RED HAT SUMMIT

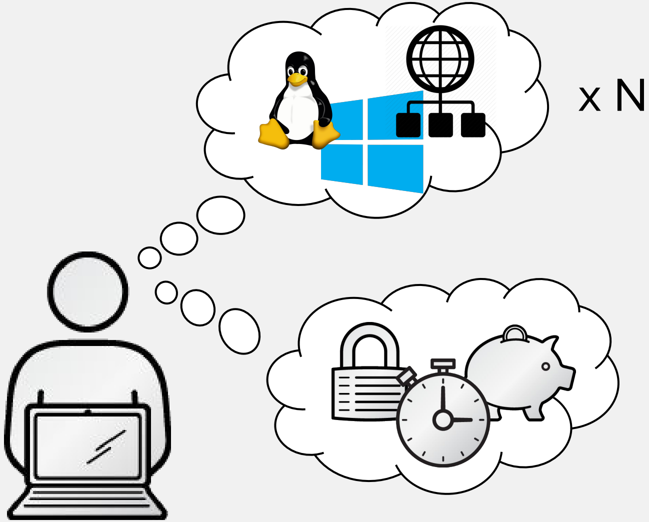
MAKING DAY-TO-DAY OPERATIONS MORE PROACTIVE, LESS REACTIVE

Phil Griffiths
Senior Solutions Architect
May 2017

WHY?

MORE THINGS THAN EVER AFFECTING YOU

I want more...
I need it now.
Security
Compliance
...



