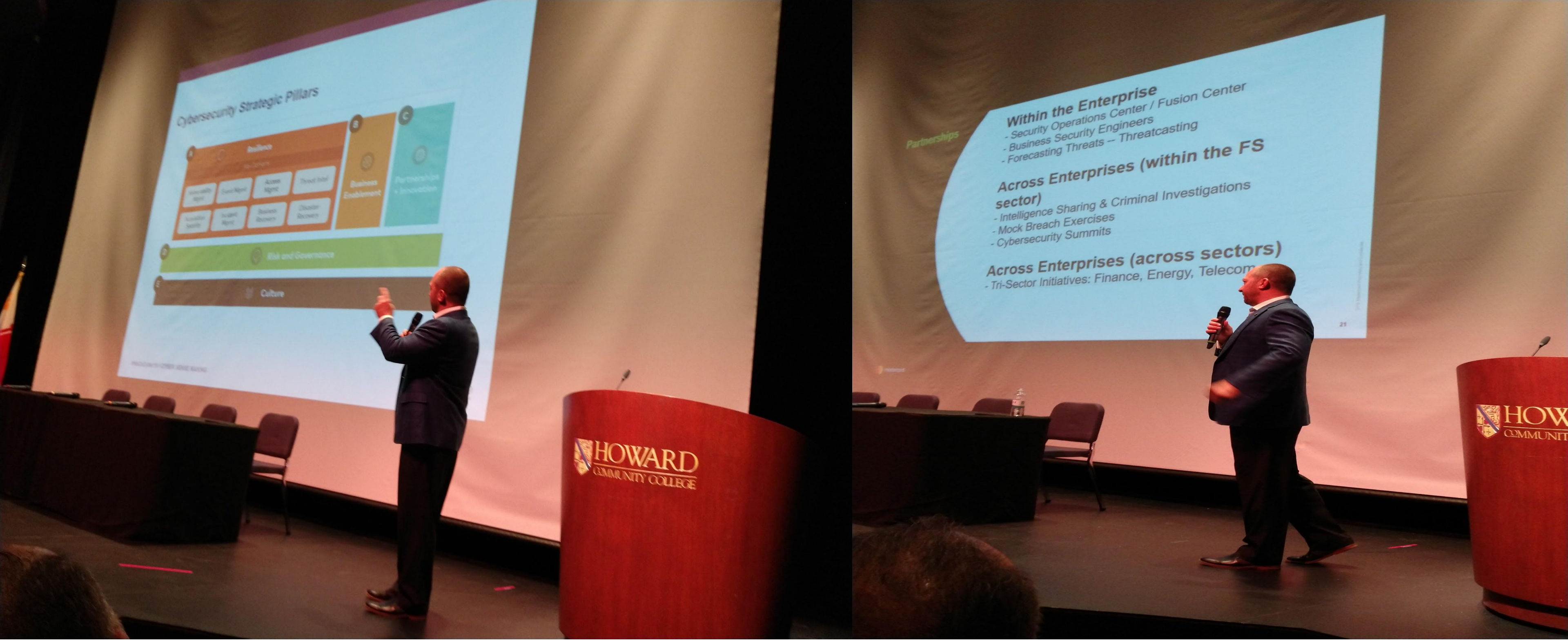
EVERYBODY IS RESPONSIBLE FOR SECURITY

MORNING KEYNOTE

Dr. Jon Brickey, SVP,
Cybersecurity Evangelist,
Mastercard

#HoCoCyber19 | CYBER SENSE MAKING

CYBER//2019
HOWARD COUNTY CHAMBER


Cybersecurity Strategic Pillars
A
Resilience
Vulnerability Mgmt
Event Mgmt
Access Mgmt
Threat Intel
Application Security
Incident Mgmt
Business Recovery
Disaster Recovery
B
Business Enablement
C
Partnerships + Innovation
D
Risk and Governance
E
Culture
HOWARD
COMMUNITY COLLEGE
Partnerships
Within the Enterprise
- Security Operations Center / Fusion Center
- Business Security Engineers
- Forecasting Threats -- Threatcasting
Across Enterprises (within the FS sector)
- Intelligence Sharing & Criminal Investigations
- Mock Breach Exercises
- Cybersecurity Summits
Across Enterprises (across sectors)
- Tri-Sector Initiatives: Finance, Energy, Telecom
21

Cybersecurity Strategic Pillar at MasterCard:

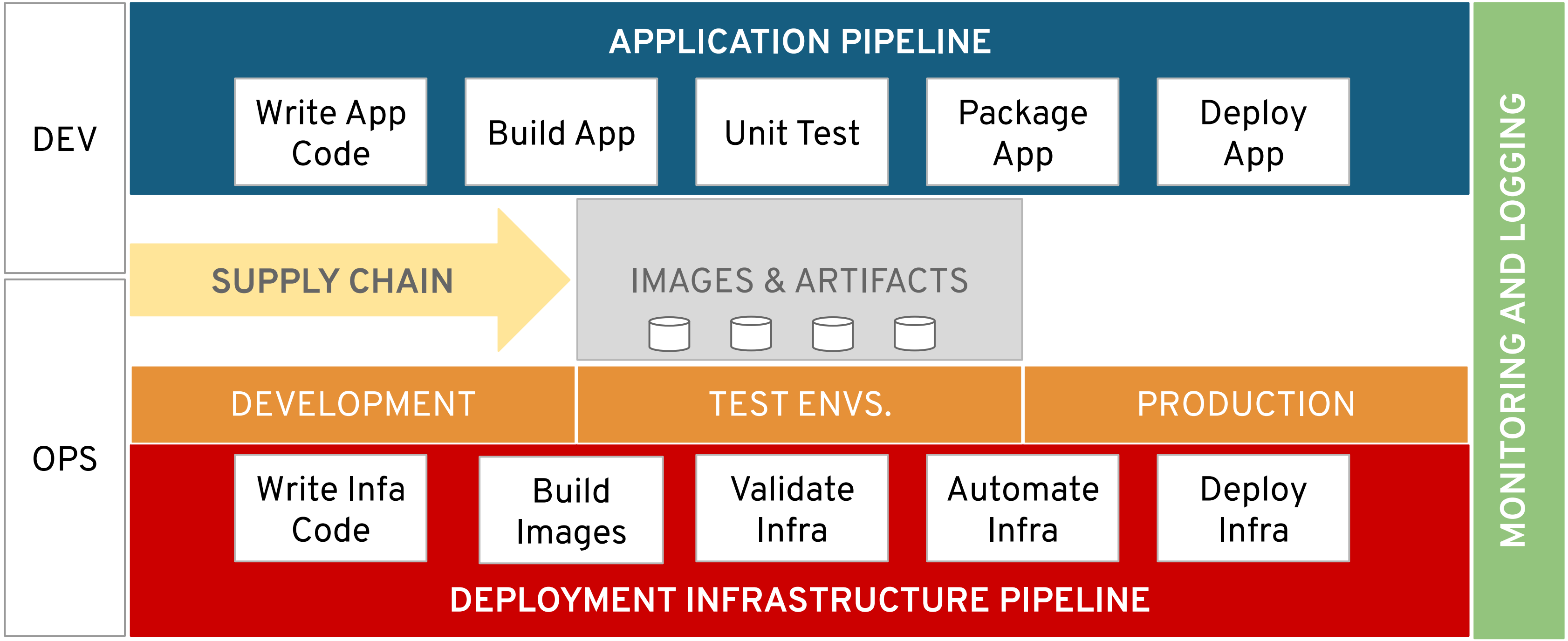
Enabling the Business with "Business Security Engineers"

(developers work with security team + trained on security and vice versa)

Implement Holistic DevSecOps, where security is built-in, continually addressed + monitored

Holistic DevSecOps

It’s not just about the application CI/CD pipeline!

