S103174 - Automating security compliance for physical, virtual, cloud, and container environments

Using Red Hat CloudForms, Red Hat Satellite, Red Hat Insights and Ansible Tower by Red Hat

Lucy Huh Kerner
Principal Technical Marketing Manager - Security, Red Hat
May 4, 2017

Why automate security compliance?

“81% of hacking-related breaches leveraged either stolen and/or weak passwords.”

2017 Verizon Data Breach Investigations Report
[http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017]

Let’s manually ensure security compliance …..

- 3 ring binder of security checks and fixes that have to be done
- Very time consuming
- Highly prone to human error
- Tedious and boring
- Non-repudiable
- Not easy to do audits
- Not repeatable or sharable

Instead, what you want is ...

- Centralized management of your ***entire*** heterogeneous infrastructure
  - You can't control what you don't know about
- Automation, Automation, Automation
- Infrastructure and Security as code
  - Repeatable, sharable, verifiable, easier to do compliance audits
- Hardened, Security compliant host at provisioning time
  - Immutable Operating System: OS can't be changed by untrusted parties
- Automated monitoring and fixing of all systems for entire lifecycle
- Proactive vs Reactive security

What tools can I use to help me with all this ?

Let’s start with SCAP. But, what is SCAP ?

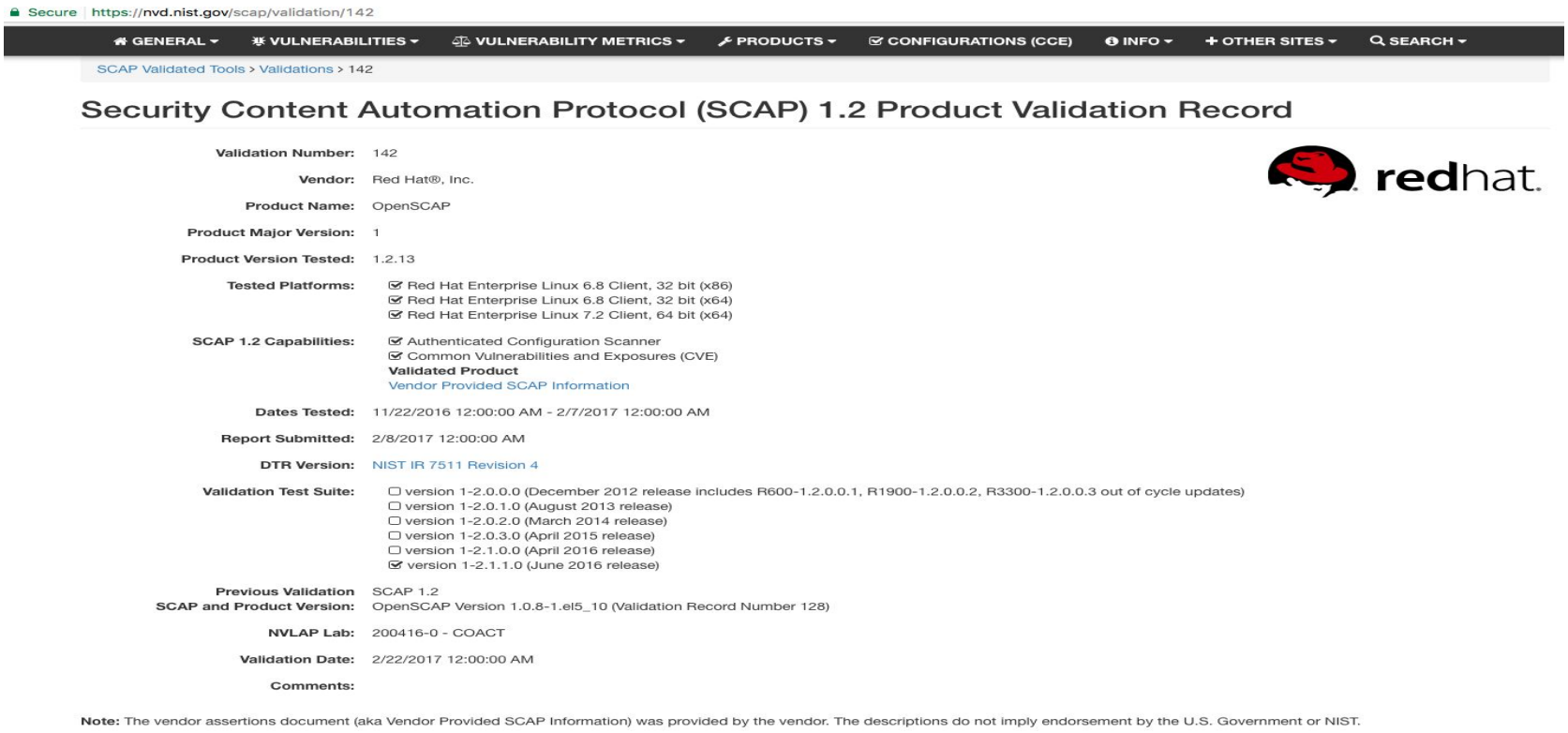
- Security Content Automation Protocol
- Managed by National Institute of Standards and Technology (NIST)
- Standardized way of maintaining security of systems
  - Vulnerability and configuration security baselines