SUPPORT

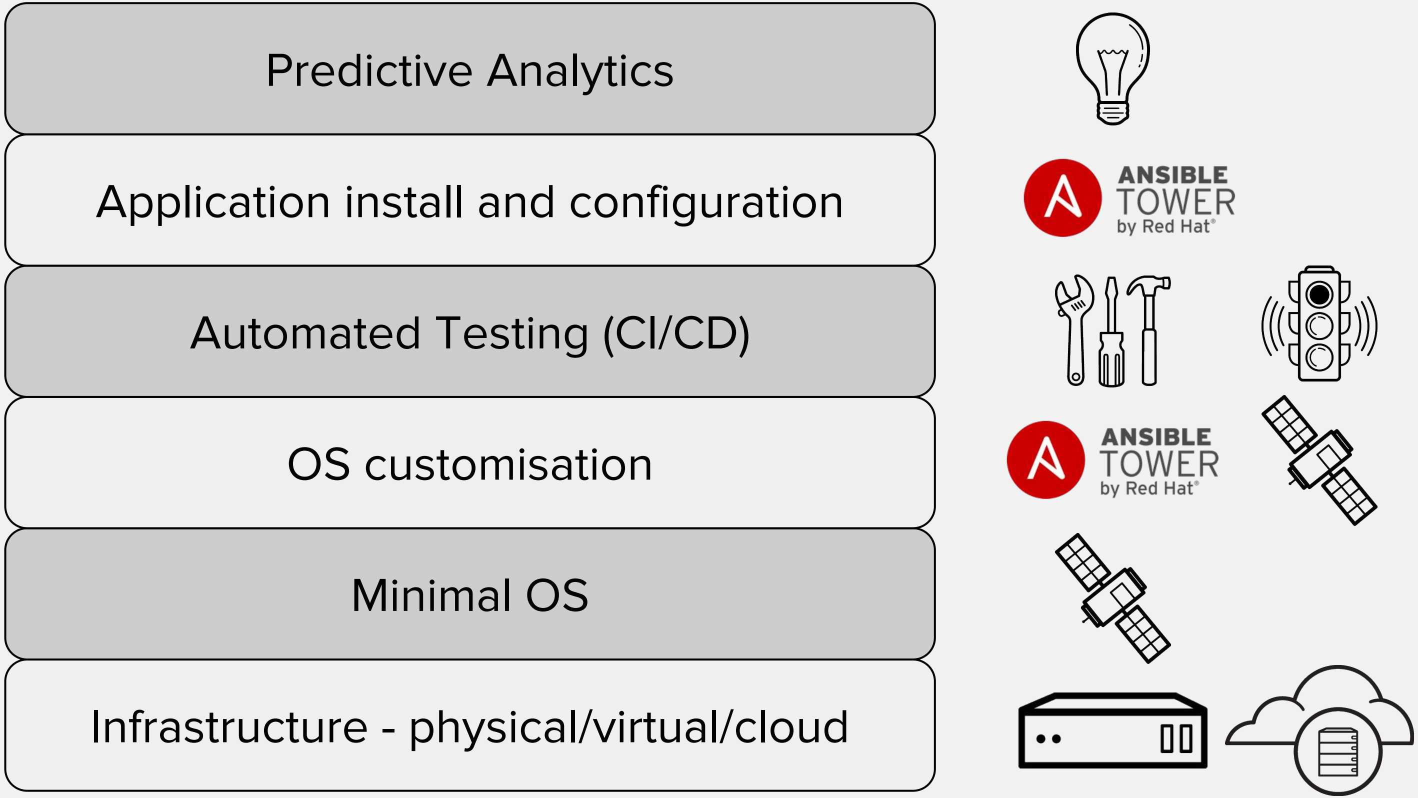
OPERATIONS

SECURITY

SUPPORT

Break-fix scenarios
No centralised audit/logging?
More support tickets than people
False positives disguise problems

BUILD THE CAKE



Predictive Analytics

Application install and configuration

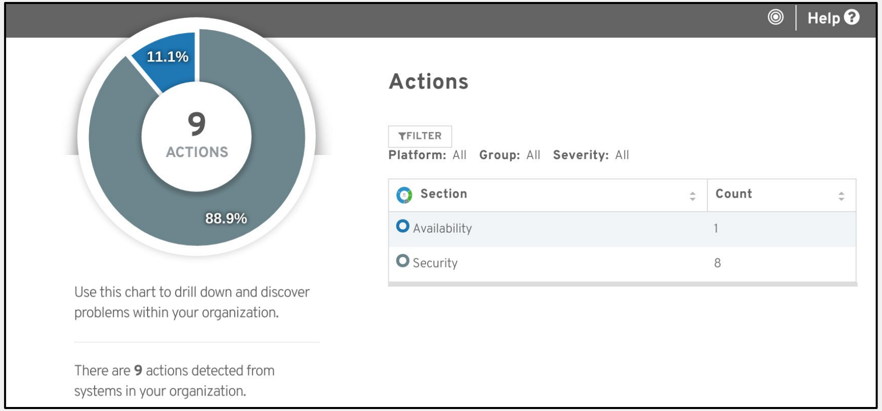
Automated Testing (CI/CD)

OS customisation

Minimal OS

Infrastructure - physical/virtual/cloud

ADD SPRINKLES...



Use this chart to drill down and discover problems within your organization.

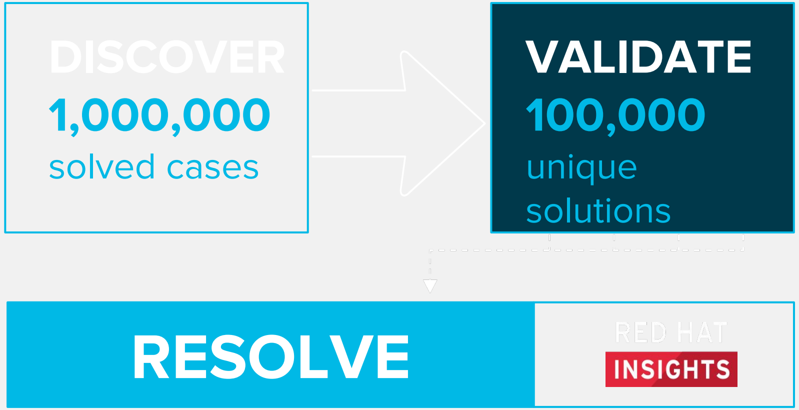
There are **9** actions detected from systems in your organization.

