Automating Security and Compliance for Hybrid Environments

Lucy Kerner
Senior Principal Security Global Technical Evangelist & Strategist
lkerner@redhat.com
Twitter: @LucyCloudBling

whoami

LUCY KERNER

Security Global Technical Evangelist & Strategist

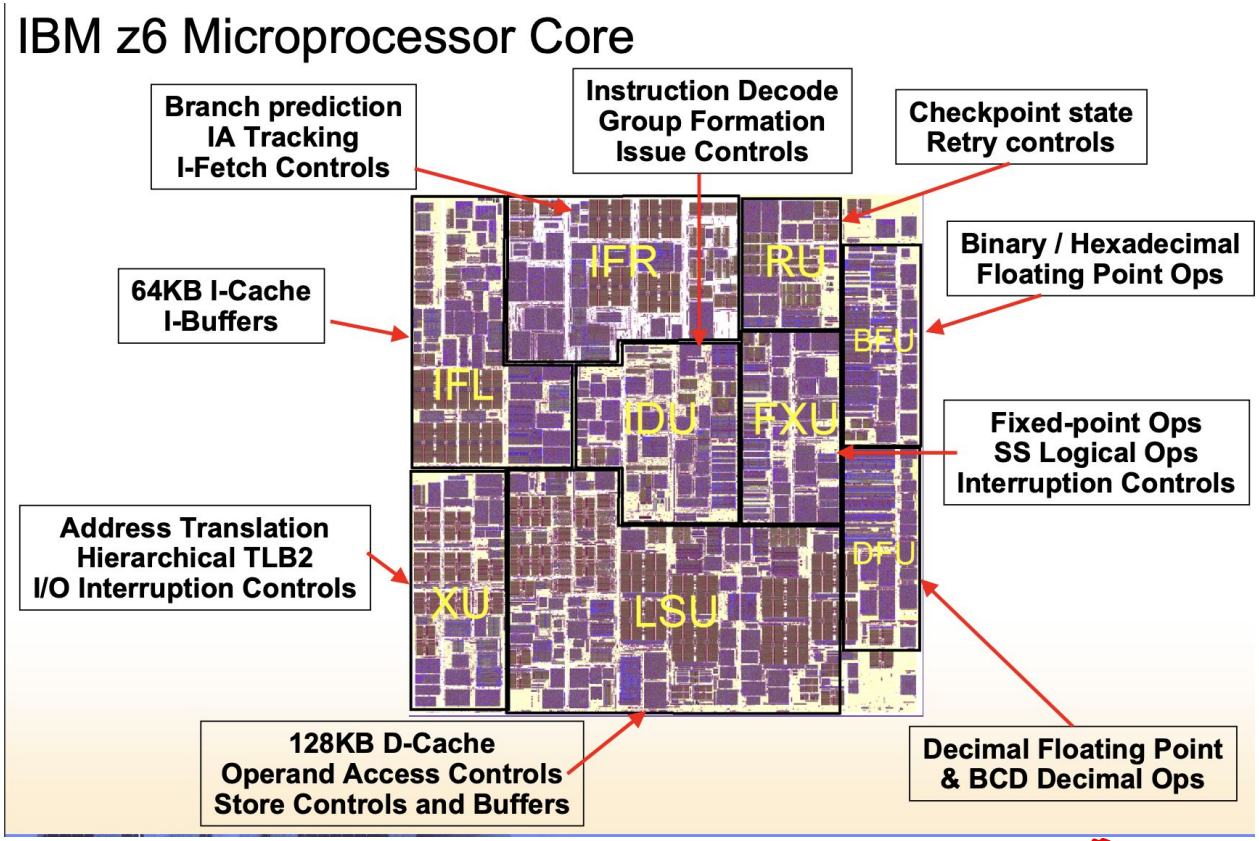
Carnegie Mellon University
Electrical & Computer ENGINEERING

IBM
Poughkeepsie

My first job after college

Red Hat

whoami



Red Hat

CYBERSECURITY ATTACKS ARE CONTINUOUSLY EVOLVING

Meltdown and Spectre

Vulnerabilities in modern processors leak passwords and sensitive data.

Red Hat

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

Red Hat

“Most breaches we become aware of are caused by failure to update software components that are known to be vulnerable for months or even years...”

René Gielen, Vice President of Apache Struts

2018 Marriott Data Breach

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

Red Hat

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

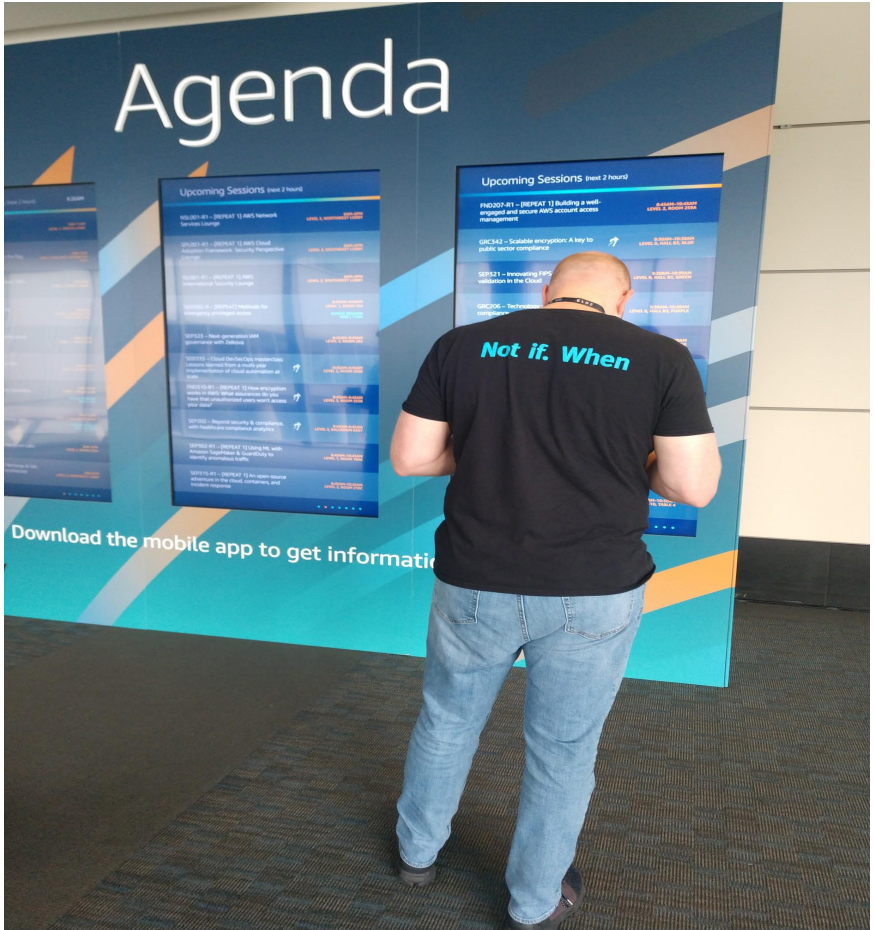
- Federal Trade Commission (FTC) claimed that Wyndham violated the FTC's standards for data security:
    - failed to use readily available security measures, such as firewalls
    - **stored credit card information in clear text**
    - failed to implement reasonable information security procedures 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

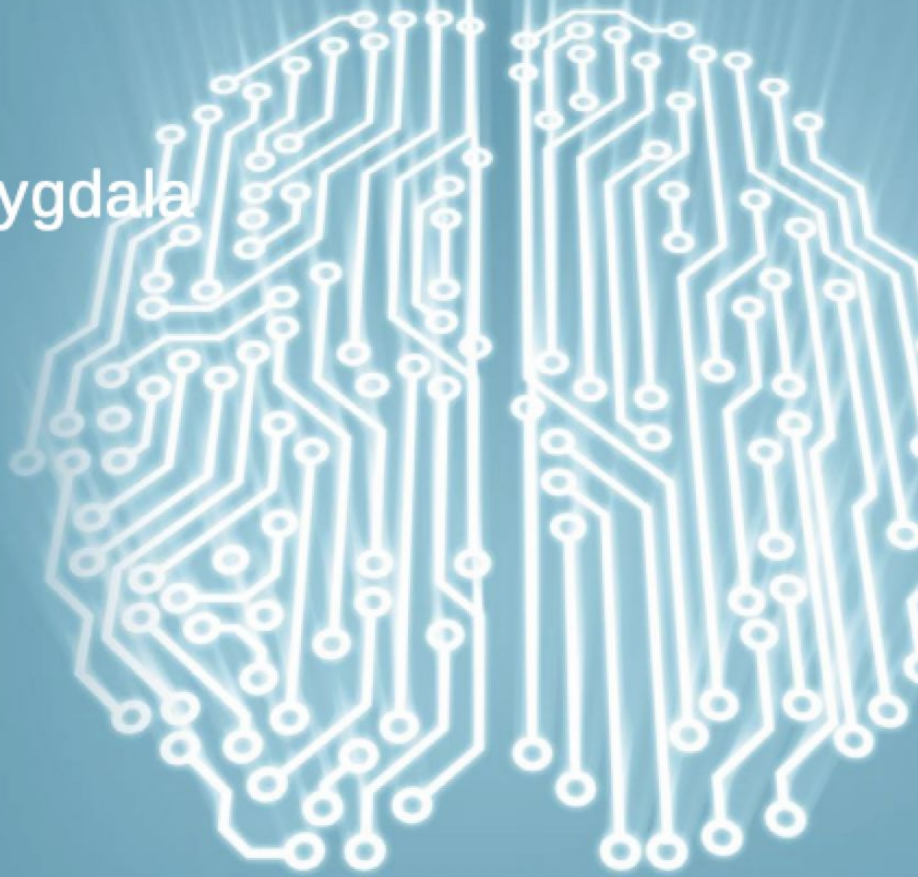
Red Hat

Not If. When.



Red Hat

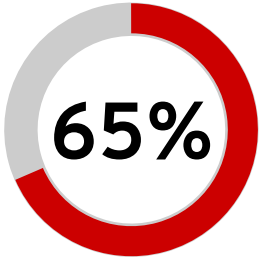
Why humans are bad at security



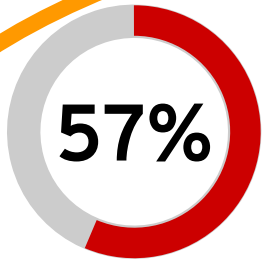
The neocortex versus the amygdala

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

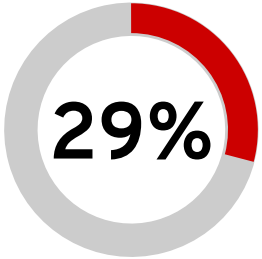
The Cyber Security Challenge is Not Getting Easier



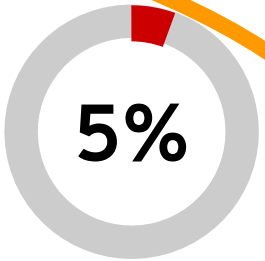
Reported increased severity of attacks [1]



Said the time to resolve an incident has grown [1]



Have their ideal security-skilled staffing level, making it the #2 barrier to cyber resilience [1]

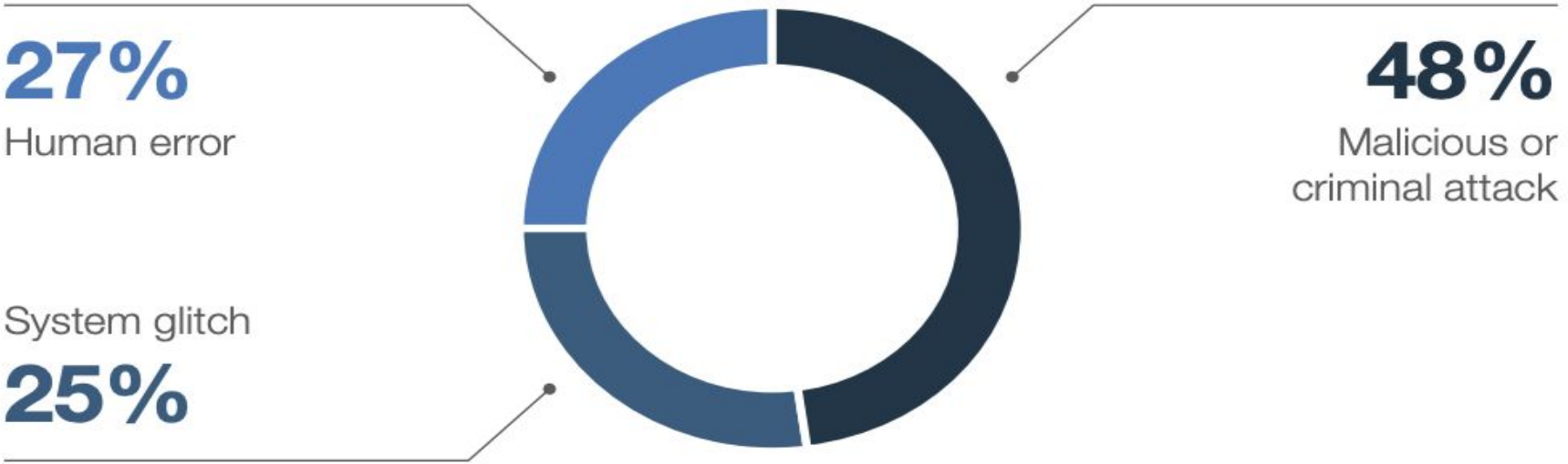


Portion of alerts coming in that the average security team examines every day [2]

[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/

Red Hat

Distribution of the benchmark sample by root cause of the data breach



"77% of firms surveyed lack proper security incident response plans"

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

Red Hat

Security, Compliance and Governance Challenges in Hybrid Environments

- Increasing complexity introduces risk
- Decreased visibility and control

- Inconsistent configurations and patching
- **"Manually monitoring & managing systems for security and compliance becomes *IMPOSSIBLE*"**
  (Chris Gardner - Forrester)

Red Hat

Top Threats to Cloud Computing

The Egregious 11

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

Red Hat

Capital One Data Theft Impacts 106M People

CapitalOne

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/

Red Hat

What We Can Learn from the Capital One Hack

- Misconfiguration of open-source web application firewall(WAF): ModSecurity (Modsec)
  - Due to the misconfiguration, the intruder was able to send a request to the local metadata service, which returned the temporary IAM credentials the WAF was using. Then, the intruder used those creds to make API calls to the S3 service and dump all the data.

- This would imply two bad configurations:
  - Whatever was on the WAF that allowed the redirection to the metadata service, and
  - The overly-permissive role assigned to the EC2 instance and allowed all the S3 access.

The type of vulnerability exploited by the intruder in the Capital One hack is a well-known method called a "Server Side Request Forgery" (SSRF) attack, in which a server (in this case, CapOne's WAF) can be tricked into running commands that it should never have been permitted to run, including those that allow it to talk to the metadata service.

