Some Call it Crazy, Others Call it OpenSCAP

Amy Farley
Technical Account Manager
North American Public Sector
Red Hat, Inc.

Abstract

Corporations have been hit hard with a number of cyber breaches often due to application stacks running on hosts lacking essential security patches. The business of monitoring critical Linux Enterprise infrastructure is complex and often hindered by poor governance, fragmented management applications, and unnecessary exposure to the public Internet. Satellite 6 has been design to address these all too common vulnerabilities by offering its users highly structured workflows for deploying standard Linux builds from early stage through to production. Satellite goes further with integrated Security Content Automation Protocol (SCAP) scanning that rolls up common vulnerability reporting and misconfigurations into an actionable dashboard tailored for large scale Linux estates. And it this is not enough, Satellite 6 offers all of its essential security services in a fully disconnected capacity further protecting critical computing assets from infiltration and common exposures.

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!

Security & Compliance Management

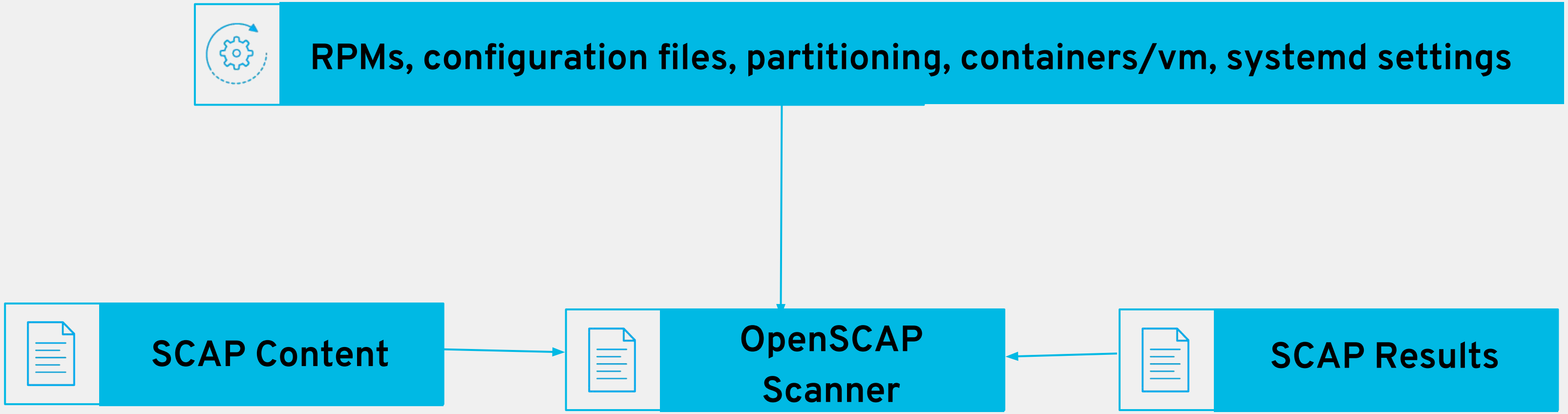
Security Automation with OpenSCAP

- 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

- 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

OpenSCAP Scanning



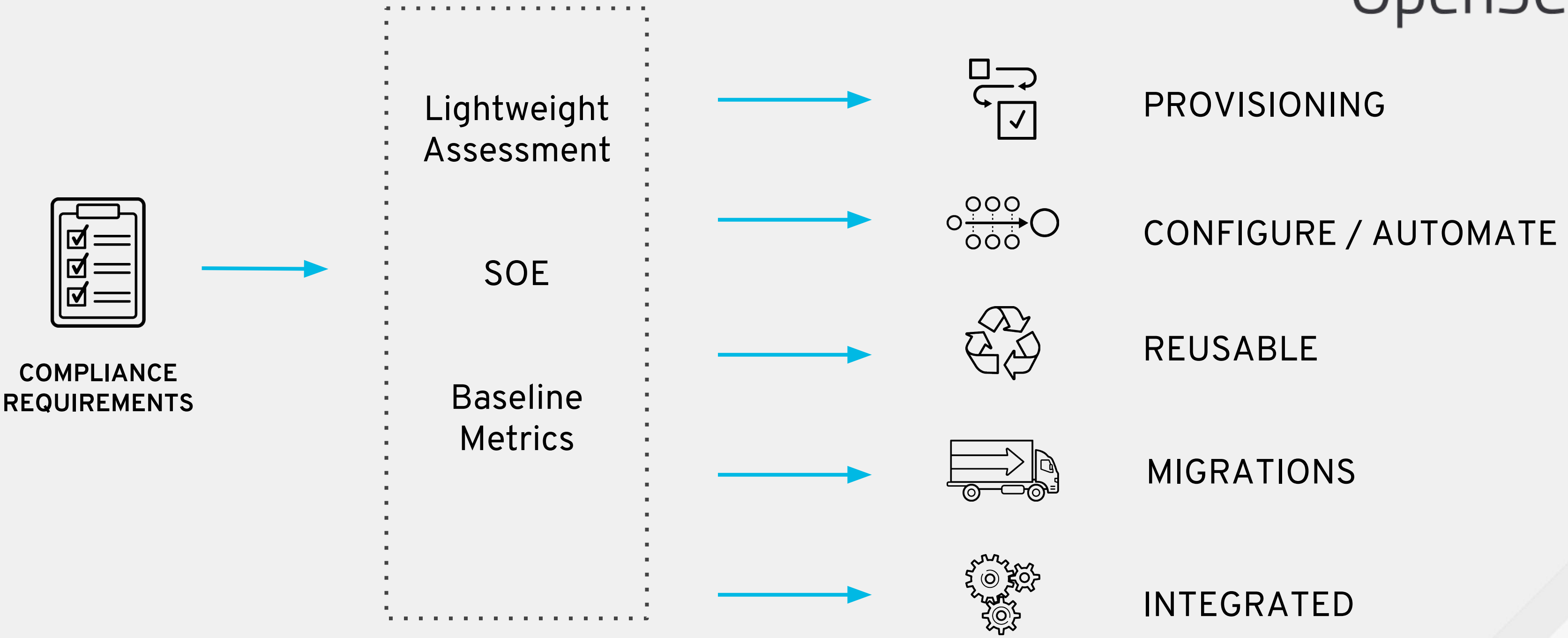
RPMs, configuration files, partitioning, containers/vm, systemd settings

SCAP Content

OpenSCAP Scanner

SCAP Results

OpenSCAP Everywhere



COMPLIANCE REQUIREMENTS

Lightweight Assessment

SOE

Baseline Metrics

PROVISIONING

CONFIGURE / AUTOMATE

REUSABLE

MIGRATIONS

INTEGRATED

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

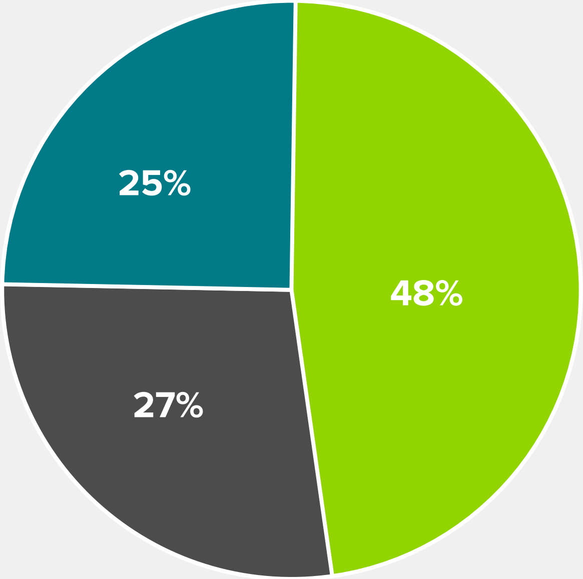
Vulnerability Management

Why so serious?