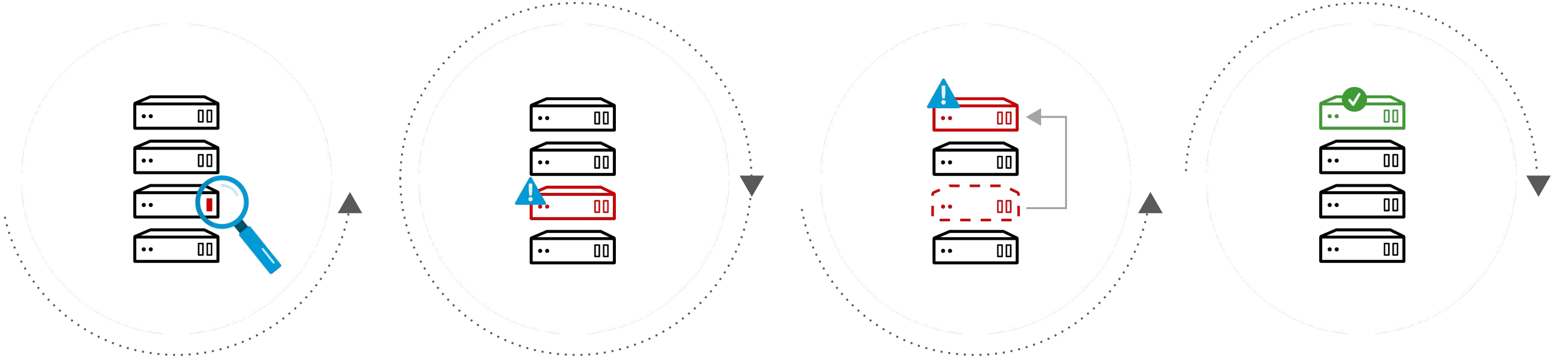


Automated Security & Compliance for Infrastructure Operations

DevSecOps in Baby Steps

More details here:

https://red.ht/securitylabs (ProactiveSecurityCompliance folder)



Vulnerability & Compliance scanning

Host hardening

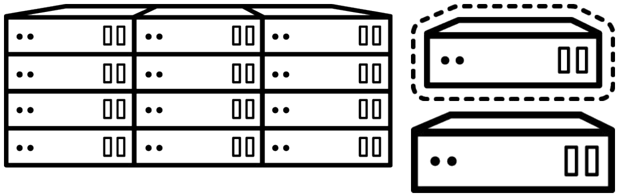
Enforcing automated compliance

Automated Patching of hosts

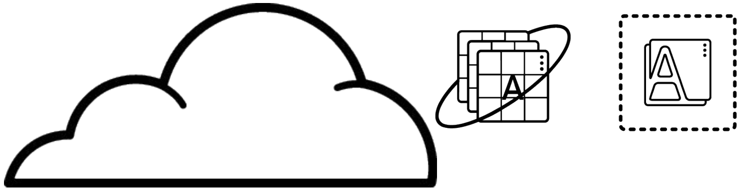
Automation & Analytics are the key to effective Security & Compliance

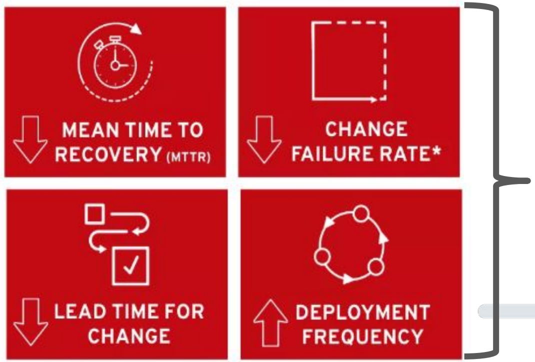
ENABLING SECURE DEVOPS AT SCALE WITH CONTAINERS AND KUBERNETES

Enabling DevSecOps with Containers
Traditional vs Cloud Native



```
# _
```





MEAN TIME TO RECOVERY (MTTR)

CHANGE FAILURE RATE*

LEAD TIME FOR CHANGE

DEPLOYMENT FREQUENCY

Antifragile

Journey to DevSecOps Panel

*“In Security, consistency and repeatability is key. Adopting containers in a container platform will **improve** your security.”*

US Courts
US Citizen and Immigration Services
Oak Ridge National Laboratory
Internal Revenue Service

US Government Panel, Openshift Commons Briefing

Journey of DevSecOps - US Department Homeland Security

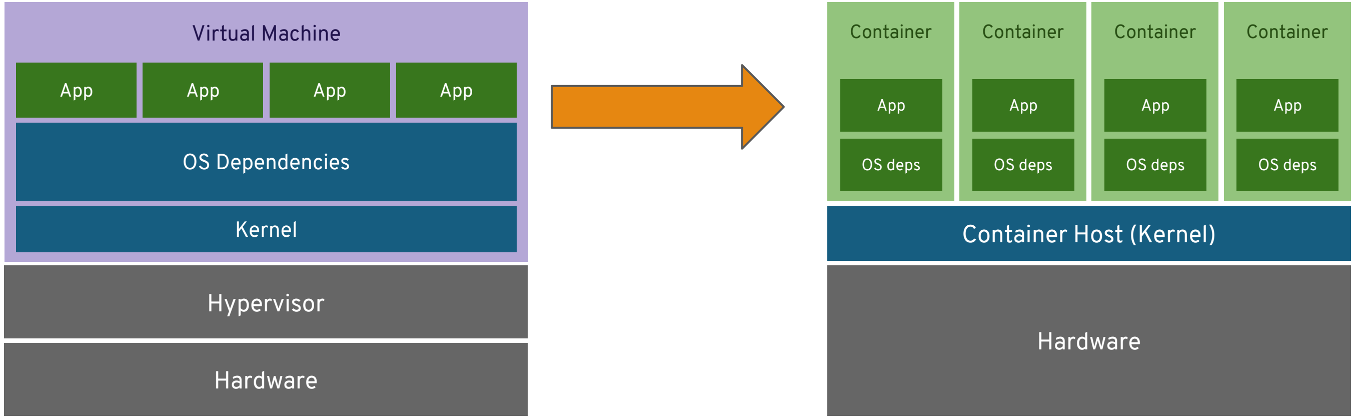
Book by Mark Schwartz, USCIS CIO: A Seat at the Table: IT Leadership in the Age of Agility

.Gov on OpenShift Panel - US Courts, USCIS/DHS, and Oak Ridge National Laboratory

Security Benefits of Containerized Infrastructure

- Standard, hardened infrastructure
  - Force applications to be in line with defined security policies
- Read-only containers = Application whitelisting
- Continually (re)deploying from known good source
  - Standardized base container images
- No humans in production - SSH turned off
- Patching improvements
- Complete record of change
- Minimal OS
- Pipeline Integration moves security left
- Kubernetes is declarative
- **Security gates: Nothing go to production unless all checks passed.**

Accelerating Application Delivery with Containers

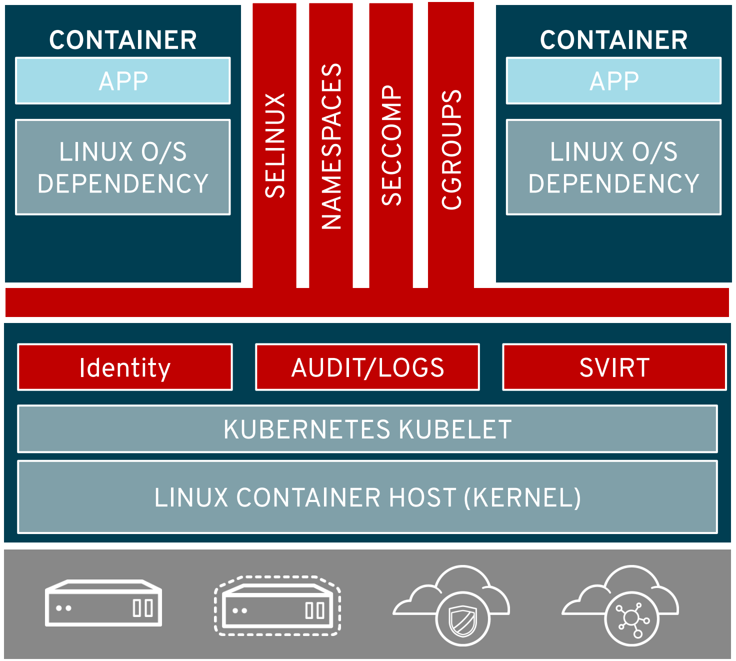


VMs virtualize the Hardware

Containers virtualize the OS kernel

CONTAINER SECURITY + ISOLATIONS STARTS WITH LINUX SECURITY

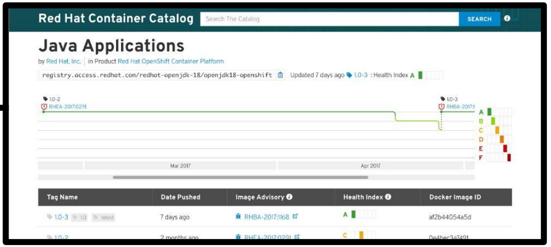
- Security in the linux host kernel applies to the container
    - RHEL CoreOS provides minimized attack surface
    - Container Security + Isolation with: Namespaces, SELinux, CGroups, Seccomp,etc
    - Protects not only the host, but containers from each other