Actions

FILTER

Platform: All **Group:** All **Severity:** All

Section	Count
○ Availability	1
○ Security	8

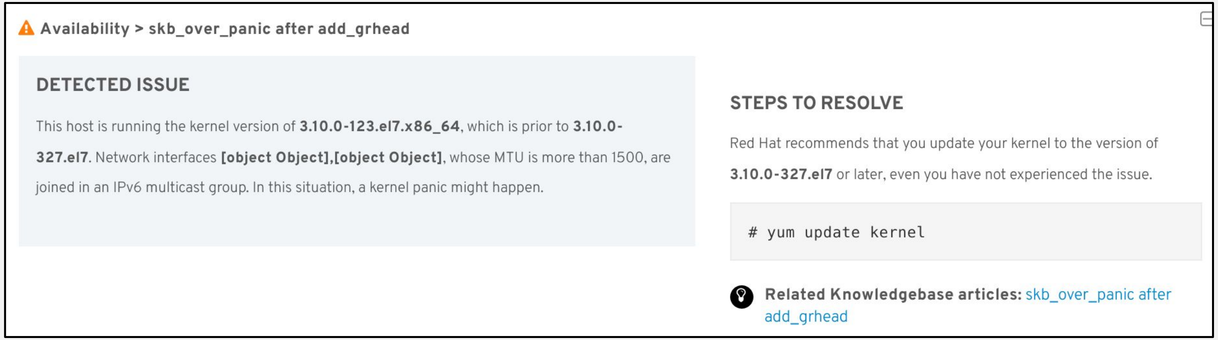


DISCOVER
1,000,000
solved cases

VALIDATE
100,000
unique solutions

RESOLVE

RED HAT
INSIGHTS



Availability > skb_over_panic after add_grhead

DETECTED ISSUE

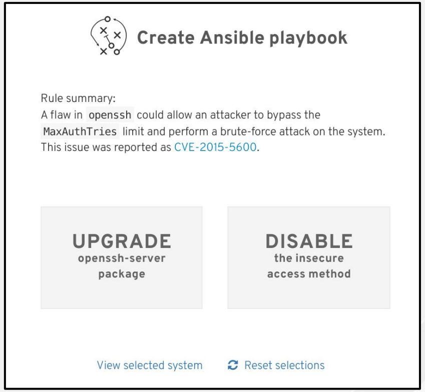
This host is running the kernel version of **3.10.0-123.el7.x86_64**, which is prior to **3.10.0-327.el7**. Network interfaces **[object Object],[object Object]**, whose MTU is more than 1500, are joined in an IPv6 multicast group. In this situation, a kernel panic might happen.

STEPS TO RESOLVE

Red Hat recommends that you update your kernel to the version of **3.10.0-327.el7** or later, even you have not experienced the issue.

```
# yum update kernel
```

Related Knowledgebase articles: skb_over_panic after add_grhead



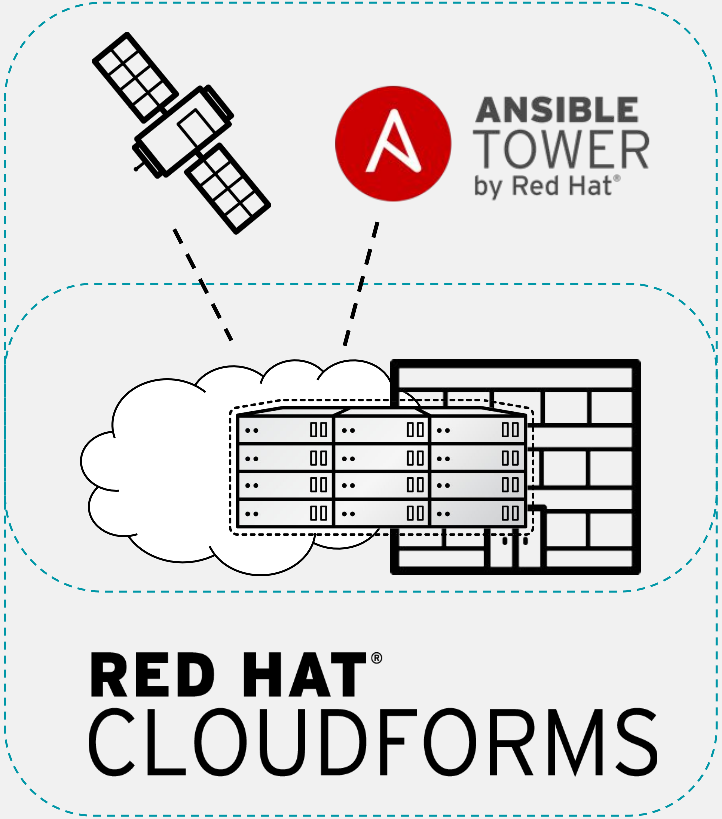
Create Ansible playbook

Rule summary:
A flaw in `openssh` could allow an attacker to bypass the `MaxAuthTries` limit and perform a brute-force attack on the system. This issue was reported as CVE-2015-5600.

