

#ANSIBLEAUTOMATES

ANSIBLE - MAKING RED HAT MANAGEMENT BETTER... FASTER... STRONGER

Chris Short

Principal Product Marketing Manager

Twitter: @ChrisShort

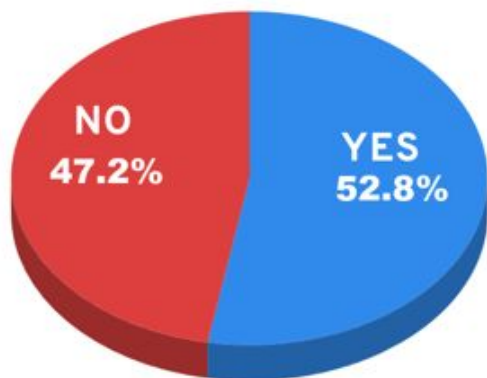
GitHub: chris-short



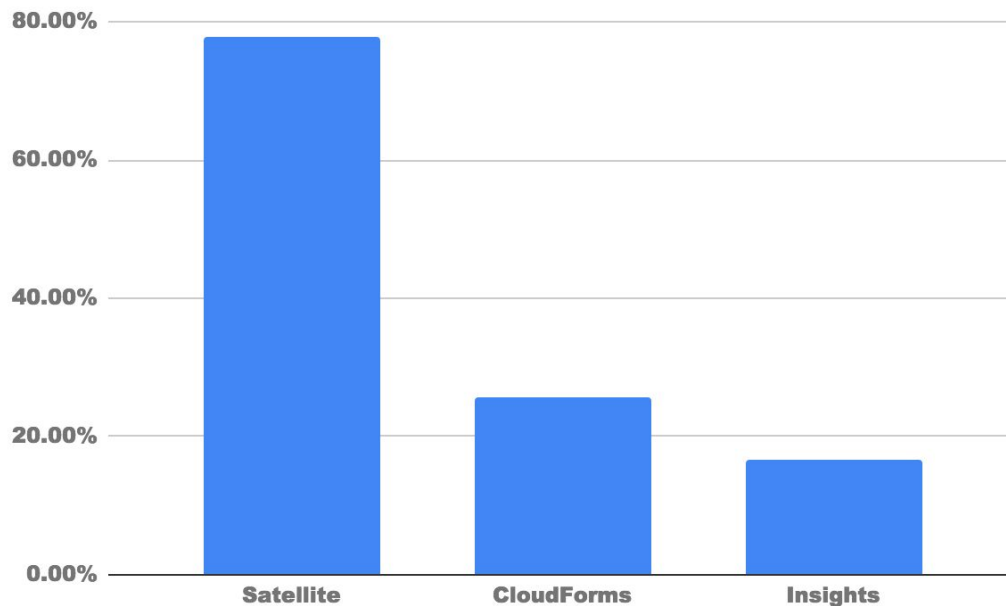
ANSIBLE

RED HAT MANAGEMENT AND YOU

USE RED HAT PRODUCTS
OTHER THAN ANSIBLE?



IF YES, WHICH MANAGEMENT PRODUCTS?



RED HAT MANAGEMENT PORTFOLIO

RED HAT MANAGEMENT PORTFOLIO

**ANSIBLE
TOWER**
by Red Hat®



**CENTRALIZE
AUTOMATION
GOVERNANCE**

Centralized Control
Team & User Delegation
Audit Trail

**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
INFRASTRUCTURE**

Governance
Self-Service Provisioning
Policy-driven Compliance

ANSIBLE

AUTOMATE YOUR I.T. PROCESSES & DEPLOYMENTS

MANAGEMENT & AUTOMATION JOURNEY

RED HAT®
SATELLITE



RED HAT®
INSIGHTS



 **RED HAT®**
ANSIBLE®
Automation



RED HAT®
CLOUDFORMS®



MANAGEMENT & AUTOMATION JOURNEY

RED HAT®
SATELLITE

Insights
inside
Satellite
5.7 and 6.1

RED HAT®
INSIGHTS

 **RED HAT®**
ANSIBLE®
Automation

RED HAT®
CLOUDFORMS®

MANAGEMENT & AUTOMATION JOURNEY

**RED HAT®
SATELLITE**



Insights
inside
Satellite
5.7 and 6.1



**RED HAT®
INSIGHTS**



**RED HAT®
ANSIBLE®
Automation**



Ansible
integrated
with
CloudForms



**RED HAT®
CLOUDFORMS®**



MANAGEMENT & AUTOMATION JOURNEY

RED HAT®
SATELLITE

Insights
inside
Satellite
5.7 and 6.1

RED HAT®
INSIGHTS

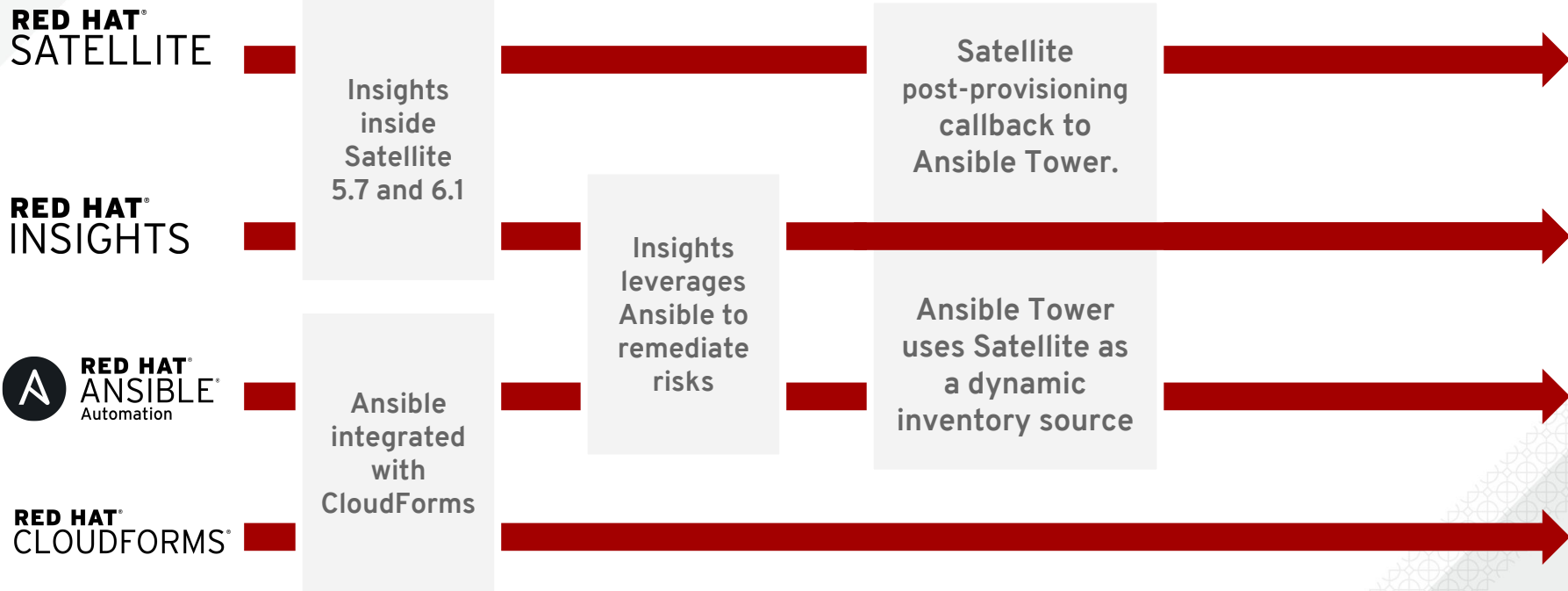
Insights
leverages
Ansible to
remediate
risks

RED HAT®
ANSIBLE®
Automation

Ansible
integrated
with
CloudForms

RED HAT®
CLOUDFORMS®

MANAGEMENT & AUTOMATION JOURNEY



MANAGEMENT & AUTOMATION JOURNEY

**RED HAT®
SATELLITE**

Insights
inside
Satellite
5.7 and 6.1

Satellite
post-provisioning
callback to
Ansible Tower.

Satellite 6.4
enhanced
integration with
Ansible

**RED HAT®
INSIGHTS**

Insights
leverages
Ansible to
remediate
risks

Ansible Tower
uses Satellite as
a dynamic
inventory source

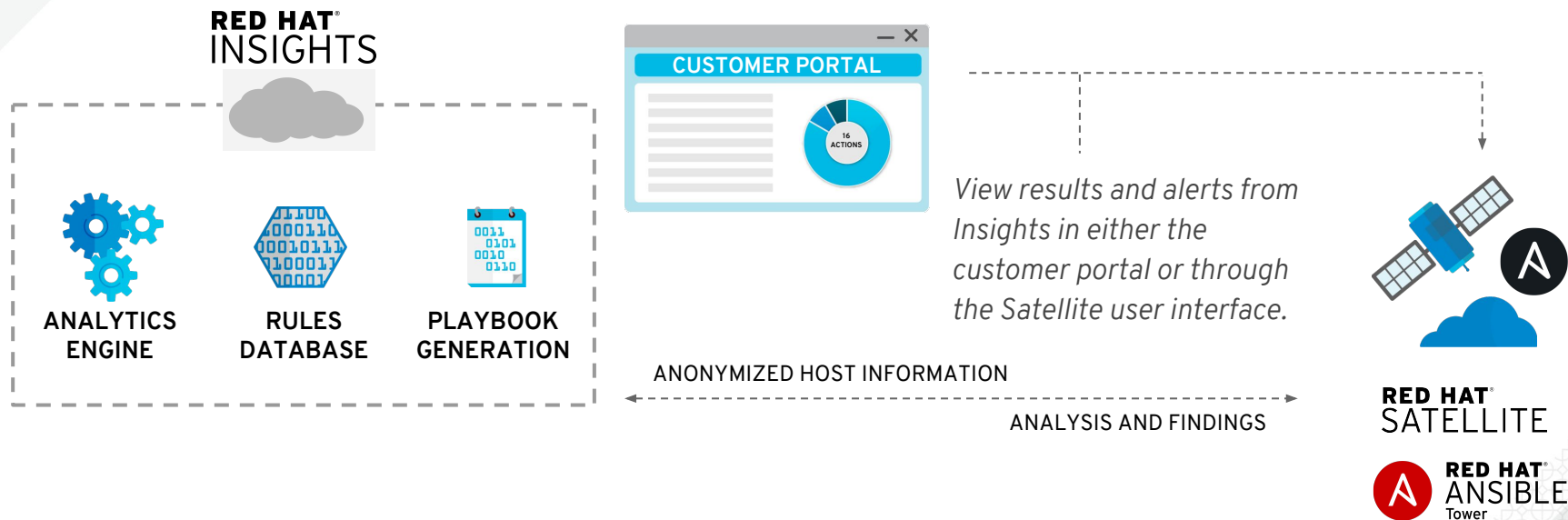
Run Ansible
playbooks from
within Satellite
6.4

**RED HAT®
ANSIBLE®
Automation**

Ansible
integrated
with
CloudForms

**RED HAT®
CLOUDFORMS®**

DELIVERING INTELLIGENT AUTOMATION



INSIGHTS

RED HAT® INSIGHTS

PREDICT RISK. GET GUIDANCE. STAY SECURE.

PREDICTIVE I.T. ANALYTICS

AUTOMATED EXPERT ASSESSMENT

AUTOMATED REMEDIATION

Overview

Actions

Inventory

Planner

Rules

Executive Report

Configuration

Customer Portal

Logout

Executive Report

[Download PDF](#)

Overall score



Weekly action count by category

5⁺
SECURITY

4⁻
AVAILABILITY

2⁻
STABILITY

0⁻
PERFORMANCE

✔ You've resolved **3 issues** in the past 30 days.

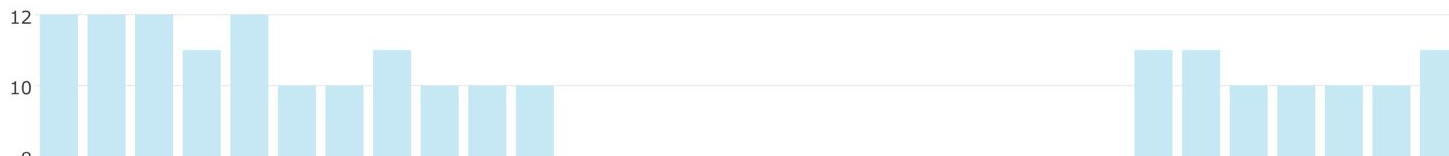
ACTION TRENDS

ACTIVE SYSTEMS

SCORE HISTORY

ALL RULE HITS

Category



Security

Red Hat Insights not only detects security issues, it also strives to let you know whether these issues leave you in a vulnerable state. SSL exploits, remote access, and local privilege escalation issues can lead to compromised data and data loss. Review and resolve these security issues to ensure your systems and data are kept safe.

INSIGHTS PLANS WITH ANSIBLE PLAYBOOKS

Solve common issues through Ansible Automation

Rule	Likelihood	Impact	Total Risk	Systems	Ansible
OpenSSH vulnerable to remote password guessing attack (CVE-2015-5600)	High	High	Critical	16	Ansible
Kernel key management subsystem vulnerable to local privilege escalation (CVE-2016-0728)	Medium	Medium	High	1	Ansible
Kernel vulnerable to privilege escalation via permission bypass (CVE-2016-5195)	Medium	Medium	High	1	Ansible
Kernel vulnerable to man-in-the-middle via payload injection (CVE-2016-5696)	Medium	High	Critical	1	Ansible

- Overview
- Actions
- Inventory
- Planner
- Rules
- Executive Reports
- Configuration
- Customer Portal
- Logout

CriticalIssues (36753)  

Actions Systems **Playbook**





INSIGHTS PLANS WITH ANSIBLE PLAYBOOKS

Solve common issues through Ansible Automation

OpenSSH vulnerable to remote password guessing attack (CVE-2015-5600) [Edit](#)

 Impact	 Likelihood	 Total Risk	Status
			✓

Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491) [Edit](#)

 Impact	 Likelihood	 Total Risk	
System	Last check in	Status	
 rhaiclient.example.com	a day ago	✓	

[Download Playbook](#) [Export CSV](#) [Add actions](#)

INSIGHTS AND ANSIBLE TOWER INTEGRATION

Connect Insights to Tower through projects and templates



Red Hat Insights can easily be integrated with Red Hat Ansible® Tower.

Single steps to integrate

1. Create Insights Credentials
2. Insights scan (link Tower & Insights)
3. Planner sync
4. Remediate

NEW CREDENTIAL

DETAILS PERMISSIONS

* NAME ? DESCRIPTION ? ORGANIZATION ?

* CREDENTIAL TYPE ?

TYPE DETAILS

* USERNAME * PASSWORD

SAVE

CREATE INSIGHTS CREDENTIALS

CREDENTIALS 8

SEARCH

+ ADD

NAME	KIND	OWNERS	ACTIONS
------	------	--------	---------

Available network credentials	Machine	admin, Red Hat's Management BU	[Edit] [Delete]
-------------------------------	---------	--------------------------------	-----------------

NEW PROJECT



DETAILS

PERMISSIONS

NOTIFICATIONS

* NAME
Insights Sync Project

DESCRIPTION
Sync with Insights

* ORGANIZATION
Red Hat's Management BU Example.com

* SCM TYPE
Red Hat Insights

SOURCE DETAILS

* CREDENTIAL
Insights Credential

SCM UPDATE OPTIONS
 Clean
 Delete on Update



SAVE

PROJECTS 5

SEARCH



KEY

+ ADD

- ISSUE: sudo vulnerable to local privilege escalation via process TTY name parsing (CVE-2017-1000368) impact: Local Privilege Escalation** SECURITY
 A local privilege escalation flaw was found in `sudo`. A local user having sudo access on the system, could use this flaw to execute arbitrary commands as root. This issue was reported as [CVE-2017-1000368](https://access.redhat.com/security/cve/CVE-2017-1000368)
- ISSUE: NetworkManager DHCP potentially vulnerable to remote code execution (CVE-2018-1111)** SECURITY
 A command injection vulnerability was found in the DHCP script provided by `dhclient`, located in `/etc/NetworkManager/dispatcher.d/11-dhclient`. An attacker on the local network who is able to spoof DHCP responses or run a malicious DHCP server can execute arbitrary commands with root privileges on DHCP client systems by exploiting this vulnerability.
- ISSUE: Kernel vulnerable to privilege escalation via permission bypass (CVE-2016-5195)** SECURITY
 A flaw was found in the Linux kernel's memory subsystem. An unprivileged local user could use this flaw to write to files they would normally only have read-only access to and thus increase their privileges on the system.
- ISSUE: Kernel vulnerable to man-in-the-middle via payload injection (CVE-2016-5696)** SECURITY
 A flaw in the Linux kernel's TCP/IP networking subsystem implementation of the [RFC 5961](https://tools.ietf.org/html/rfc5961) challenge ACK rate limiting was found that could allow an attacker located on different subnet to inject or take over a TCP connection between a server and client without needing to use a traditional man-in-the-middle (MITM) attack.
- ISSUE: Kernel vulnerable to local privilege escalation via exceptions triggered after the POP SS and MOV to SS instructions (CVE-2018-8897, CVE-2018-1087)** SECURITY
 A flaw was found in the way the Linux kernel's KVM hypervisor handles exceptions triggered after the POP SS and MOV to SS instructions. It has been assigned [CVE-2018-8897](https://access.redhat.com/security/cve/CVE-2018-8897) and [CVE-2018-1087](https://access.redhat.com/security/cve/CVE-2018-1087). These issues could lead to denial of service for unpatched systems. These instructions hold delivery of interrupts, data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction. An unprivileged KVM guest user could use this flaw to crash the guest or potentially escalate their privileges in the guest.
- ISSUE: Decreased security in OpenSSH settings (Ciphers and MACs)** SECURITY
 Recommended security practices for configuring OpenSSH server are not being followed. Some of the earlier OpenSSH HMAC algorithms and ciphers have been found to be vulnerable to attacks.

VIEW DATA IN INSIGHTS REMEDIATE INVENTORY CLOSE

Example.com Satellite Inventory

- DETAILS
- PERMISSIONS
- GROUPS
- HOSTS**
- SOURCES
- COMPLETED JOBS
- REMEDIATE INVENTORY

SEARCH

+ ADD HOST

HOSTS

ACTIONS

SEE RISKS FROM INSIGHTS INSIDE TOWER

ic1.example.com

foreman_location_defaultlocation VIEW MORE

ic2.example.com

foreman_content_view_rhel7

foreman_environment_ktd default_organization_library_rhel7_3

foreman_hostgroup_rhel7

foreman_lifecycle_environment_library

foreman_location_defaultlocation VIEW MORE

foreman_content_view_rhel7

foreman_environment_ktd

foreman_hostgroup_rhel7

foreman_lifecycle_environment_library

Insights Remediation Template

- DETAILS
- PERMISSIONS
- NOTIFICATIONS
- COMPLETED JOBS
- ADD SURVEY

* NAME

DESCRIPTION

* JOB TYPE PROMPT ON LAUNCH

* INVENTORY PROMPT ON LAUNCH

* PROJECT

* PLAYBOOK PROMPT ON LAUNCH

Choose a playbook

- fix-all.yml
- ic1-ic4-fix-all.yml
- ic1-ic4-payload-ssh.yml
- ic8-ic9-all.yml
- payload-injection.yml

* CREDENTIAL PROMPT ON LAUNCH

FORKS

* VERBOSITY PROMPT ON LAUNCH

INSTANCE GROUPS

SKIP TAGS PROMPT ON LAUNCH

LABELS

OPTIONS

- Enable Privilege Escalation
- Allow Provisioning Callbacks
- Enable Concurrent Jobs
- Use Fact Cache

EXTRA VARIABLES

1	---	
---	-----	--

PROMPT ON LAUNCH

SELECT A PLAYBOOK FROM INSIGHTS

DETAILS



STATUS ● Successful

STARTED 9/12/2018 9:35:20 AM

FINISHED 9/12/2018 9:35:56 AM

TEMPLATE [Insights Scan](#)

JOB TYPE Run

LAUNCHED BY [admin](#)

INVENTORY [Example.com Satellite Inventory](#)

PROJECT ● [Insights Facts Playbook](#)
[Download](#)

REVISION 77cbb77

PLAYBOOK [Sample Playbook](#)

MACHINE CREDENTIAL [Example.com](#)

FORKS 0

VERBOSITY 0 (Normal)

INSTANCE GROUP tower

Insights Scan

PLAYS 1 TASKS 8 HOSTS 11 ELAPSED 00:00:36

SEARCH



KEY



```

110 ic1.example.com : ok=4 changed=0 unreachable=0 failed=0
111 ic2.example.com : ok=4 changed=0 unreachable=0 failed=0
112 ic3.example.com : ok=4 changed=0 unreachable=0 failed=0
113 ic4.example.com : ok=4 changed=0 unreachable=0 failed=0
114 ic5.example.com : ok=4 changed=0 unreachable=0 failed=0
115 ic6.example.com : ok=4 changed=0 unreachable=0 failed=0

```

09:35:56



```

120 workstation.example.com : ok=4 changed=0 unreachable=0 failed=0
121

```

^ TOP

ANSIBLE & INSIGHTS

While Insights includes Ansible playbooks for risks, Insights alone can't perform remediation of the risks.

Insights

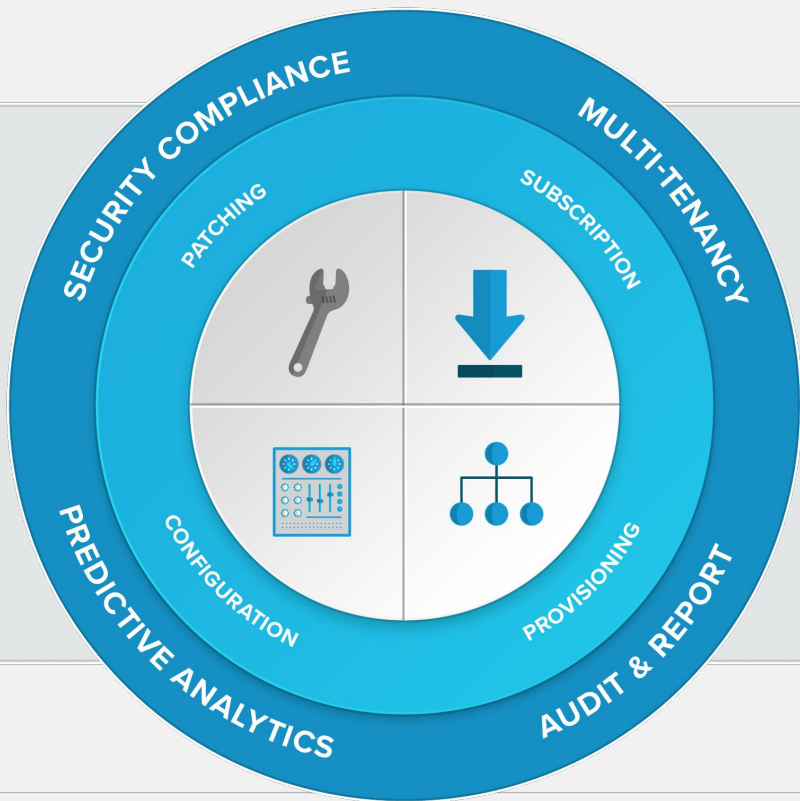
- Insights provides Ansible Playbooks for resolving many common risks.
- Dynamically generates Ansible Playbooks for risk remediation
- Playbooks can be downloaded and run via `ansible-playbook` or Satellite

Insights connected to Ansible Tower

- View identified risks in the Tower inventory
- Execute generated Ansible Playbook as a Tower job
- Use Tower for enterprise risk remediation

SATELLITE

RED HAT SATELLITE



- Define & manage Standard Operating Environments
- Quickly respond to security vulnerabilities (Heartbleed/ShellShock)
- Comply with your organization's security policies
- Deploy all Red Hat Infrastructure as well as third-party software

SATELLITE AND ANSIBLE TOWER INTEGRATION

Documented best practices to help optimize use of both products



By integrating Red Hat Satellite with Red Hat Ansible® Tower, administrators can now perform the following functions:

Dynamic inventory

Allows Ansible Tower to use Satellite as a dynamic inventory source.

Provisioning callbacks

Allows systems provisioned via Satellite to “callback” to Ansible Tower so that playbook runs can happen post-provisioning.

Example.com Satellite credentials

DETAILS

PERMISSIONS

* NAME ? Example.com Satellite credentials

DESCRIPTION ? Example.com Satellite credentials

ORGANIZATION Red Hat's Management BU Example.com

* CREDENTIAL TYPE ? Red Hat Satellite 6

TYPE DETAILS

* SATELLITE 6 URL ? https://sat.example.com

* USERNAME admin

* PASSWORD REPLACE ENCRYPTED

SAVE



CREDENTIALS 9

SEARCH [] []

KEY []

+ ADD

NAME ^	KIND	OWNERS	ACTIONS
--------	------	--------	---------

Available network credentials	Machine	admin, Red Hat's Management BU	[] []
-------------------------------	---------	--------------------------------	---------

PROVISIONING CALLBACKS

A definition straight from the Tower documentation

Provisioning callbacks are a feature of Tower that allow a host to initiate a playbook run against itself, rather than waiting for a user to launch a job to manage the host from the tower console.

- Monitor
- Content
- Containers
- Hosts
- Configure
- Infrastructure
- Insights
- Administer

Provisioning Templates

ansible_ Search

Create Template Build PXE Default Documentation

Name	Host Group / Environment	Kind	Snippet	Locked	Actions
ansible_provisioning_callback			✓	🔒	Clone
ansible_tower_callback_script			✓	🔒	Clone
ansible_tower_callback_service			✓	🔒	Clone
Kickstart default		Provisioning template		🔒	Clone
ansible_tower_callback		Finish template		🔒	Clone
[RHTE] Kickstart default			✓		Clone
[RHTE] Kickstart default finish			✓		Clone
Satellite Kickstart Default		Provisioning template		🔒	Clone
Satellite Kickstart Default		Provisioning template		🔒	Clone
Satellite Kickstart Default		Finish template		🔒	Clone

POST-PROVISIONING CALLBACK

- Monitor
- Content
- Containers
- Hosts
- Configure
- Infrastructure
- Insights
- Administer

Template Type Association History Locations Organizations Help

Warning! This template is locked. You may only change the associations. Please clone it to customize.

Name * Satellite Kickstart Default

```

if salt_enabled %>
  snippet 'puppet_setup' %>
end -%>

if salt_enabled %>
  snippet 'saltstack_setup' %>
end -%>

= snippet('ansible_provisioning_callback') %>

nc

if @provisioning_type == nil || @provisioni
form
Inf
/root/install.post.Log

```

POST-PROVISIONING CALLBACK

Submit Cancel

Audit Comment field is saved with the template auditing to document the template changes

RED HAT SATELLITE Default Organisation Any Location Admin User

Monitor Content Containers Hosts Configure Infrastructure Insights Administer

Create Template Build PXE Default Documentation

Name	Host Group / Environment	Kind	Snippet	Locked	Actions
ansible_provisioning_callback			✓	🔒	Clone
ansible_tower_callback_script			✓	🔒	Clone
ansible_tower_callback_service			✓	🔒	Clone
Kickstart default		Provisioning template		🔒	Clone
		Finish template		🔒	Clone
kickstart default finish			✓		Clone
			✓		Clone
			✓		Clone
[RHTE] Kickstart default finish		Provisioning template			Clone
[RHTE] Kickstart default finish		Finish template			Clone
Satellite Kickstart Default		Provisioning template		🔒	Clone
Satellite Kickstart Default clone		Provisioning template			Clone
Satellite Kickstart Default Finish		Finish template		🔒	Clone

20 per page 1-13 of 13

POST-PROVISIONING CALLBACK

- Monitor
- Content
- Containers
- Hosts
- Configure
- Infrastructure
- Insights
- Administer

Template Type Association History Locations Organizations Help

Warning! This template is locked. You may only change the associations. Please [clone](#) it to customize.

Name *

Default

Template *

Input Diff Preview Fullscreen ruby Default

```
<%>
kind: snippet
name: ansible_provisioning_callback
model: ProvisioningTemplate
snippet: true
<%>
<% if host_param_true?('ansible_tower_provisioning') -%>
<%>
  rhel_compatible = @host.operatingsystem.family == 'Redhat' && @host.operatingsystem.name != 'Fedora'
  os_major = @host.operatingsystem.major.to_i
  has_systemd = (@host.operatingsystem.name == 'Fedora' && os_major >= 20) || (rhel_compatible && os_major >= 7)
<%>
<% if has_systemd -%>
<% save_to_file('/etc/systemd/system/ansible-callback.service',
  snippet('ansible_tower_callback_service')) %>
# Runs during first boot, removes itself
```

POST-PROVISIONING CALLBACK

The Audit Comment field is saved with the template auditing to document the template changes

Submit Cancel


```
<%#
kind: snippet
name: ansible_provisioning_callback
model: ProvisioningTemplate
snippet: true
-%>
<% if host_param_true?('ansible_tower_provisioning') -%>
<%
  rhel_compatible = @host.operatingsystem.family == 'Redhat' && @host.operatingsystem.name != 'Fedora'
  os_major = @host.operatingsystem.major.to_i
  has_systemd = (@host.operatingsystem.name == 'Fedora' && os_major >= 20) || (rhel_compatible && os_major >= 7)
-%>
<% if has_systemd -%>
<%= save_to_file('/etc/systemd/system/ansible-callback.service',
  snippet('ansible_tower_callback_service')) %>
# Runs during first boot, removes itself
systemctl enable ansible-callback
<% else -%>
# Assume systemd is not available
<%= save_to_file('/root/ansible_provisioning_call.sh', snippet('ansible_tower_callback_script')) %>
(crontab -u root -l 2>/dev/null; echo "@reboot /root/ansible_provisioning_call.sh" ) | crontab -u root -
<% end -%>
-%>
```

POST-PROVISIONING CALLBACK

Monitor

Content

Containers

Hosts

Configure

Infrastructure

Insights

Administer

Template *

Input Diff Preview Fullscreen

ruby Default

```

<%#
kind: snippet
name: ansible_tower_callback_service
model: ProvisioningTemplate
snippet: true
-%>
[Unit]
Description=Provisioning callback to Ansible Tower
Wants=network-online.target
After=network-online.target

[Service]
Type=oneshot
ExecStart=/usr/bin/curl -k -s --data "host_config_key=<%= host_param('ansible_host_config_key') -%>" https://<%= host_param
ExecStartPost=/usr/bin/systemctl disable ansible-callback

[Install]
WantedBy=multi-user.target

```

POST-PROVISIONING CALLBACK

The Audit Comment field is saved with the template auditing to document the template changes

Submit Cancel

```
<%=#
kind: snippet
name: ansible_tower_callback_service
model: ProvisioningTemplate
snippet: true
- %>
[Unit]
Description=Provisioning callback to Ansible Tower
Wants=network-online.target
After=network-online.target

[Service]
Type=oneshot
ExecStart=/usr/bin/curl -k -s --data "host_config_key=<%= host_param('ansible_host_config_key') -%>" https://<%= host_param
ExecStartPost=/usr/bin/systemctl disable ansible-callback

[Install]
WantedBy=multi-user.target
|
```

POST-PROVISIONING CALLBACK

```
<%#  
kind: snippet  
name: ansible_tower_callback_service  
model: ProvisioningTemplate  
snippet: true  
-%>
```

```
[Unit]  
Description=Provisioning callback to Ansible Tower  
Wants=network-online.target  
After=network-online.target
```

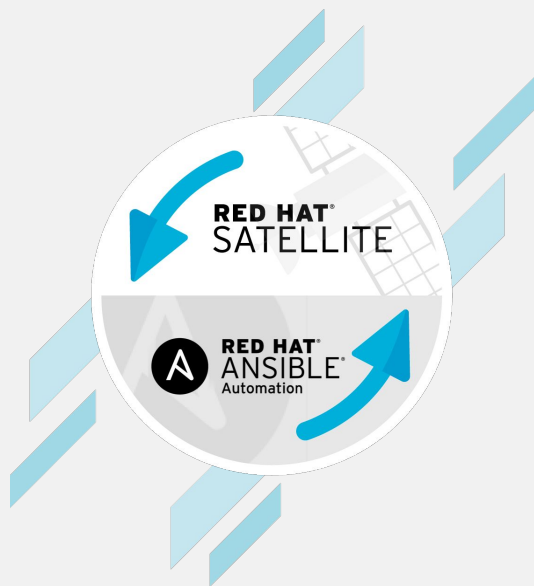
```
[Service]  
Type=oneshot  
ExecStart=/usr/bin/curl -k -s --data "host_config_key=<%=  
host_param('ansible_host_config_key') -%>" https://<%=  
host_param('ansible_tower_fqdn') -%>/api/v2/job_templates/<%=  
host_param('ansible_job_template_id') -%>/callback/
```

```
[Install]  
WantedBy=multi-user.target
```

POST-PROVISIONING CALLBACK

SATELLITE 6.4 - ANSIBLE INTEGRATION

Basic Ansible capabilities are now part of Satellite



Satellite 6.4 has integration with Ansible for the purposes of remote execution and desired state management

Remote Execution

Run Ansible Playbooks inside of Satellite

Deploy Insights using Ansible

Install Insights on all your hosts

RHEL System Roles

Deploy RHEL System Roles to hosts managed by Satellite

DEMO: SATELLITE 6.4, INSIGHTS, & ANSIBLE

The screenshot shows the 'Run / Playbook Builder' dialog box in the Ansible Playbook Builder interface. The dialog has a title bar with a close button. Below the title bar, there are four radio button options: 'Create new play', 'Add to existing play', 'Override group', and 'Specify system'. The 'Add to existing play' option is selected. To the right of these options are three input fields: 'Play name', 'Play description', and 'Play tags'. Below these options is a section titled 'Actions available for your inventory' which contains a table of actions. The table has columns for 'Action', 'Type', 'Status', and 'Affected Systems'. The first row is 'Action', which is highlighted in blue. Below the table, there is a 'Filter by user roles' section with a search bar and a list of roles. At the bottom right of the dialog, there are 'Cancel' and 'Save' buttons.

Run / Playbook Builder

Create new play

Add to existing play

Override group

Specify system

All selected

Play name

Play description

Play tags

Actions available for your inventory

Action	Type	Status	Affected Systems
Action			
Action			
Action			

Filter by user roles

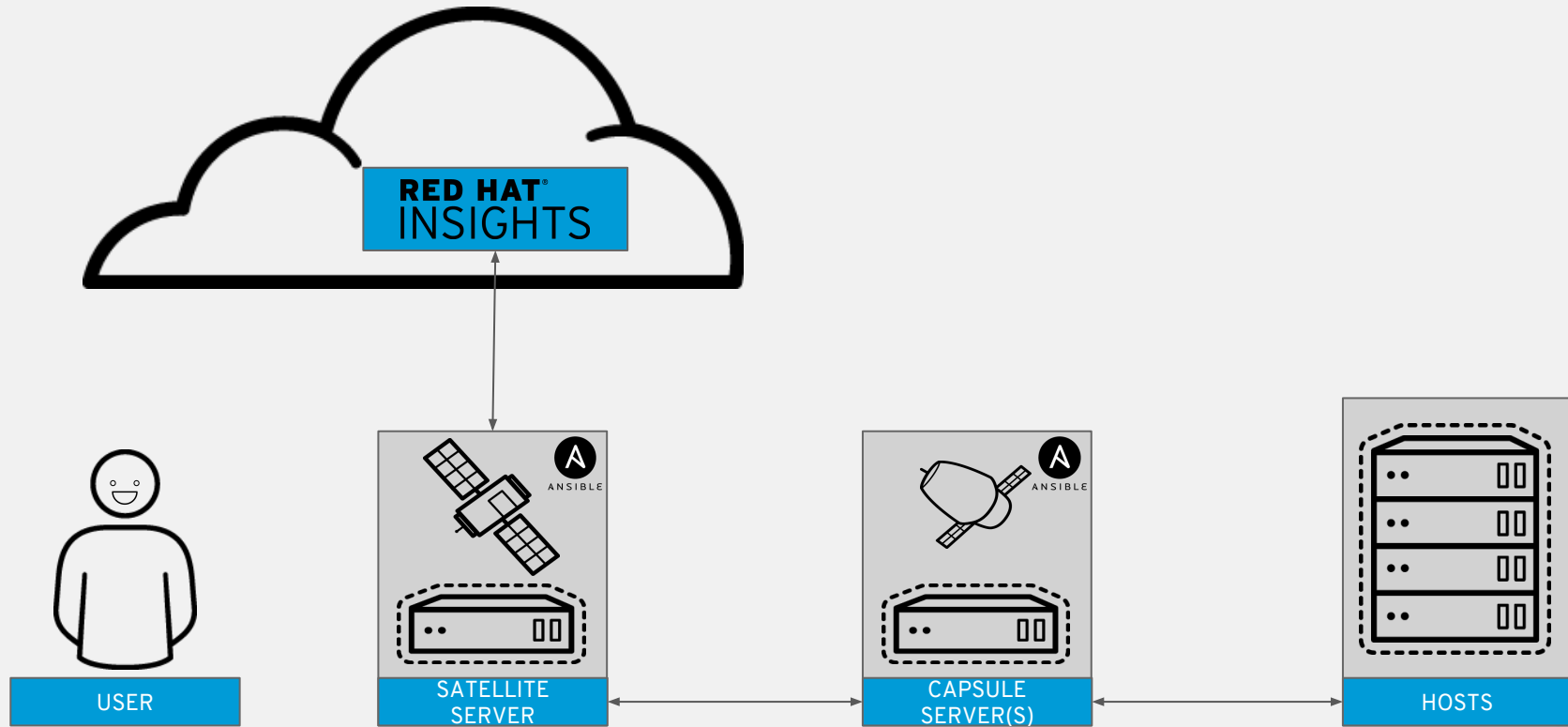
Cancel Save

The action is selected, so click Save.

That was magical...

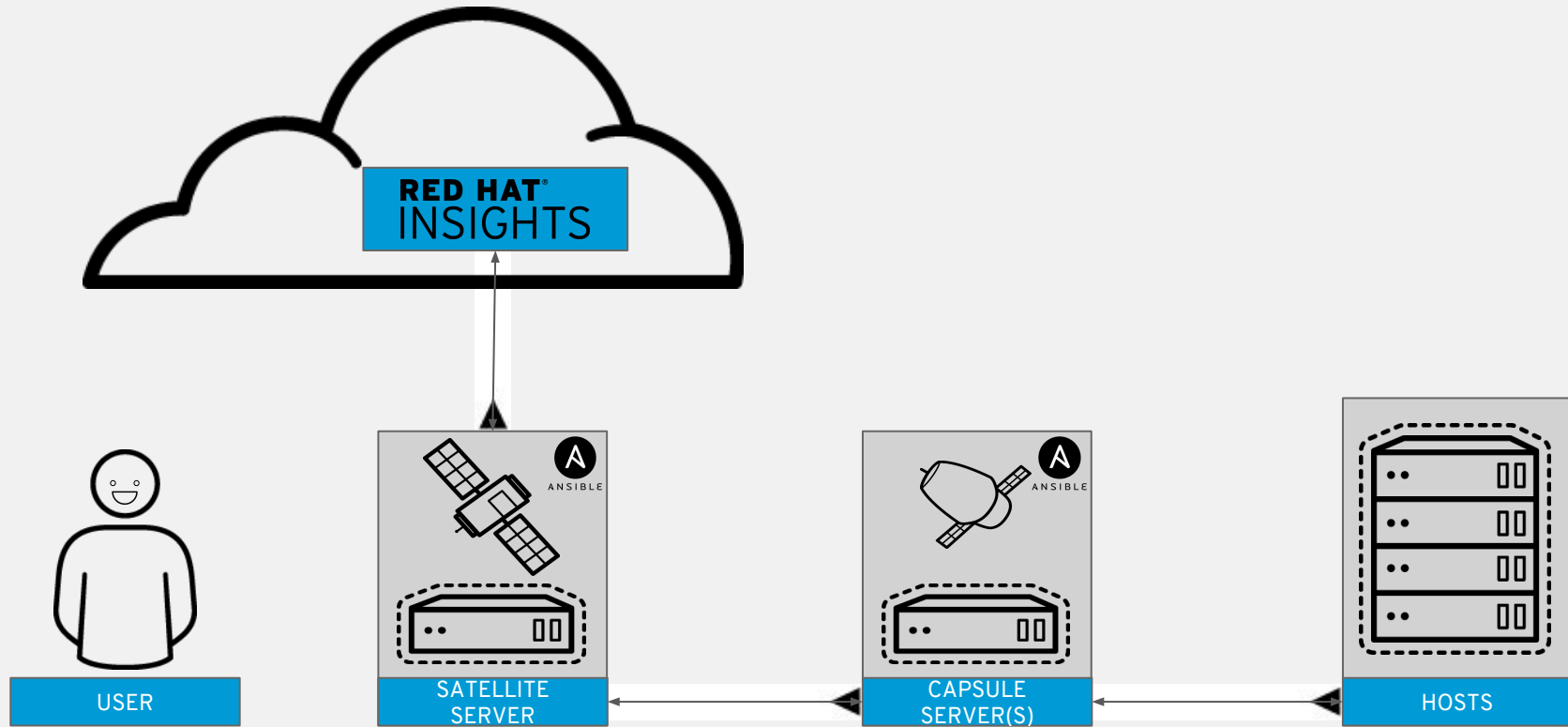
How does this work?

Basic Communication Flow



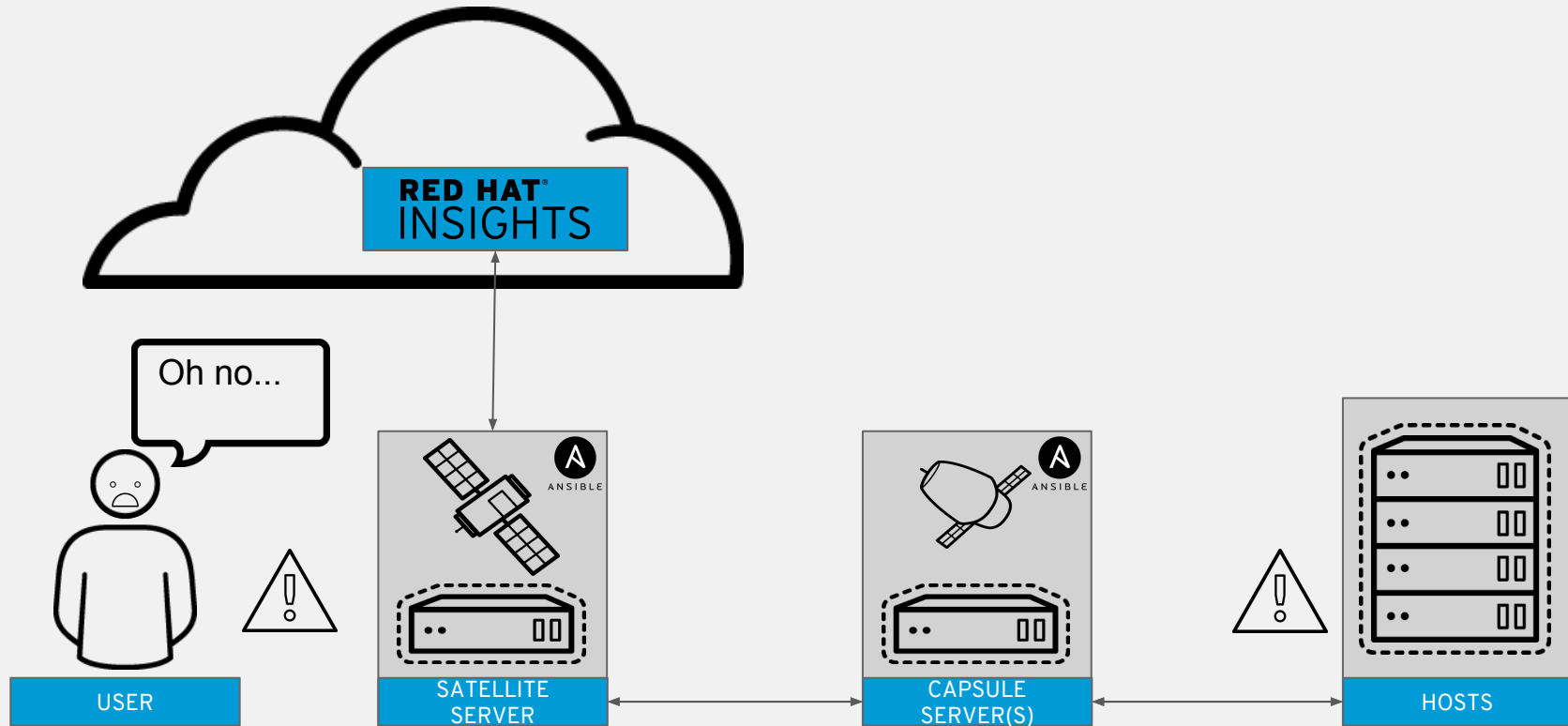
Data Sent to Insights for examination

Insights does this daily, automatically



Risk Found!

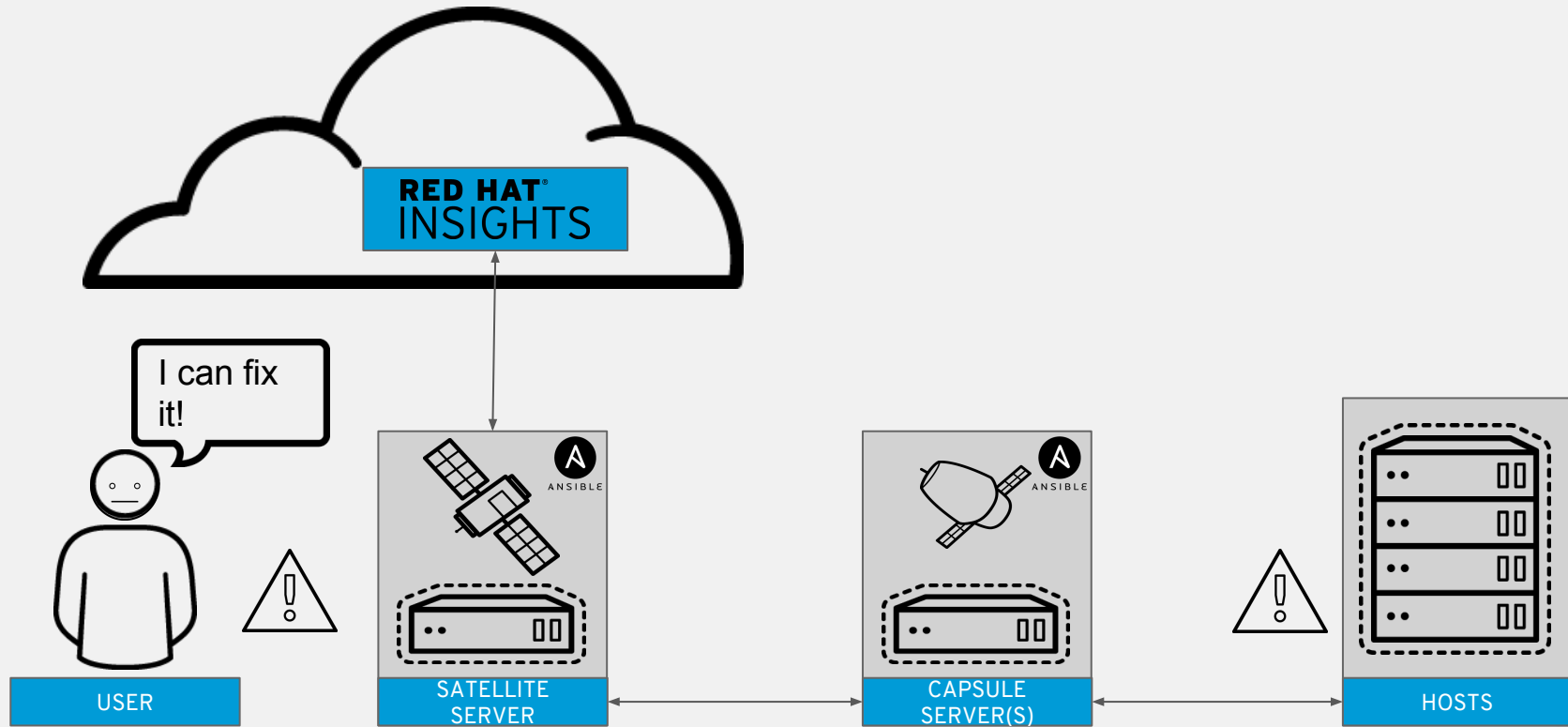
Satellite reads the data from Insights, dashboard widgets show the new risk



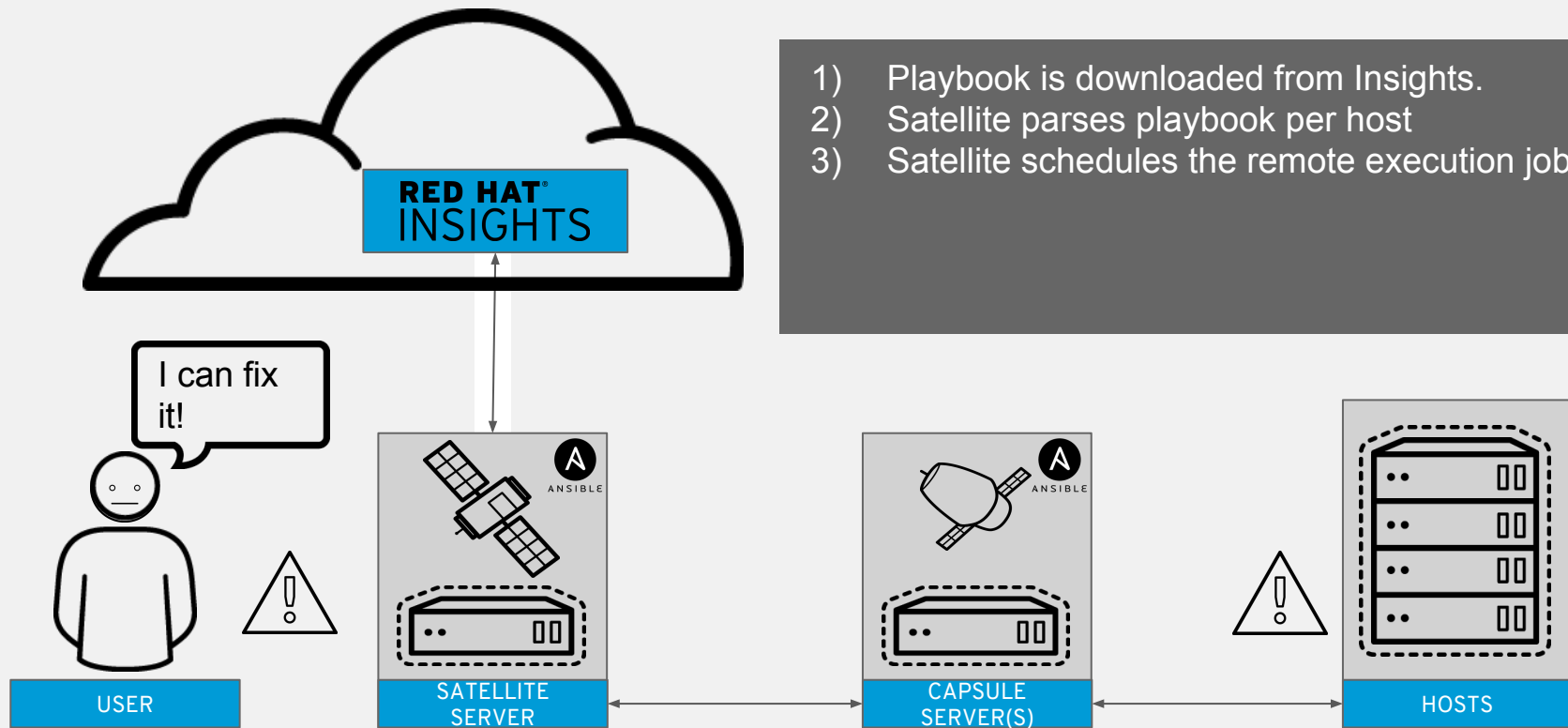
*Satellite does not store any information from Insights in the database. It is all real time.

Create a Remediation Plan

A user creates the remediation plan through Satellite

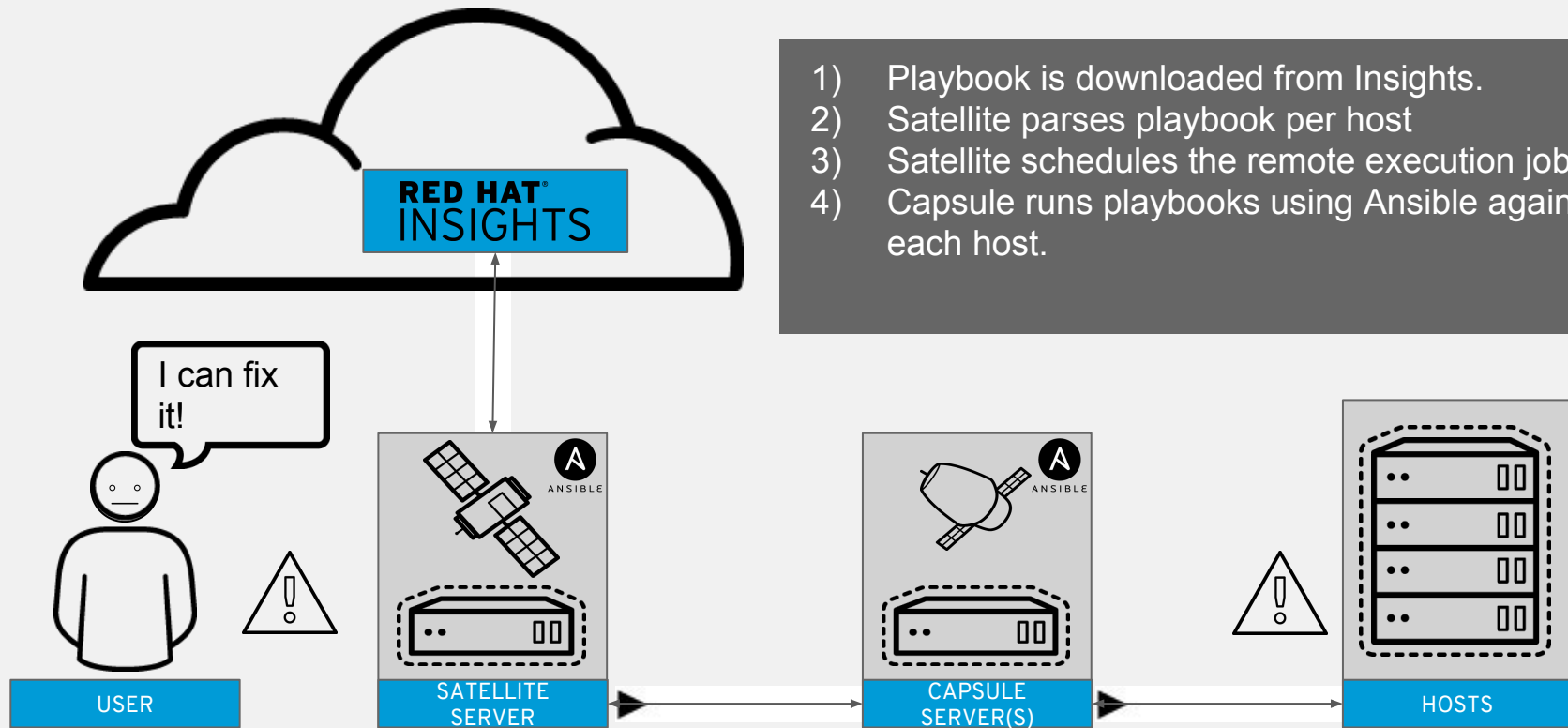


Plan Executes



- 1) Playbook is downloaded from Insights.
- 2) Satellite parses playbook per host
- 3) Satellite schedules the remote execution job(s)

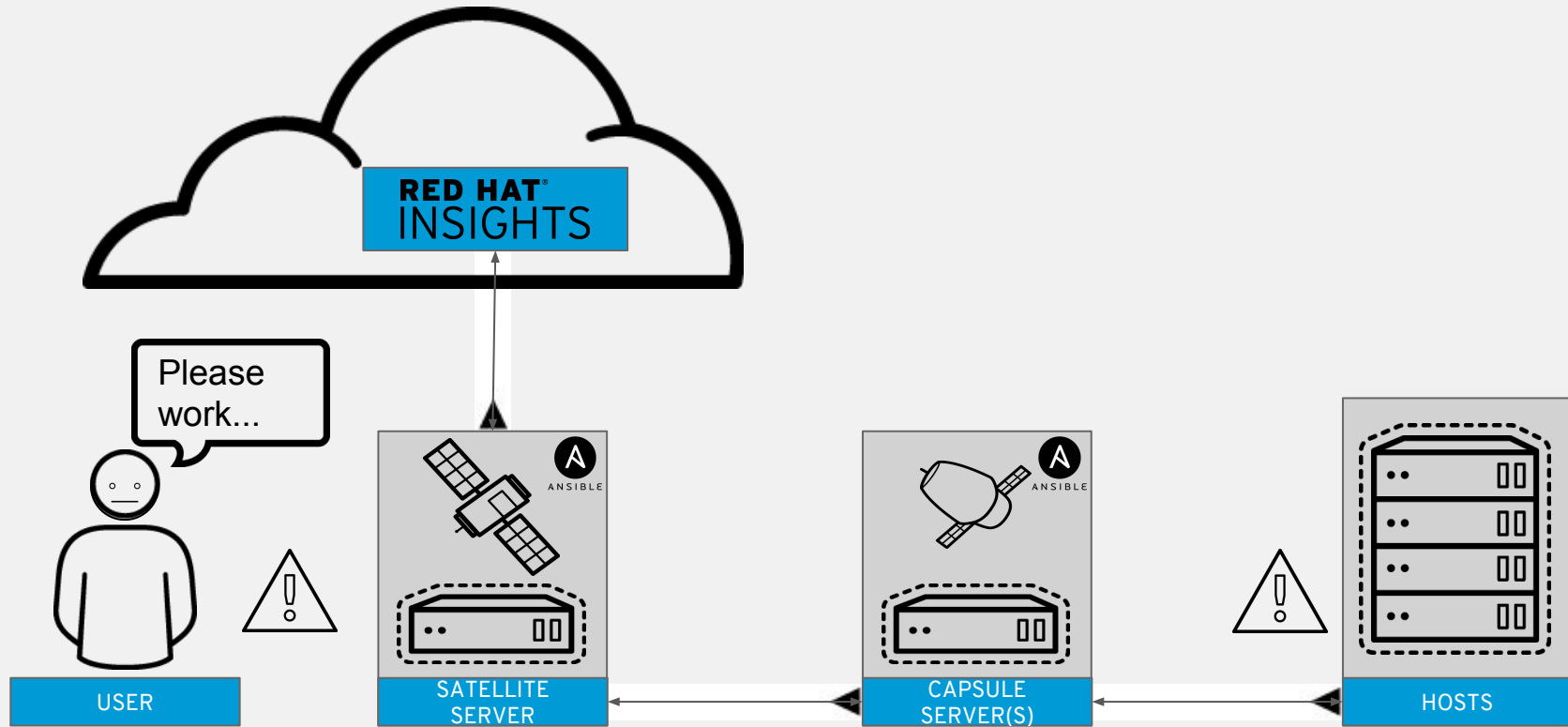
Plan Executes



- 1) Playbook is downloaded from Insights.
- 2) Satellite parses playbook per host
- 3) Satellite schedules the remote execution job(s)
- 4) Capsule runs playbooks using Ansible against each host.

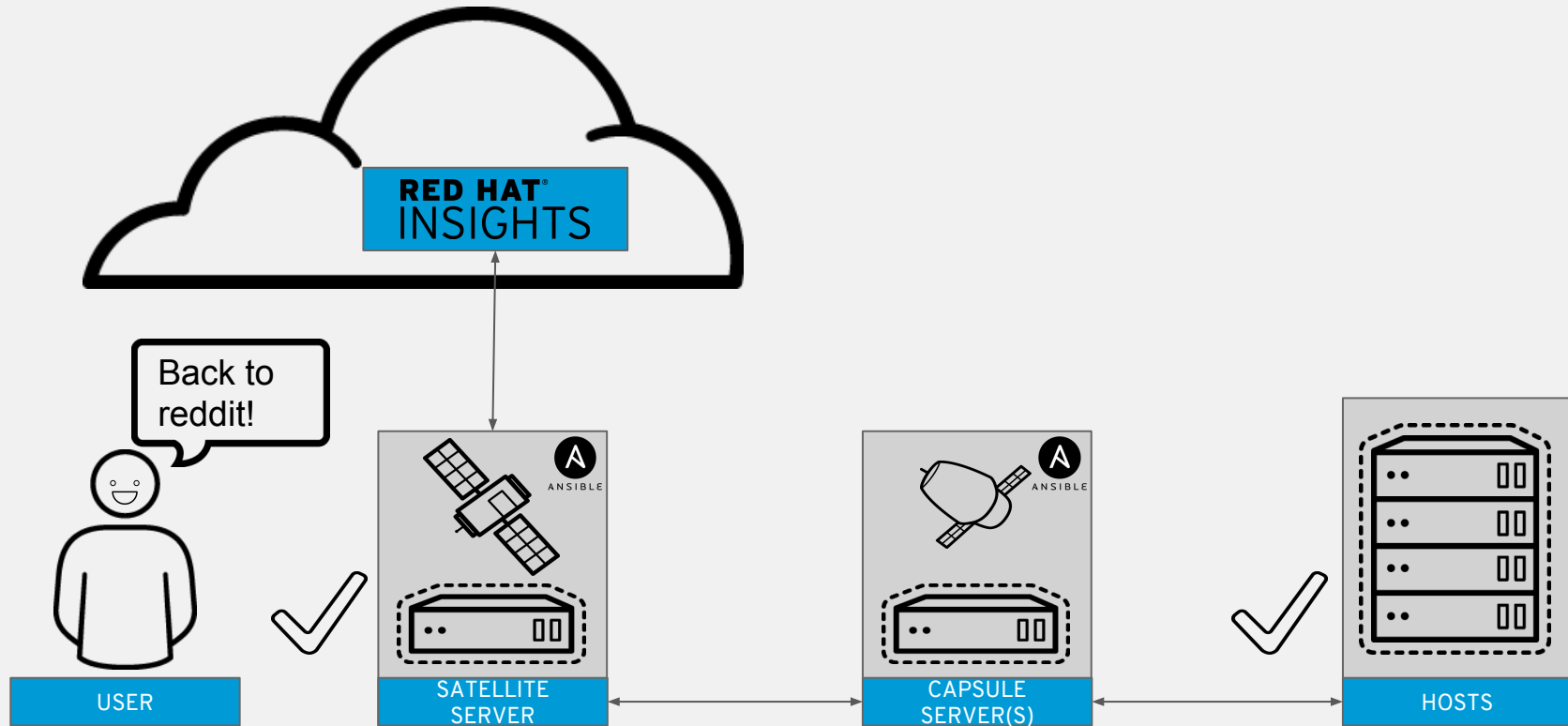
Data Sent to Insights for examination

Rescan is done after remediation completes



Data Sent to Insights for examination

The dashboard will pull updated info from Insights, showing the risk was resolved.



ANSIBLE & SATELLITE

While Satellite has Ansible capabilities built in, Ansible Tower is still critical for enterprise automation

Satellite's use of Ansible is for RHEL-specific purposes

- Ansible Playbooks can be executed against managed RHEL hosts
- Ansible Roles provide desired state
- Automation will be limited to RHEL use cases only

Satellite connected to Ansible Tower

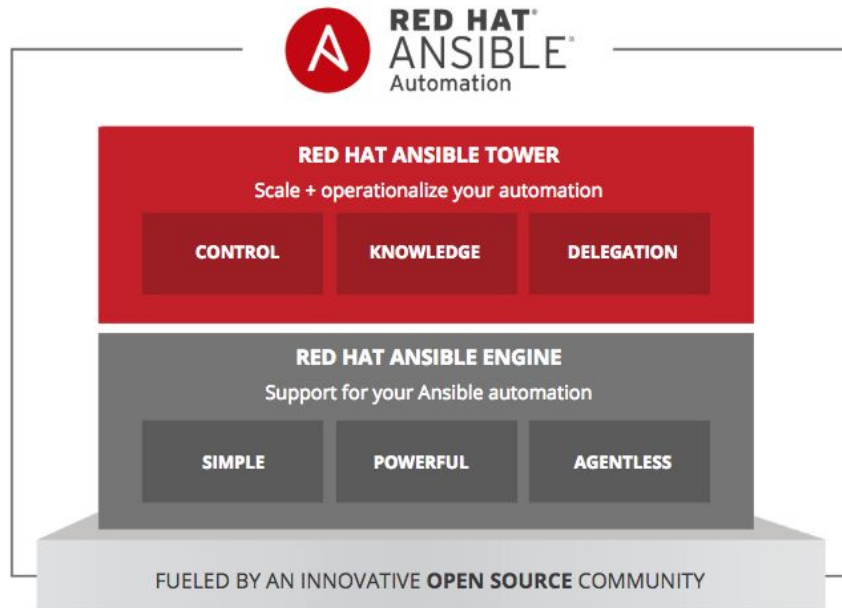
- For enterprise-wide, open-ended IT orchestration and automation
- Management of non-RHEL systems alongside RHEL systems
- Automate Satellite actions alongside other enterprise requirements

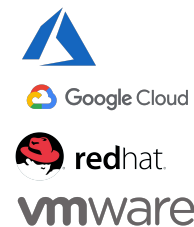
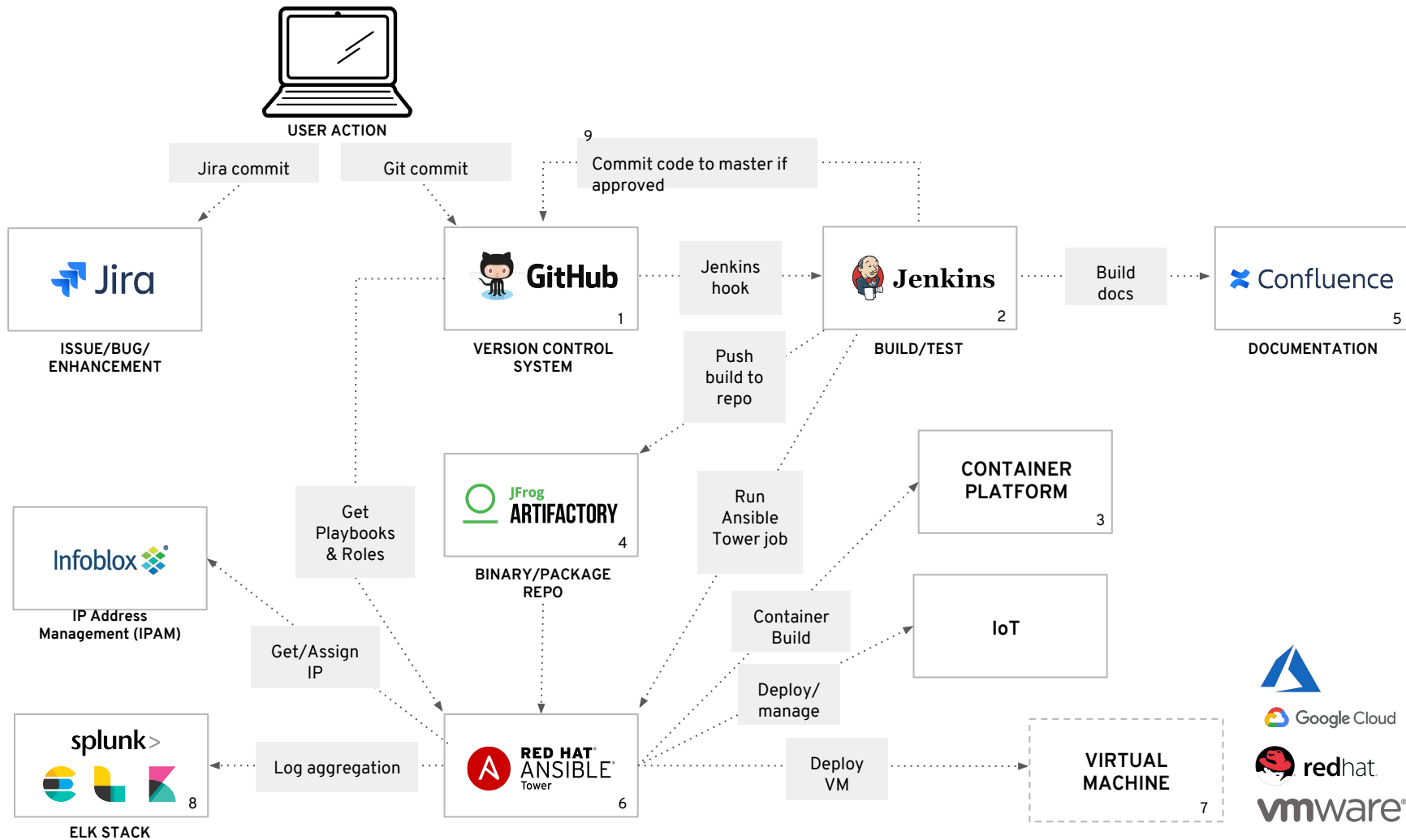
ANSIBLE TOWER

WHAT IS ANSIBLE TOWER?

Ansible Tower is an **enterprise framework** for controlling, securing and managing your Ansible automation – with a **UI and RESTful API**.

- **Role-based access control** keeps environments secure, and teams efficient.
- Non-privileged users can **safely deploy** entire applications with **push-button deployment** access.
- All Ansible automations are **centrally logged**, ensuring **complete auditability and compliance**.



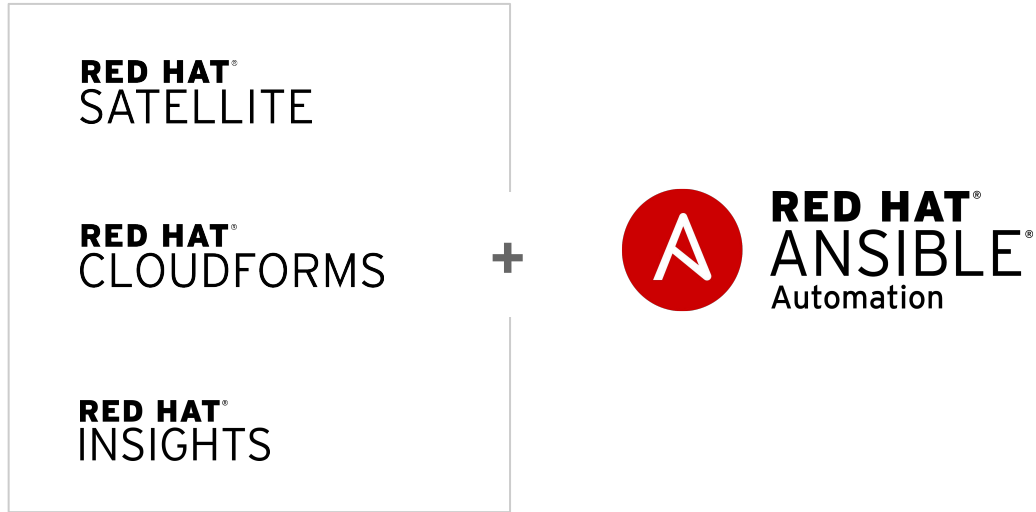


**LOTS OF PRODUCTS,
LOTS OF CAPABILITIES.**

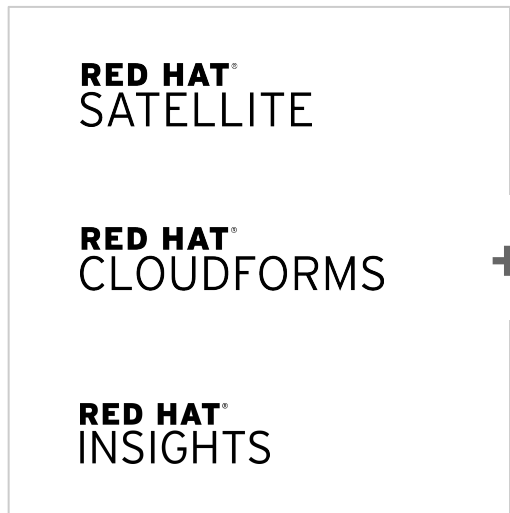
AN AUTOMATED ECOSYSTEM



AN AUTOMATED ECOSYSTEM



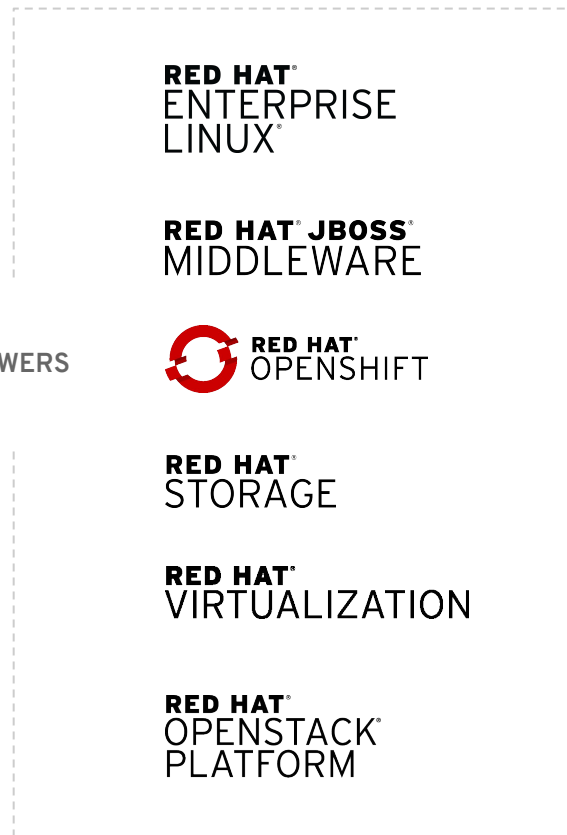
AN AUTOMATED ECOSYSTEM



+



POWERS



NEXT STEPS

- Review the available resources for more information
- Check with your account teams
 - You may already have subscriptions
 - Free evaluations are available

RED HAT®
SATELLITE

Satellite 6.4
Available now



Ansible Engine 2.7
Available now



Ansible Tower 3.4
Available now

Insights Resources

Webpages and Docs:

- Red Hat Insights Product page - <http://access.redhat.com/insights/>
- Red Hat Insights Customer Portal - <https://access.redhat.com/products/red-hat-insights/>
- Red Hat Insights Documentation - https://access.redhat.com/documentation/en-us/red_hat_insights/1.0/
- Red Hat Insights Blog Site - <https://access.redhat.com/blogs/insights>

Videos:

- Vimeo Video: [Proactive detection and remediation using Insights and Ansible Engine](#)
- Vimeo Video: [Proactive issues detection and remediation using Insights and Ansible Tower](#)
- Vimeo video: [Red Hat Insights reporting capabilities into Ansible Tower](#)

Satellite Resources


Webpages and Docs:

- Red Hat Satellite Product page - <http://redhat.com/satellite>
- Red Hat Satellite Customer Portal - <https://access.redhat.com/products/red-hat-satellite>
- Red Hat Satellite Documentation - https://access.redhat.com/documentation/en-us/red_hat_satellite/
- Red Hat Consulting offering: Transition to Red Hat Satellite 6 - <https://www.redhat.com/en/resources/consulting-offering-transition-to-satellite-6-datasheet>

Training:

- **NEW COURSE** - RH053: Satellite Technical Overview: <https://www.redhat.com/en/services/training/rh053-red-hat-satellite-technical-overview>
- RH053 is also on Udemy: <https://www.udemy.com/red-hat-satellite-technical-overview-rh053/>
- RH403: Red Hat Satellite 6 Administration: <https://www.redhat.com/en/services/training/rh403-red-hat-satellite-6-administration>

Videos:

 @ChrisShort YouTube Video: Find It. Fix It. Before It Breaks: <https://youtu.be/mCBhUuxRCgA>

Ansible Resources

Webpages and Docs:

- Ansible page - <https://www.ansible.com/>
- Ansible Documentation - <https://docs.ansible.com/>
- Red Hat Consulting for Ansible: <https://www.ansible.com/products/consulting>

Training:

- <https://www.ansible.com/products/training-certification>
 - AUTOMATION WITH ANSIBLE I (DO407)
 - RED HAT CERTIFICATE OF EXPERTISE IN ANSIBLE AUTOMATION (EX407)
 - AUTOMATION WITH ANSIBLE II: RED HAT ANSIBLE TOWER (DO409)
 - ANSIBLE FOR NETWORK AUTOMATION (DO457)

Questions?

THANK YOU



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



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



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



twitter.com/RedHat