AUTOMATE SECURITY PROCESSES

Automated quality and security: because you can't inspect quality into a product

Automatically prohibit untrusted containers via Openshift policy



Red Hat Container Catalog

Java Applications

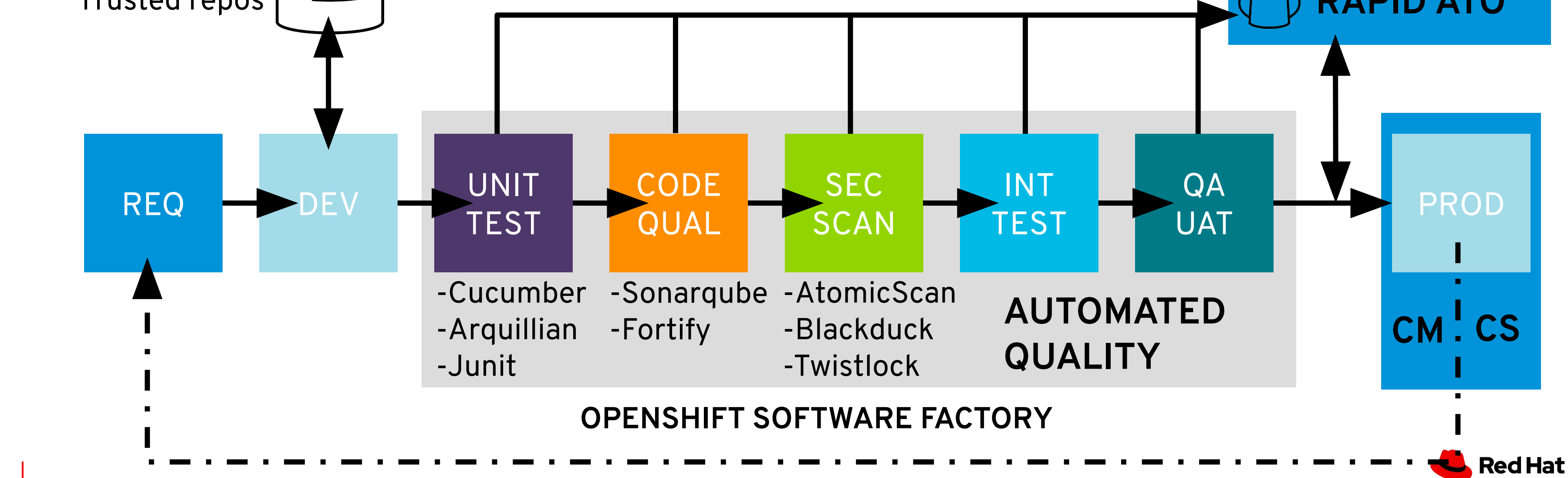
by Red Hat, Inc. | in Product Red Hat OpenShift Container Platform

`registry.access.redhat.com/redhat-openjdk-18/openjdk18-openshift` Updated 7 days ago 1.0-3 : Health Index A

Tag Name	Date Pushed	Image Advisory	Health Index	Docker Image ID
1.0-3 1.0 latest	7 days ago	RHBA-2017:1168	A	af2b44054a5d
1.0-2	2 months ago	RHEA-2017:0291	C	0e4bec3a7491

Secure Supply Chain of Quality Parts

- Quality Assurance
- Certifications
- Signing & Secure
- Distribution



Trusted repos

-Cucumber
-Arquillian
-Junit

-Sonarqube
-Fortify

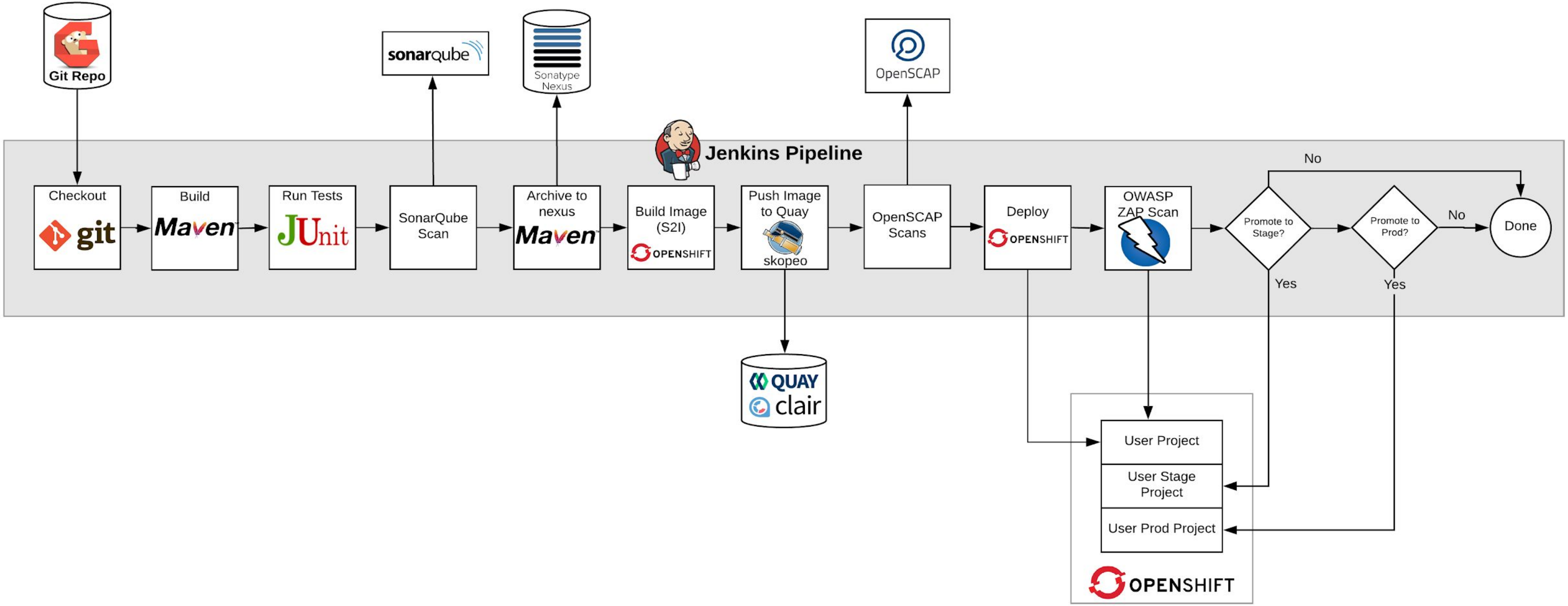
-AtomicScan
-Blackduck
-Twistlock

AUTOMATED QUALITY

OPENSHIFT SOFTWARE FACTORY

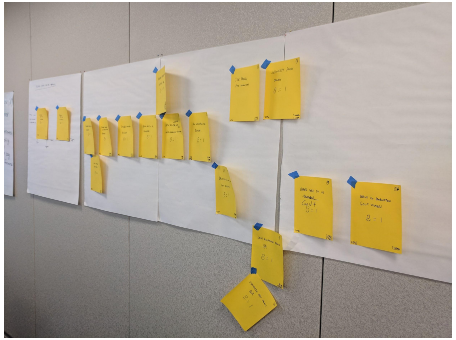
DevSecOps & Building Security into the Application

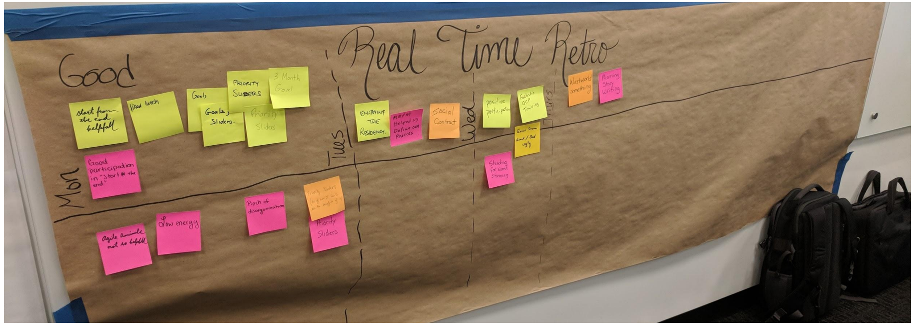
Automated 'Secure Software Factory' Example