OPERATIONS

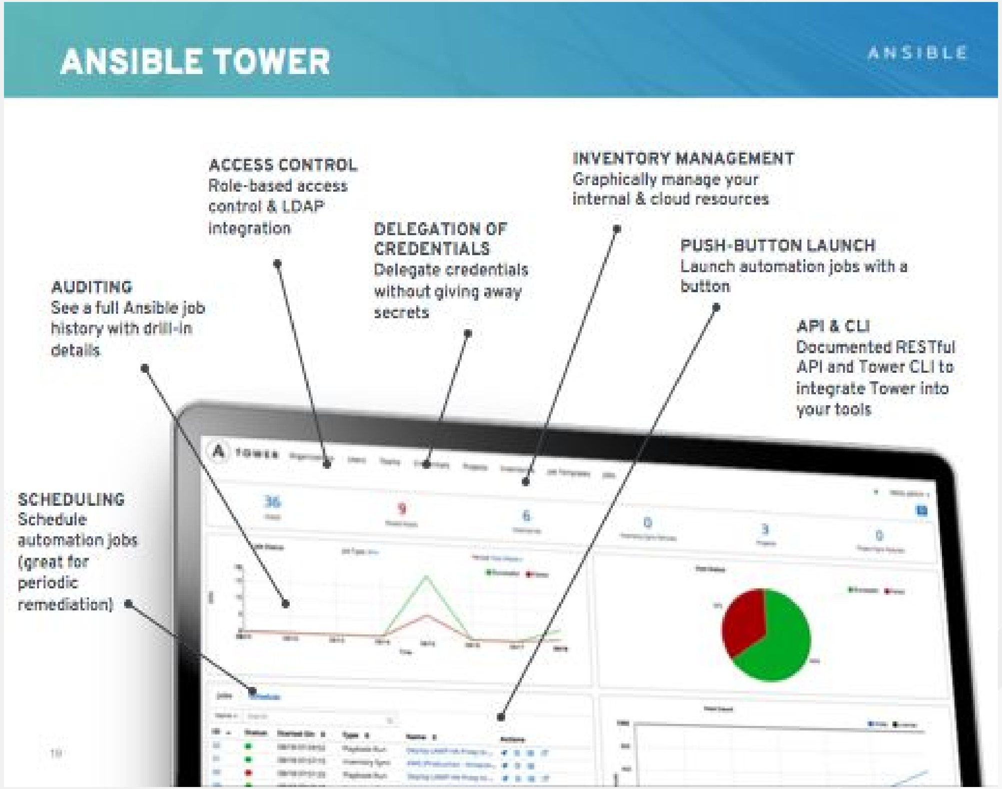
Manual or semi-manual
Mostly homebrew scripts
Everyone has *their* favourites
Configuration management (drift)