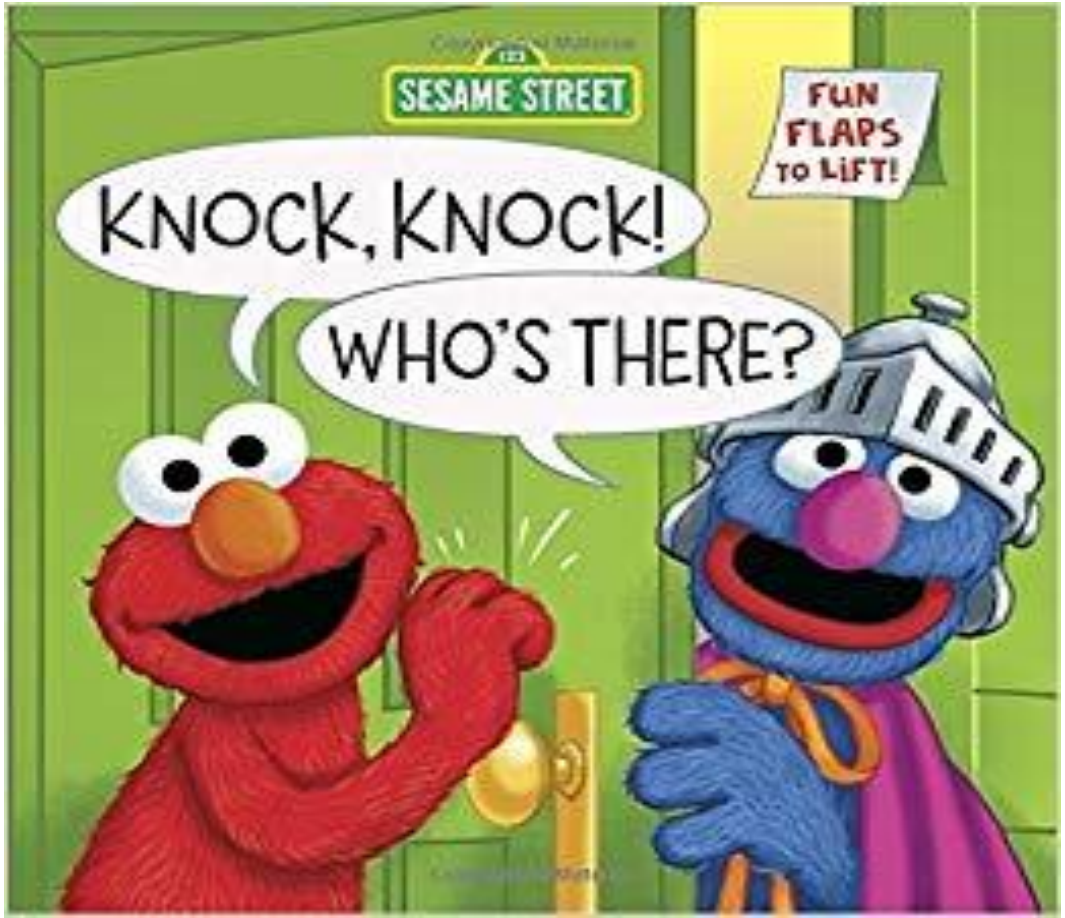
"SSRF has become the most serious vulnerability facing organizations that use public clouds," Johnson wrote.

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/

Red Hat

A Related Knock Knock Joke



Red Hat

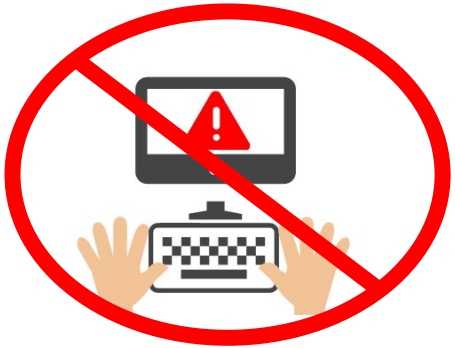
Knock Knock

Who’s There?

Boo

Boo Who?

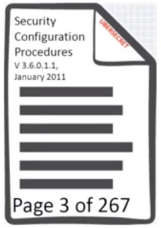
Automation for Increased Security and Compliance



Continuous Monitoring & Controlled Remediations for Security + Compliance

Bake Security into Dev & Ops

OLD



NEW

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

Red Hat

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

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

Red Hat

“We cannot be left behind. China, Russia, and North Korea are already massively implementing Automation and DevSecOps.” [1]

[1] Quote from Nicolas Chaillan, US DoD Special Advisor for Cloud Security and DevSecOps

Red Hat

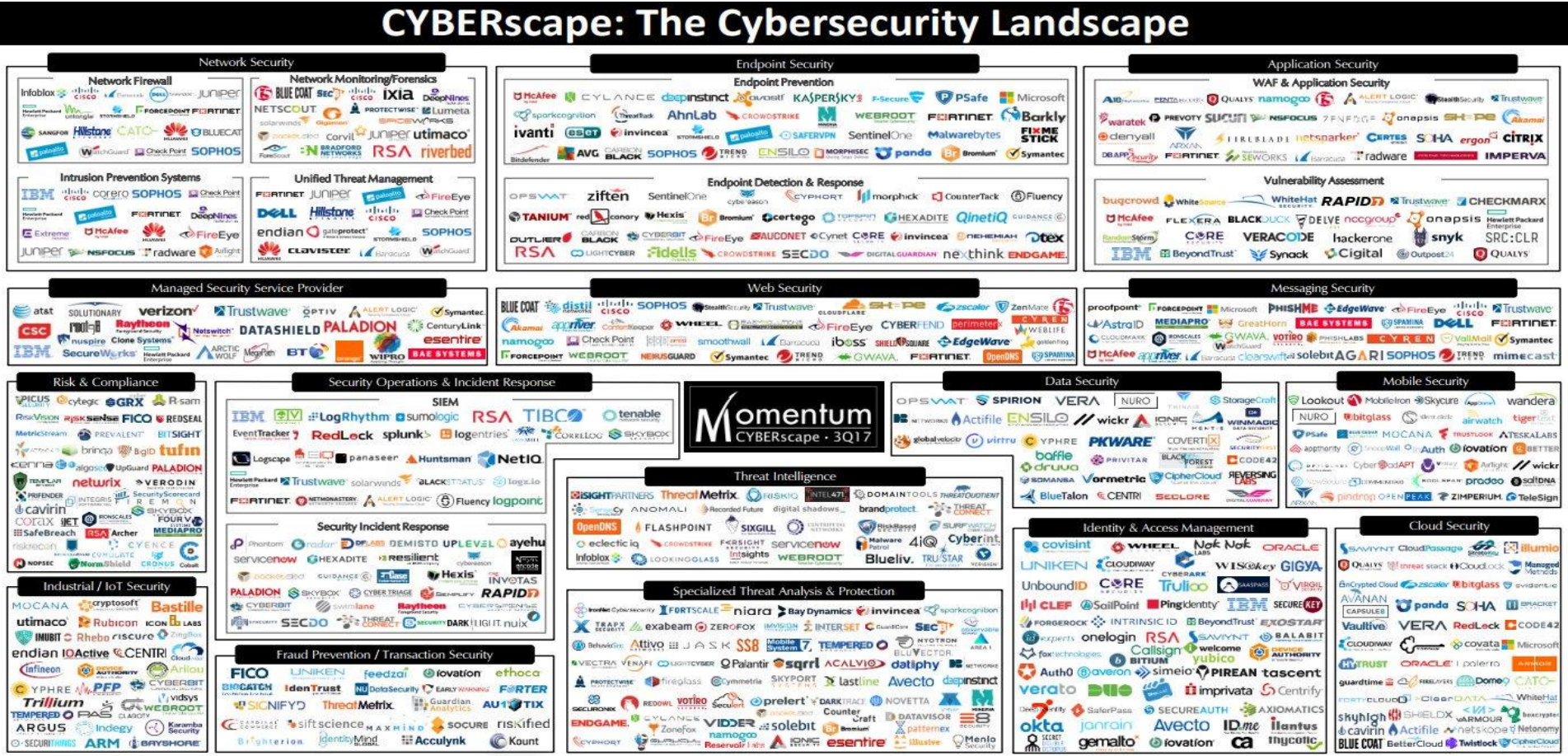
“Automate anything you can as this reduces the human error associated with many breaches we see.” [1]

[1] 2019 and 2018 Verizon Data Breach Investigations Report

Red Hat

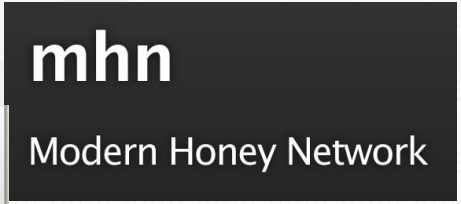
How can Red Hat help?

Welcome to the Vast World of Cybersecurity Tools



Source: Momentum Partners

Growing # of open source security tools...



Growing # of cloud and container security vendors

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/

Evolution of Traditional Security Vendors

“Secure DevOps + Serverless Security”

“Qualys Cloud Platform”

“Securing the Cloud Generation”

Red Hat

NOT Zero Sum

Red Hat

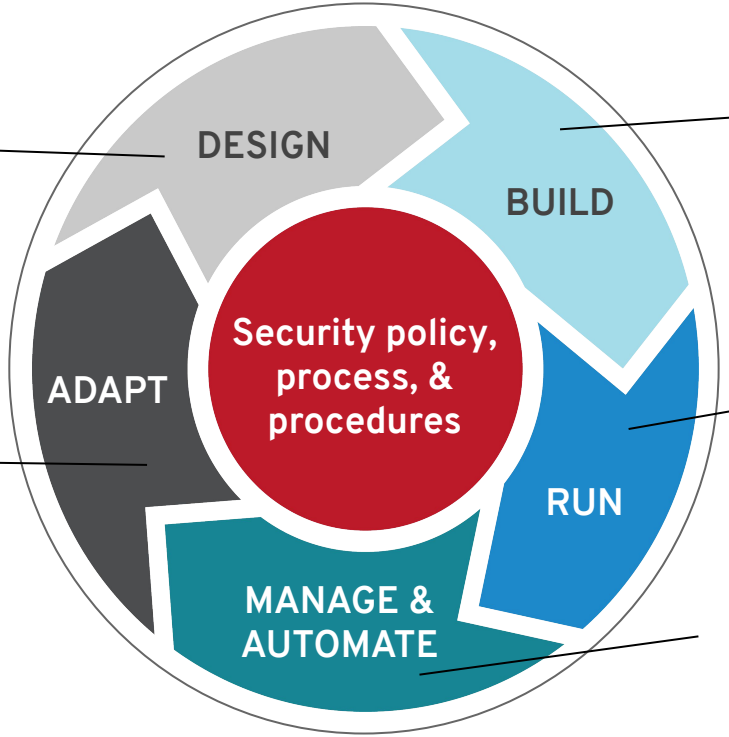
“Security is a process, NOT a product.”

– Bruce Schneier

(American cryptographer, security blogger, and author)

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

Red Hat

SECURITY THROUGHOUT THE STACK + LIFECYCLE

DESIGN

- RED HAT CONSULTING Guided Transition
- RED HAT SERVICES
- RED HAT TRAINING

BUILD

- RED HAT OPENSHIFT Container Platform
- RED HAT MIDDLEWARE
- 3scale BY RED HAT

RUN

- RED HAT ENTERPRISE LINUX
- RED HAT CoreOS
- RED HAT VIRTUALIZATION
- RED HAT OPENSTACK PLATFORM
- RED HAT STORAGE

MANAGE & AUTOMATE

- RED HAT ANSIBLE Automation
- RED HAT SATELLITE
- RED HAT CLOUDFORMS

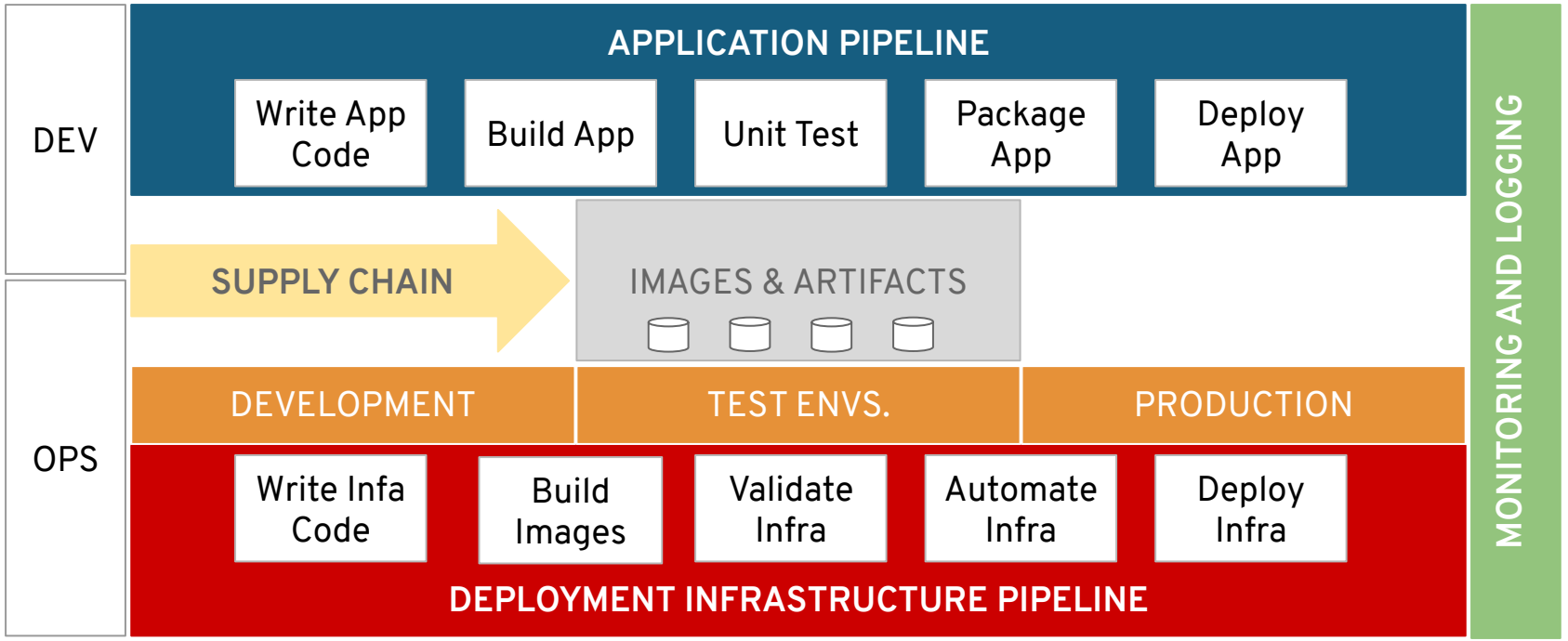
ADAPT

- RED HAT INSIGHTS
- RED HAT SECURITY ADVISORIES

TESTED, CERTIFIED, STABLE, AND SUPPORTED OPEN SOURCE SOFTWARE

Holistic DevSecOps with Red Hat

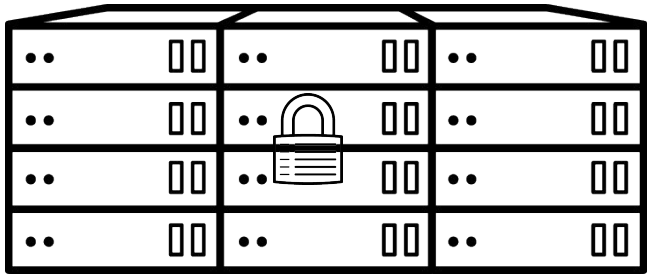
It's not just about the application CI/CD pipeline!



Red Hat

Automated Security and Compliance with Red Hat

Applications



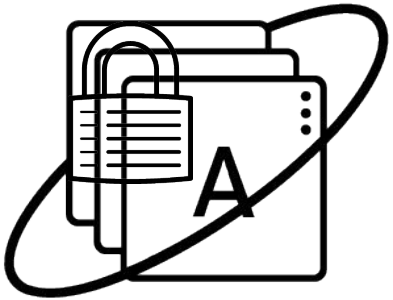
Infrastructure and Operations

Security Operations Center (SOC)

Red Hat

Automated Security and Compliance with Red Hat

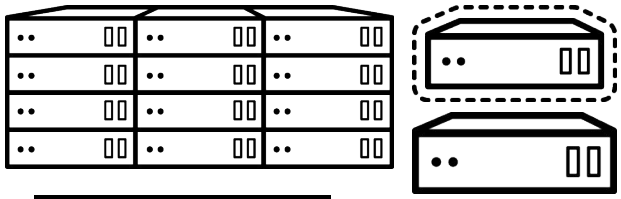
DevSecOps and Building Security into the Application



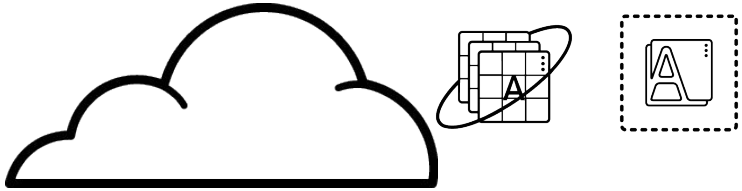
Applications

Red Hat

Enabling DevSecOps with Containers
Traditional vs Cloud Native



Red Hat Ansible Automation



Red Hat Ansible Automation

Red Hat OpenShift Container Platform

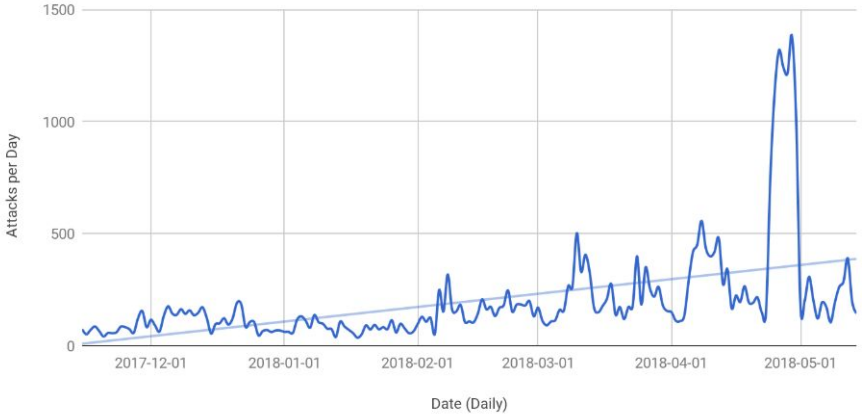
Red Hat Insights

Antifragile

DEVELOPERS AREN'T SECURITY EXPERTS

L7 ATTACKS ON THE RISE

"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/

Red Hat

MICROSERVICES

A BLESSING AND A CURSE FOR SECURITY

"The softest target in most organizations is the app layer and attackers know this. Microservices thus both make this problem harder and easier for the defenders"

Many separate APIs and ports per app == numerous doors for attackers

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/

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** ...

Open Sourcing the Kubernetes Security Audit

By Chris Aniszczyk | August 6, 2019 | Blog

Last year, the Cloud Native Computing Foundation (CNCF) began the process of performing a
audits for its projects in order to improve the overall security of our ecosystem. The idea was t
gather feedback from the CNCF community as to whether or not this pilot program was usefu
process were CoreDNS, Envoy and Prometheus. These first public audits identified security issu
vulnerabilities. With these results, project maintainers for CoreDNS, Envoy and Prometheus hav
vulnerabilities and add documentation to help users.

The main takeaway from these initial audits is that a public security audit is a great way to tes
along with its vulnerability management process and more importantly, how resilient the open
With CNCF graduated projects especially, which are used widely in production by some of the
imperative that they adhere to the highest levels of security best practices.

Findings

- Kubernetes Security Review
- Attacking and Defending Kubernetes Installations
- Whitepaper
- Threat Model


MORNING KEYNOTE
Dr. Jon Brickey, SVP,
Cybersecurity Evangelist,
Mastercard
CYBER//2019
HOWARD
COMMUNITY COLLEGE

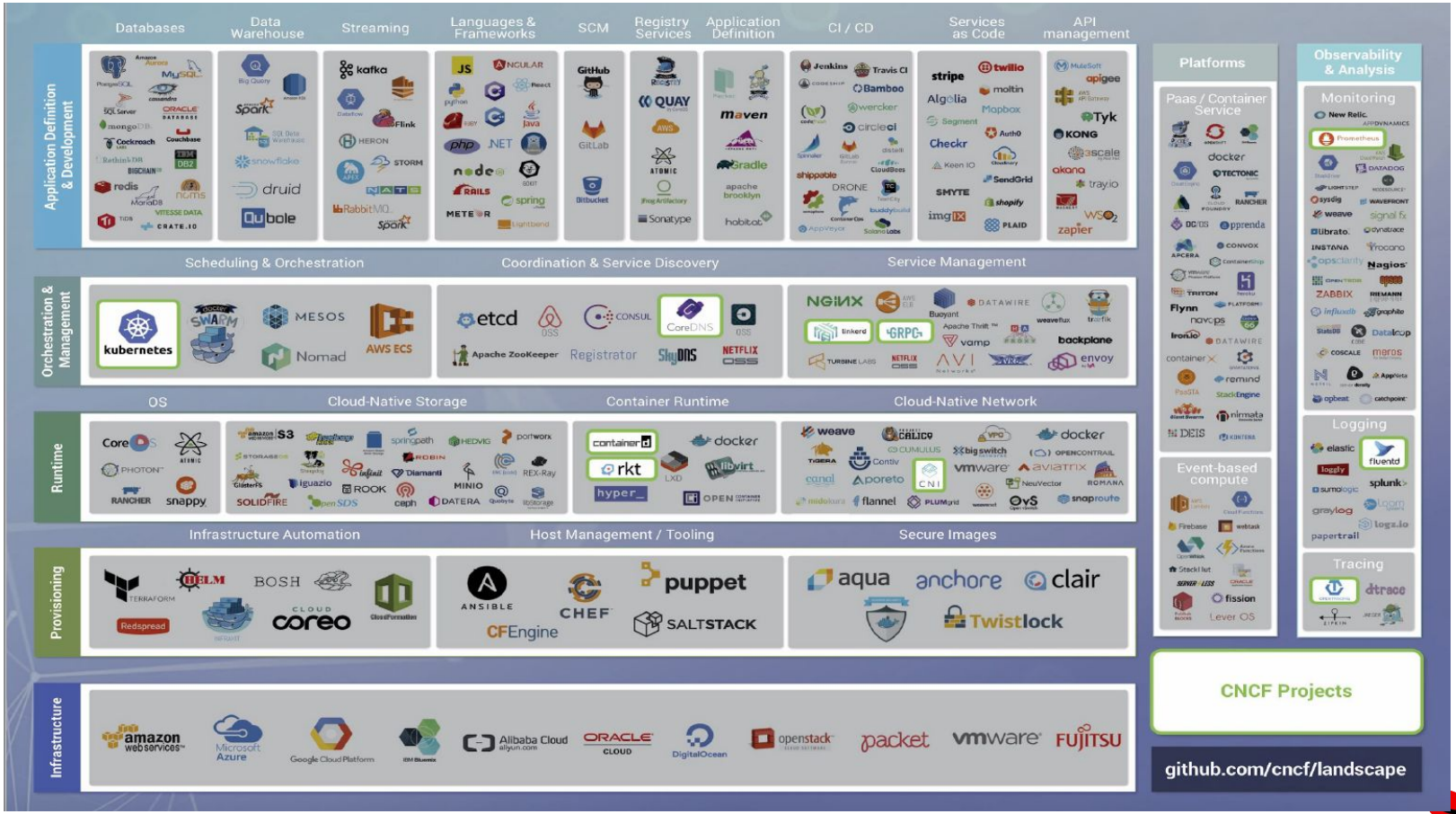
Cybersecurity Strategic Pillar at MasterCard:

Enabling the Business with “Business Security Engineers”

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

Red Hat

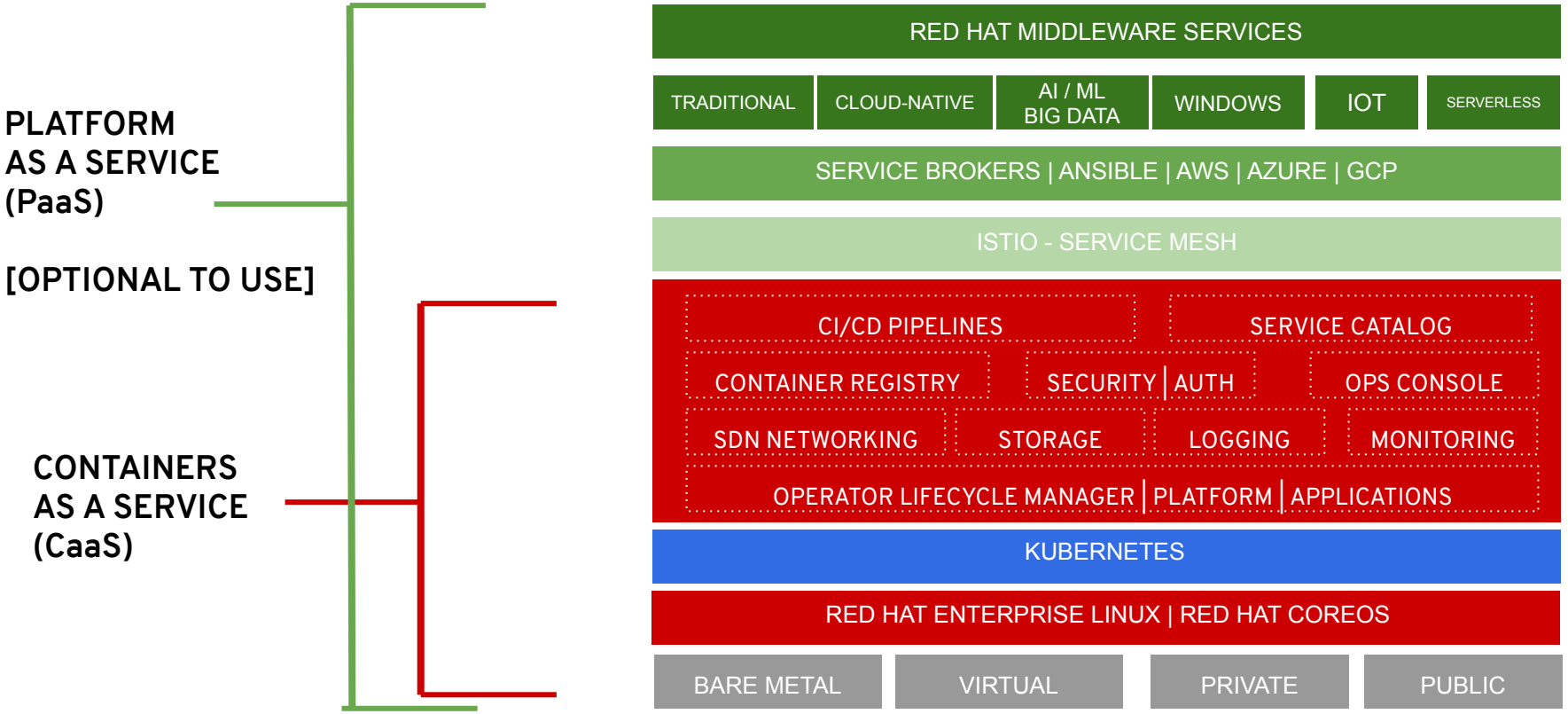
LANDSCAPE OF OPEN SOURCE PROJECTS



How will you integrate these projects to create an Enterprise Ready Distribution?

Red Hat

Easy Button and Integrated with Red Hat OpenShift



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

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

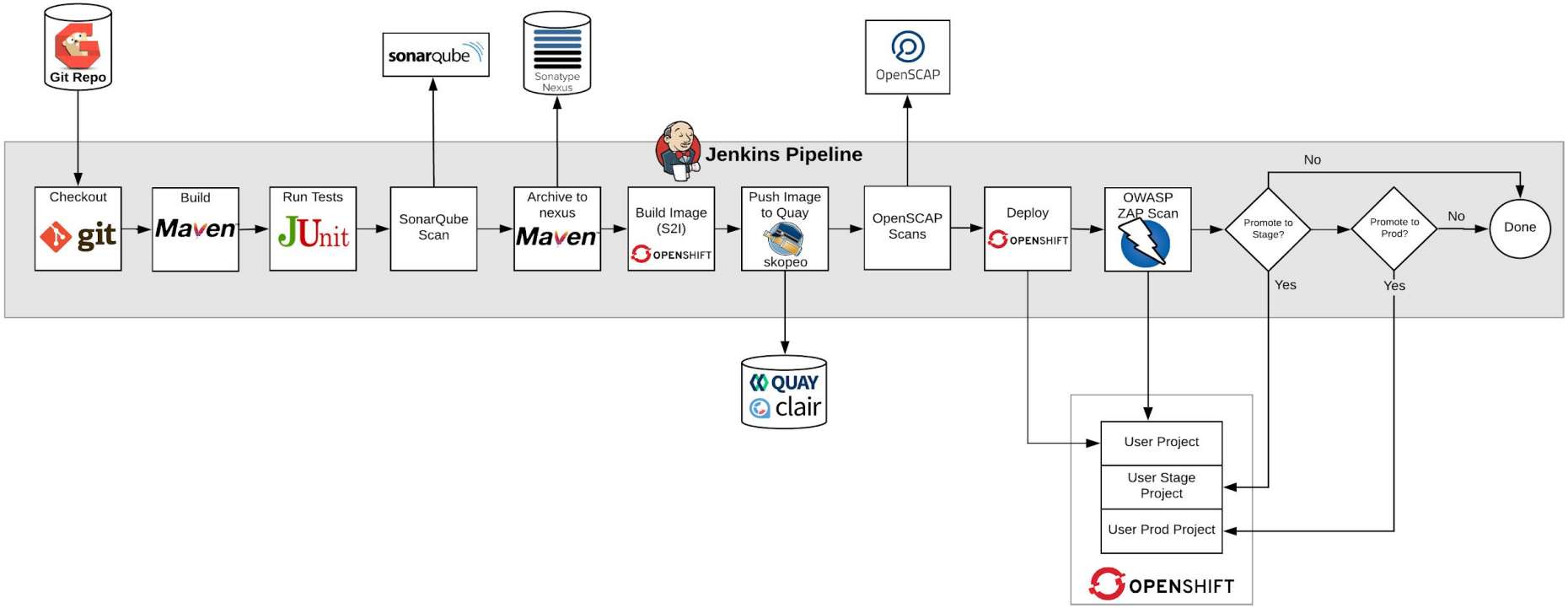
Automated analysis with SonarQube, OWASP Dependency Check, NPM Audit, OWASP Zed Attack Proxy, OpenSCAP, etc...

AUTOMATED OPERATIONS

OpenShift Operators to monitor and respond to changing needs, load, threats, etc..

Red Hat

DevSecOps and Building Security into the Application with an Automated 'Software Factory'



Red Hat

2019 Red Hat Summit Security Hands-On Labs

https://red.ht/securitylabs

The DevSecOps pipeline from the previous slide was implemented in the 'Proactive Security' lab that my team and I created. See link above for more details. You'll also find all 3 Security hands-on labs that we created for Red Hat Summit 2019.

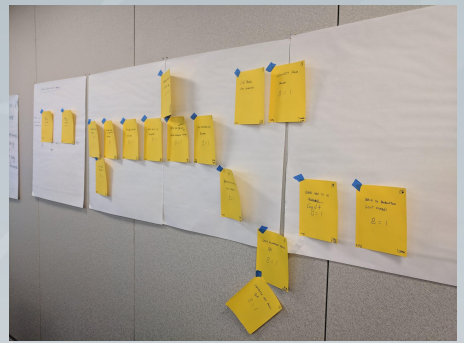
Red Hat

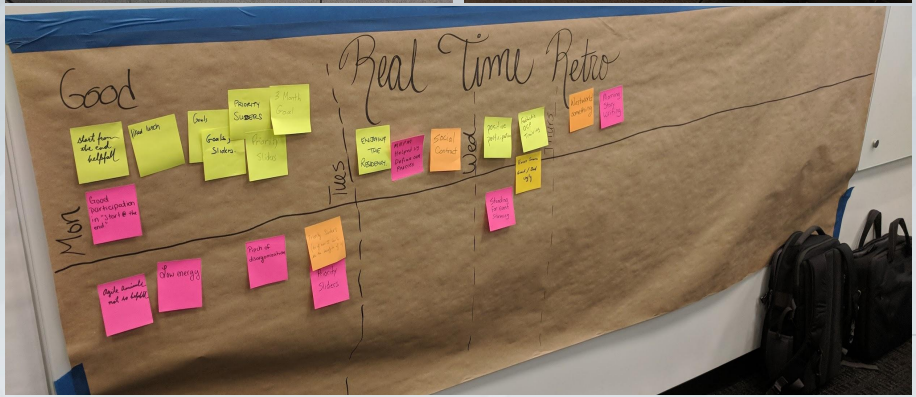
Red Hat Provides You the Easy Button to Accelerate Your DevSecOps!

- **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
  - Other useful tools:
    - CASL-Ansible(ansible to automate OpenShift), infra-ansible (ansible for infr. automation), openshift-applier (apply ocp objects to openshift cluster)

Red Hat

Accelerating DevSecOps with Red Hat Open Innovation Labs

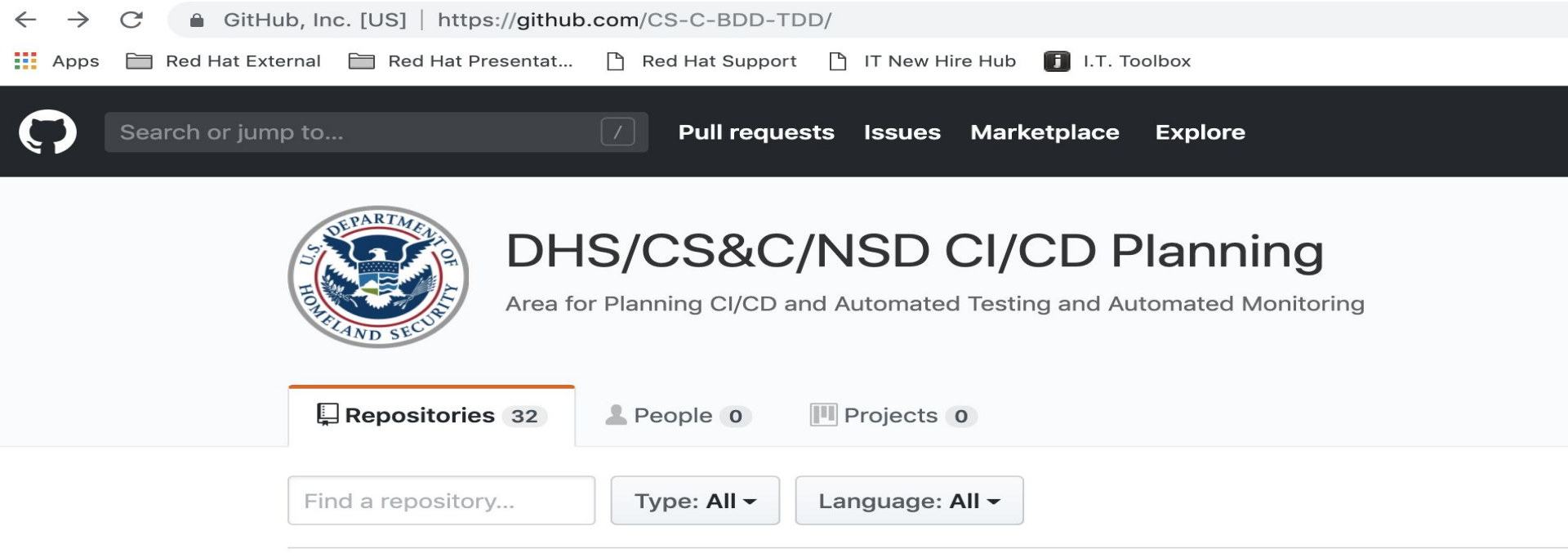




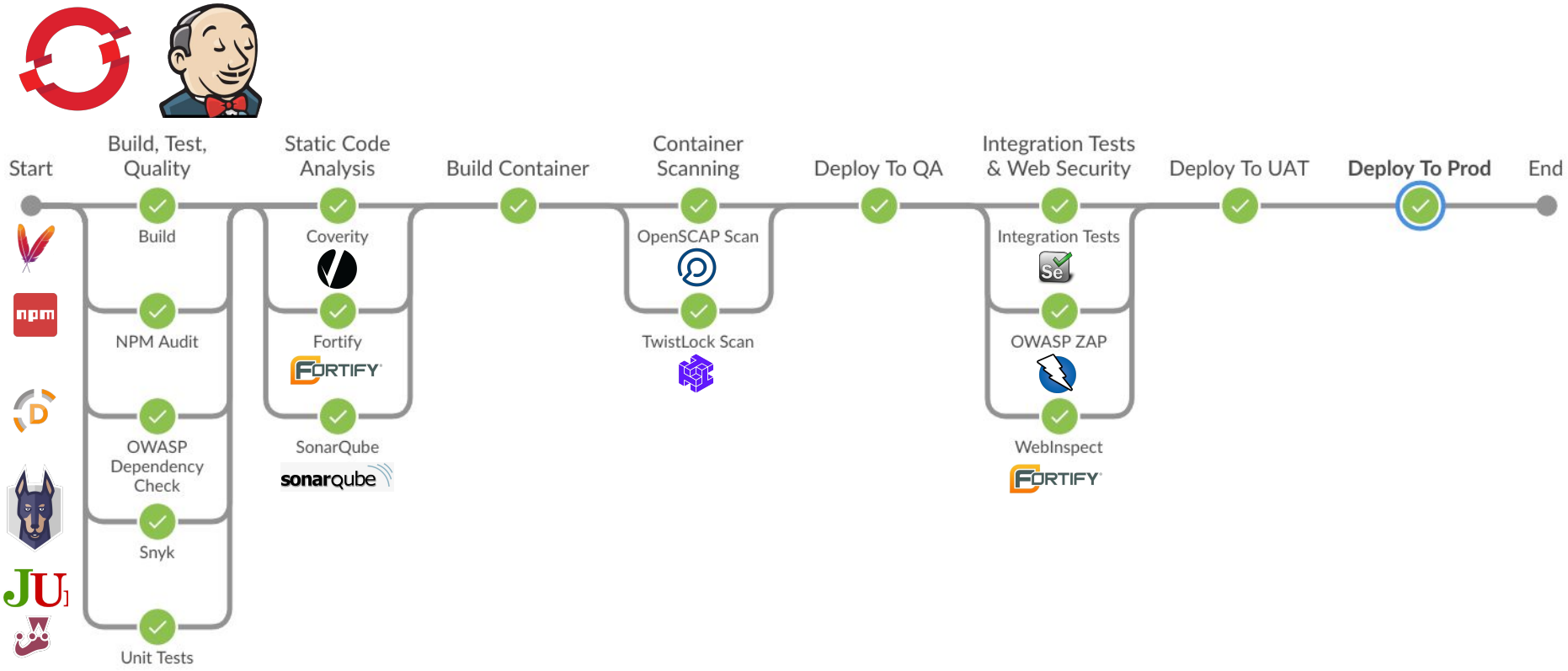
Red Hat

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

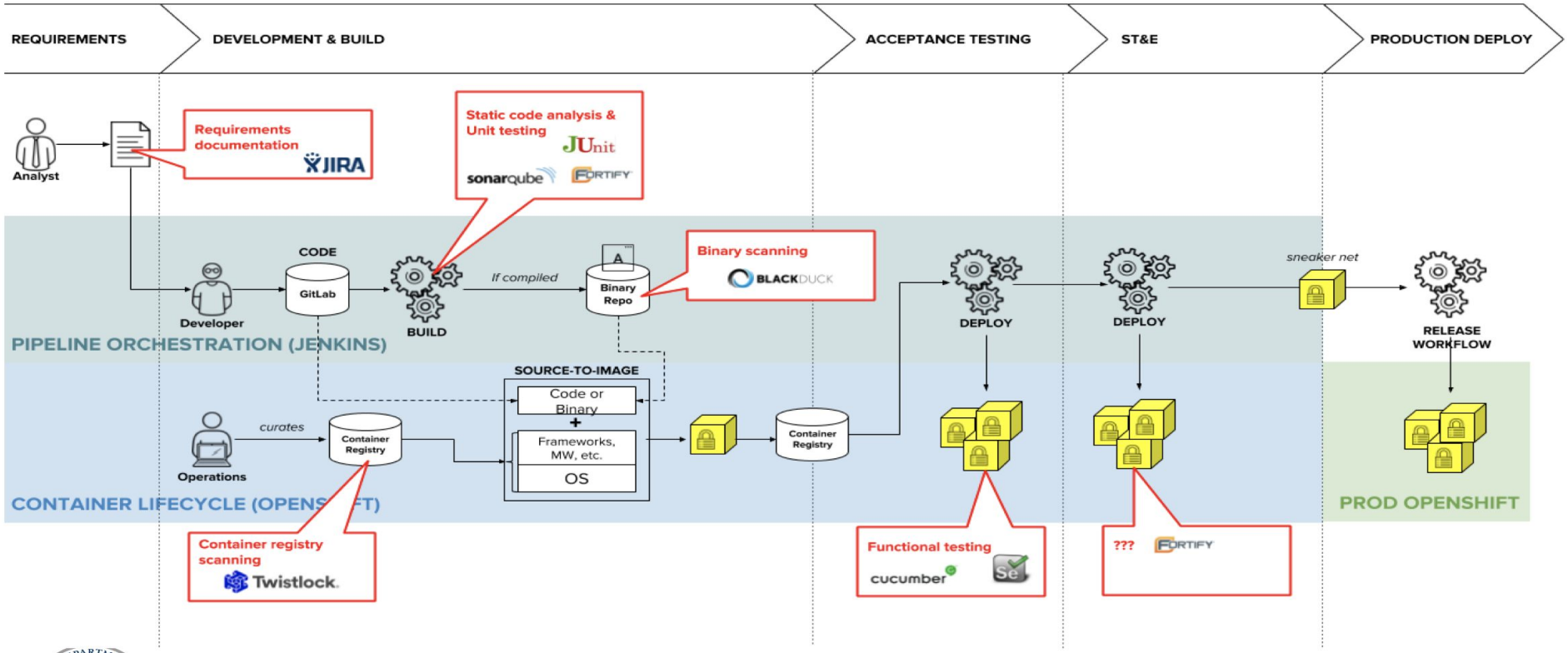
- Quote from DHS: “Successful adoption of DevSecOps Best Practices through Red Hat Labs Residency”



Security Enabled Pipeline at DHS



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

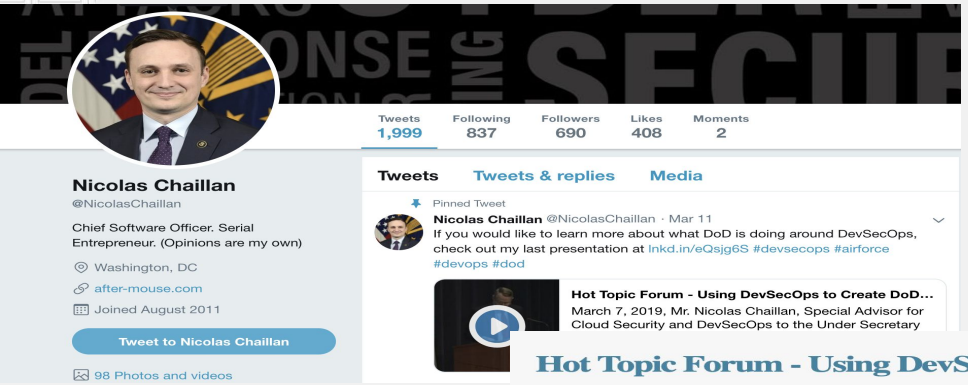


Evaluation of DevSecOps tools

- 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.

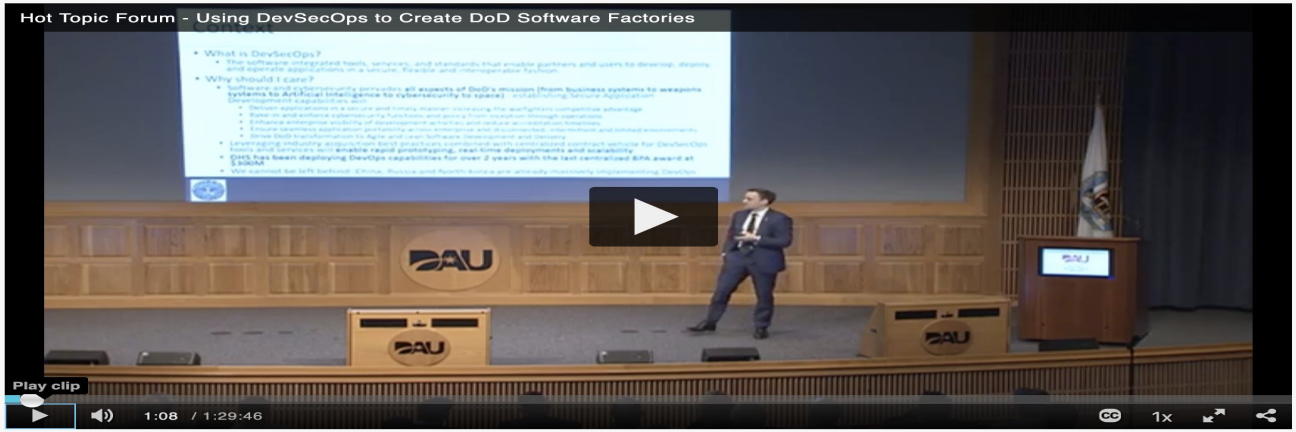
DevSecOps at the US Department of Defense

https://twitter.com/nicolaschaillan



Hot Topic Forum - Using DevSecOps to Create DoD Software Factories

March 7, 2019, Mr. Nicolas Chaillan, Special Advisor for Cloud Security a and Sustainment, presented his vision for how to transform DoD software acquisition into secure, responsive software facto warfighter needs. As a result, DoD's ability to keep pace with our potential adversaries is falling behind. Mr. Chaillan tools to revolutionize the Department's ability to provide responsive, timely and secure software capabilities for our warfigh



Journey to DevSecOps Panel

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

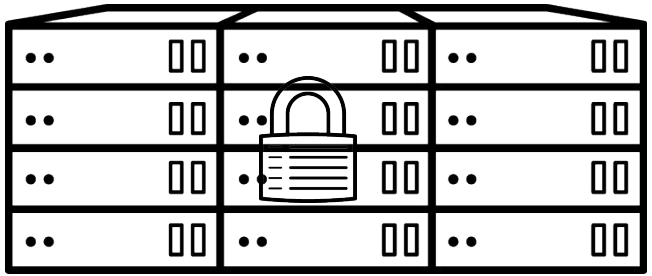
US Courts
US Citizen and Immigration Services
Oak Ridge National Laboratory
Internal Revenue Service

US Government Panel, Openshift Commons Briefing

Journey of DevSecOps - US Department Homeland Security

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

Automated Security and Compliance with Red Hat



Infrastructure and Operations

Red Hat

2019 Red Hat Summit Security Hands-On Labs

https://red.ht/securitylabs

(Everything you are about to see in the slides in this section has been implemented in the 'Proactive Security' lab that my teammates and I created. See the link above for more details.)

Red Hat

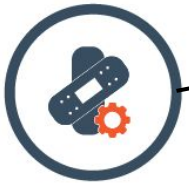
Automated Security and Compliance for Infrastructure & Operations

Infrastructure and Application Hardening Improvements with Automation

Vulnerability +Compliance Scanning on Hosts

Host Hardening

Enforcing Automated Compliance with Security Policies



Patch Automation

Automated Patching of Hosts

Automated hardening of hacked web application

Security at Scale with Predictive Analytics

AUTOMATION IS KEY

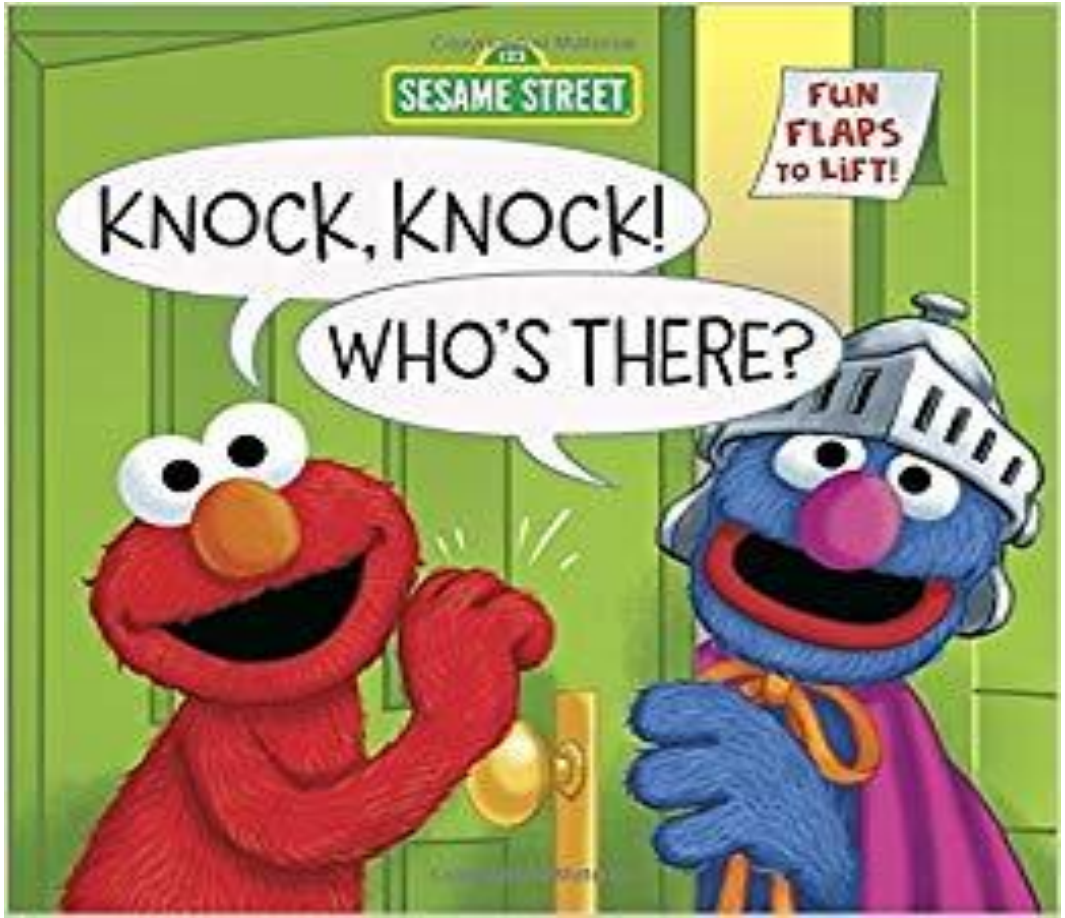
Introduce more automation in small incremental improvements to improve security & reduce risk wherever you are on the DevSecOps journey

Red Hat

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

Red Hat

A Related Knock Knock Joke



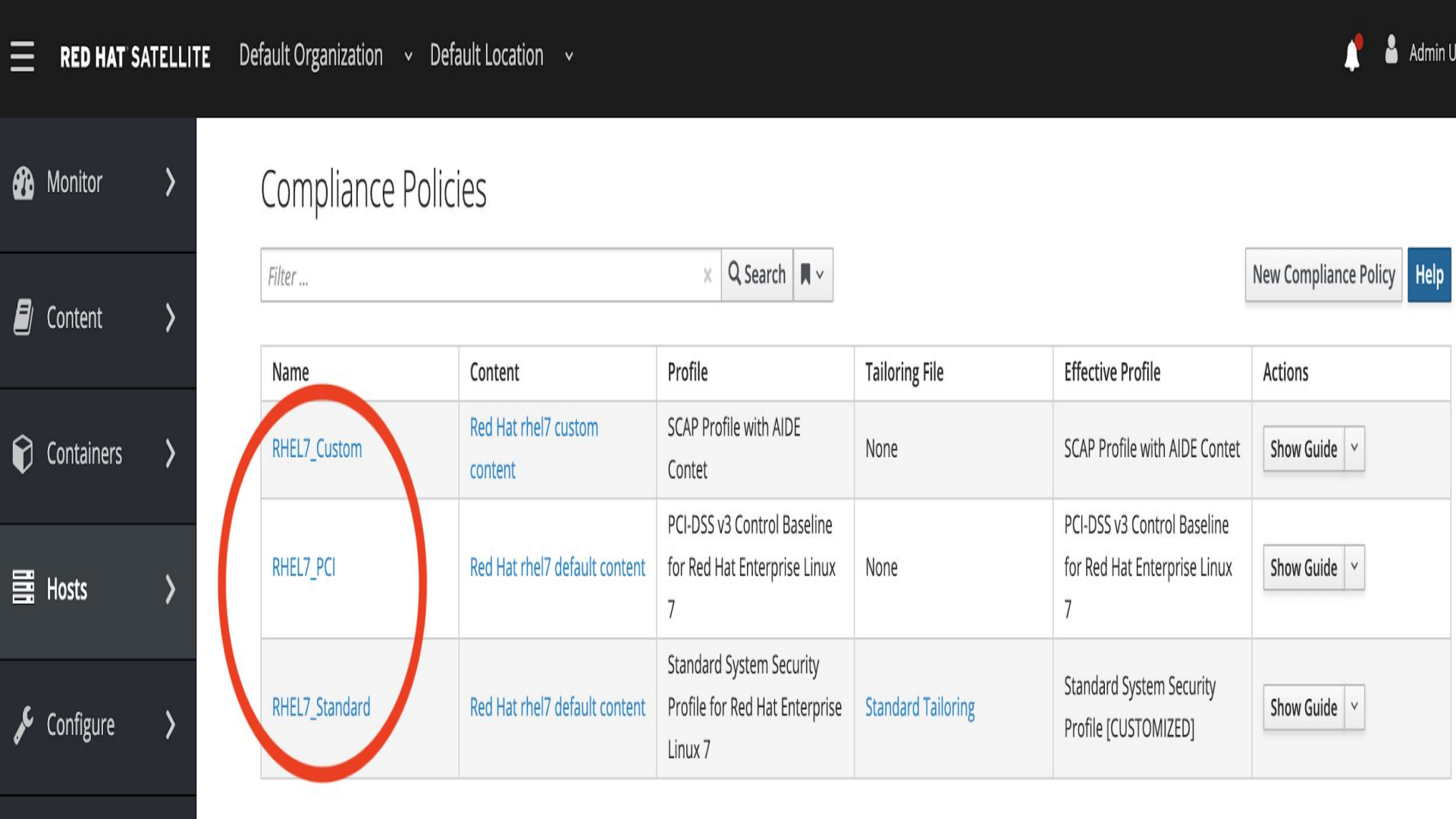
Red Hat

Knock Knock

Who's There?

Thank

Thank Who?


RED HAT SATELLITE
Default Organization
Default Location
Admin U
Monitor
Content
Containers
Hosts
Configure
Compliance Policies
Filter ...
Search
New Compliance Policy
Help
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

Compliance Policies

Filter ... | Search | New Compliance Policy | Help

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]	

Show Guide
- Edit
- Delete

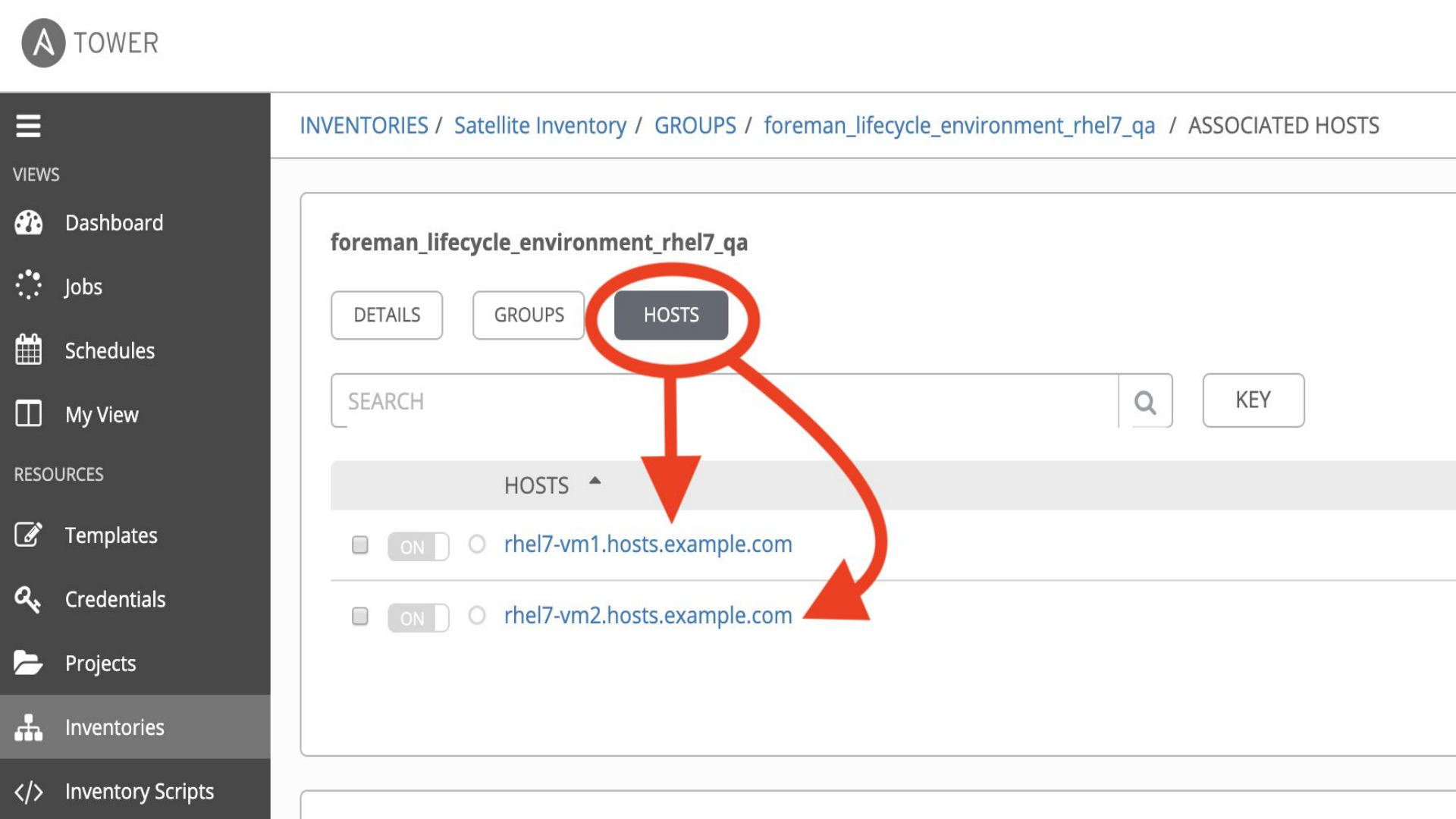
Policies » RHEL7_PCI

General | SCAP Content | Schedule | Locations | Organizations | Host Groups

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

Submit | Cancel


TOWER
VIEWS
Dashboard
Jobs
Schedules
My View
RESOURCES
Templates
Credentials
Projects
Inventories
Inventory Scripts
INVENTORIES / Satellite Inventory / GROUPS / foreman_lifecycle_environment_rhel7_qa / ASSOCIATED HOSTS
foreman_lifecycle_environment_rhel7_qa
DETAILS
GROUPS
HOSTS
SEARCH
KEY
HOSTS
ON
rhel7-vm1.hosts.example.com
ON
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

SURVEY PREVIEW

HOSTS

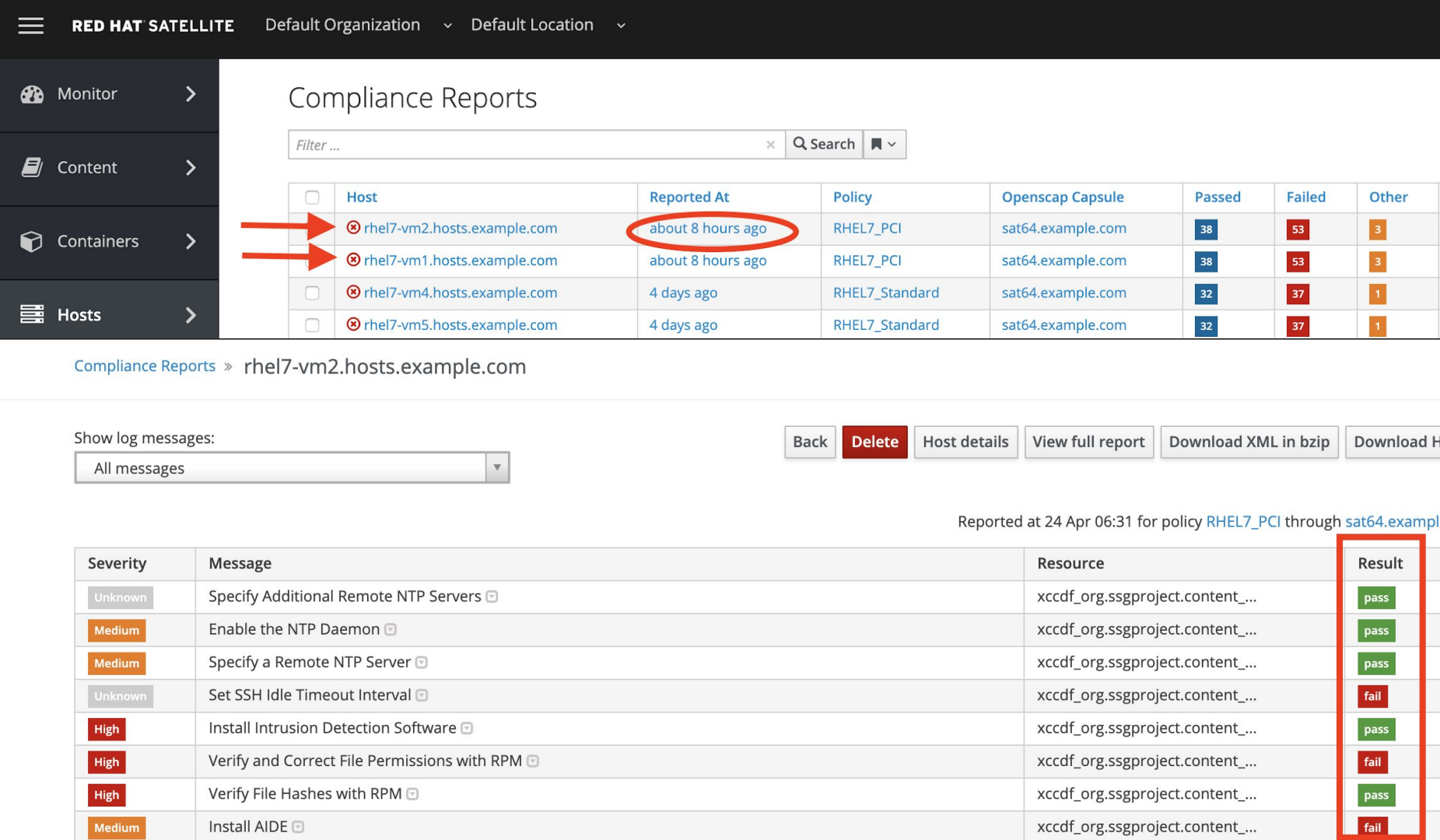
enter host pattern matching group and name from inventory

foreman_lifecycle_environment_rhel7_qa

* CHOOSE PROFILE

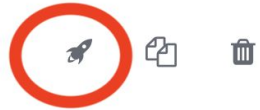
× RHEL7_PCI

CANCEL NEXT


RED HAT SATELLITE
Default Organization
Default Location
Monitor
Content
Containers
Hosts
Compliance Reports
Filter ...
Search
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
Compliance Reports » rhel7-vm2.hosts.example.com
Show log messages:
All messages
Back
Delete
Host details
View full report
Download XML in bzip
Download HTML
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 Job Template

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

SURVEY PREVIEW

* WHICH HOSTS?

foreman_lifecycle_environment_rhel7_qa

CANCEL NEXT

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

8 Roles

Login to Follow | View on GitHub

Name | Filter by Name... | Name | ↓a

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	

RedHatOffici...

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

Login to Follow | Issue Tracker | GitHub Repo

build passing

Details | Read Me

Info

Minimum Ansible Version	2.5
Installation	`$ ansible-galaxy install redhatofficial.rhel7_pci_dss`
Last Commit	10 days ago
Last Import	5 days ago
Tags	compliance, complianceascode, hardening, openscap, pcidss, redhat, redhatofficial, scap, security, ssg, system

Content Score

Quality Score 5 / 5

Last scored 5 days ago. Show Details

Community Score No Surveys 0 / 5

Based on 0 surveys. Show Details

Tell us about this collection

Quality of docs? - +

Ease of use? - +

Does what it promises? Y N

Works without change? Y N

Used in production? Y N

Compliance Reports

Filter ... | Search

Delete re

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

Red Hat

"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 "

Red Hat

RHEL7_Standard

Publish New Version | Select Action

Content Views » RHEL7_Standard » Versions

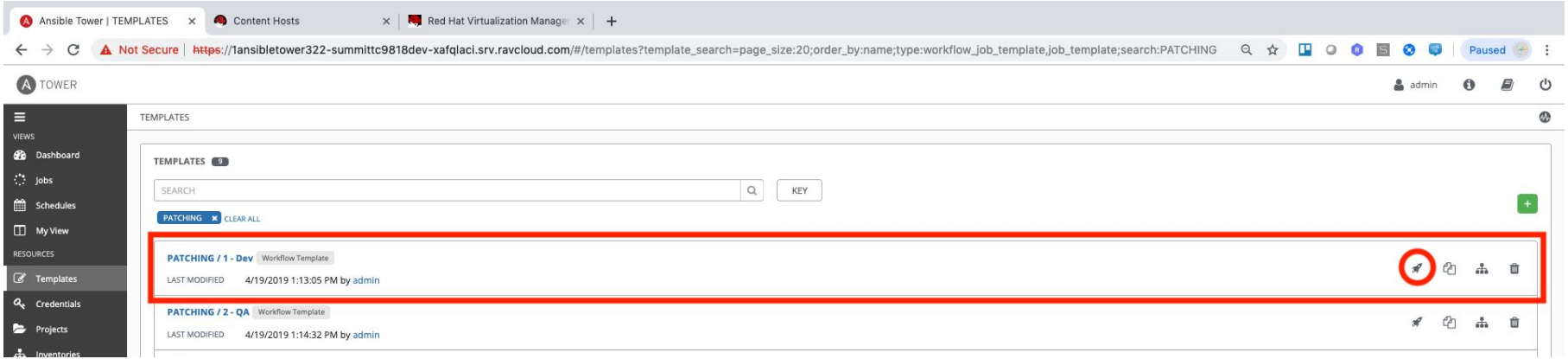
Details | Versions | Yum Content | File Repositories | Puppet Modules | Container Images | OSTree Content | History | Tasks

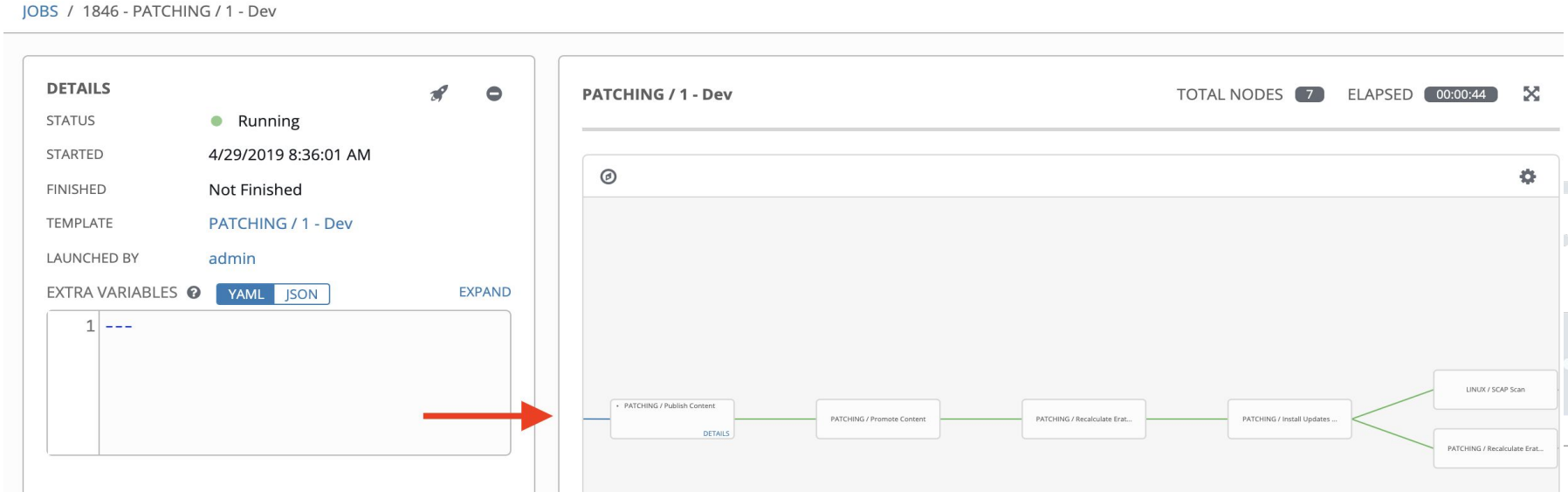
Filter... Search

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

20 per page

Showing 1 - 1 of 1 « ‹ 1 of 1 › »


Ansible Tower | TEMPLATES
Content Hosts
Red Hat Virtualization Manage
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
TEMPLATES
TEMPLATES 9
SEARCH
KEY
PATCHING
CLEAR ALL
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
YAML
JSON
EXPAND
1 ---
PATCHING / 1 - Dev
TOTAL NODES 7
ELAPSED 00:00:44
PATCHING / Publish Content
DETAILS
PATCHING / Promote Content
PATCHING / Recalculate Erat...
PATCHING / Install Updates ...
LINUX / SCAP Scan
PATCHING / Recalculate Erat...

RHEL7_Standard

Content Views » RHEL7_Standard » Versions

Details | Versions | Yum Content | File Repositories | Puppet Modules | Container Images

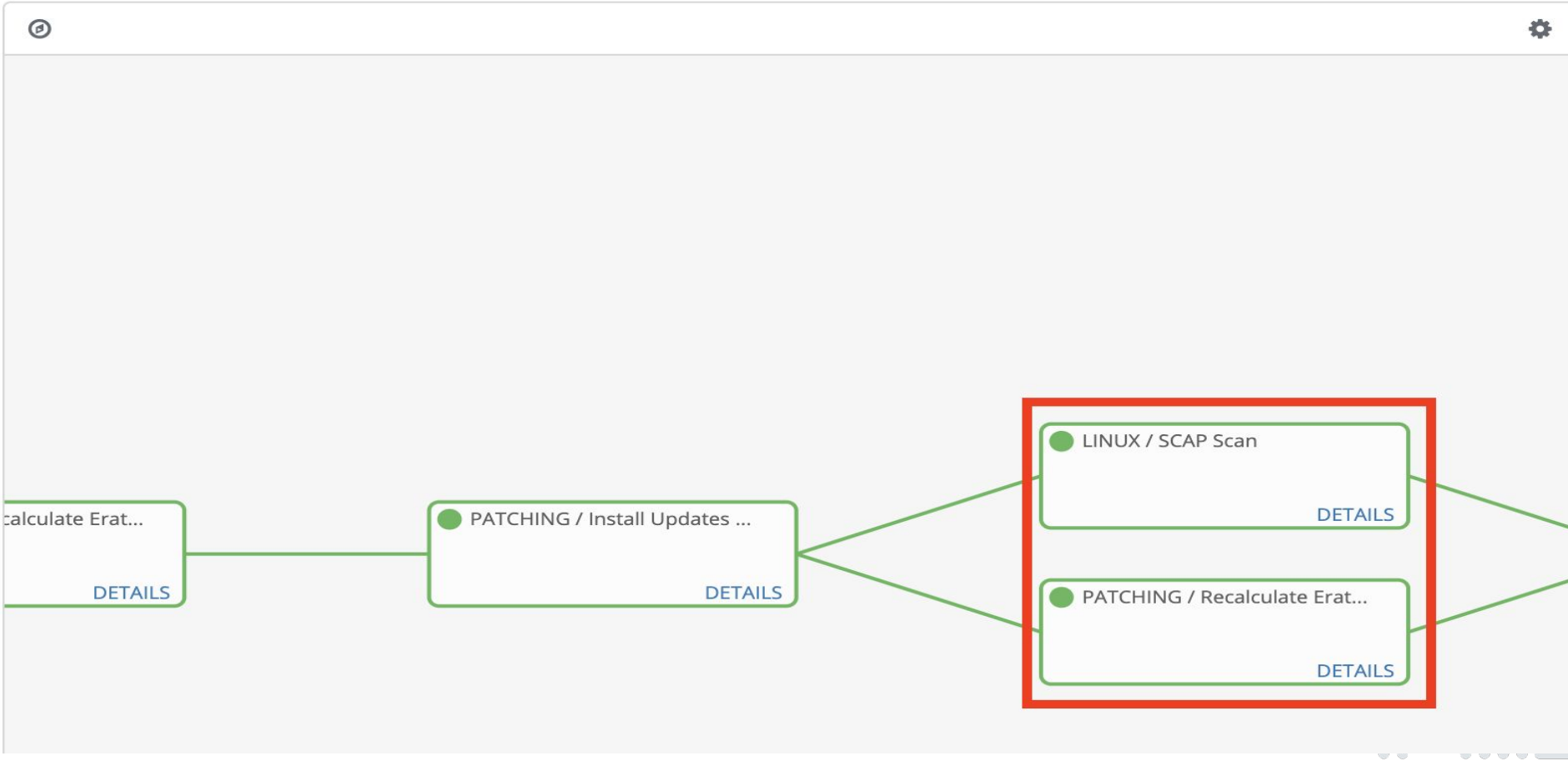
Filter... Search

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

20 per page

PATCHING / 1 - Dev

TOTAL NODES 7 ELAPSED 00:14:03



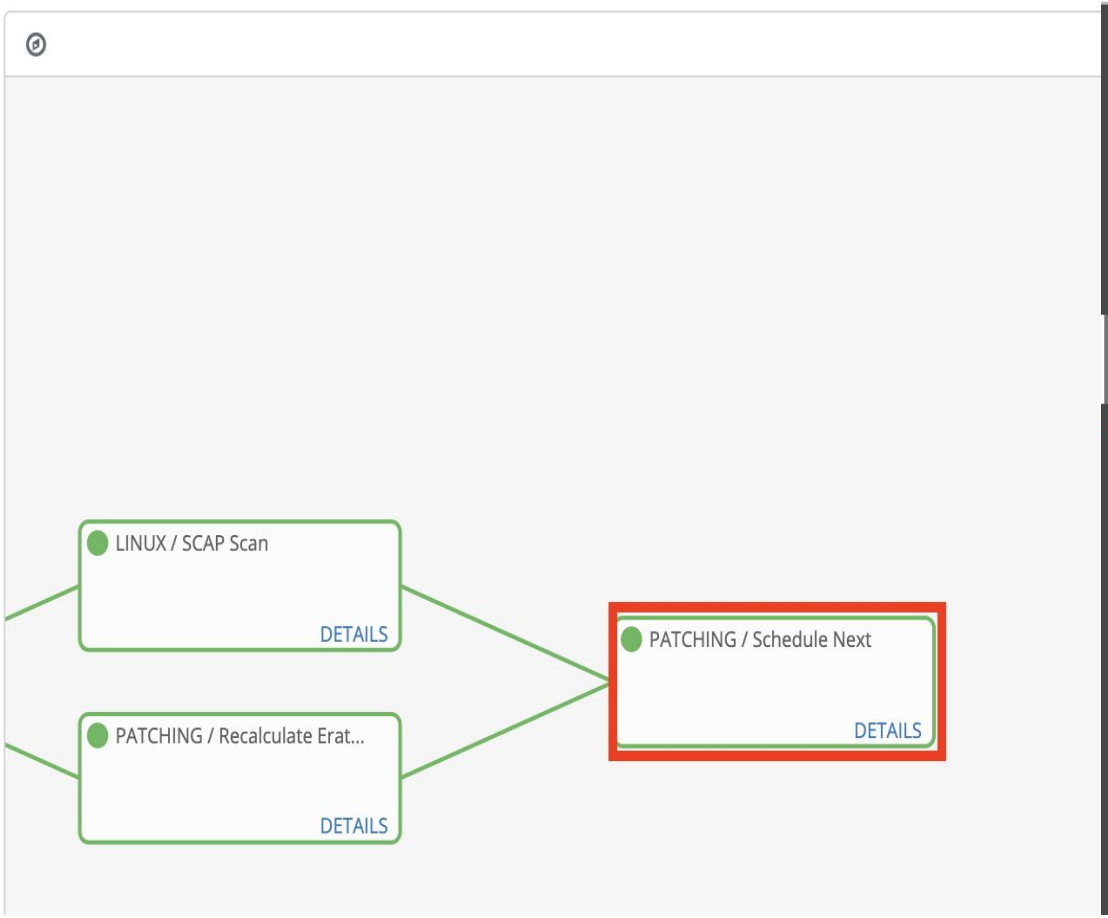
Compliance Reports

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

PATCHING / 1 - Dev

TOTAL NODES 7



TOWER

VIEWS

Dashboard

Jobs

Schedules

My View

RESOURCES

Templates

Credentials

Projects

Inventories

SCHEDULES

SCHEDULED JOBS 4

SEARCH

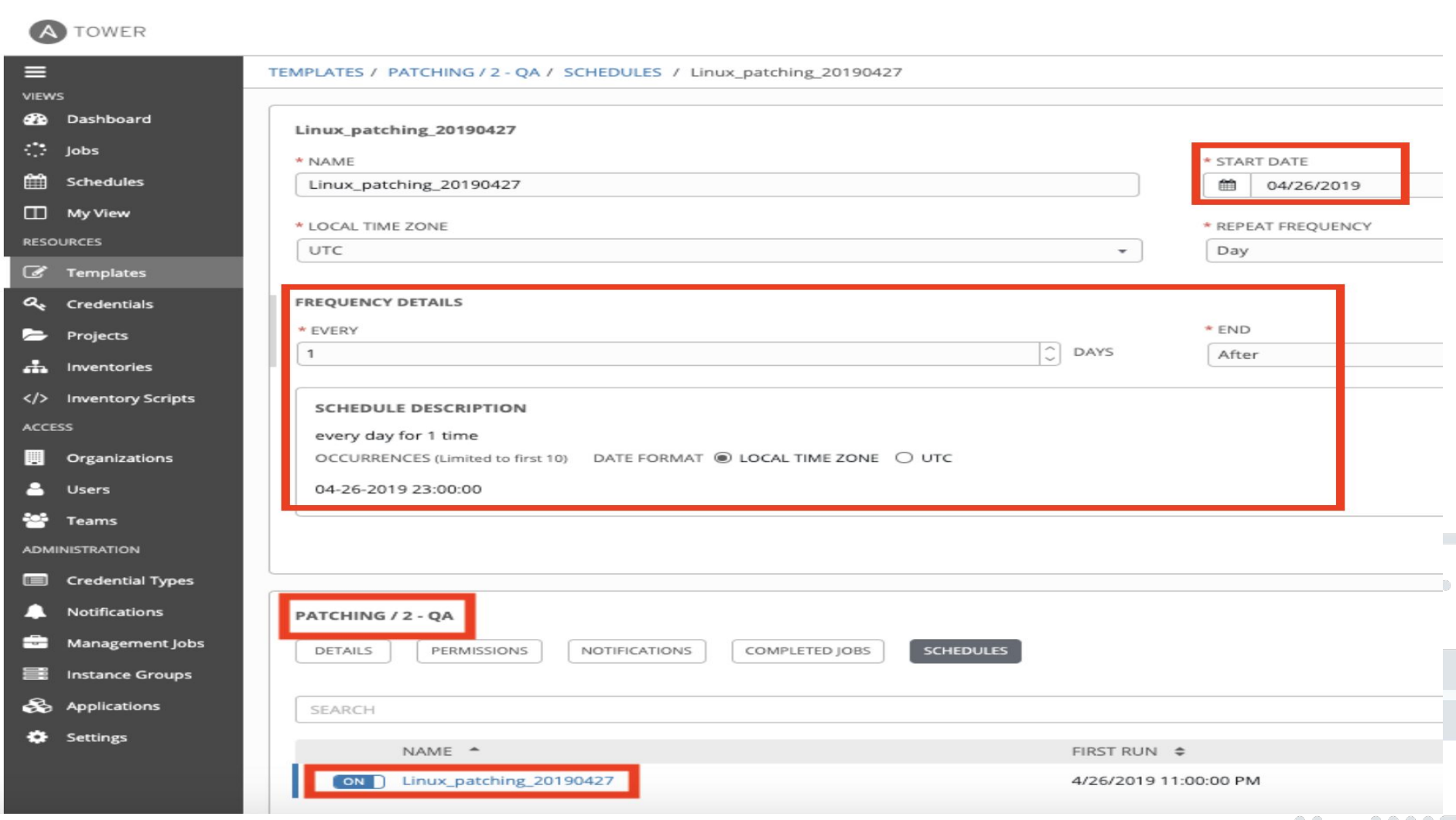
NAME

ON Cleanup Job Schedule

ON Cleanup Activity Schedule

ON Nightly Clean All Jobs

ON Linux_patching_20190506


TOWER
VIEWS
Dashboard
Jobs
Schedules
My View
RESOURCES
Templates
Credentials
Projects
Inventories
Inventory Scripts
ACCESS
Organizations
Users
Teams
ADMINISTRATION
Credential Types
Notifications
Management Jobs
Instance Groups
Applications
Settings
TEMPLATES / PATCHING / 2 - QA / SCHEDULES / Linux_patching_20190427
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
DETAILS
PERMISSIONS
NOTIFICATIONS
COMPLETED JOBS
SCHEDULES
SEARCH
NAME
FIRST RUN
ON
Linux_patching_20190427
4/26/2019 11:00:00 PM

Proactive Security and Automated Risk Management at Scale with Predictive Analytics

Red Hat

RED HAT SATELLITE

Red Hat Access | Admin User

EXAMPLE.COM | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Red Hat Insights | Administer

Inventory

Page Filters

Find a system

Actions

9 Systems

	System Type	System Name	Last Check In	Status
	RHEL Server	ic1.example.com	20 hours ago	19 Actions
	RHEL Server	ic2.example.com	20 hours ago	19 Actions
	RHEL Server	ic3.example.com	20 hours ago	20 Actions
	RHEL Server	ic4.example.com	20 hours ago	21 Actions
	RHEL Server	ic5.example.com	20 hours ago	19 Actions
	RHEL Server	ic6.example.com	19 hours ago	20 Actions
	RHEL Server	ic7.example.com	19 hours ago	20 Actions
	RHEL Server	ic8.example.com	19 hours ago	6 Actions
	RHEL Server	ic9.example.com	19 hours ago	6 Actions

Inventory

▼ Page Filters ▼

Find a system

Actions ^

- Create a new Plan/Playbook
- Add to existing Plan/Playbook
- Group systems
- Unregister

2 Systems (2 Selected)

System Name	Last Check In	Status
ic1.summit.example.com	3 hours ago	19 Actions
ic4.summit.example.com	8 minutes ago	18 Actions

Plan / Playbook Builder

Create new plan GUID Insights Fix ALL

Add to existing plan Plan Name

Actions available for 2 selected systems

Action	Total Risk	Ansible	Affected Systems
Filter by rule name			
OpenSSH vulnerable to remote password guessing attack (CVE-2015-5600)			1
Remote code execution vulnerability in libresolv via crafted DNS response (CVE-2015-7547)			1
Dnsmasq vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)			1
Remote code execution vulnerability in NSS via crafted base64 data (CVE-2017-5461)			1
Kdump crashkernel reservation failed due to improper configuration of crashkernel parameter			1
Kernel key management subsystem vulnerable to local privilege escalation (CVE-2016-0728)			2
Kernel vulnerable to privilege escalation via permission bypass (CVE-2016-5195)			2
Kernel vulnerable to denial of service via Bluetooth stack (CVE-2017-1000251/Blueborne)			2
Kernel is vulnerable to memory corruption or local privilege escalation (CVE-2017-1000253)			2
Kernel and glibc vulnerable to local privilege escalation via stack and heap memory clash (CVE-2017-1000364 and CVE-2017-1000366)			2
sudo vulnerable to local privilege escalation via process TTY name parsing (CVE-2017-1000368) impact: Local Privilege Escalation			2
Kernel vulnerable to local privilege escalation via n_hdlc module (CVE-2017-2636)			2
Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre)			1
Virtualization and kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre)			1
Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5753/Spectre, CVE-2017-5715/Spectre, CVE-2017-5754/Meltdown)			2

Cancel Save

TOWER

admin

TEMPLATES / CREATE JOB TEMPLATE

VIEWS
- Dashboard
- Jobs
- Schedules
- My View

RESOURCES
- Templates
- Credentials
- Projects
- Inventories
- Inventory Scripts

ACCESS
- Organizations
- Users
- Teams

ADMINISTRATION
- Credential Types
- Notifications
- Management Jobs

NEW JOB TEMPLATE

DETAILS | PERMISSIONS | NOTIFICATIONS | COMPLETED JOBS | SCHEDULES | ADD SURVEY

* NAME: GUID Insights Fix ALL

DESCRIPTION:

* JOB TYPE: Run (PROMPT ON LAUNCH)

* INVENTORY: Insights Inventory (PROMPT ON LAUNCH)

* PROJECT: Insights Planner Sync

* PLAYBOOK: Insights Fix All-41778.yml

CREDENTIAL: Insights Fix All Machine Credentials (PROMPT ON LAUNCH)

FORKS: DEFAULT

LIMIT: (PROMPT ON LAUNCH)

* VERBOSITY: 0 (Normal) (PROMPT ON LAUNCH)

JOB TAGS: (PROMPT ON LAUNCH)

SKIP TAGS: (PROMPT ON LAUNCH)

LABELS:

ANSIBLE ENVIRONMENT: Use Default Environment

INSTANCE GROUPS:

JOB SLICING: 1

SHOW CHANGES: OFF (PROMPT ON LAUNCH)

OPTIONS
- [x] Enable Privilege Escalation
- [ ] Allow Provisioning Callbacks
- [ ] Enable Concurrent Jobs
- [ ] Use Fact Cache

EXTRA VARIABLES: YAML | JSON (PROMPT ON LAUNCH)

```
1 ---
```

GUID Insights Fix ALL Job Template

INVENTORY Insights Inventory

PROJECT Insights Planner Sync

CREDENTIALS Insights Fix All Machine Credentials

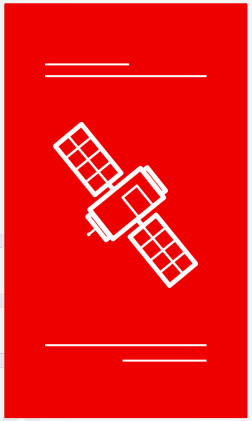
LAST MODIFIED 4/24/2019 6:08:47 PM by admin

Red Hat Insights Rules for Red Hat OpenShift Container Platform

- Communication fails between components when certificates have expired in Openshift
- Image build failure when creating a large number of concurrent builds
- Containers allow non-privileged user to modify filesystem inside containers when created with cri-o
- Docker registry pod restarts occasionally when liveness and readiness probes collide
- Failed api connection between docker and OpenShift when version of docker and openshift are incompatible
- Insufficient space available when image garbage collection fails to run in OpenShift
- GlusterFS storage disconnects from pods when restarting atomic-openshift-node server
- Master controller fails to start when changes are made to the SDN plugin if there are headless services in the cluster
- Failure to connect to service when configured IP is in use by another service
- Pod creation fails when is under high load due to iptables-restore process
- Excessive load time for new routes when a large number of routes exist
- Router does not work when deleting route with host set to "localhost"

Red Hat Smart Management

Red Hat Satellite

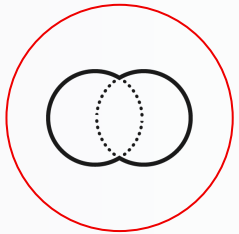


+

Cloud management services for Red Hat Enterprise Linux

Vulnerability

Compliance



System comparison

Red Hat

Red Hat

John Spinks

Manage my Red Hat infrastructure

https://cloud.redhat.com

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

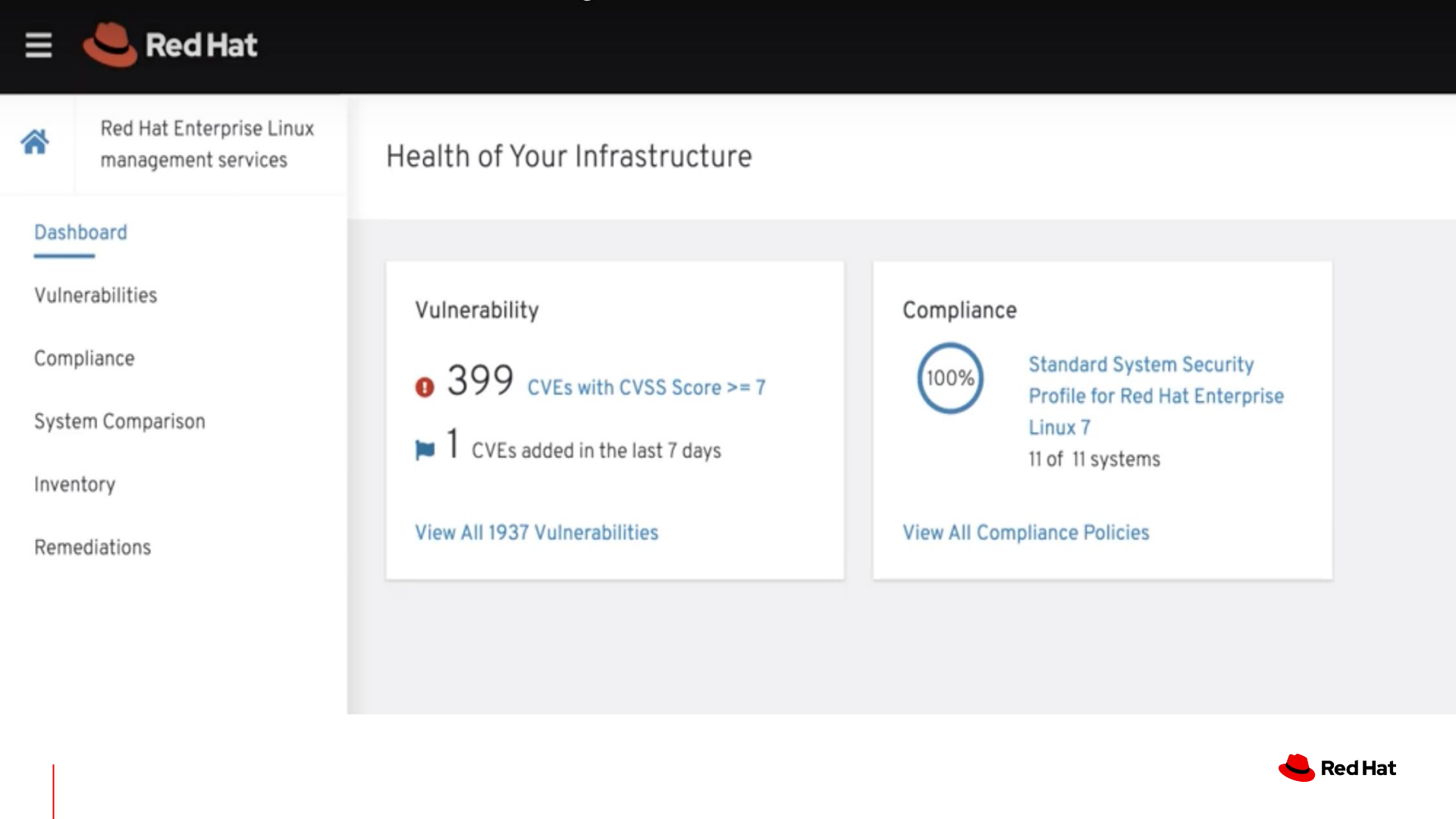
Red Hat OpenShift

Feedback

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

Red Hat

Privacy Policy | Terms of Use | All Policies and Guidelines

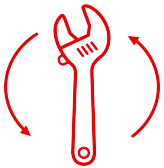

Red Hat
Red Hat Enterprise Linux management services
Health of Your Infrastructure
Dashboard
Vulnerabilities
Compliance
System Comparison
Inventory
Remediations
Vulnerability
399 CVEs with CVSS Score >= 7
1 CVEs added in the last 7 days
View All 1937 Vulnerabilities
Compliance
100%
Standard System Security Profile for Red Hat Enterprise Linux 7
11 of 11 systems
View All Compliance Policies
Red Hat

Vulnerability

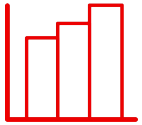
Remediate all Common Vulnerabilities and Exposures (CVEs) with errata

Vulnerability offers

Assess and monitor the risk of vulnerabilities that impact Red Hat products with operational ease



Remediate known Common Vulnerabilities and Exposures (CVEs)



Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

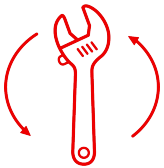
Red Hat

Compliance

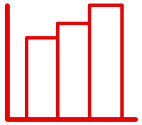
Built on OpenSCAP reporting

Compliance offers

Assess and monitor the degree/level of compliance to a policy for Red Hat products with operational ease



Remediate known issues of non-compliance in the Red Hat environment via Ansible playbooks based on business risk & relevance



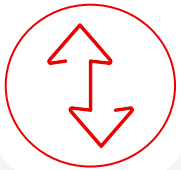
Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

Red Hat

System Comparison

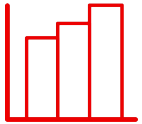
Compare system profiles

System Comparison offers



Compare system configuration of one host to other hosts

Filter displayed profile facts, highlighting areas that match, are different, or where information is missing.



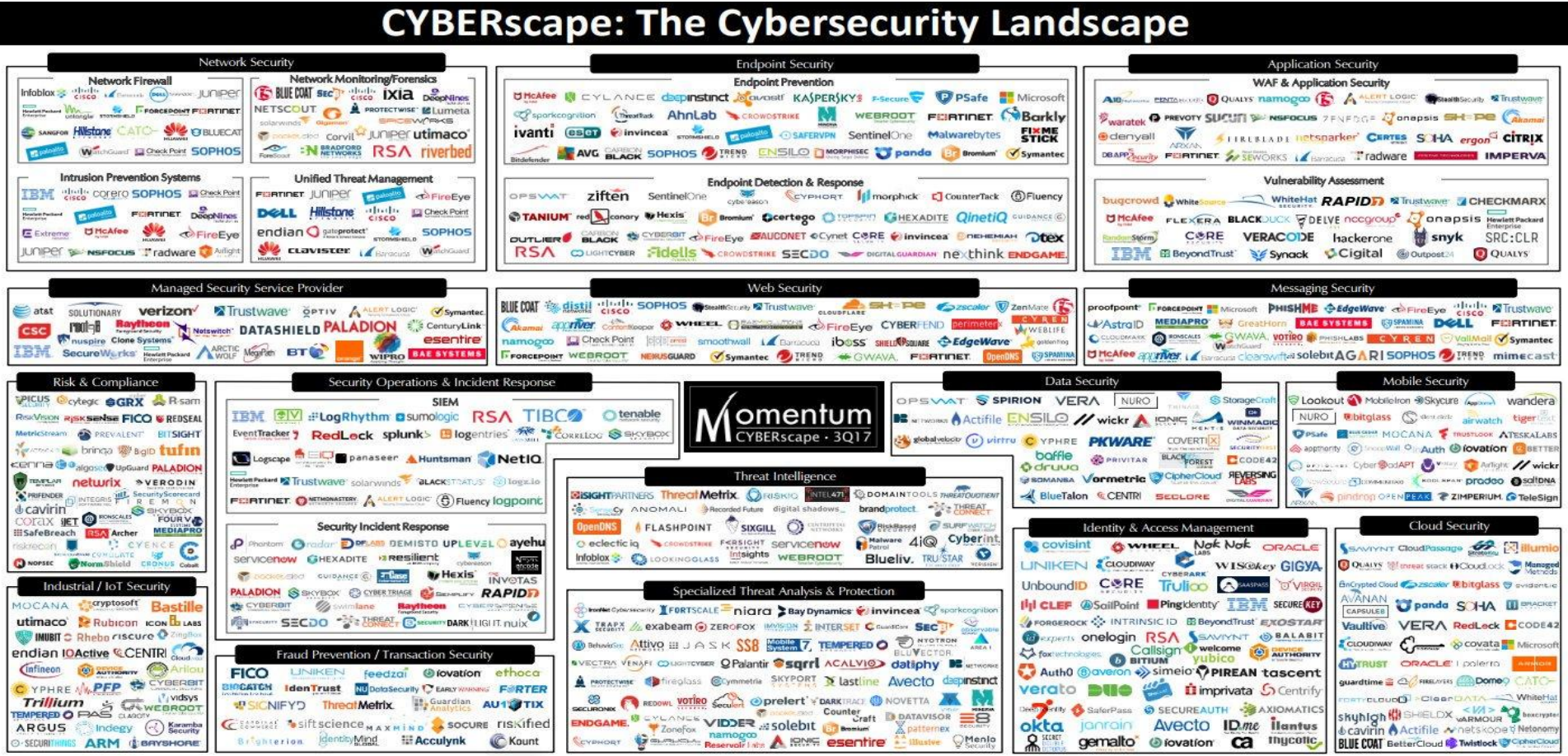
Ability to generate CSV view-based output

Red Hat

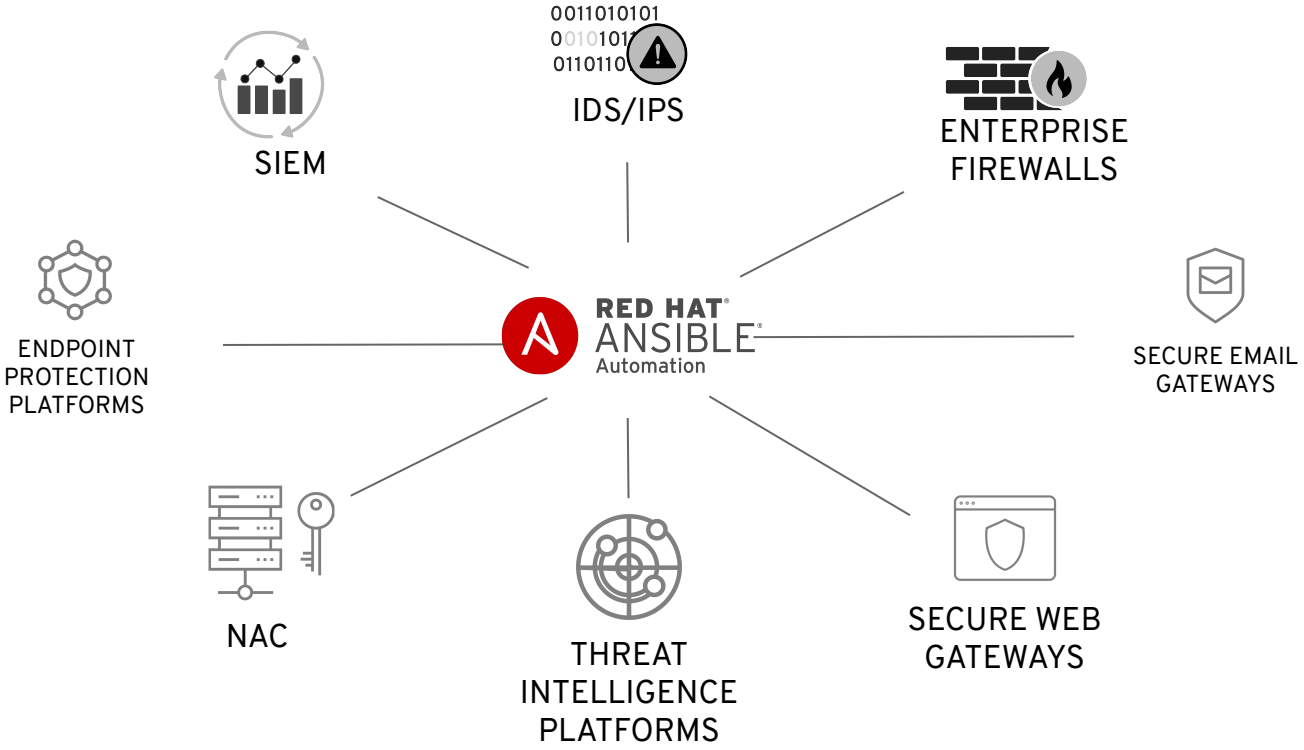
Automated Security and Compliance with Red Hat

Security Operations Center
(SOC)

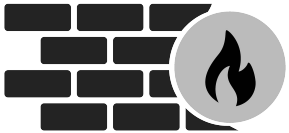
Welcome to the Vast World of Cybersecurity Tools



Source: Momentum Partners


0011010101
SIEM
IDS/IPS
ENTERPRISE FIREWALLS
ENDPOINT PROTECTION PLATFORMS
RED HAT
ANSIBLE
Automation
SECURE EMAIL GATEWAYS
NAC
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS

Who Are We Working With?



Enterprise Firewalls

Check Point
SOFTWARE TECHNOLOGIES LTD

paloalto NETWORKS

Intrusion Detection & Prevention Systems

SNORT®

CISCO

Security Information & Events Management

splunk>

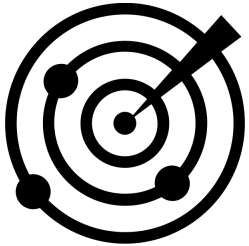
IBM

Red Hat

What Does It Do?

Triage Of Suspicious Activities

Enabling programmatic access to log configurations such as destination, verbosity, etc.



Threat Hunting

Automating alerts, correlation searches and signature manipulation

Incident Response

Creating new security policies to whitelist, blacklist or quarantine a machine

https://galaxy.ansible.com/ansible_security

Apps | Red Hat External | Red Hat Presentat... | Red Hat Support | IT New Hire Hub | I.T. Toolbox

GALAXY

- Home
- Search
- Community

Community Authors > ansible_security

ansible_security

ansible-security

Red Hat

https://github.com/ansible-security

The Ansible integrations with 3rd party security tools can be found here

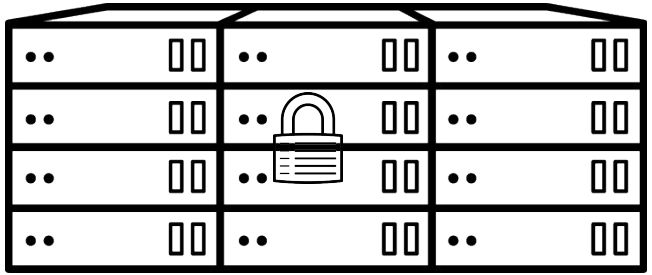
Name | Filter by Name... | Name

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

Automated Security and Compliance with Red Hat

Applications



Infrastructure and Operations

Security Operations Center (SOC)

Takeaways

- Identify your **risk tolerance**. There's no such thing as 100% security.
- Security is **everyone's** job. Take a **holistic, continuous, defense-in-depth** approach to security.
- **Prevention, Detection, Response**. Implement security hygiene practices (regular patches, etc).
- Have a method of inventorying the scope of open-source usage
- Leverage the security technologies that **you already have** (in the OS, Automation tools, etc)
- Identify **focus areas for automation to improve security , take baby steps**
- Learn from **examples (both successes + failures(breaches)**
- 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)

Red Hat

Red Hat Training 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)
5. RH413: Red Hat Security and Server Hardening (with exam)

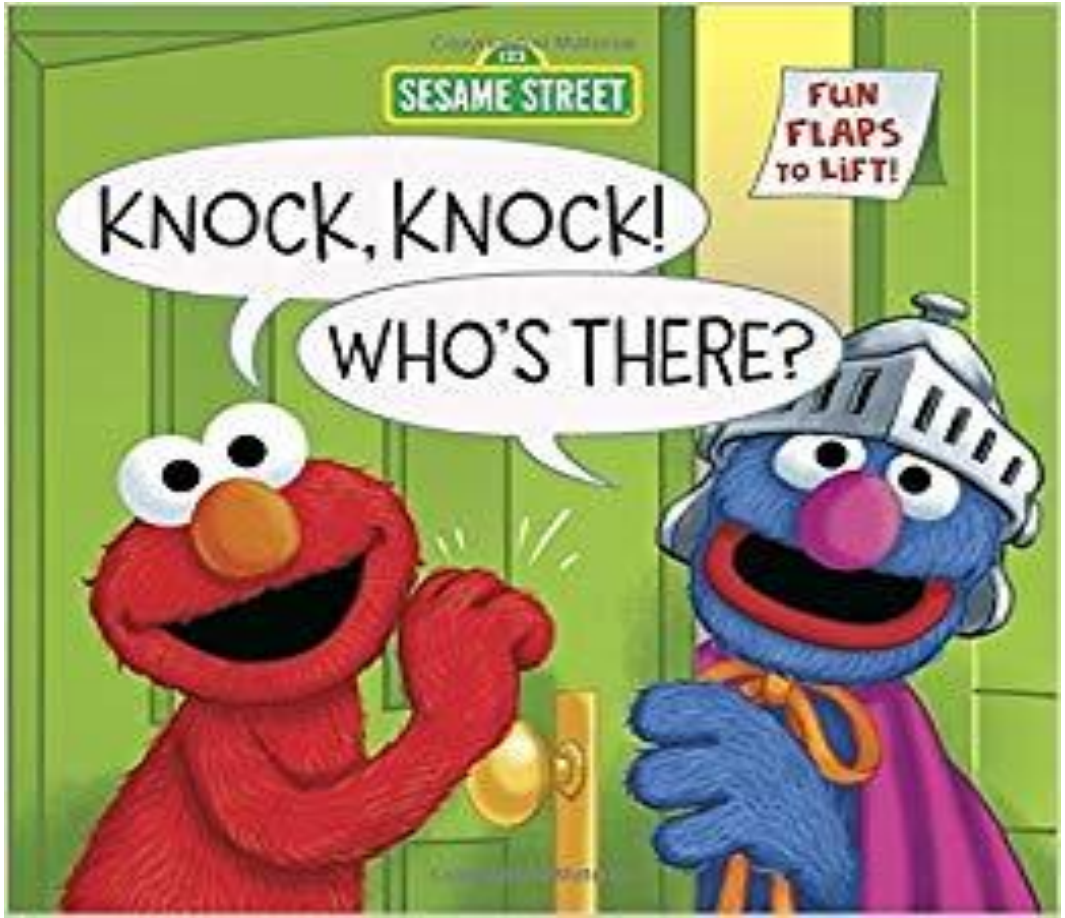
Red Hat Security Related Links

- 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 Our Last Knock Knock Joke



Red Hat

Knock Knock

Who’s There?

Police

Police Who?

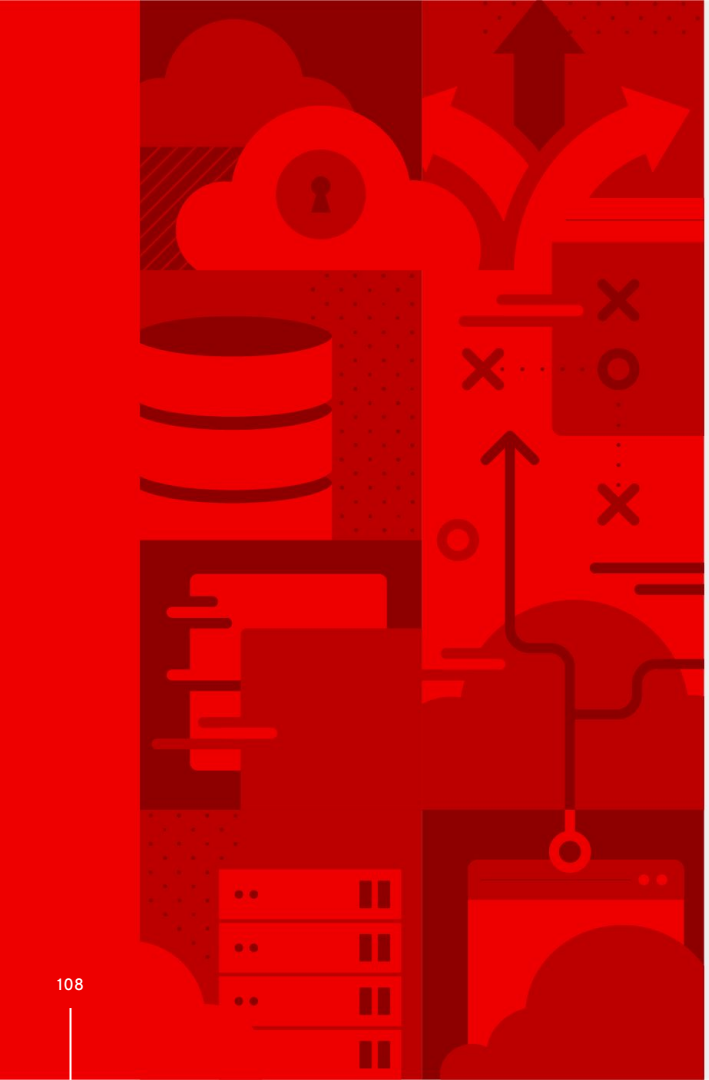
Next Steps

- Speak with a Red Hat expert here at Security Symposium
- Look for the slides in a “Thank You” email from us in the next few days
- Stay up to date with Red Hat at redhat.com/security
- Visit redhat.com/events to find out about workshops and other events like this one coming to your area

Thank you for coming.

Feedback or questions?

infrastructure@redhat.com



Questions?

lkerner@redhat.com

Red Hat

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.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat

Thank you to our partner