Ansible playbook to deploy this entire DevSecOps pipeline can be found here: http://tiny.cc/80hjbz
See the full documentation here: https://red.ht/securitylabs

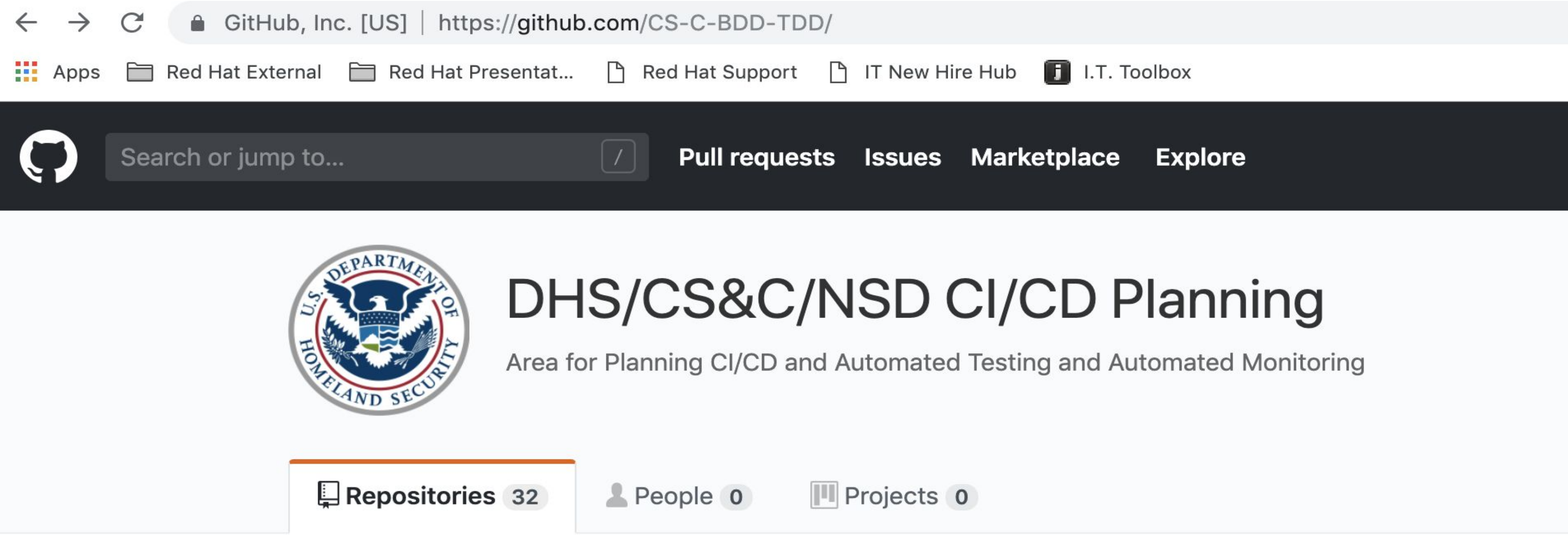
Accelerating DevSecOps with Red Hat Open Innovation Labs





DHS documented their entire Red Hat Innovation Labs & DevSecOps journey on Github:

https://github.com/CS-C-BDD-TDD



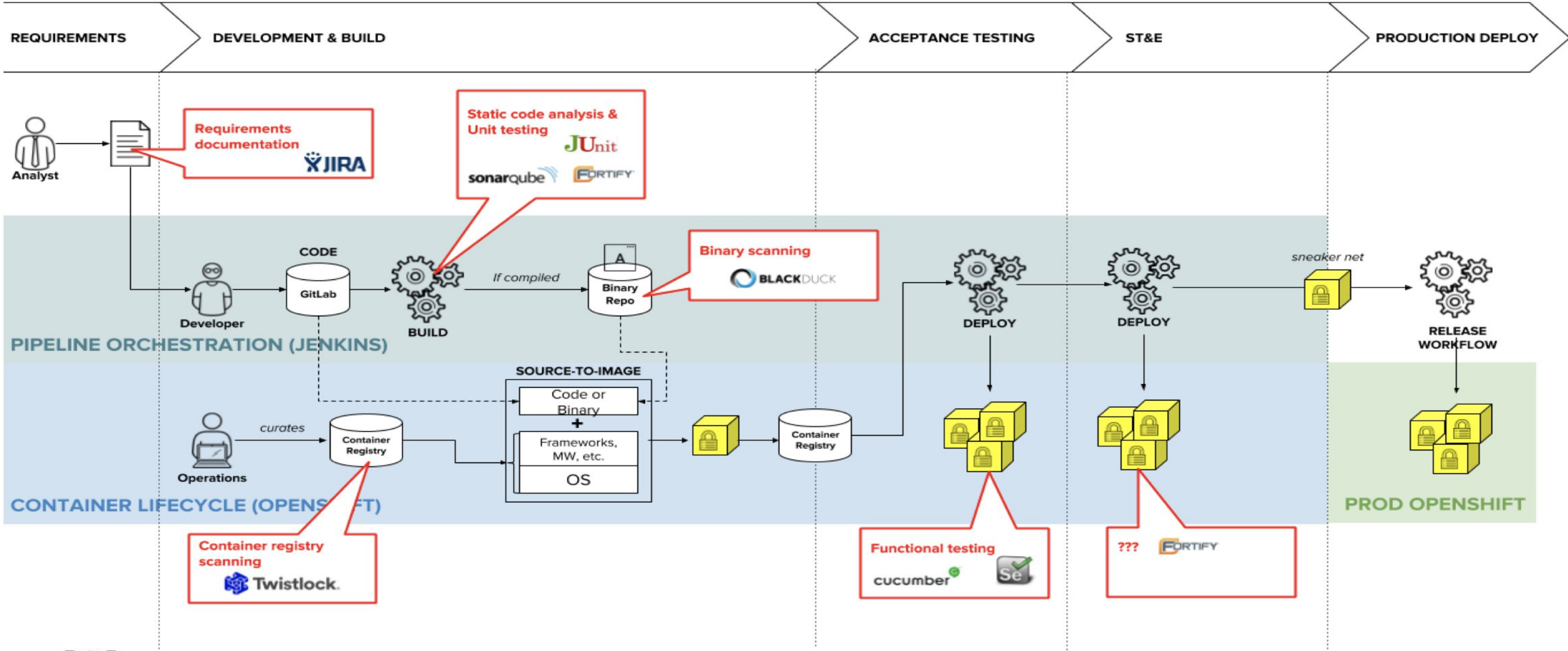
GitHub, Inc. [US] | https://github.com/CS-C-BDD-TDD/

DHS/CS&C/NSD CI/CD Planning

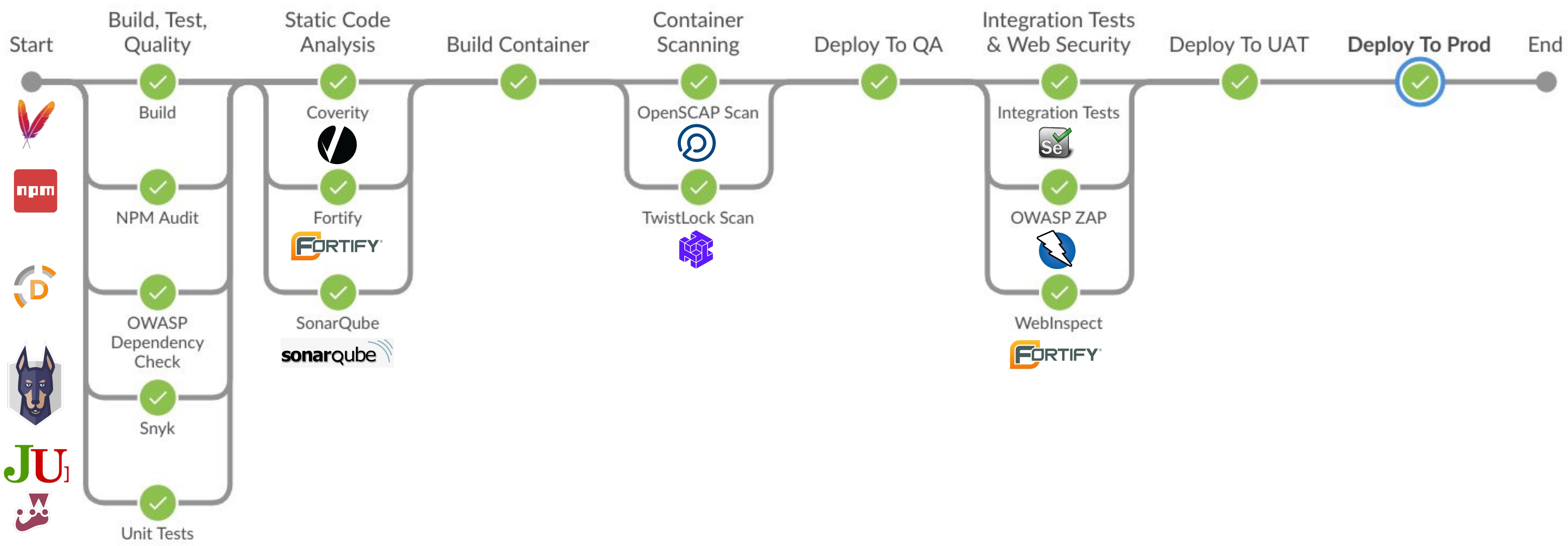
Area for Planning CI/CD and Automated Testing and Automated Monitoring