AUTOMATION IS THE KEY



ANSIBLE TOWER by Red Hat®

RED HAT® CLOUDFORMS



ANSIBLE TOWER

ACCESS CONTROL
Role-based access control & LDAP integration

INVENTORY MANAGEMENT
Graphically manage your internal & cloud resources

DELEGATION OF CREDENTIALS
Delegate credentials without giving away secrets

PUSH-BUTTON LAUNCH
Launch automation jobs with a button

AUDITING
See a full Ansible job history with drill-in details

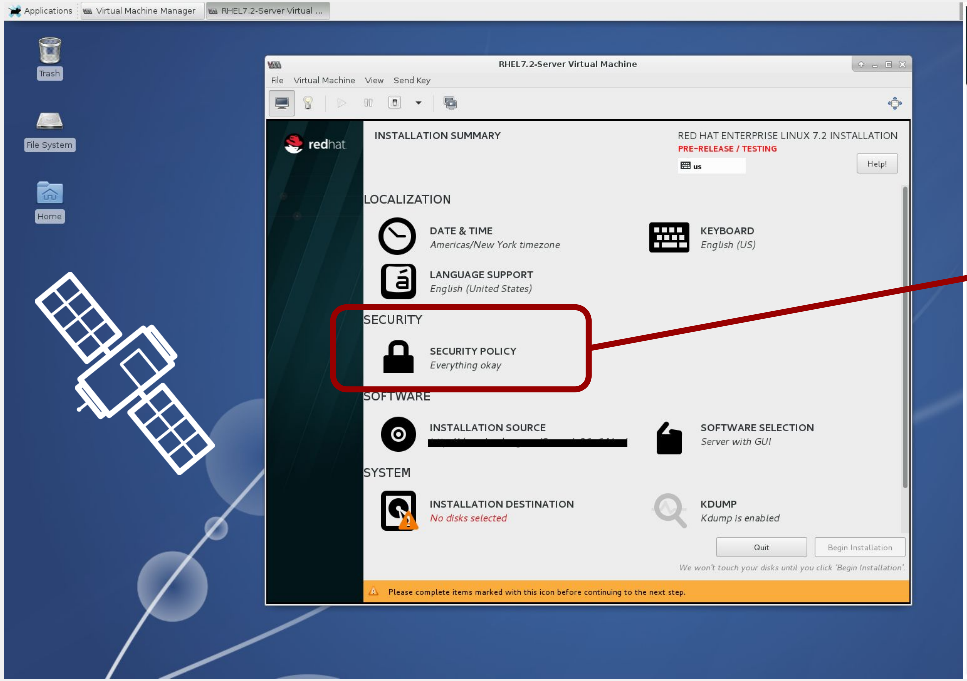
API & CLI
Documented RESTful API and Tower CLI to integrate Tower into your tools

SCHEDULING
Schedule automation jobs (great for periodic remediation)

SECURITY

Port scanning
One way traffic - security team
Can’t see wood for the trees
Only fix critical **red** issues

APPLY POLICY AT DAY-1 *BUILD* TIME...



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION

PRE-RELEASE / TESTING

us

Help!

LOCALIZATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY POLICY
Everything okay

SOFTWARE

INSTALLATION SOURCE
[redacted]

SOFTWARE SELECTION
Server with GUI

SYSTEM

INSTALLATION DESTINATION
No disks selected

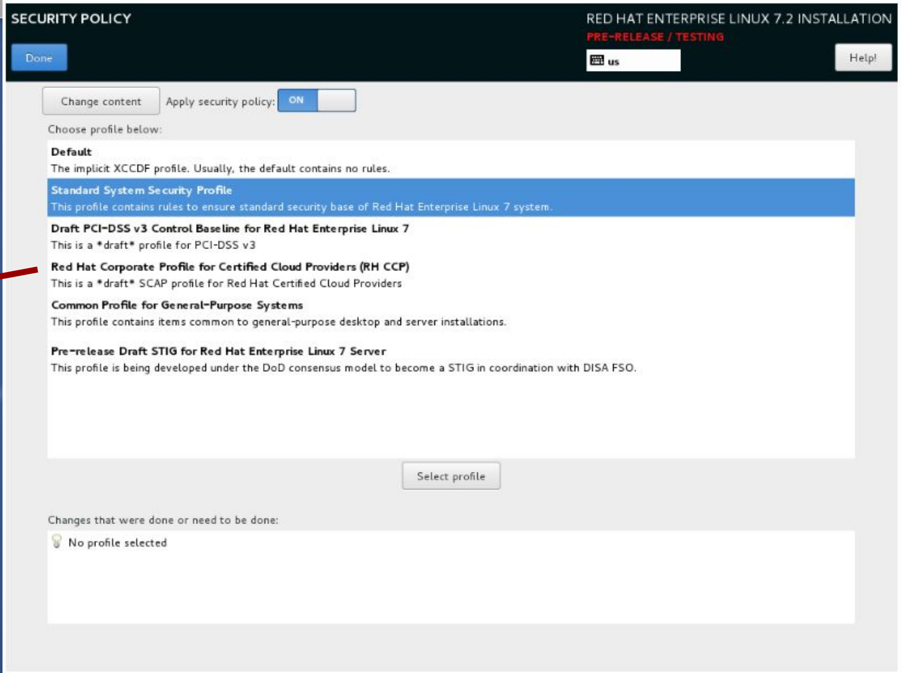
KDUMP
Kdump is enabled

Quit

Begin Installation

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.



SECURITY POLICY

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION

PRE-RELEASE / TESTING

Done

us

Help!

Change content

Apply security policy: ON

Choose profile below:

Default
The implicit XCCDF profile. Usually, the default contains no rules.

Standard System Security Profile
This profile contains rules to ensure standard security base of Red Hat Enterprise Linux 7 system.

Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
This is a *draft* profile for PCI-DSS v3

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
This is a *draft* SCAP profile for Red Hat Certified Cloud Providers

Common Profile for General-Purpose Systems
This profile contains items common to general-purpose desktop and server installations.