“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”

Focus on the Biggest Security Threats, Not the Most Publicized
Gartner, November 2017

MULTIPLE SOURCES OF RISKS



Cyber criminals and hackers are more:

- Dangerous
- Sophisticated
- Global
- Profit-oriented
- Nation state sponsored

🟦 Human error ⬛ System glitch 🟩 Malicious or criminal attack

2016 Cost of Data Breach Study: Global, June, 2016. Ponemon Institute LLC© Research Report

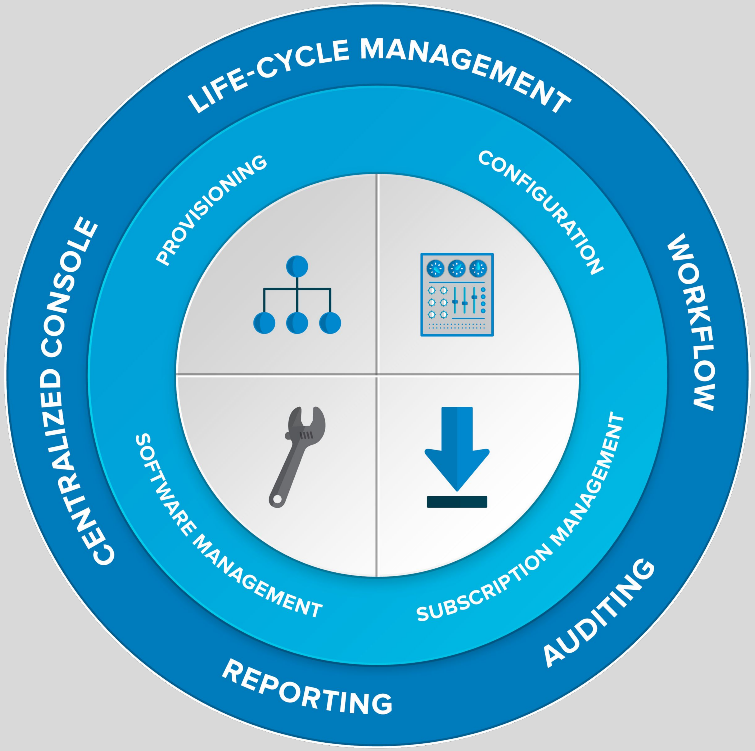
RED HAT® SATELLITE

Responsive SOE with Red Hat Satellite

Establish the core to manage change

redhat.

- **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.



Vulnerability Management with Satellite

Library	Dev	QE	Production
CV	CV	CV	CV
CV	CV	CV	CV
CV Tomcat v11.0	CV Tomcat v10.0	CV Tomcat v8.0	CV Tomcat v4.0
CV RHEL v4.0	CV RHEL v3.0 ⚠	CV RHEL v2.0 ⚠	CV RHEL v1.0 ⚠

Shellshock* is made public. What do you do?

[*] - or other ‘well-named’ vulnerability

Vulnerability Management with Satellite

Library	Dev	QE	Production
CV	CV	CV	CV
CV	CV	CV	CV
CV Tomcat v11.0	CV Tomcat v10.0	CV Tomcat v8.0	CV Tomcat v4.0
CV RHEL v4.0	CV RHEL v3.1 ✓	CV RHEL v2.1 ✓	CV RHEL v1.1 ✓

In-place updates of already published content.

Vulnerability Management with Satellite

Library	Dev	QE	Production
CV	CV	CV	CV
CV	CV	CV	CV
CV Tomcat v11.0	CV Tomcat v10.0	CV Tomcat v8.0	CV Tomcat v4.0
CV RHEL v4.0	CV RHEL v3.1 ✓	CV RHEL v2.1 ✓	CV RHEL v1.1 ✓

In-place updates of already published content.

Demo

Q & A

Resources

- **Satellite 6 Disconnected Operations Guide**
  https://github.com/sideangleside/sat6-disconnected-operations-guide
- **Subscription-manager for the former Red Hat Network User: Part 7 - understanding the Red Hat Content Delivery Network**
  https://access.redhat.com/blogs/1169563/posts/2641311
- **Understanding Red Hat Content Delivery Network Repositories and their usage with Satellite 6**
  https://access.redhat.com/articles/1586183

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
-