#redhat #rhsummit

We are leveraging CI/CD as a key practice in the enablement of DevSecOps to automate manual processes and inefficiencies in the current process.



Security Enabled Pipeline at US Department of Defense (DHS)



Evaluation of DevSecOps tools

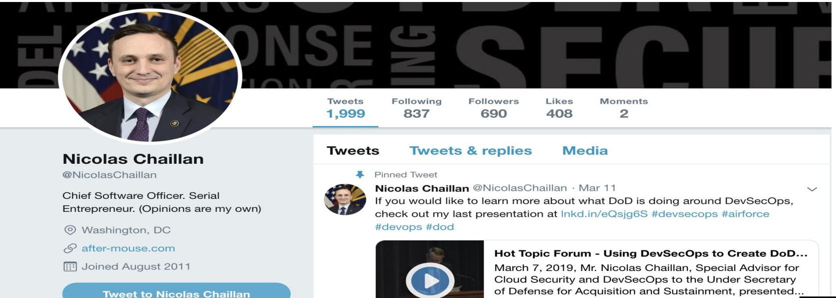
- Key tools leveraged so far: Jenkins, SonarQube, Selenium, Jest, Junit, Serenity, Cucumber, Nexus, OWASP Dependency Checker, Twistlock, Ansible, Github, Jira, Confluence and Slack.
- Leveraging Red Hat OpenShift for gaining experience in working with containers in a managed environment.
- Will be utilizing VMC as a tool for testing the pipeline across air-gapped environments.
- Still to integrate OWASP ZAP, BlackDuck and Fortify into the pipeline.
- Provide feedback to stakeholders for decision-making.

Red Hat Provides You the Easy Button to Accelerate Your DevSecOps!

- **Red Hat Innovation Labs “easy button” Ansible playbook to deploy CI/CD environment onto OpenShift**
  - Deploys these tools:
    - SonarQube and associated PostgreSQL database
    - Sonatype Nexus as an artifact repository
    - Jenkins
    - Hoverfly - create isolated test environments by simulating test dependencies.
    - Selenium Grid- parallel tests

  - Example pipelines which use this tooling: https://github.com/redhat-cop/container-pipelines and labs-ci-cd

Scaling DevSecOps across the US Department of Defense



Nicolas Chaillan
@NicolasChaillan

Chief Software Officer. Serial Entrepreneur. (Opinions are my own)

Washington, DC
after-mouse.com
Joined August 2011

Pinned Tweet

Nicolas Chaillan @NicolasChaillan · Mar 11
If you would like to learn more about what DoD is doing around DevSecOps, check out my last presentation at lnkd.in/eQsjg6S #devsecops #airforce #devops #dod

Hot Topic Forum - Using DevSecOps to Create DoD...
March 7, 2019, Mr. Nicolas Chaillan, Special Advisor for Cloud Security and DevSecOps to the Under Secretary of Defense for Acquisition and Sustainment, presented...
cdnapisec.kaltura.com

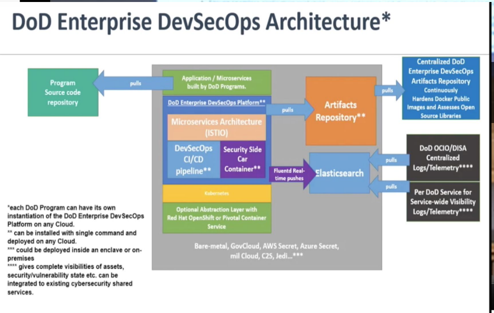
https://twitter.com/nicolaschaillan

"We're doing DevSecOps in the DoD, including for weapon systems"

Hot Topic Forum - Using DevSecOps to Create DoD Software Factories

<div><div><div><div><div><div><div><div>March 7, 2019, Mr. Nicolas Chaillan, Specia
and Sustainment, presented his vision for how to transform DoD software acquisition into se
warfighter needs. As a result, DoD's ability to keep pace with our potential adversaries is fall
tools to revolutionize the Department's ability to provide responsive, timely and secure softw

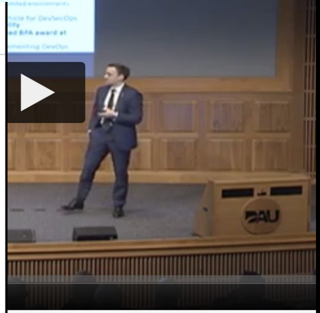
Hot Topic Forum - Using DevSecOps to Create DoD Software Factories



DoD Enterprise DevSecOps Architecture*

Program Source code repository
pulls
Application / Microservices built by DoD Programs.
DoD Enterprise DevSecOps Platform**
Microservices Architecture (ISTIO)
DevSecOps CI/CD pipeline**
Security Side Car Container**
Kubernetes
Optional Abstraction Layer with Red Hat OpenShift or Pivotal Container Service
Bare-metal, GovCloud, AWS Secret, Azure Secret, mil Cloud, C2S, Jedi...***
pulls
Artifacts Repository**
pulls
Centralized DoD Enterprise DevSecOps Artifacts Repository Continuously Hardens Docker Public Images and Assesses Open Source Libraries
Fluentd Real-time pushes
Elasticsearch
pulls
DoD OCIO/DISA Centralized Logs/Telemetry****
pulls
Per DoD Service for Service-wide Visibility Logs/Telemetry****

*each DoD Program can have its own instantiation of the DoD Enterprise DevSecOps Platform on any Cloud.
** can be installed with single command and deployed on any Cloud.
*** could be deployed inside an enclave or on-premises
**** gives complete visibilities of assets, security/vulnerability state etc. can be integrated to existing cybersecurity shared services.



DevNation Federal 2019 - DoD Software Factory with the DoD Enterprise DevSecOps Initiative