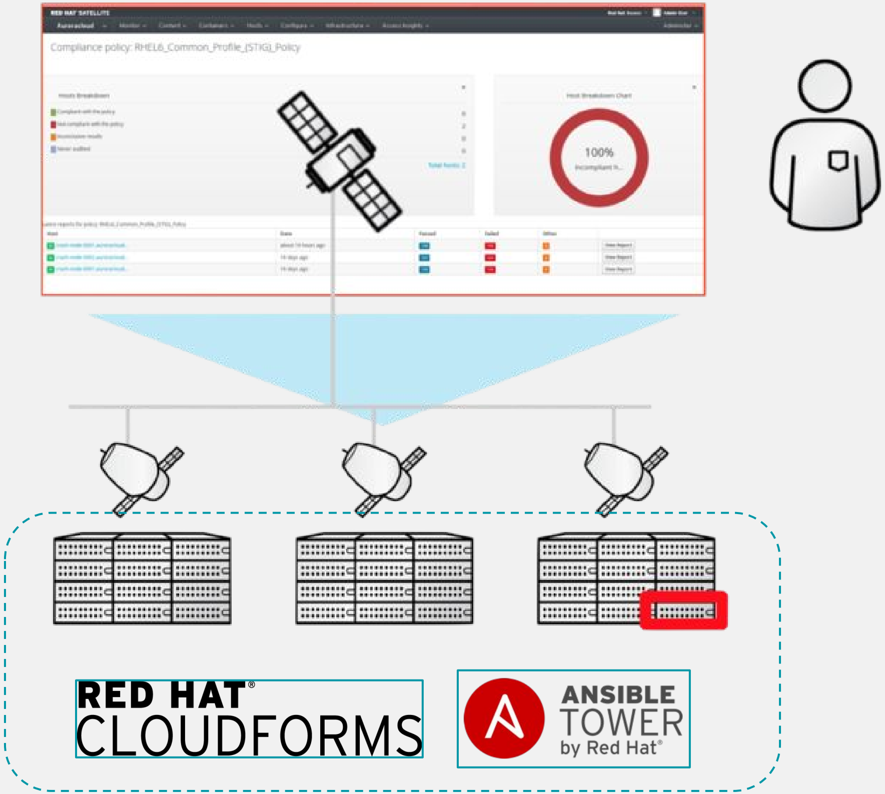
Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server
This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

Select profile

Changes that were done or need to be done:

No profile selected

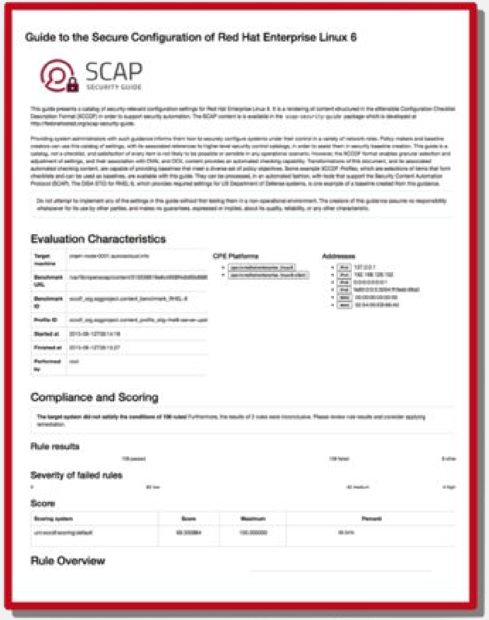
... THEN DAY-2 OPS COMPLIANCE



Compliance policy: RHEL6_Common_Profile_(STIG)_Policy

Hosts Breakdown

- 🟩 Compliant with the policy
- 🟥 Not compliant with the policy
- 🟧 Inconclusive results
- 🟦 Never audited



Guide to the Secure Configuration of Red Hat Enterprise Linux 6

SCAP SECURITY GUIDE

[illegible]

[illegible]

[illegible]

Evaluation Characteristics

Target machine	[illegible]
Benchmark URL	[illegible]
Benchmark ID	[illegible]
Profile ID	[illegible]
Started at	[illegible]
Finished at	[illegible]
Performed by	root

CPE Platforms

Addresses

Compliance and Scoring

[illegible]

Rule results

Severity of failed rules

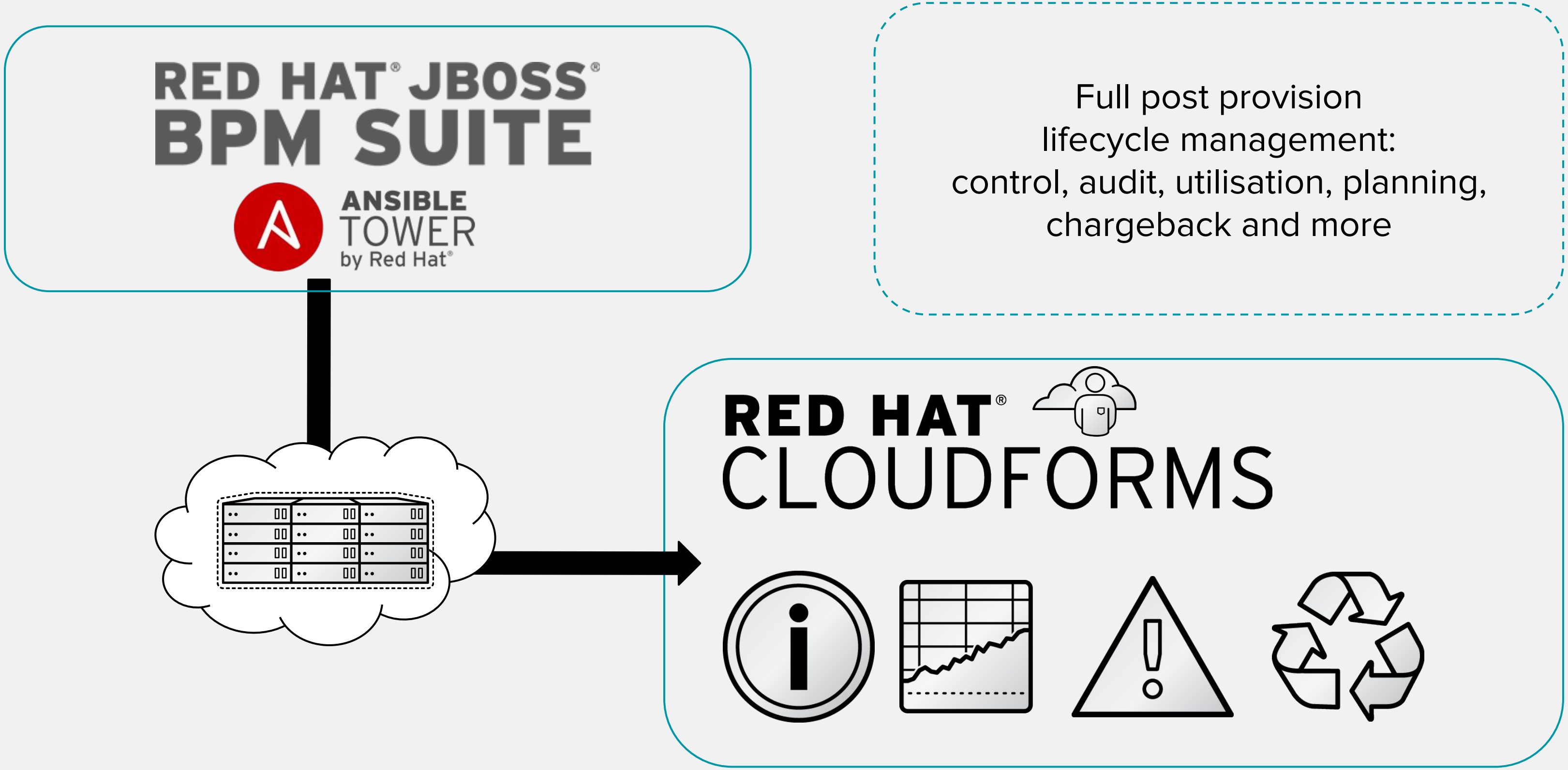
Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	[illegible]	100.000000	[illegible]

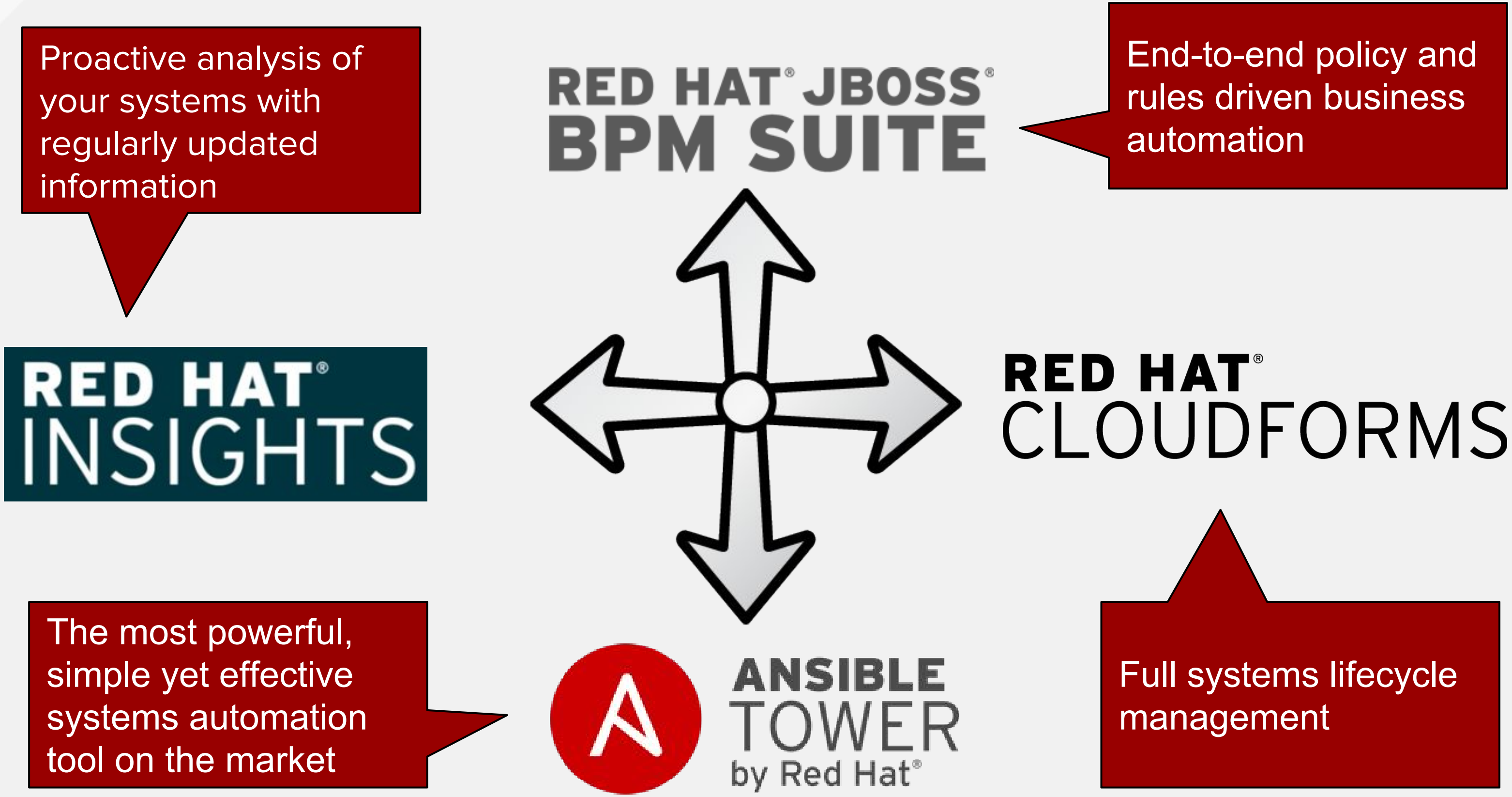
Rule Overview

JOIN THE DOTS.

BUSINESS PROCESS AUTOMATION, MEET SYSTEMS AUTOMATION



Full post provision lifecycle management: control, audit, utilisation, planning, chargeback and more



Proactive analysis of your systems with regularly updated information

RED HAT® INSIGHTS

RED HAT® JBOSS® BPM SUITE

End-to-end policy and rules driven business automation

RED HAT® CLOUDFORMS

Full systems lifecycle management

ANSIBLE TOWER by Red Hat®

The most powerful, simple yet effective systems automation tool on the market

RED HAT SUMMIT

THANK YOU

- plus.google.com/+RedHat
- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHatNews

RED HAT
SUMMIT

LEARN. NETWORK.
EXPERIENCE
OPEN SOURCE.