Configuration and Vulnerability Scanner

WHAT IS OpenSCAP?

Ships FREE with RHEL and Satellite !!!

NIST **validated** and **certified** SCAP scanner by Red Hat



PRESS RELEASE

Red Hat Adds New NIST Certification for OpenSCAP, Expands Footprint for Open IT Security Standards

Community-driven security compliance scanner certified for mission-critical deployments on Red Hat Enterprise Linux 6 and 7 by National Institute of Standards and Technology

IN SHORT

OpenSCAP adds new NIST certification for Red Hat Enterprise Linux 6 and 7

MENTIONED IN THIS ARTICLE

Red Hat, OpenSCAP, Red Hat Enterprise Linux, COACT

FOR MORE INFORMATION

Read more about the new OpenSCAP certification from NIST

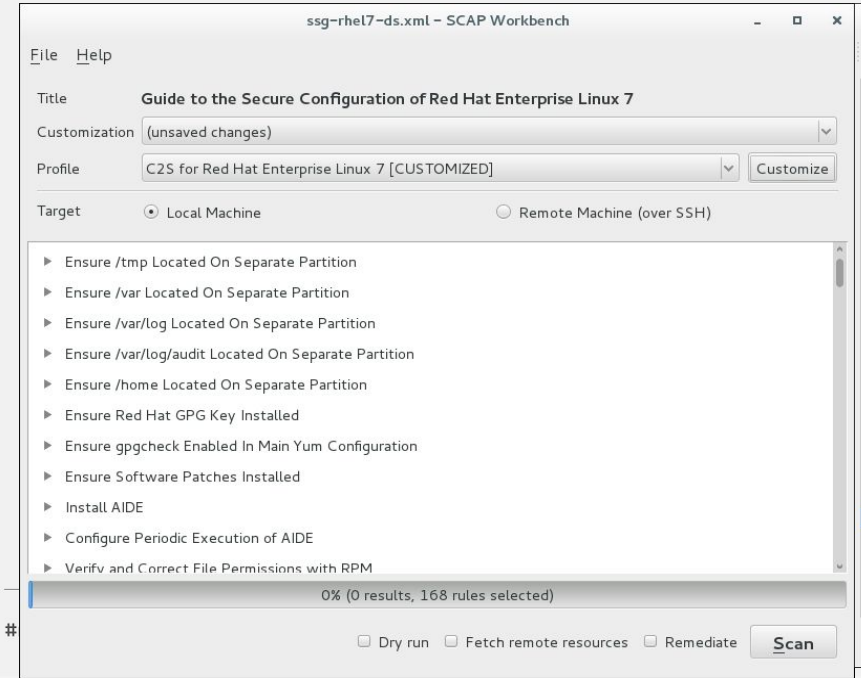
Learn more about OpenSCAP and SCAP Security Guide content

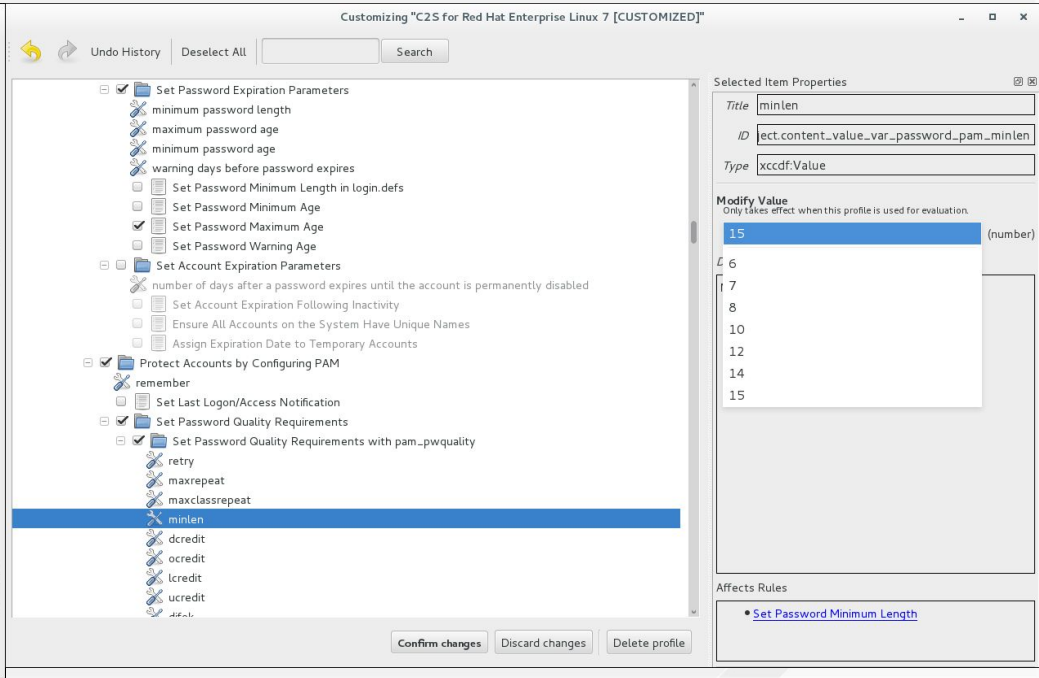
RALEIGH, N.C. — March 17, 2017 — Red Hat, Inc. (NYSE: RHT), the world's leading provider of open source solutions, today announced that OpenSCAP 1.2, an open source Security Content Automation Protocol (SCAP) scanner, has been certified by the National Institute of Standards and Technology as a U.S. government evaluated configuration and vulnerability scanner for Red Hat Enterprise Linux 6 and 7-based systems. This certification shows that OpenSCAP can analyze and evaluate security automation content correctly and has the functionality and documentation required by NIST to run in sensitive, security-conscious environments.

> *"NIST's new certification of OpenSCAP on the world's leading enterprise Linux platform provides a flexible, powerful SCAP scanner built on open standards, making it easier for agencies and other organizations to add verifiable, repeatable security scanning to their repertoires.*
>
> **DAVID EGTS,** CHIEF TECHNOLOGIST, PUBLIC SECTOR, RED HAT

SCAP Workbench

- GUI tool that serves as an SCAP scanner and provides tailoring functionality for SCAP content, but only scans a single machine





But… I don’t just have 1 machine …

- We have over 1000 linux hosts all living in different environments(VmWare vCenter, Microsoft Azure, etc). How do we scan, report on, and remediate all of these systems?
- How do we provide a customized self service portal for users to provision a security compliant host at provisioning time while still having tight control over our entire infrastructure?
- How do we do ongoing automated security compliance and remediation for our entire heterogeneous infrastructure?
- How do I ensure that all the 200+ container images in our environment and all future container images that will enter our environment are free of vulnerabilities in an automated fashion?

The secret is to use a combination of …..

+

RED HAT®
CLOUDFOR

ANSIBLE
TOWER
by Red Hat®

RED HAT®
SATELLI

RED HAT®
INSIGHTS

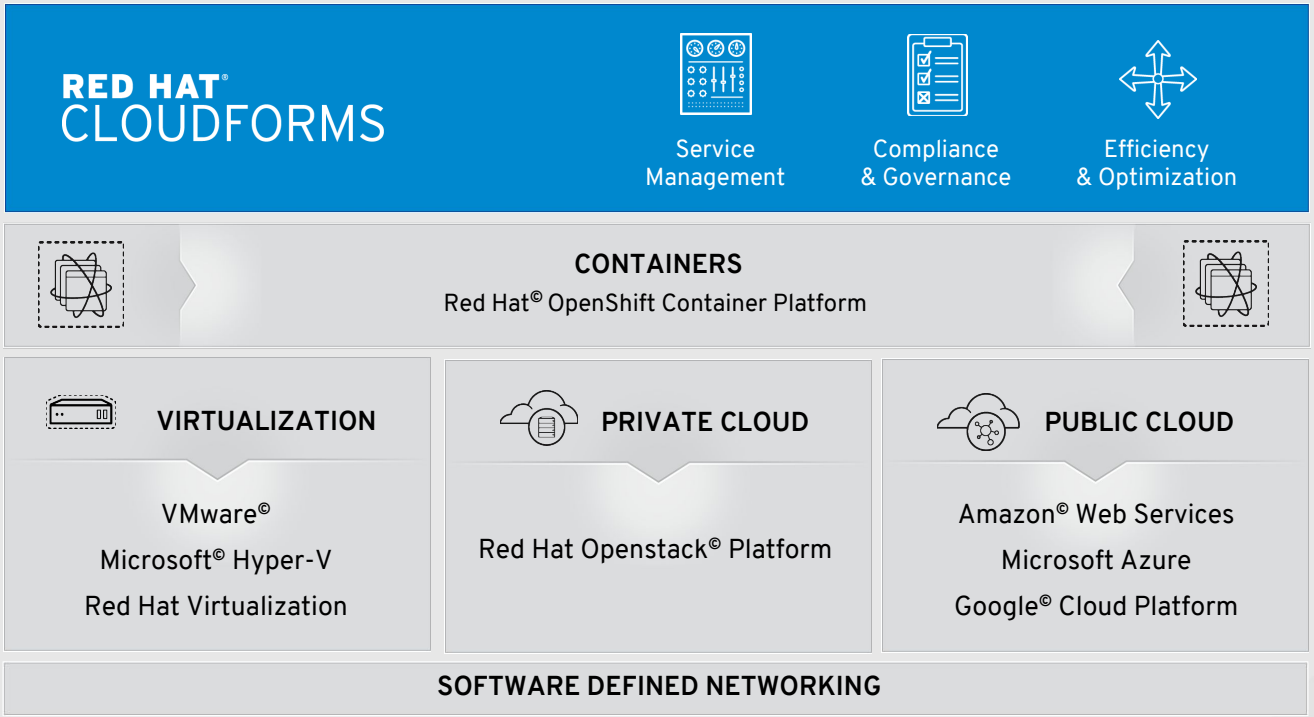
Using Red Hat's management products + OpenSCAP, how do I:

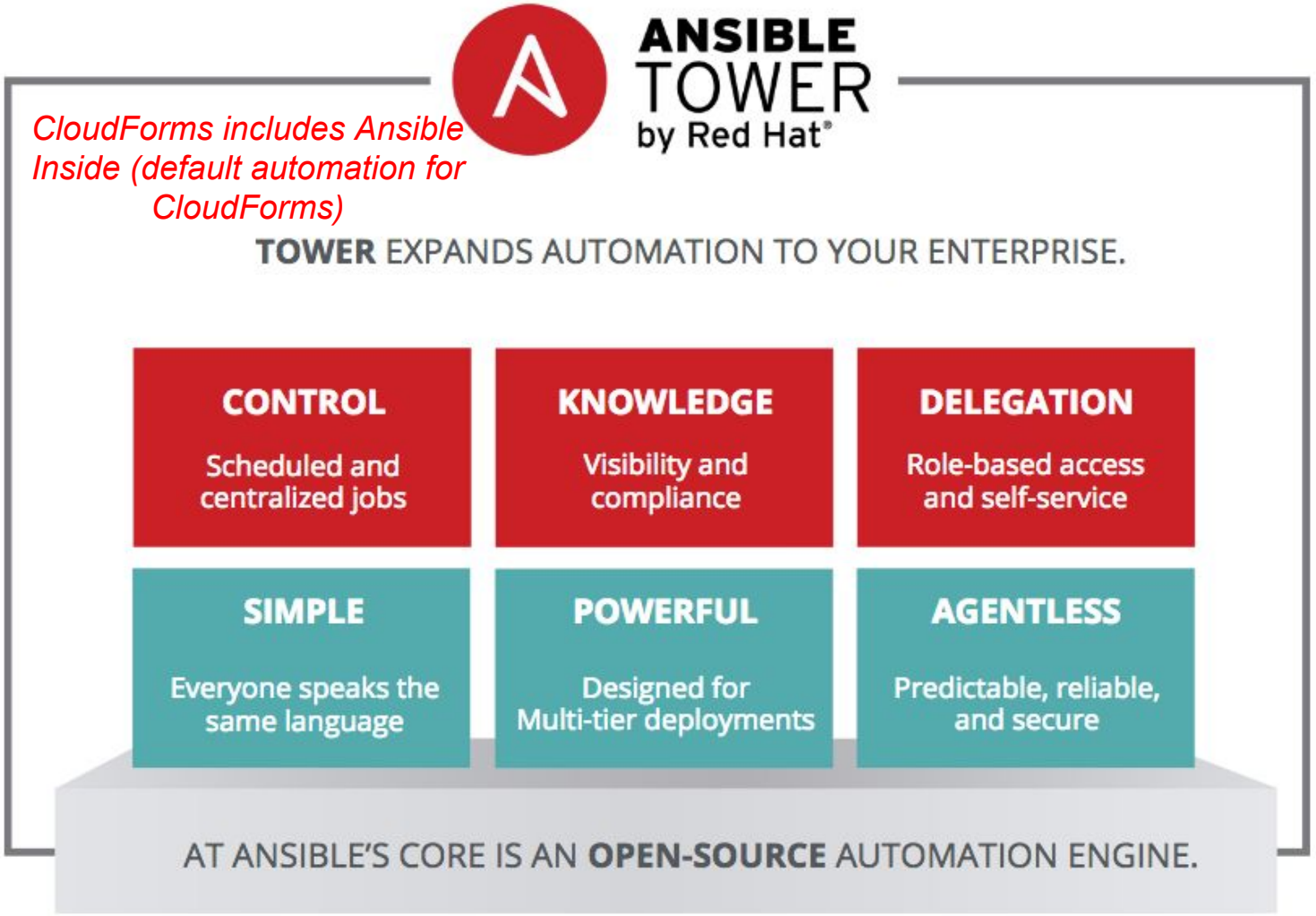
1) Create a security compliant host at provisioning time
2) Automate ongoing security compliance
3) Ensure governance and Control
4) Do proactive vs reactive security with Red Hat Insights

**All in a heterogeneous infrastructure with a mix of physical, virtual , cloud, and container environments **

Creating a security compliant host at provisioning time with Red Hat CloudForms and Ansible Tower

Unified Management with Red Hat CloudForms




ANSIBLE
TOWER
by Red Hat
CloudForms includes Ansible Inside (default automation for CloudForms)
TOWER EXPANDS AUTOMATION TO YOUR ENTERPRISE.
CONTROL
Scheduled and centralized jobs
KNOWLEDGE
Visibility and compliance
DELEGATION
Role-based access and self-service
SIMPLE
Everyone speaks the same language
POWERFUL
Designed for Multi-tier deployments
AGENTLESS
Predictable, reliable, and secure
AT ANSIBLE'S CORE IS AN OPEN-SOURCE AUTOMATION ENGINE.

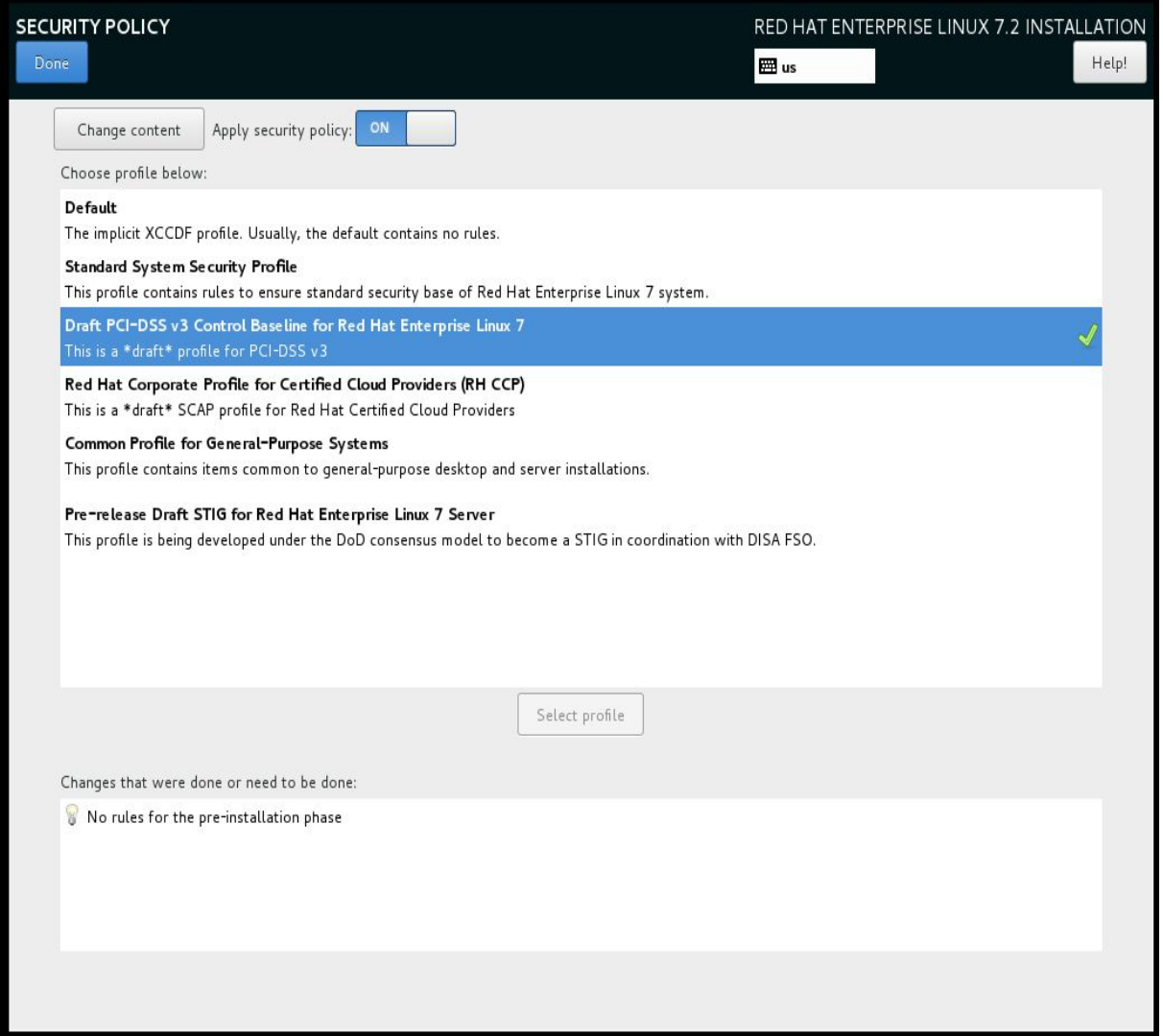
DEMO #1

Creating a security compliant host at provisioning time

1. Push an order button in CloudForms which, behind the scenes will:
   - Provision a VM in VmWare
   - Register it with Satellite
   - Make it compliant to the Defense Information Systems Agency(DISA) Security Technical Implementation Guide (STIG)
2. Do all this WITHOUT writing a single line of code and WITH multi-tenancy
   - Users from different tenants have their own “order buttons”
3. Admin has tight control of ***entire*** heterogenous infrastructure and only allows certain people provision in Amazon vs VMWare based on tenancy, utilization, etc

Now, let's see this in action!

You can also create a security compliant host in RHEL 7.2, RHEL 7.3 + Satellite 6



Of course, can kickstart too or create security compliant host(s) using Satellite 6 as well vs RHEL GUI install.

Automating ongoing security compliance with Red Hat CloudForms, Satellite, OpenSCAP, and Ansible Tower

DEMO #2

Automate ongoing security compliance

1. Push a button on a VM in CloudForms and do an OpenSCAP scan on it for a chosen security profile (PCI-DSS, DISA STIG, Standard, etc or your custom profile)
   - When the scan PASSES:
     i. Tag the VM as scap-compliant:<name of profile>
   - When the scan FAILS:
     i. Tag the VM as scap-noncompliant:<name of profile>
     ii. Email owner of VM
     iii. Open a ticket in a ticketing system, such as ServiceNow with the name of the failed VM and all other details about VM(size, IP address,etc)
2. Create reports of ALL scap-compliant/non-compliant VMs based on security profile
3. Push a button to fix the VM based on security profile. Once that looks good, do the fix for ALL machines in my environment at the push of a button.

Now, let's see this in action!

The Power and Flexibility of the Red Hat CloudForms control/policy engine

DEMO #3

Power and Flexibility of the CloudForms control engine

1. Check to see if your VM is vulnerable to shellshock. If yes, then fix the VM using a button in CloudForms that launches an Ansible playbook to remediate the VM against the shellshock vulnerability.

2. In CloudForms, check to see if an Openshift container image has any severity high vulnerabilities. If yes, then Openshift will prevent that vulnerable image from ever running in Openshift again.

Now, let's see this in action!

Proactive Security and Automated Risk Management with Red Hat Insights

RED HAT® INSIGHTS

RED HAT MANAGEMENT

Insights introduces automated risk management, reduces complexity, and allows you to *FIX* faster.

ANSIBLE by Red Hat®

AUTOMATE YOUR IT PROCESSES & DEPLOYMENTS

- Simple & powerful language
- No agents to install
- Scale with **Ansible Tower**

RED HAT® INSIGHTS

PREVENT CRITICAL ISSUES BEFORE THEY OCCUR

- Continuous Insights
- Verified Knowledge
- Proactive Resolution

RED HAT® SATELLITE

BUILD A TRUSTED & SECURE RED HAT ENVIRONMENT

- Manage the Red Hat Lifecycle
- Provision & Configure at Scale
- Standardize Your Environment

RED HAT® CLOUDFORMS

DELIVER SERVICES ACROSS YOUR HYBRID CLOUD

- Hybrid Cloud Management
- Self-Service Provisioning
- Policy-driven Compliance

DEMO #4

Proactive Security with Red Hat Insights

1. See the payload injection issue on your VM in Red Hat Insights from either Satellite or CloudForms.
    - Upon fixing, notice that the issue no longer exists

Now, let's see this in action!

SUMMARY

1) Create a security compliant host at provisioning time
2) Automate ongoing security and compliance
3) Ensure governance and Control
4) Do proactive vs reactive security with Red Hat Insights

All with ***FLEXIBILITY + CHOICE*** using a combination of OpenSCAP, Red Hat CloudForms, Red Hat Satellite, Ansible Tower, and Red Hat Insights

RED HAT®
CLOUDFORMS

ANSIBLE
TOWER
by Red Hat®

RED HAT®
SATELLITE

RED HAT®
INSIGHTS

OpenSCAP

Lucy Kerner
Principal Technical Product Marketing Manager - Security , Red Hat
lkerner@redhat.com
@LucyCloudBling


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos

RED HAT SUMMIT

THANK YOU


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos

LEARN. NETWORK.
EXPERIENCE
OPEN SOURCE.