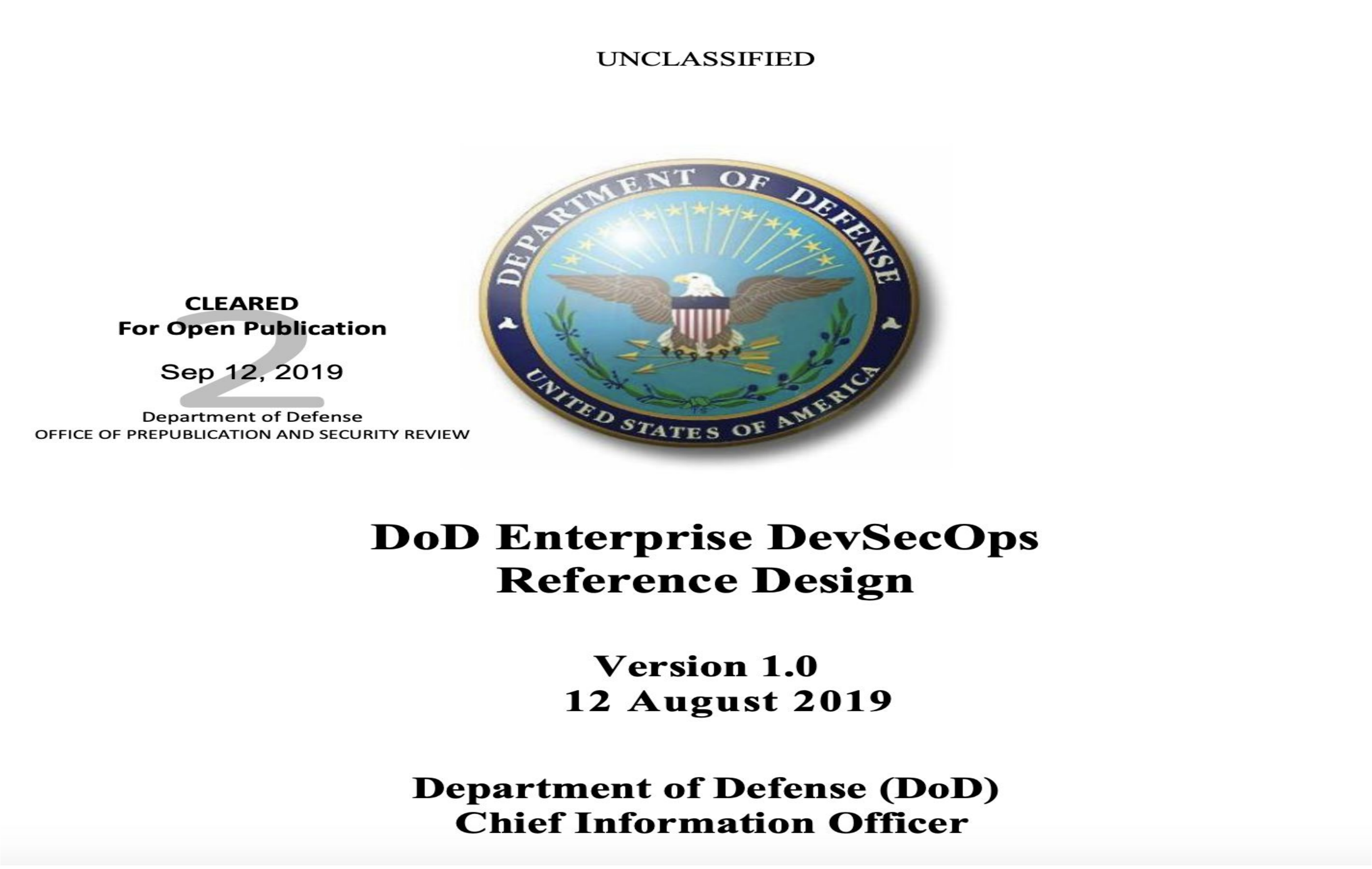
Headquarters U.S. Air Force

Integrity - Service - Excellence

DoD Enterprise DevSecOps Initiative (Software Factory)

Mr. Nicolas Chaillan
Chief Software Officer, U.S. Air Force
Co-Lead, DoD Enterprise DevSecOps Initiative

v1.01 – Unclassified



UNCLASSIFIED

CLEARED
For Open Publication

Sep 12, 2019

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Enterprise DevSecOps Reference Design

Version 1.0
12 August 2019

Department of Defense (DoD)
Chief Information Officer

Enabling Faster & Scalable DevSecOps with Red Hat OpenShift Container Platform

AUTOMATED BUILDS

CI/CD using Jenkins

Tekton

Source-2-Image

Buildah

CONTINUOUS BUILT-IN SECURITY

Automated analysis with SonarQube, OWASP Dependency Check, NPM Audit, OWASP Zed Attack Proxy, OpenSCAP, etc...

AUTOMATED OPERATIONS

RHEL CoreOS immutable OS, OpenShift Operators to monitor and respond to changing needs, load, threats, etc..

COMPREHENSIVE CONTAINER SECURITY WITH RED HAT OPENSHIFT

CONTROL

Application Security

- Container Content
- CI/CD Pipeline
- Container Registry
- Deployment Policies

DEFEND

Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

EXTEND

- Security Ecosystem

Takeaways

- There's no such thing as 100% security. Security is a **process, NOT a product**.
    - No silver bullet product for security. Leverage the security technologies that **you already have** (in the OS, Automation tools, etc)
    - Identify your **risk tolerance**.
        - Understand scope of open-source usage + consume it securely
    - Security is **everyone's** job. Take a **holistic, continuous, defense-in-depth** approach to security. Cross-training across Dev/Ops/Security.
    - Security is not *just* about technology - the **human factor** can be your weakest link! (social engineering breaches, insider threats, lack of skills, bad processes in place, etc)
- Identify **focus areas for automation to improve security across App, Ops, SOC. Take baby steps** (example: using a common automation language across departments)
    - **Implement Holistic DevSecOps**
    - **Prevention, Detection, Response**. Implement security hygiene practices (regular automated patches, etc).
    - Learn from **examples - both from successes + failures(breaches)**
        - **Read** the **Cloud Security Alliance 'Top Threats to Cloud Computing'** paper

NEXT STEPS AND RESOURCES

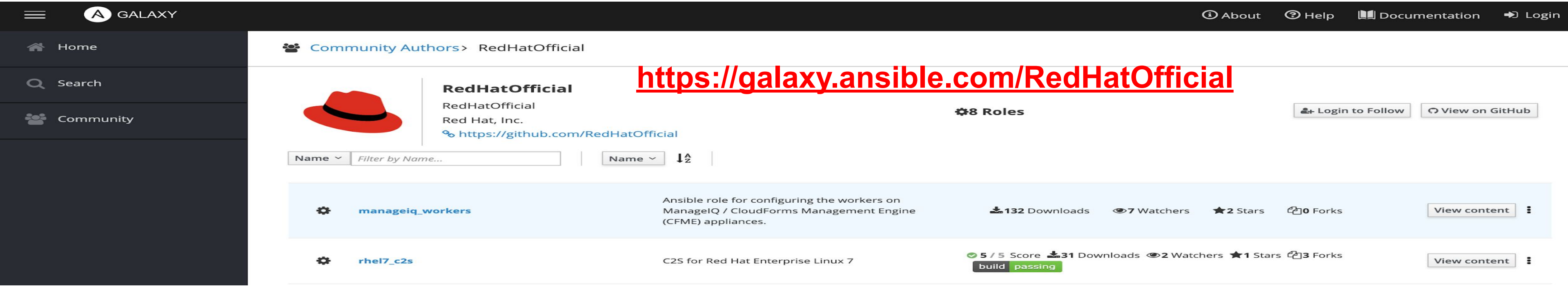
Red Hat Automated Security & Compliance Free Hands-On Lab Exercises (@ 12:30pm today!)

1. **Red Hat Security Hands-On Labs:**
    a. Red Hat Enterprise Linux Security Technologies
    b. Creating Customized Security Policy Content
    c. Implementing Proactive Security and Compliance & DevSecOps

2. **All lab docs, scripts, and Ansible playbooks are here:**
   https://red.ht/securitylabs

3. **Your Red Hat Team can provision these free Red Hat Security hands-on labs for you for individual or workshop use.**

Red Hat Created and Supported Ansible hardening playbooks to Automate Security Compliance



