

# Security Blankets

Compliance is hard, but consistent system deployment shouldn't be

Amy Farley  
Product Manager

Mike Ralph  
Technical Account Manager

# /whois Amy Farley



- Red Hat
  - Product Manager - Identity
- Love/hate relationship with tech from an early age
- Avid geek/infosec nerd
- Teacher
- Customer Experience Test Monkey
- Connect smart people together for answers

# /whois Mike Ralph

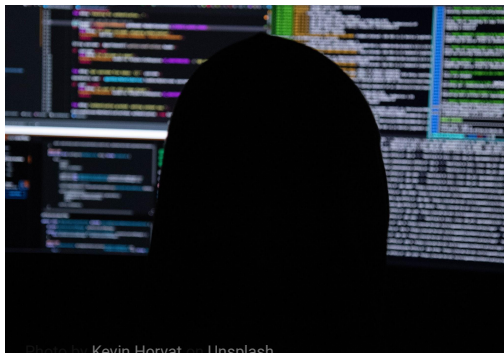


Photo by Kevin Horvat on Unsplash

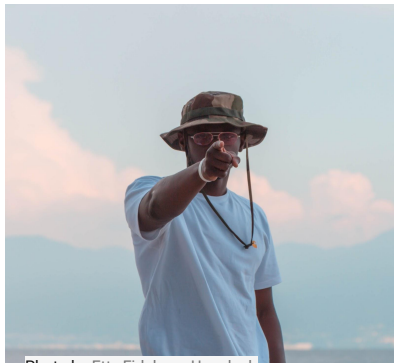


Photo by Eddy Fidele on Unsplash

- Red Hat
    - Technical Account Manager - Public Sector
  - Unix Systems Admin - too many years to admit
  - InfoSec Nerd
- 
- These photos are not me

## Outline

- Choose framework (STIG)
    - HIPAA, C2S, PCI-DSS, etc...
  - Have a repeatable deployment system (Satellite 6.5+)
    - VMWare, cloud providers
  - Verification system (OpenSCAP)
    -
  - Remediation system (Ansible)
    - Other options are Chef, Puppet, Salt, manual (ie scripting)
  - Demo
- 
- Cloud.redhat.com overview

---

A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila. — Mitch Ratliff

# We need to have “the talk” about Security



Photo by [Ben White](#) on [Unsplash](#)



Photo by [Jeremy Readle](#) on [Unsplash](#)

"We can evade reality but we cannot evade the consequences of evading reality."

–Ayn Rand

## WHY DOES THIS PRESENTATION MATTER?



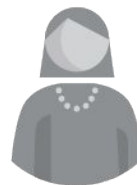
### CEO

- I don't want to end up on the news.



### CIO

- My Security Officer keeps talking about a STIG or something.



### DEV MANAGER

- I want root and I want it now!
- yum -y install \*



### OPERATIONS MANAGER

- Does your Security Officer annoy you? Ask me how to make them go away today!

## “Who are the Victims?”

### Size doesn't matter...

- 16% Public Sector Entities
- 15% Healthcare Organizations
- 10% FSI
- 43% Small Businesses

**No one is too big or too little to fail...**



Photo by [Icons8 team](#) on [Unsplash](#)



## “What Tactics?”

### Everything is automated...

- 52% Hacking
- 33% Social Attacks
- 28% Malware
- 21% Errors
- 15% Authorized User Misuse
- 4% Physical Actions

**Why should your hackers be the only ones that benefit?**



Image by [B\\_A](#) from [Pixabay](#)

# NIST, STIG, HIPAA... Which to choose?



Image by [Arek Socha](#) from [Pixabay](#)

- If your industry does not have one that is required, choose one that fits your requirements.

- Depending on your industry, you might be tied to a specific framework.



Image by [Arek Socha](#) from [Pixabay](#)

---

# Security and Compliance Mangement

---

Repeatability is key, if you cannot repeat the process reliably then you will just end up causing more work for yourself.

---

# Provision and Secure @ Build-time

---

If you cannot verify your systems comply with the framework why have it?

You should verify compliance on a regular basis for insight into your environment to ensure nothing has changed.

# Security Automation with OpenSCAP



- NIST validated and certified Security Content Automation Protocol (SCAP) scanner by Red Hat
- Scans systems and containers for:
  - known vulnerabilities = unpatched software
  - compliance with security policies (PCI-DSS, US Gov baselines, etc)
- Ansible remediation playbooks provided (new with RHEL 7.5)
- Included in Red Hat Enterprise Linux base repository

# Security Automation with OpenSCAP



OpenSCAP

- Red Hat natively ships NIST validated National Checklist content
- SCAP Workbench
  - GUI front end tool for OpenSCAP that serves as an SCAP scanner
  - Local scanning of a single machine
  - Provides tailoring functionality for SCAP content



# SCAP Workbench

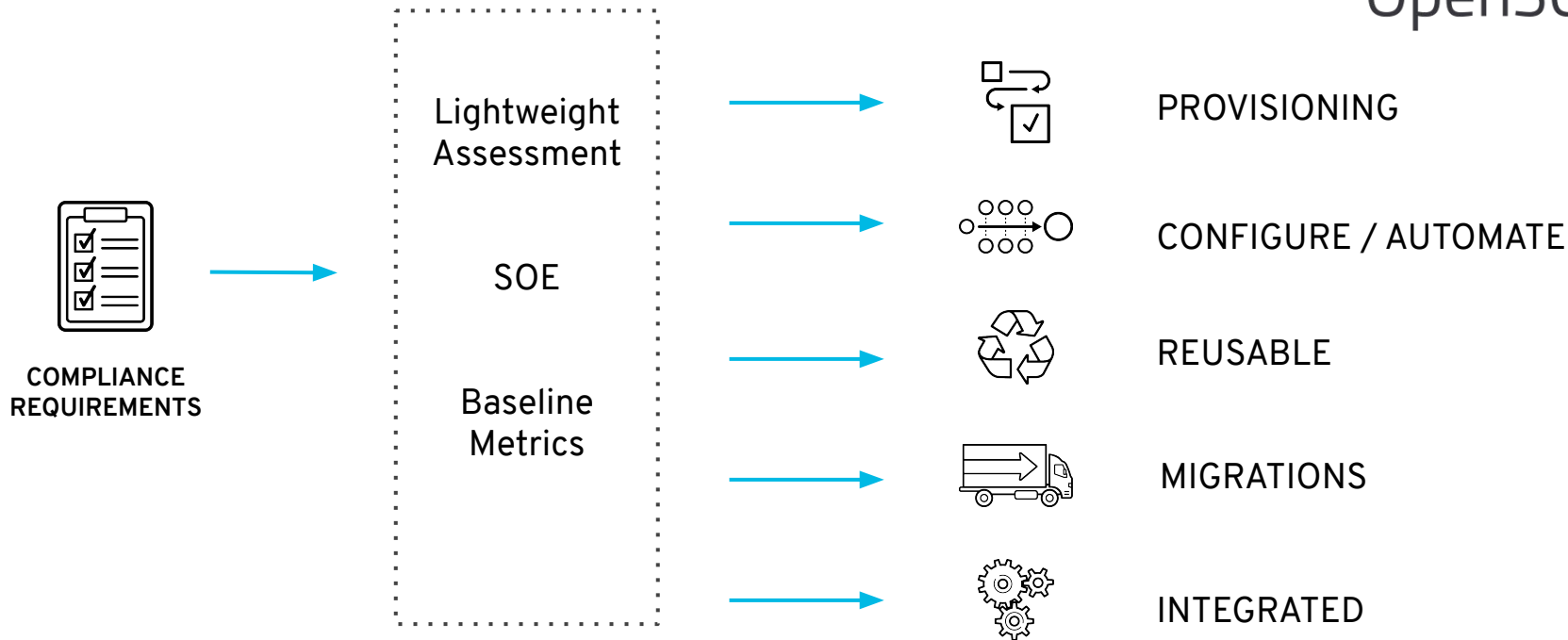


- Found [here](#):
- Runs on a network-connected server
- Runs scans locally or via ssh
- Can create mitigation (tailoring) files (ansible, bash, puppet)
- Reporting
- [Documentation](#)

# OpenSCAP Everywhere



OpenSCAP



# Portfolio Capabilities



OpenSCAP

## Use-case

**RED HAT®**  
**ENTERPRISE**  
**LINUX®**

- I want to scan a single system
- I want to remediate a single system
- I want to author a new Policy
- I want to modify an existing Policy

**RED HAT®**  
**SATELLITE**

- I want to scan groups of systems
- I want to delegate scanning OR reporting to an external identity
- I want to ensure a standard, secure SOE to build the foundation for DevOPS



**RED HAT®**  
**ANSIBLE®**  
Tower

- I want to delegate and automate remediation
- I want to ensure compliance at build time across my entire RHEL-estate
- I want to empower my Organization to become more independent

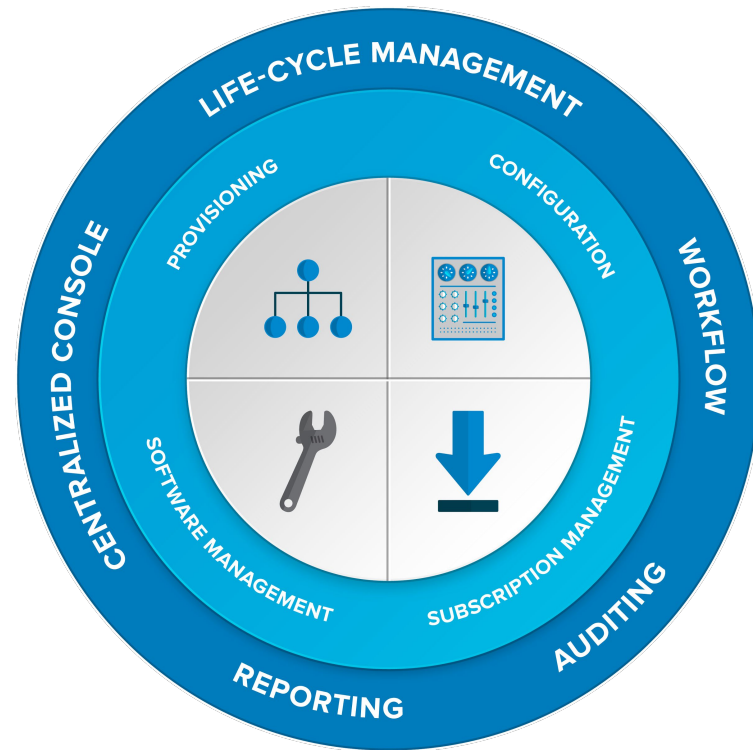
---

# Automated Provisioning with Satellite 6

## Responsive SOE with Red Hat Satellite

Establish the core to manage change

- **Provisioning**  
bare metal, virtual, and public or private clouds
- **Configuration**  
analyze and automatically remediate configuration drift and enforce desired host state
- **Software Management**  
systematic process to apply content, including patches, to deployed systems in all stages, from development to production
- **Subscription Management**  
report and map Red Hat-purchased products to registered systems for end-to-end subscription consumption visibility.



# Satellite 6.6

## Partition Tables

/ kickstart

✕

Q Search

▼

Create Partition Table

Documentation

Name	OS Family	Operating Systems	Snippet	Locked	Actions
Kickstart default	Red Hat	RHEL Server 7.7			Clone ▼
Kickstart default STIG	Red Hat	RHEL Server 7.7			Clone ▼
Kickstart default thin	Red Hat				Clone ▼

20 ^ per page

1-3 of 3

« < 1 of 1 > »

```
<%#
kind: ptable
name: Kickstart default
model: Ptable
oses:
- CentOS
- Fedora
- RedHat
%>
zerombr
clearpart --all --initlabel
part pv.253 --fstype="lvm" --ondisk=vda --size=30207
part /boot --fstype="xfs" --ondisk=vda --size=512
volgroup rhel --pesize=4096 pv.253
logvol /var --fstype="xfs" --size=4096 --name=var --vgname=rhel
logvol /var/log/audit --fstype="xfs" --size=2048 --name=var_log_audit --vgname=rhel
logvol /tmp --fstype="xfs" --size=4096 --name=tmp --vgname=rhel
logvol / --fstype="xfs" --size=11767 --name=root --vgname=rhel
logvol swap --fstype="swap" --size=2048 --name=swap --vgname=rhel
logvol /home --fstype="xfs" --size=2048 --name=home --vgname=rhel
logvol /var/log --fstype="xfs" --size=4096 --name=var_log --vgname=rhel
```

## Assigned Ansible Roles

10 ^ per page	1-2 of 2	«	<	1	of 1	>	»
RedHatInsights.insights-client							
theforeman.foreman_scap_client							



Found 12 reports from the last  days

## Details

[Audits](#)[Facts](#)[Reports](#)[YAML](#)[Content](#)[Compliance](#)[Properties](#)[Metrics](#)[Templates](#)[VM](#)[NICs](#)

## Properties

Status	⊗ Error
Compliance	⊗ Incompliant
Build	✓ Installed
Configuration	✓ No changes
Errata	⊗ Security errata applicable
Subscription	✓ Fully entitled
Details	<a href="#">idm3.amyra.com</a>

## Installable Errata


Current Lifecycle Env

Filter...



Search

<input type="checkbox"/>	Type	Id	Title	Issued
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2758</a>	Generated network interfaces (docker0) will now persist zone assignments	9/25/18
<input type="checkbox"/>	⚠ Security Advisory - Moderate	<a href="#">RHSA-2018:2768</a>	Moderate: nss security update	9/25/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2764</a>	initscripts bug fix update	9/25/18
<input type="checkbox"/>	⚠ Security Advisory - Important	<a href="#">RHSA-2018:2748</a>	Important: kernel security and bug fix update	9/25/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2761</a>	kexec-tools bug fix update	9/25/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2753</a>	systemd bug fix update	9/25/18
<input type="checkbox"/>	🔧 Product Enhancement Advisory - None	<a href="#">RHEA-2018:2397</a>	microcode_ctl bug fix and enhancement update	9/11/18
<input type="checkbox"/>	⚠ Security Advisory - Important	<a href="#">RHSA-2018:2570</a>	Important: bind security update	8/27/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2528</a>	tuned bug fix update	8/20/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2447</a>	systemd bug fix update	8/16/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2463</a>	audit bug fix update	8/16/18
<input type="checkbox"/>	⚠ Security Advisory - Moderate	<a href="#">RHSA-2018:2439</a>	Moderate: mariadb security and bug fix update	8/16/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2441</a>	initscripts bugfix update	8/16/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2446</a>	kexec-tools bug fix update	8/16/18
<input type="checkbox"/>	🔧 Product Enhancement Advisory - None	<a href="#">RHEA-2018:2464</a>	device-mapper-multipath enhancement update	8/16/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2451</a>	selinux-policy bug fix update	8/16/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2456</a>	tuned bug fix update	8/16/18
<input type="checkbox"/>	✳ Bug Fix Advisory - None	<a href="#">RHBA-2018:2442</a>	dracut bug fix update	8/16/18


## Installable Errata

Current Lifecycle Envi 

severity = Critical

 Search 

<input type="checkbox"/>	Type	Id	Title
<input type="checkbox"/>	 Security Advisory - Critical	<a href="#">RHSA-2017:2836</a>	Critical: dnsmasq security update
<input type="checkbox"/>	 Security Advisory - Critical	<a href="#">RHSA-2017:1100</a>	Critical: nss and nss-util security update
<input type="checkbox"/>	 Security Advisory - Critical	<a href="#">RHSA-2018:1453</a>	Critical: dhcp security update

20  per page

Installable Errata

Current Lifecycle Envi

severity = Critical

x Search

<input type="checkbox"/>	Type	Id	Title
<input checked="" type="checkbox"/>	Security Advisory - Critical	<a href="#">RHSA-2017:2836</a>	Critical: dnsmasq security update
<input checked="" type="checkbox"/>	Security Advisory - Critical	<a href="#">RHSA-2017:1100</a>	Critical: nss and nss-util security update
<input checked="" type="checkbox"/>	Security Advisory - Critical	<a href="#">RHSA-2018:1453</a>	Critical: dhcp security update

20

 per page

---

# Demo

---

# Questions?

# Resources

## SCAP workbench:

- <https://www.open-scap.org/tools/scap-workbench/>
- [https://static.open-scap.org/scap-workbench-1.1/#\\_obtain\\_scap\\_content](https://static.open-scap.org/scap-workbench-1.1/#_obtain_scap_content)

## Security Guide:

- [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/security\\_guide/sect-using\\_scap\\_workbench](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sect-using_scap_workbench)

## Compliance as Code (Upstream Projects)

The screenshot shows the GitHub repository page for ComplianceAsCode. The repository name is "ComplianceAsCode / content". It has 128 watches, 749 stars, and 313 forks. The navigation bar includes links for Code, Issues (389), Pull requests (18), Actions, Projects (5), Wiki, Security, and Insights. The main content area features a description: "Security compliance content in SCAP, Bash, Ansible, and other formats" with a link to <https://www.open-scap.org/security-po...>. Below the description are tags for various security frameworks and tools: security, compliance, scap, xccdf, oval, cpe, cce, usgcb, pci-dss, ospp, stig, application-security, security-tools, security-hardening, security-automation, security-profile, hardening, information-security, cybersecurity, and ansible. A statistics bar shows 13,936 commits, 1 branch, 42 releases, and 112 contributors. At the bottom, there are buttons for "New pull request", "Create new file", "Upload files", "Find File", and "Clone or download".

ComplianceAsCode / content

Watch 128 Star 749 Fork 313

<> Code Issues 389 Pull requests 18 Actions Projects 5 Wiki Security Insights

Security compliance content in SCAP, Bash, Ansible, and other formats <https://www.open-scap.org/security-po...>

security compliance scap xccdf oval cpe cce usgcb pci-dss ospp stig application-security security-tools

security-hardening security-automation security-profile hardening information-security cybersecurity ansible

13,936 commits 1 branch 42 releases 112 contributors View license

Branch: master New pull request Create new file Upload files Find File Clone or download



# Resources

- **Alternate Content Sources and You (or How to rebuild your Satellite and not have to download all the content from the CDN again)**  
<http://www.outsidaz.org/2017/12/21/alternate-content-sources-and-you-or-how-to-rebuild-your-satellite-and-not-have-to-download-all-the-content-from-the-cdn-again/>
- **Satellite 6: sync repository from an alternate / local content source**  
<https://access.redhat.com/articles/1531833>
- **Addressing CVE-2015-7547, CVE-2015-5229, and any other scary errata via Red Hat Satellite 6.1** - <https://access.redhat.com/blogs/1169563/posts/2171601>

# THANK YOU



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[twitter.com/RedHat](https://twitter.com/RedHat)