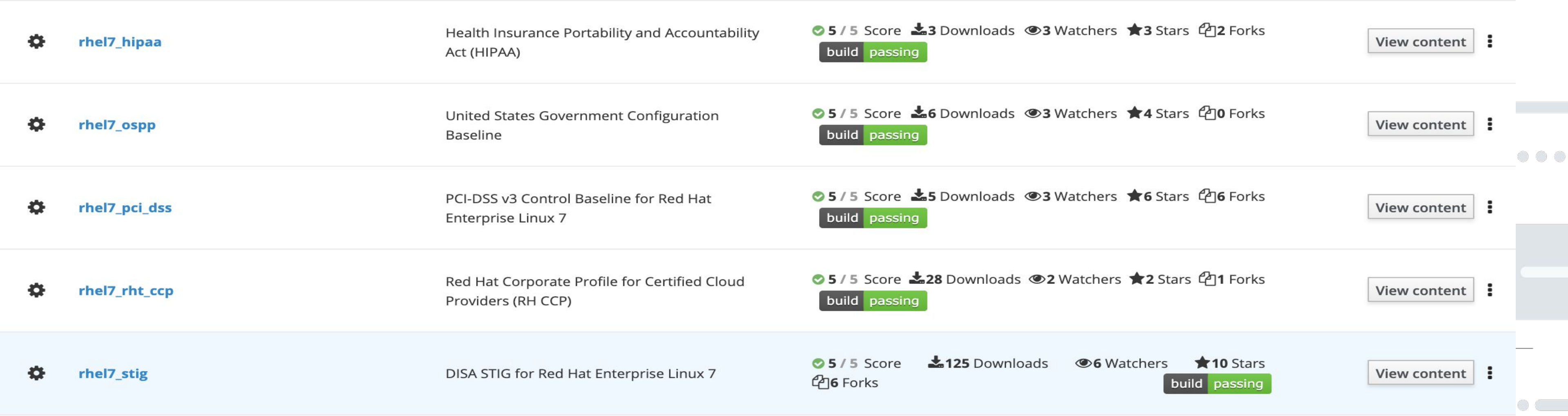
Community Authors > RedHatOfficial

https://galaxy.ansible.com/RedHatOfficial

RedHatOfficial
RedHatOfficial
Red Hat, Inc.
https://github.com/RedHatOfficial

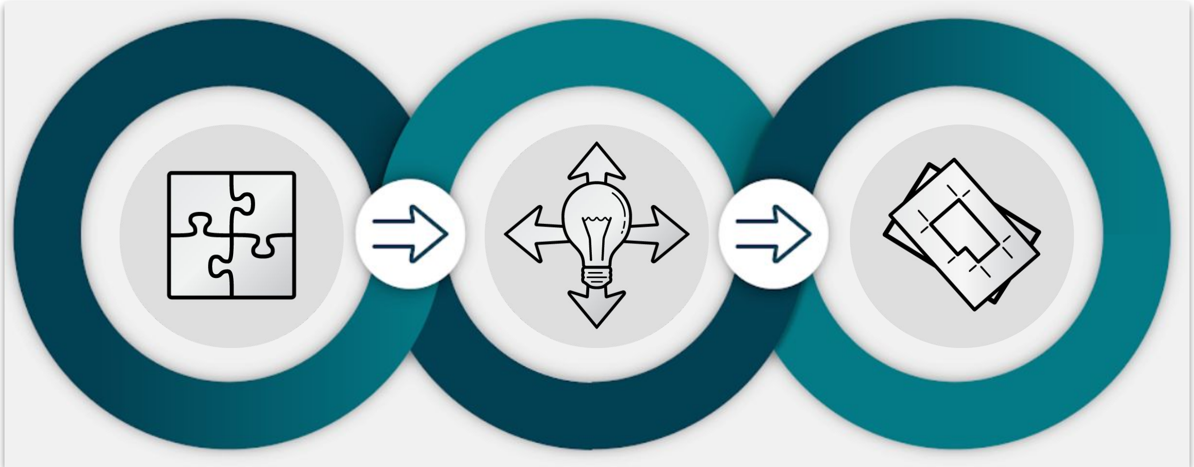
8 Roles

manageiq_workers	Ansible role for configuring the workers on ManageIQ / CloudForms Management Engine (CFME) appliances.	132 Downloads 7 Watchers 2 Stars 0 Forks	View content
rhel7_c2s	C2S for Red Hat Enterprise Linux 7	5 / 5 Score 31 Downloads 2 Watchers 1 Stars 3 Forks build passing	View content



rhel7_hipaa	Health Insurance Portability and Accountability Act (HIPAA)	5 / 5 Score 3 Downloads 3 Watchers 3 Stars 2 Forks build passing	View content
rhel7_ospp	United States Government Configuration Baseline	5 / 5 Score 6 Downloads 3 Watchers 4 Stars 0 Forks build passing	View content
rhel7_pci_dss	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	5 / 5 Score 5 Downloads 3 Watchers 6 Stars 6 Forks build passing	View content
rhel7_rht_ccp	Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	5 / 5 Score 28 Downloads 2 Watchers 2 Stars 1 Forks build passing	View content
rhel7_stig	DISA STIG for Red Hat Enterprise Linux 7	5 / 5 Score 125 Downloads 6 Watchers 10 Stars 6 Forks build passing	View content

SECURITY AND COMPLIANCE DISCOVERY SESSION WITH RED HAT CONSULTING SERVICES

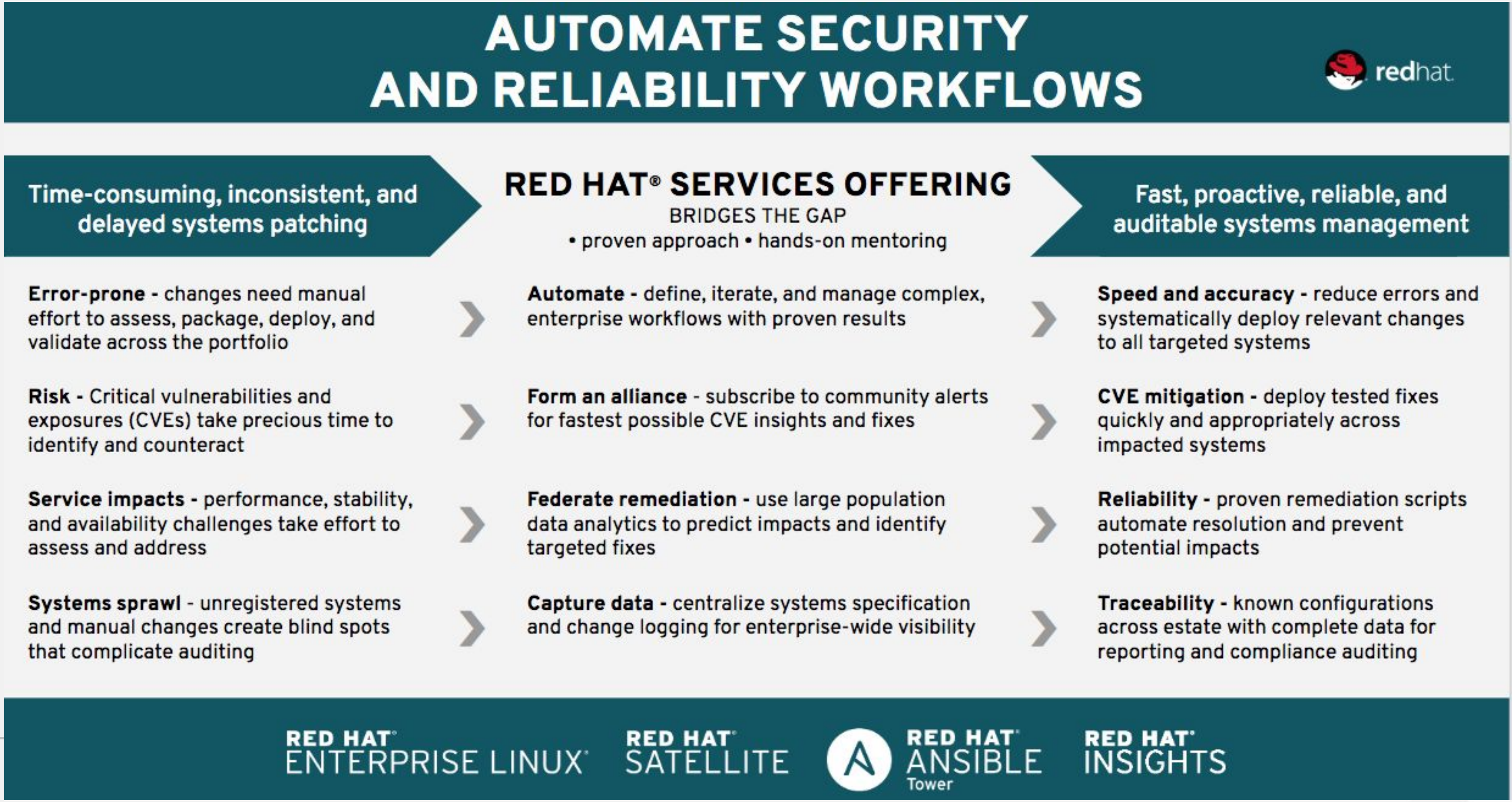


Develop a security and compliance challenges overview

Identify potential approaches and frameworks

Create an action plan to address vulnerabilities

Security & Red Hat Consulting Services



AUTOMATE SECURITY AND RELIABILITY WORKFLOWS

Time-consuming, inconsistent, and delayed systems patching	RED HAT® SERVICES OFFERING BRIDGES THE GAP • proven approach • hands-on mentoring	Fast, proactive, reliable, and auditable systems management
Error-prone - changes need manual effort to assess, package, deploy, and validate across the portfolio	**Automate -** define, iterate, and manage complex, enterprise workflows with proven results	**Speed and accuracy -** reduce errors and systematically deploy relevant changes to all targeted systems
Risk - Critical vulnerabilities and exposures (CVEs) take precious time to identify and counteract	**Form an alliance** - subscribe to community alerts for fastest possible CVE insights and fixes	**CVE mitigation -** deploy tested fixes quickly and appropriately across impacted systems
Service impacts - performance, stability, and availability challenges take effort to assess and address	**Federate remediation -** use large population data analytics to predict impacts and identify targeted fixes	**Reliability -** proven remediation scripts automate resolution and prevent potential impacts
Systems sprawl - unregistered systems and manual changes create blind spots that complicate auditing	**Capture data -** centralize systems specification and change logging for enterprise-wide visibility	**Traceability -** known configurations across estate with complete data for reporting and compliance auditing

RED HAT® ENTERPRISE LINUX® RED HAT® SATELLITE RED HAT® ANSIBLE Tower RED HAT® INSIGHTS

Red Hat Security Training and Certification Offerings

1. **D0500:** DevOps Culture and Practice Enablement
2. **D0700:** Container Adoption Boot Camp
3. **D0426:** Securing Containers and OpenShift (with exam)

   <Also free OpenShift hands-on training on : http://learn.openshift.com/
4. **RH415:** Red Hat Security: Linux in Physical, Virtual, Cloud (with exam)

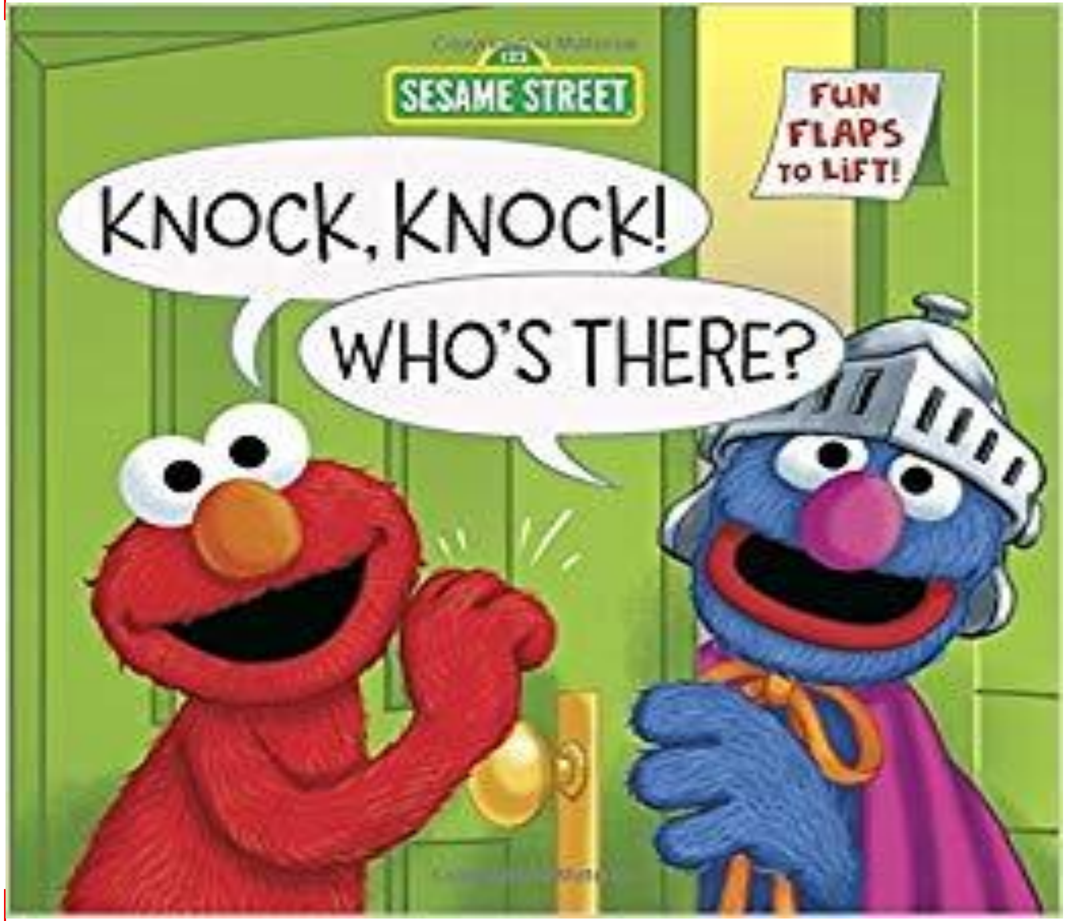
Red Hat Security Related Links

- Solution Brief: Increase Security and Compliance with Advanced Automation
  - https://www.redhat.com/en/resources/automate-security-compliance-solution-brief
- Whitepaper: Red Hat Automated Security and Compliance
  - https://www.redhat.com/en/resources/red-hat-automated-security-and-compliance
- Video: https://www.redhat.com/en/about/videos/red-hat-automated-security-compliance-for-telecommunications-service-providers
- Red Hat Consulting Services Datasheet: Automate Security and Reliability Workflows
  - https://www.redhat.com/en/resources/services-consulting-automate-security-reliability-datasheet
- Red Hat provided and supported Ansible security hardening Ansible playbooks in Ansible Galaxy
  - https://galaxy.ansible.com/RedHatOfficial
- Red Hat Security Hands-on Labs : https://red.ht/securitylabs

Red Hat Security Related Links (cont..)

- Guide to continuous security
  - https://www.redhat.com/en/technologies/guide/it-security
- Understanding IT Security
  - https://www.redhat.com/en/topics/security
- Container Security
  - https://www.redhat.com/en/topics/security/container-security
- Red Hat Product Security
  - https://access.redhat.com/security/overview

Ending with a Cybersecurity Knock Knock Joke

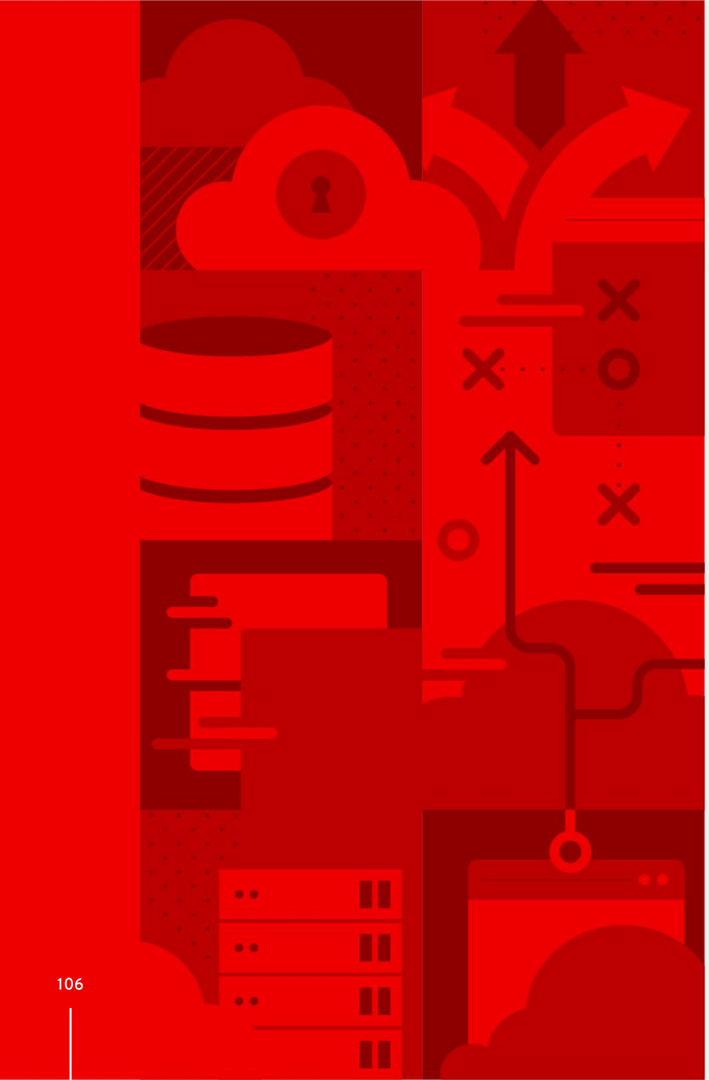


Knock Knock

Who’s There?

Boo

Boo Who?



Questions?

lkerner@redhat.com

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

in linkedin.com/company/red-hat

▶ youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat