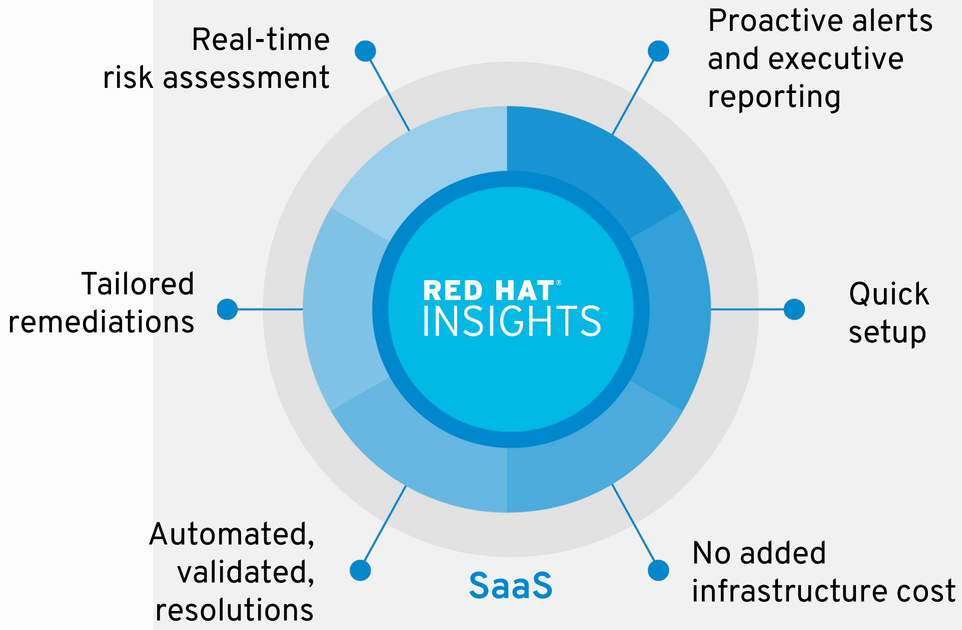
30 MINUTES TO A MORE SECURE, PREDICTABLE, AND STABLE INFRASTRUCTURE

Zbigniew Parys
Solution Architect

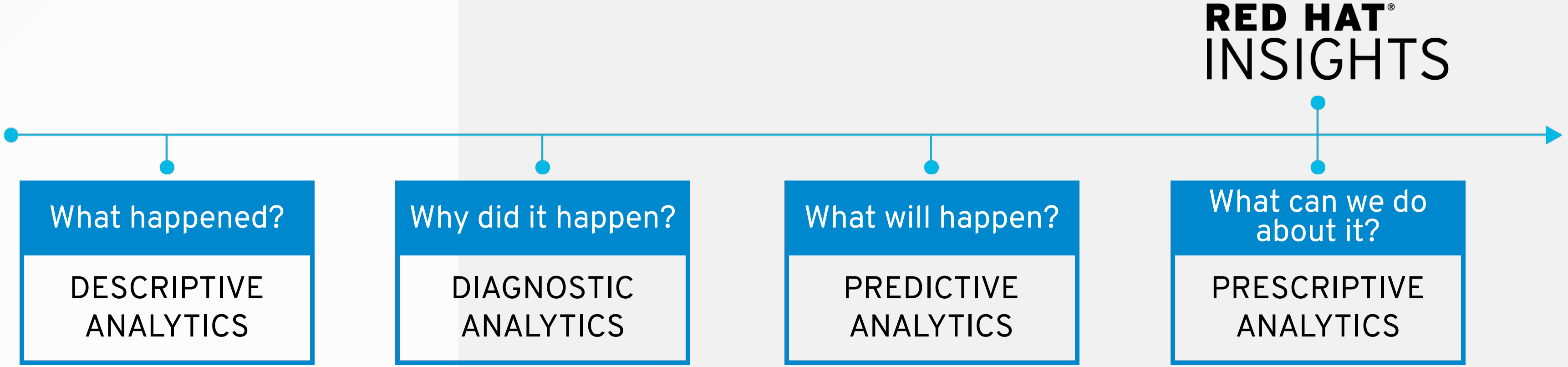
zbigniew.parys@redhat.com

WHAT'S RED HAT® INSIGHTS



Real-time risk assessment
Proactive alerts and executive reporting
Tailored remediations
RED HAT® INSIGHTS
Quick setup
Automated, validated, resolutions
SaaS
No added infrastructure cost

I.T. OPERATIONAL ANALYTICS (ITOA)



RED HAT® INSIGHTS

What happened?
DESCRIPTIVE ANALYTICS

Why did it happen?
DIAGNOSTIC ANALYTICS

What will happen?
PREDICTIVE ANALYTICS

What can we do about it?
PRESCRIPTIVE ANALYTICS

> *" ...by 2018, 25% of the Global 2000 will have deployed an IT Operations Analytics platform (...) up from about 2% today."*

— **WILL CAPPELLI,** *vice president & research analyst* , **Gartner**

WHY RED HAT INSIGHTS?

ACTIONABLE INTELLIGENCE POWERED BY RED HAT

Confidently scale complex environments with no added infrastructure cost.

CONTINUOUS VULNERABILITY ALERTS

Maximize uptime and avoid fire-fighting so businesses can focus on strategic initiatives.

INCREASED VISIBILITY TO SECURITY RISKS

Get ahead of security risks and fix them before businesses are impacted.

AUTOMATED REMEDIATION

Minimize human error, do more with less, and fix things faster.

Beyond Red Hat Satellite

RED HAT® SATELLITE

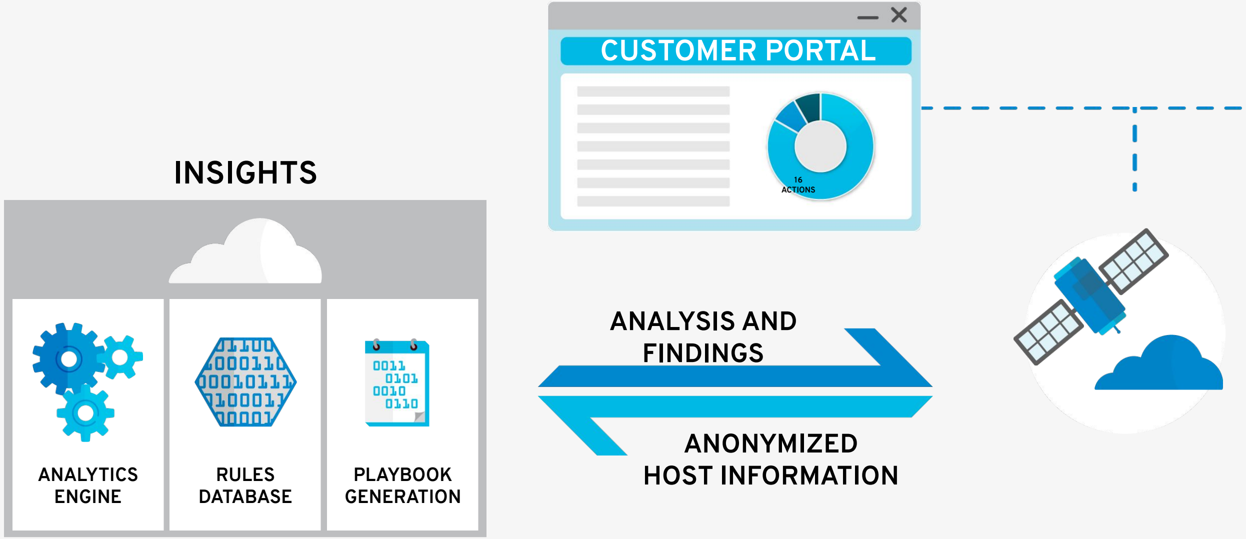
Lifecycle management keeps Red Hat infrastructures

- running efficiently
- properly secured
- compliant

Do you feel comfortable that...

- Your IT environment is operating smoothly and as intended?
- Your team is doing everything possible to avoid disruptions and minimize risk?
- There aren’t any issues you should proactively address?
- What is the least risky method to fix issues or perform maintenance?

RED HAT® INSIGHTS



INSIGHTS

ANALYTICS ENGINE

RULES DATABASE

PLAYBOOK GENERATION

CUSTOMER PORTAL

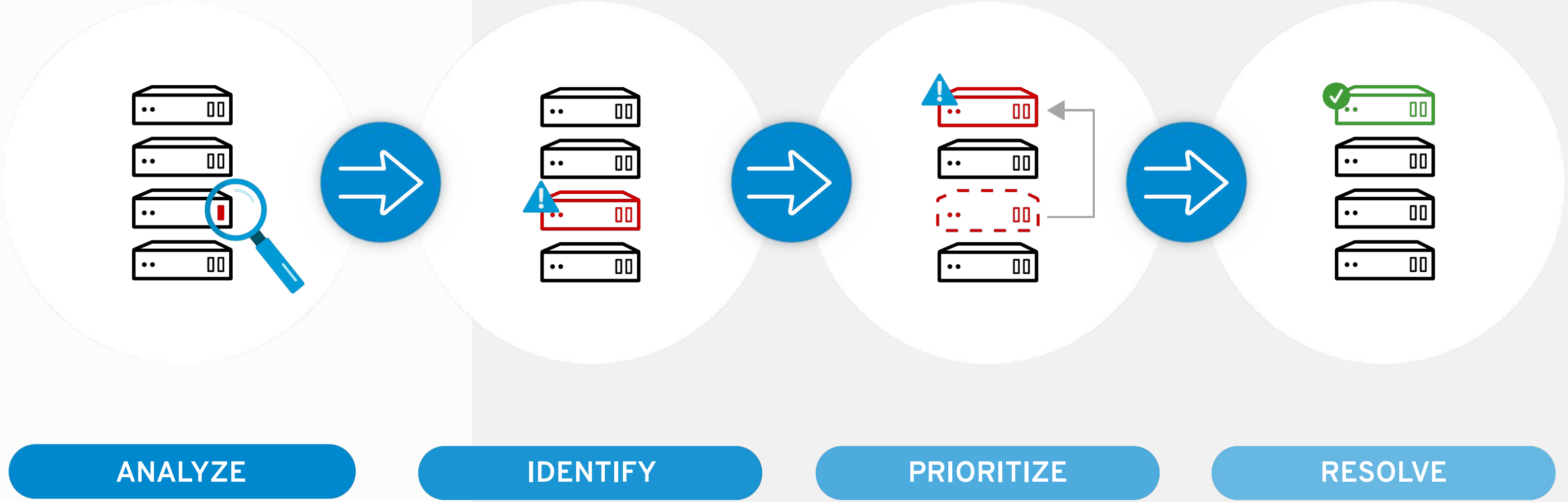
ANALYSIS AND FINDINGS

ANONYMIZED HOST INFORMATION

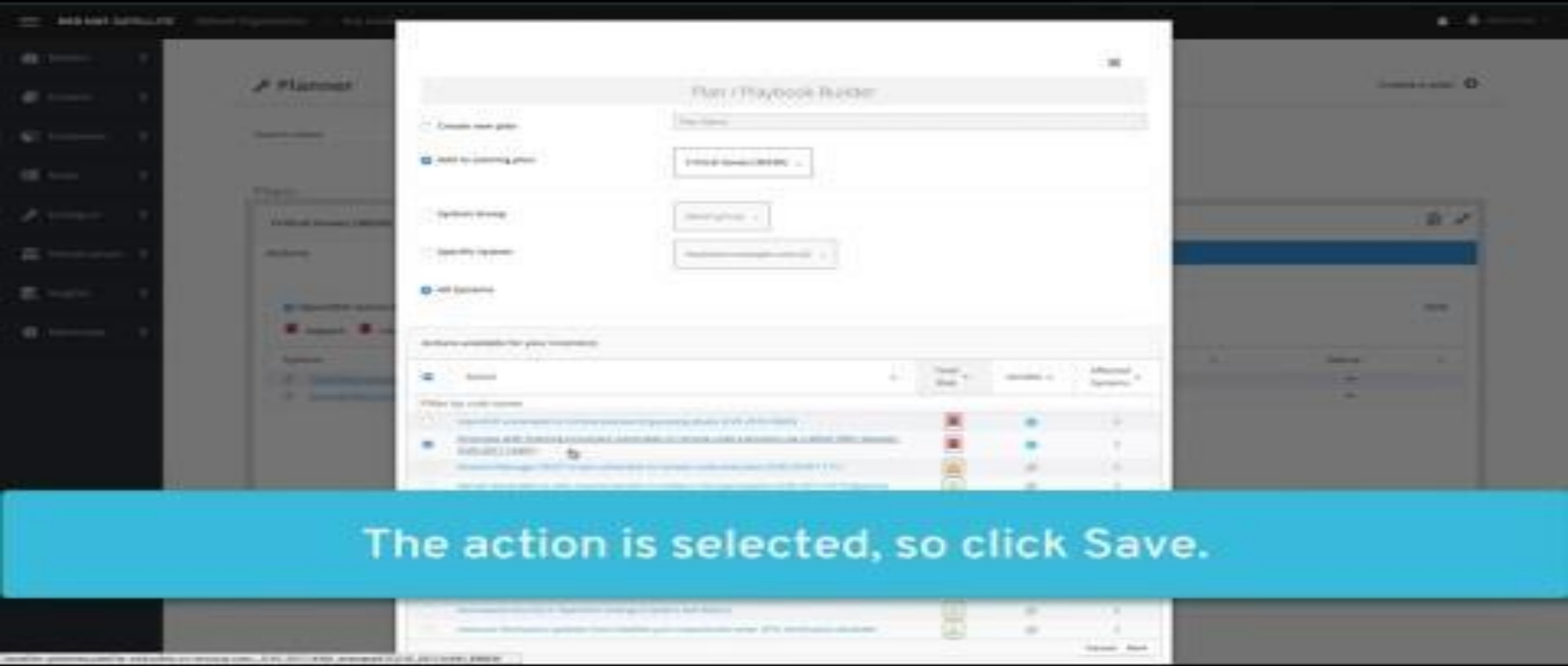
View results and alerts from Insights in either the Customer Portal or through the Satellite user interface.

MANAGING INFRASTRUCTURE RISK

Automated remediation



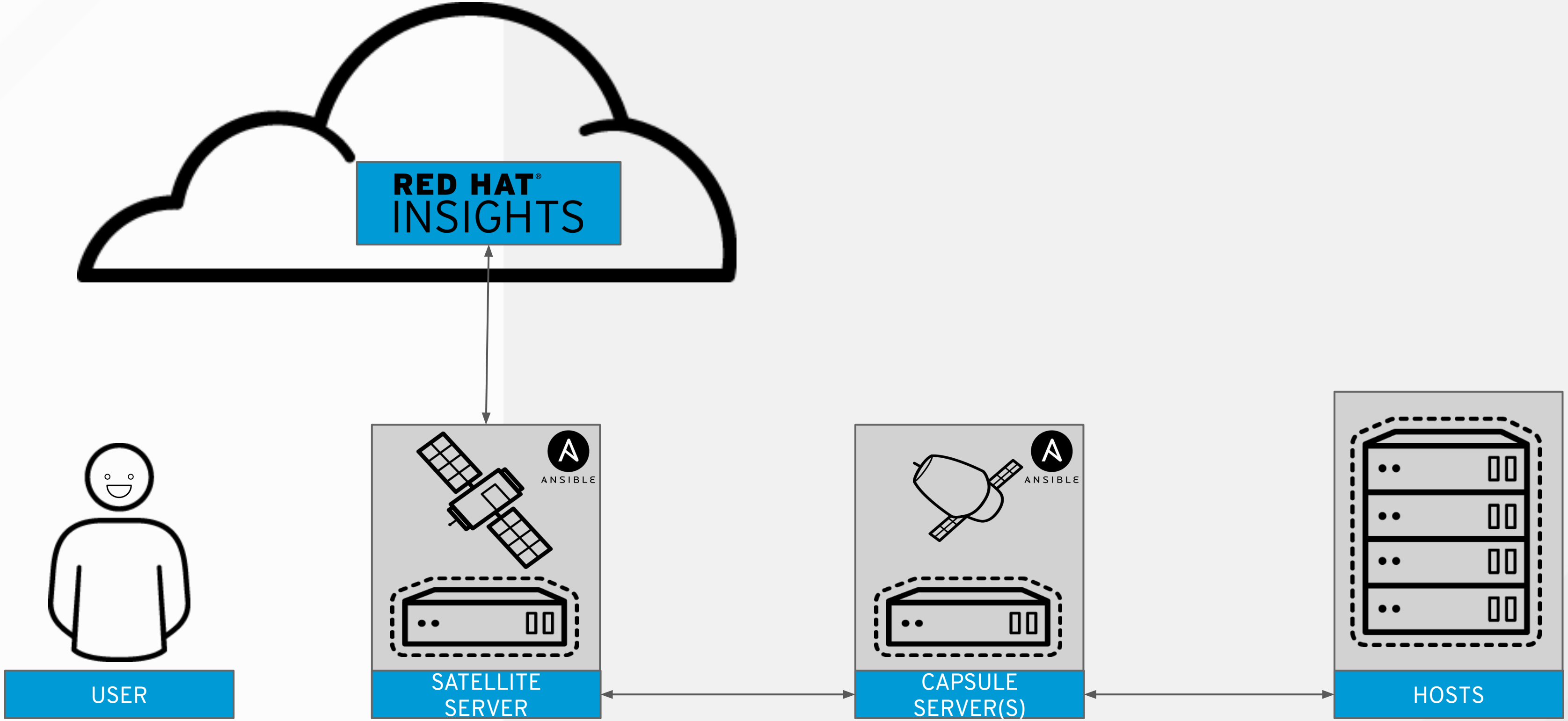
DEMO: SATELLITE 6.4, INSIGHTS, & ANSIBLE



The action is selected, so click Save.

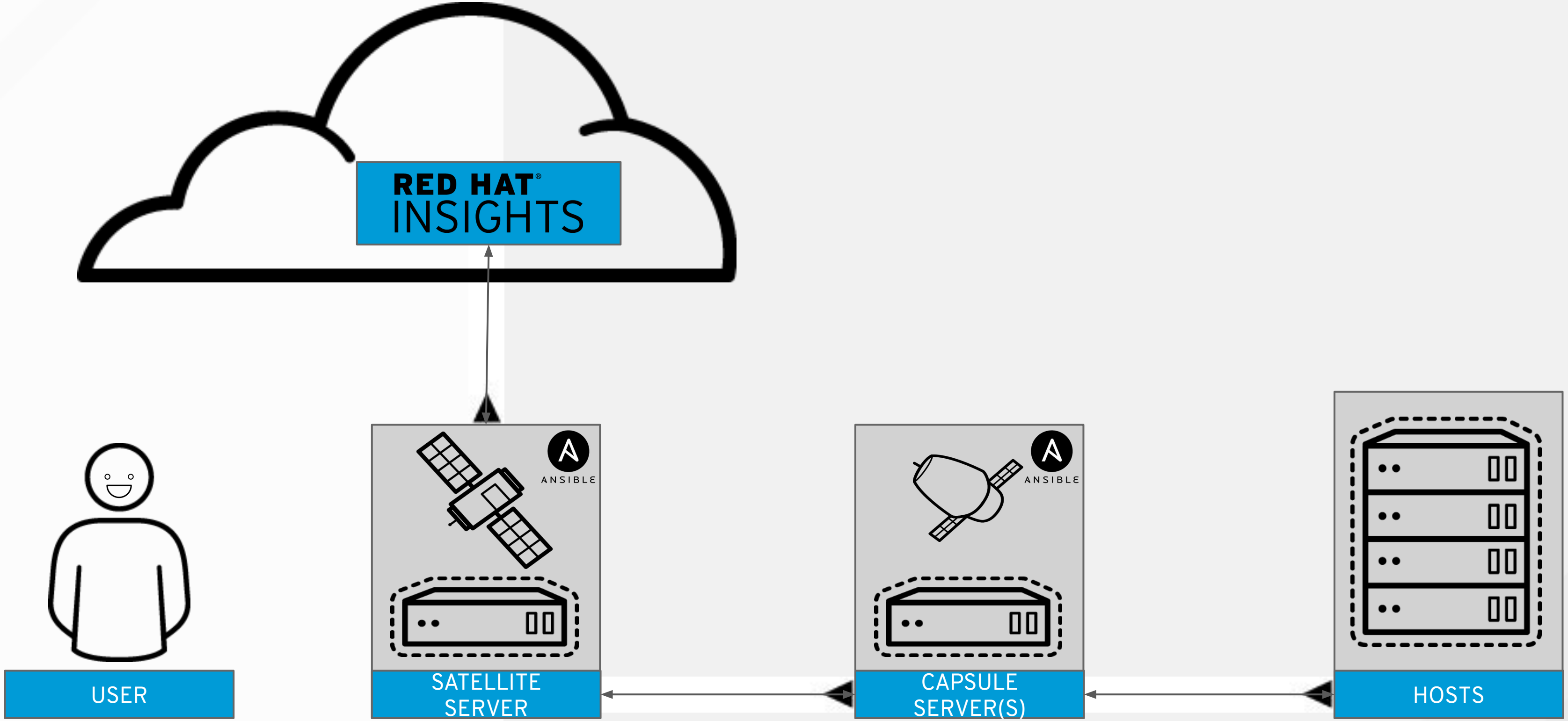
GREAT DEMO…
WHAT’S HAPPENING IN THE BACKGROUND?

Basic Communication Flow



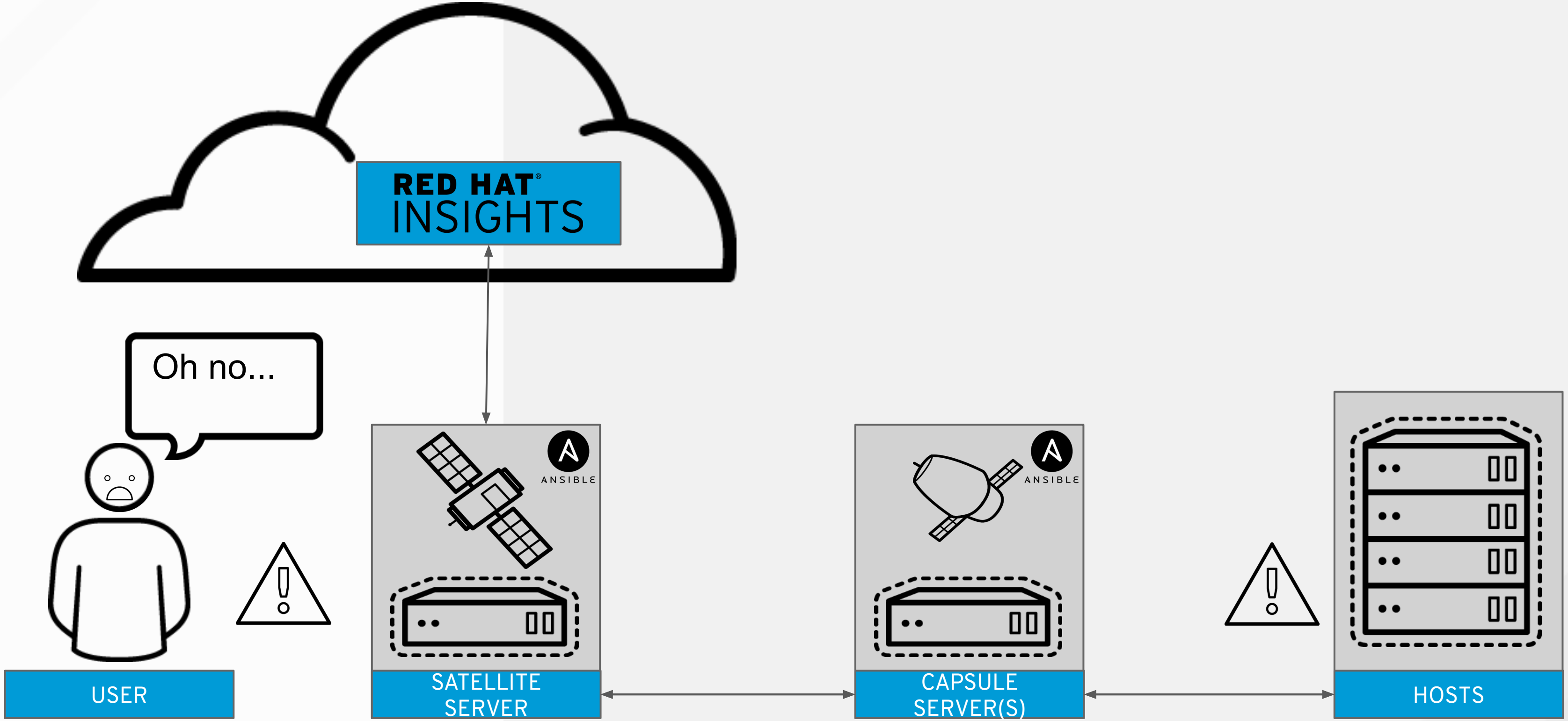
Data Sent to Insights for examination

Insights does this daily, automatically



Risk Found!

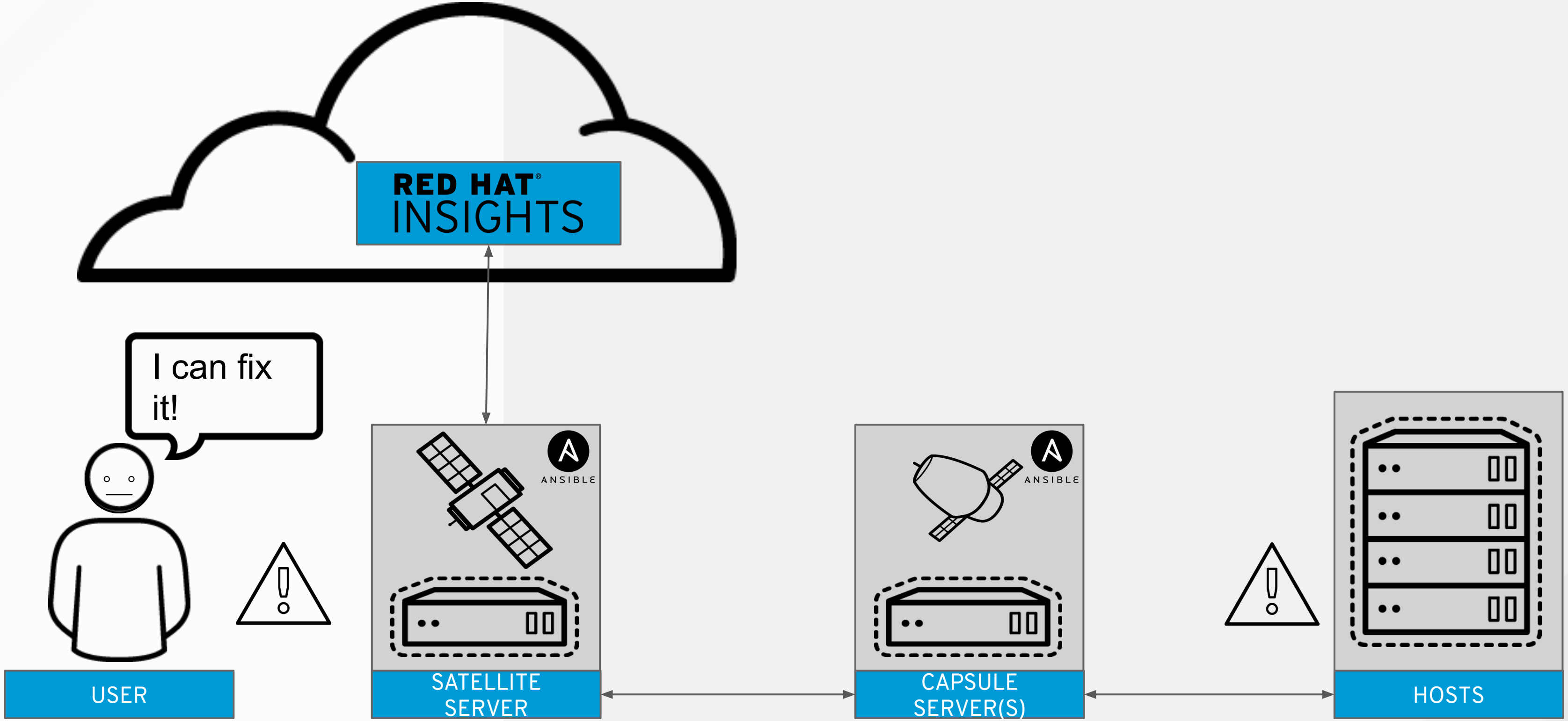
Satellite reads the data from Insights, dashboard widgets show the new risk



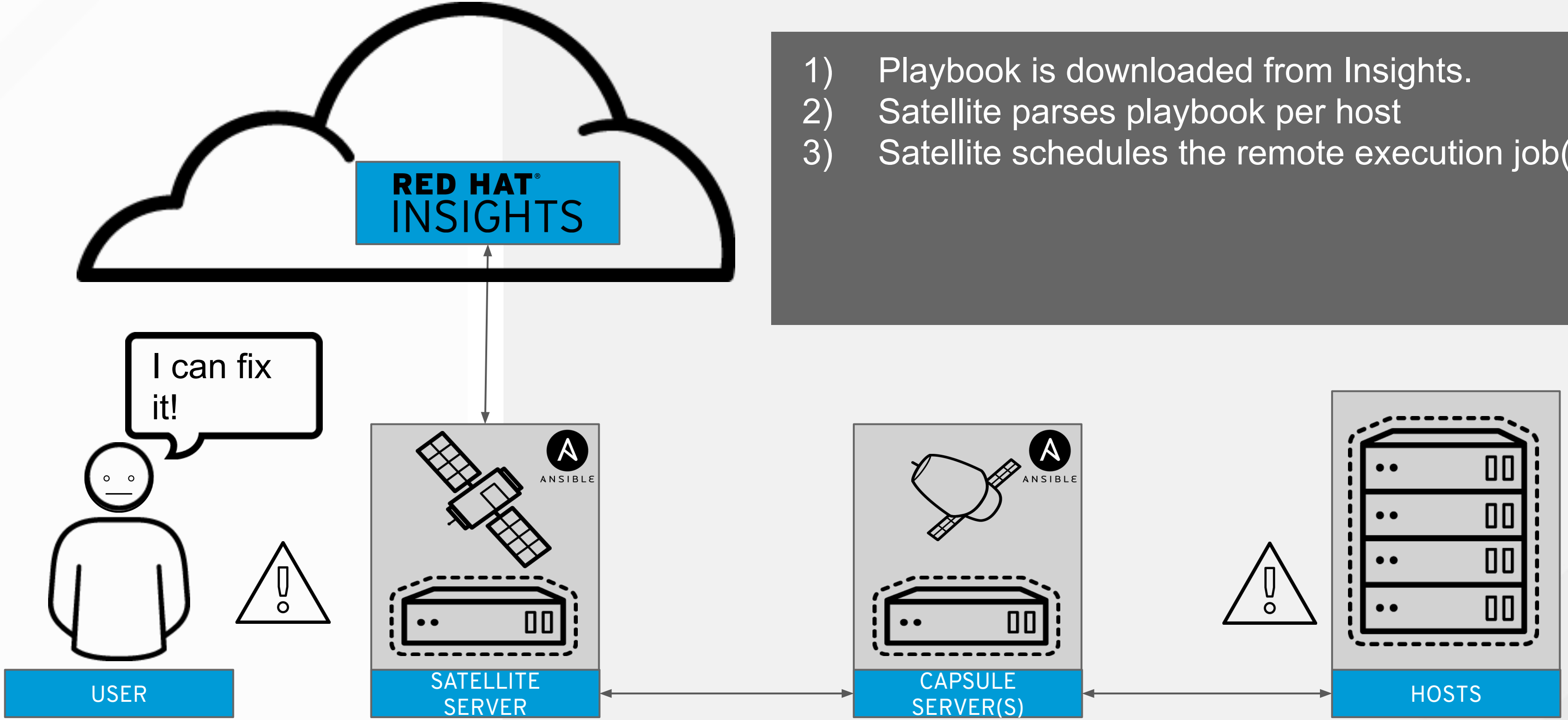
*Satellite does not store any information from Insights in the database. It is all real time.

Create a Remediation Plan

A user creates the remediation plan through Satellite



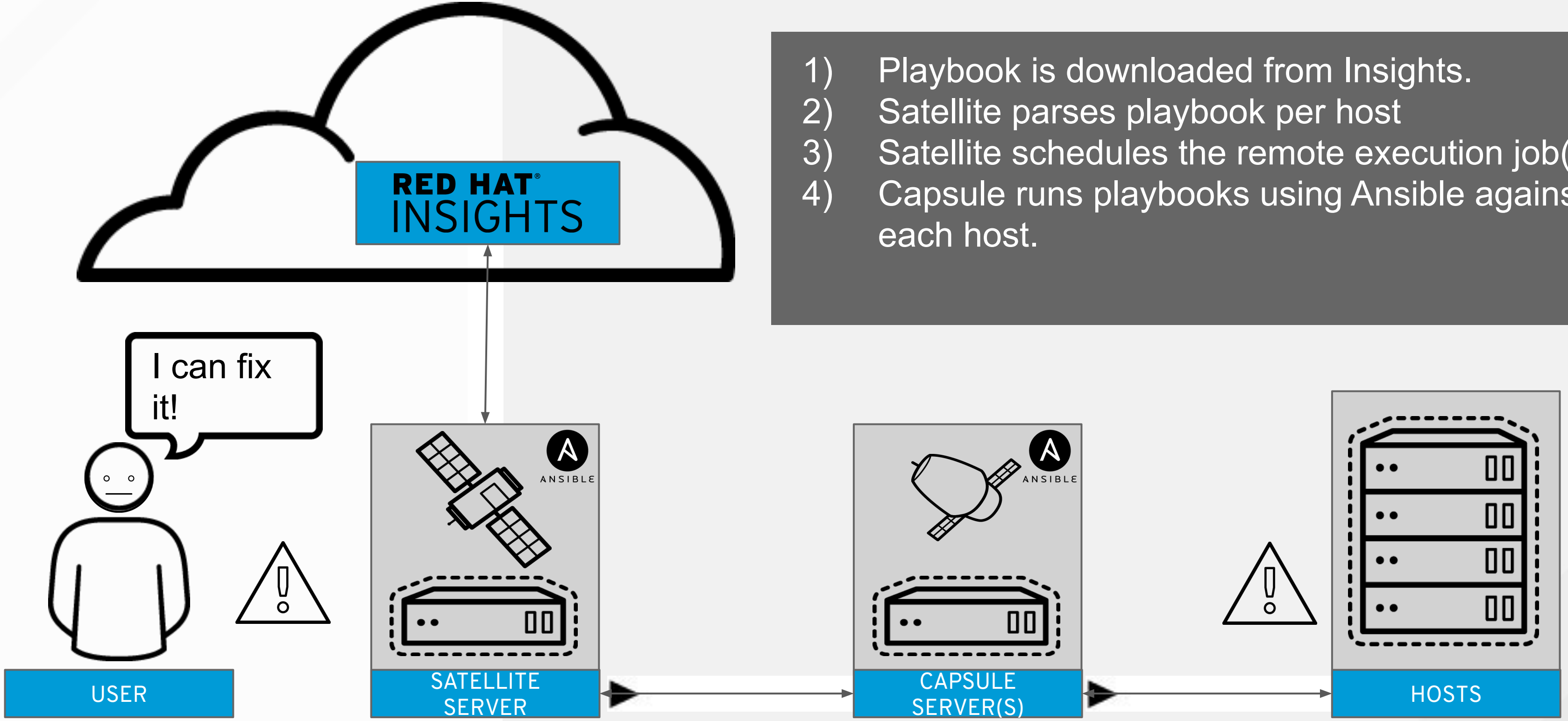
Plan Executes



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

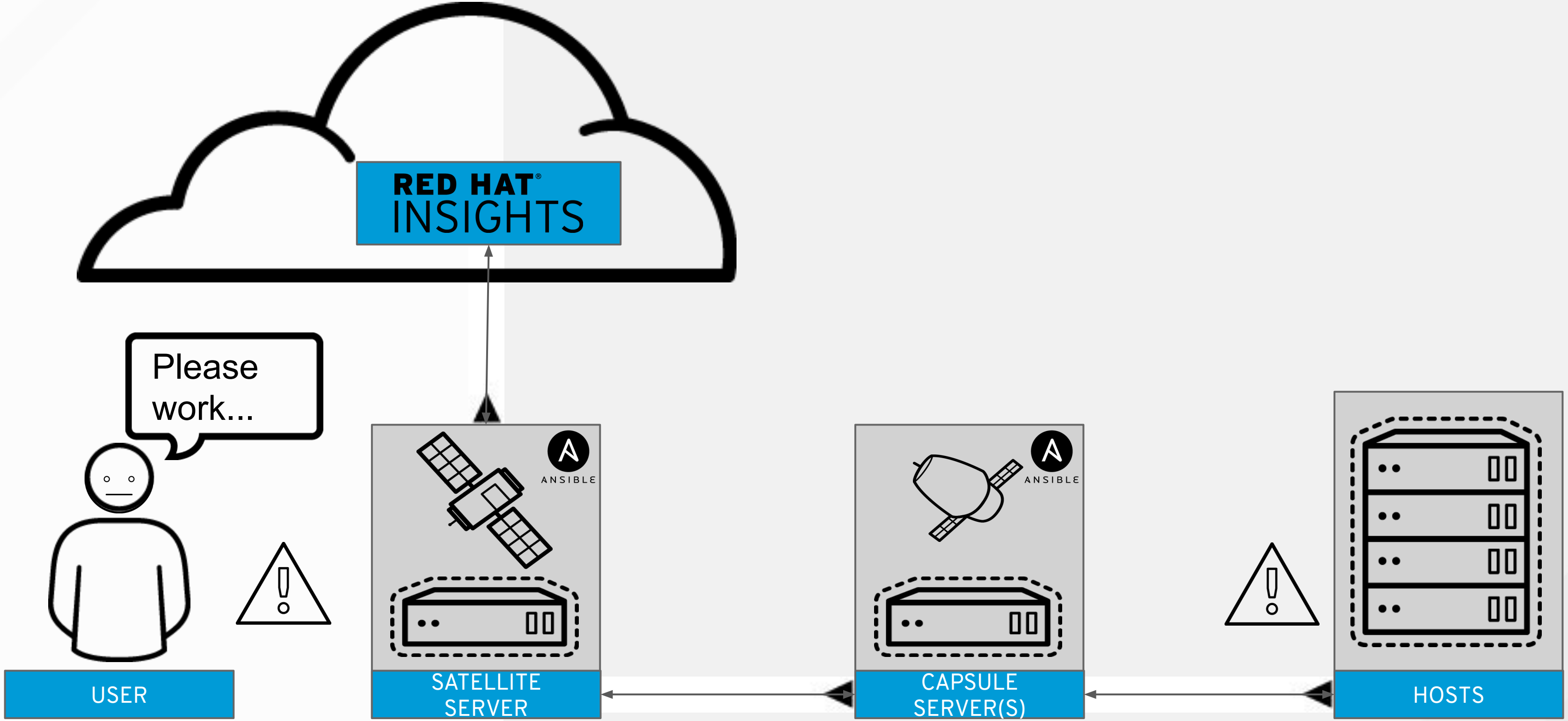
Plan Executes

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.



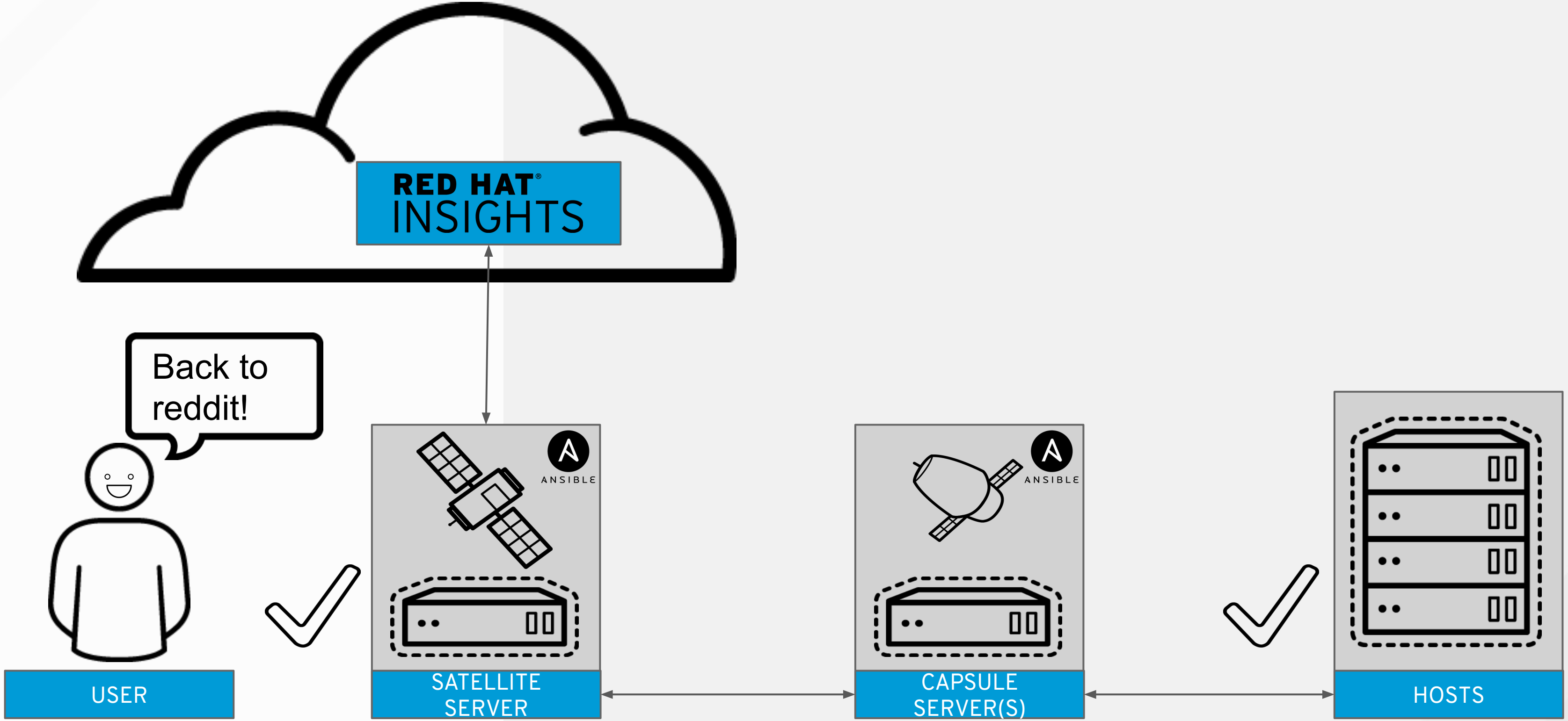
Data Sent to Insights for examination

Rescan is done after remediation completes



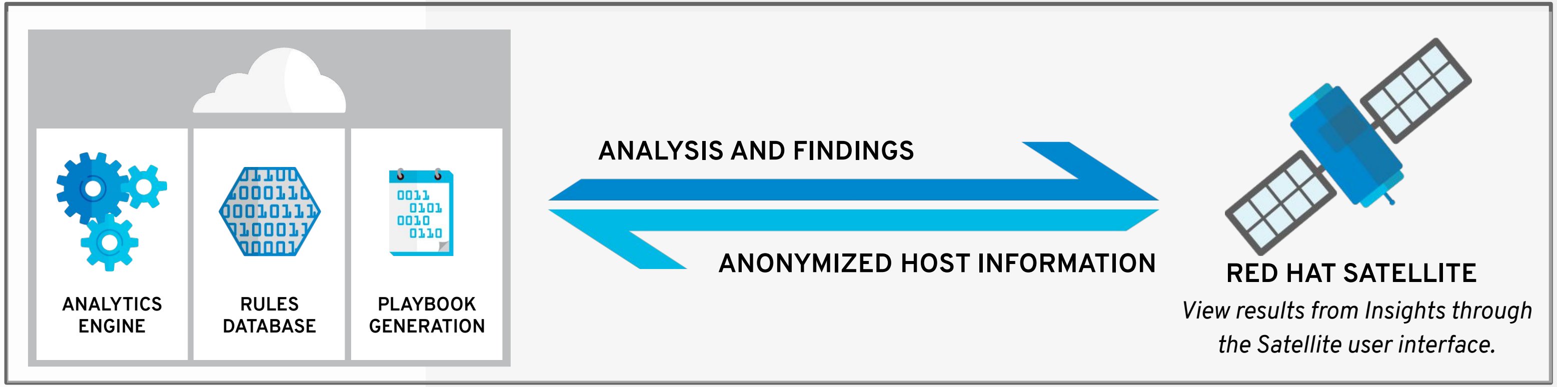
Data Sent to Insights for examination

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



WHY USE INSIGHTS WITH SATELLITE?

Stop reacting to problems once they occur. Predict & fix them now.



View results from Insights through the Satellite user interface.

ACTIONABLE INTELLIGENCE POWERED BY RED HAT

Confidently scale complex environments.

CONTINUOUS VULNERABILITY ALERTS

Maximize uptime and avoid fire-fighting.

INCREASED VISIBILITY TO SECURITY RISKS

Get ahead of security risks and fix them before it's a problem.

AUTOMATED REMEDIATION

Minimize human error, do more with less, and fix things faster.

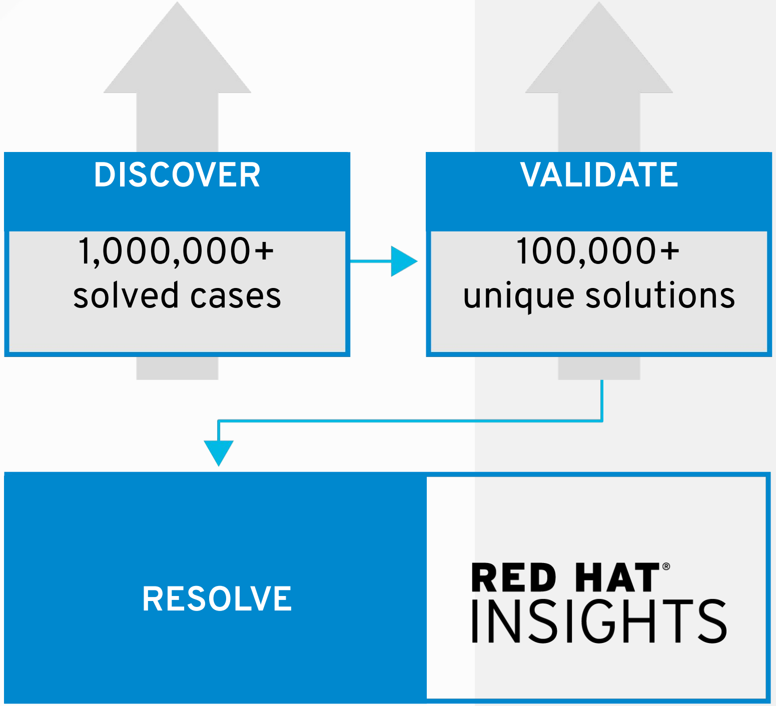
SATELLITE + INSIGHTS CAPABILITIES

Getting more from the purchase of Smart Management

CATEGORIES	CAPABILITIES	SATELLITE	INSIGHTS
Red Hat subscription management	Subscription knowledge and control	✓	
Provisioning	Bare-metal, VM, & cloud	✓	
	System discovery	✓	
Security & compliance	Automated remediation		✓
	Predictive IT analytics		✓
	Risk assessment		✓
	SCAP operations	✓	
Configuration management	System configuration	✓	
	Drift management	✓	
Software management	Content repository	✓	
	Patch management	✓	

RED HAT INSIGHTS CAPABILITIES

PROACTIVE and CONTINUOUS ASSESSMENT

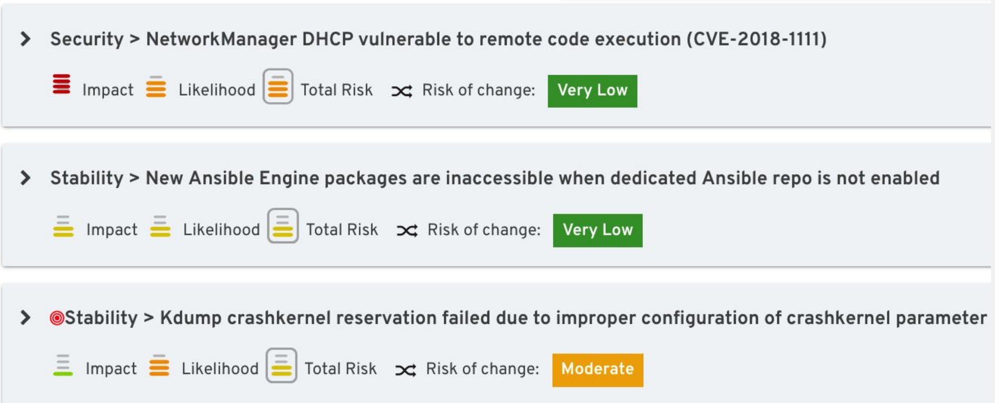


- Continuous identification of new risks driven by unique industry data
- Based on real-world results from millions of enterprise deployments

> *“ 85% of critical issues raised to Red Hat® support are already known to Red Hat or our partners.”*
>
> – RED HAT GLOBAL SUPPORT SERVICES

GET AHEAD OF KEY SECURITY RISKS

Don’t wait for your security team to tap you on the shoulder



> Security > NetworkManager DHCP vulnerable to remote code execution (CVE-2018-1111)

Impact Likelihood Total Risk Risk of change: Very Low

> Stability > New Ansible Engine packages are inaccessible when dedicated Ansible repo is not enabled

Impact Likelihood Total Risk Risk of change: Very Low

> Stability > Kdump crashkernel reservation failed due to improper configuration of crashkernel parameter

Impact Likelihood Total Risk Risk of change: Moderate

- Prioritizes security response by analyzing runtime configuration and usage

- Automates security analysis, beyond just CVEs

> “ …*when a vulnerability is released, it’s likely to be exploited within* ***40-60*** *days. However, it takes security teams between* ***100-120*** *days on average to remediate…*”

– KENNA SECURITY GROUP

HOW IS DATA COLLECTED?

Dynamically or Statically

Performance issue:
Network interface is not performing at maximum speed

→

Recommended action:
Check cable, connections, and remote switch settings.

Security risk detected:
Privilege escalation

→

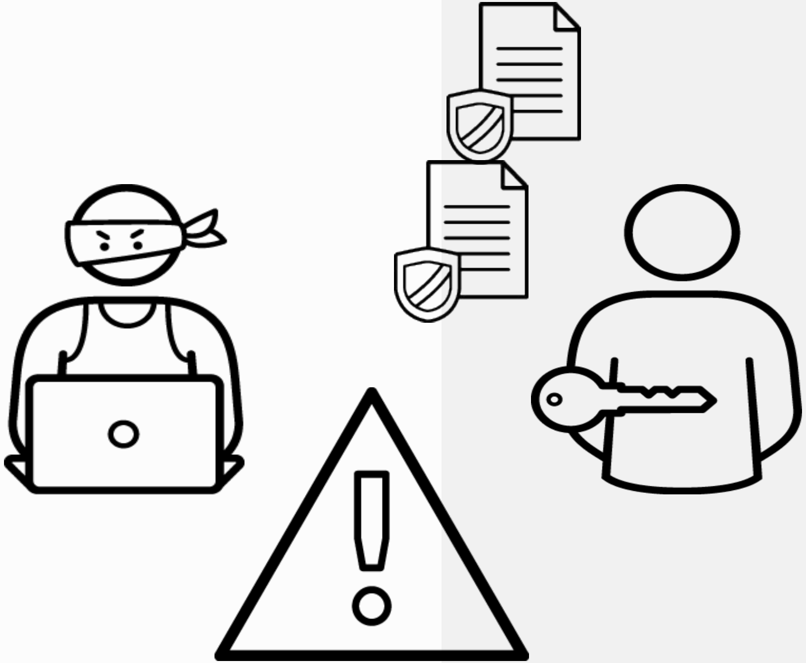
Recommended action:
Apply mitigation and update the Kernel.

Availability/stability:
Unexpected behavior with syntax in bonding config

→

Recommended action:
Change uppercase to lowercase in the config file.

CONCERNED ABOUT SECURITY?

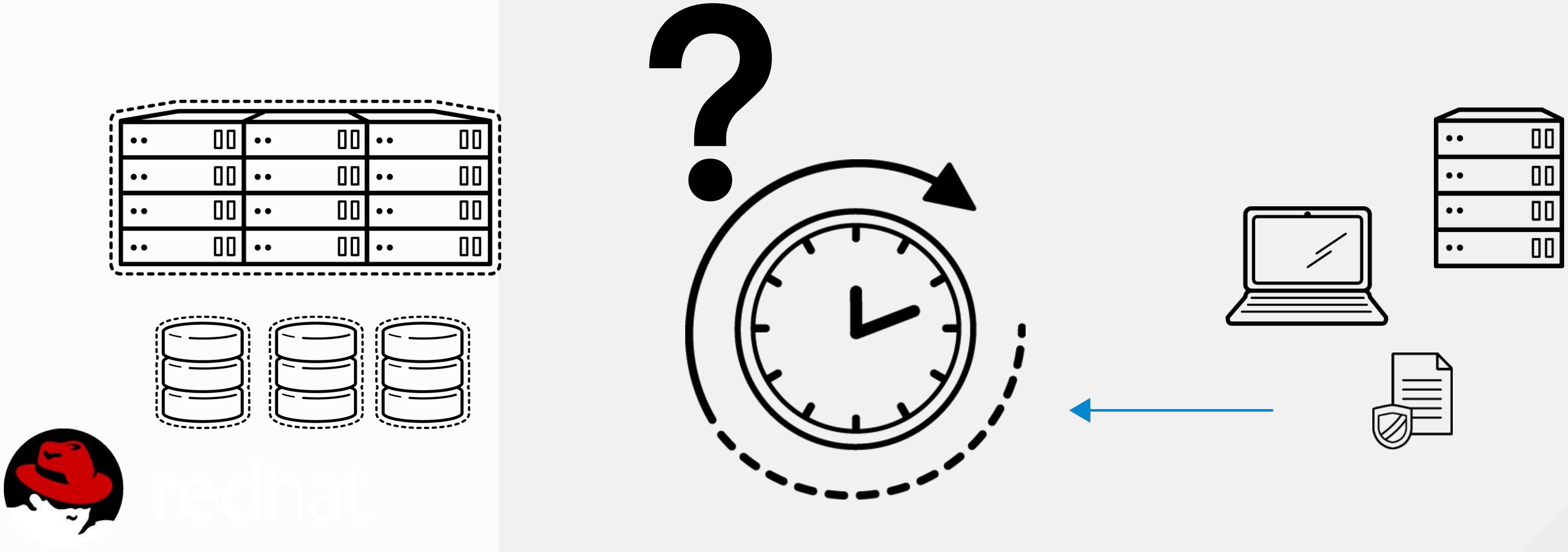


DATA SECURITY ASSURED

- Data encryption using LUKS
- Data sent over TLS
- Truster certificate bundled
- Hostname and IP obfuscation available
- System information to be tailored

HOW LONG DOES RED HAT HOLD DATA?

Red Hat does not permanently store your data



HOW TO DEPLOY RED HAT INSIGHTS

INSTALLATION AND REGISTRATION

Simple and Straightforward

? To install, run (as root) `# yum install insights-client`
Package name to change to `insights-client` in next RHEL release.
Verify latest RPM version!

- Currently **3.0.3-9 for RHEL7, 1.0.8 for RHEL6**
- Check Insights FAQ/KCS for up to date info
  - https://access.redhat.com/insights/getting-started
- After registration, running `insights-client` as root should always return “`Upload completed successfully!!`

INSTALLATION AND REGISTRATION

Dependencies

Insights currently requires:

- `bash`
- `python, python-magic, python-requests, python-setuptool`
- `libcgroup and libcgroup-tools`
- `pciutils`

Man page available via `$ man insights-client`

DATA COLLECTION

Don’t you believe us? Ok, try it yourself!

Follow these steps and verify for yourself what Red Hat is collecting from your systems:

```
# insights-client --register
# insights-client --no-upload
Starting to collect Insights data
See Insights data in
/var/tmp/TAFHhW/insights-amaya-insights2-20180129165816.tar.gz
```

Now you can inspect for yourself what we are collecting!

```
# tar xvzf
/var/tmp/TAFHhW/insights-amaya-insights2-20180129165816.tar.gz
```

DATA COLLECTION

Very small amount of data and only data that is needed for rule analysis

Example files:

- `/etc/redhat-release`
- `/proc/meminfo`
- `/var/log/messages`
- `/boot/grub/grub.conf`
- `/boot/grub2/grub.cfg`
- `/etc/modprobe.conf`

We do not collect logs files, but rather the lines that match a potential rule (i.e. page allocation failure)

Commands:

- `/bin/rpm -qa`
- `/bin/uname -a`
- `/usr/sbin/dmidecode`
- `/bin/netstat -i`
- `/bin/ps auxcww`

CONFIGURATION AND LOG FILES

Main configuration file:

- `/etc/insights-client/insights-client.conf`
- See comments in the configuration file for information about each parameter or run `$ man insights-client.conf` after installation.

Log files:

- `/var/log/insights-client/insights-client.log*`
- Logs are not collected in sosreport but functionality planned for sosreport
  - Obfuscation (`insights-client.conf` file):
  - Obfuscate IP addresses: `obfuscate=True` OR
  - Obfuscate hostnames: `obfuscate_hostname=True`

Blacklist

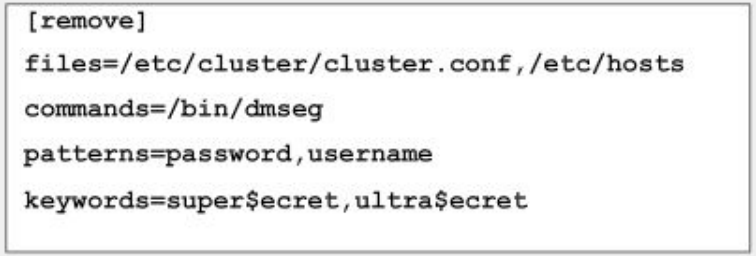
- Add items using `/etc/insights-client/remove.conf`

HOW TO BLACKLIST ITEMS?

There are two ways to blacklist items in redhat-access-insights.conf:

- Preset options (check in dictionary)
  - Obfuscate IP address: obfuscate=True
  - Obfuscate hostname: obfuscate_hostaname=True

- Using [remove] section
  - There are four options available:
    - Files
    - Commands
    - Patterns
    - Keywords



```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmseg
patterns=password,username
keywords=super$ecret,ultra$ecret
```

DATA COLLECTION

Worried about Red Hat knowing TOO MUCH about you???

Insights only collects 1% of the data a sosreport does!!

```
# ls -lh
/var/tmp/TAFHhW/insights-amaya-insights2-20180129165816.tar.gz
-rw-r--r--. 1 root root 138K Jan 29 16:58
/var/tmp/TAFHhW/insights-amaya-insights2-20180129165816.tar.gz
# ls -lh
/var/tmp/sosreport-amaya-insights2-20180129165924.tar.xz
-rw-------. 1 root root 12M Jan 29 16:59
/var/tmp/sosreport-amaya-insights2-20180129165924.tar.xz
```

Remember that you can control the data that is sent to us and how it is sent!

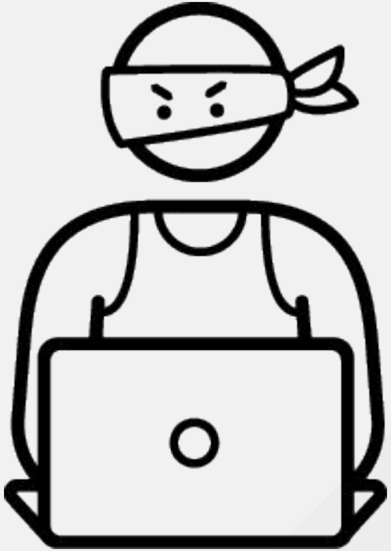
DATA COLLECTION

Remember: Red Hat is not watching, you control it all!!!!

- Blacklisting information
- Obfuscation of data
- Total control on data upload
- Red Hat holds your data for a maximum of 15 days if no other upload is made (on an encrypted data store)

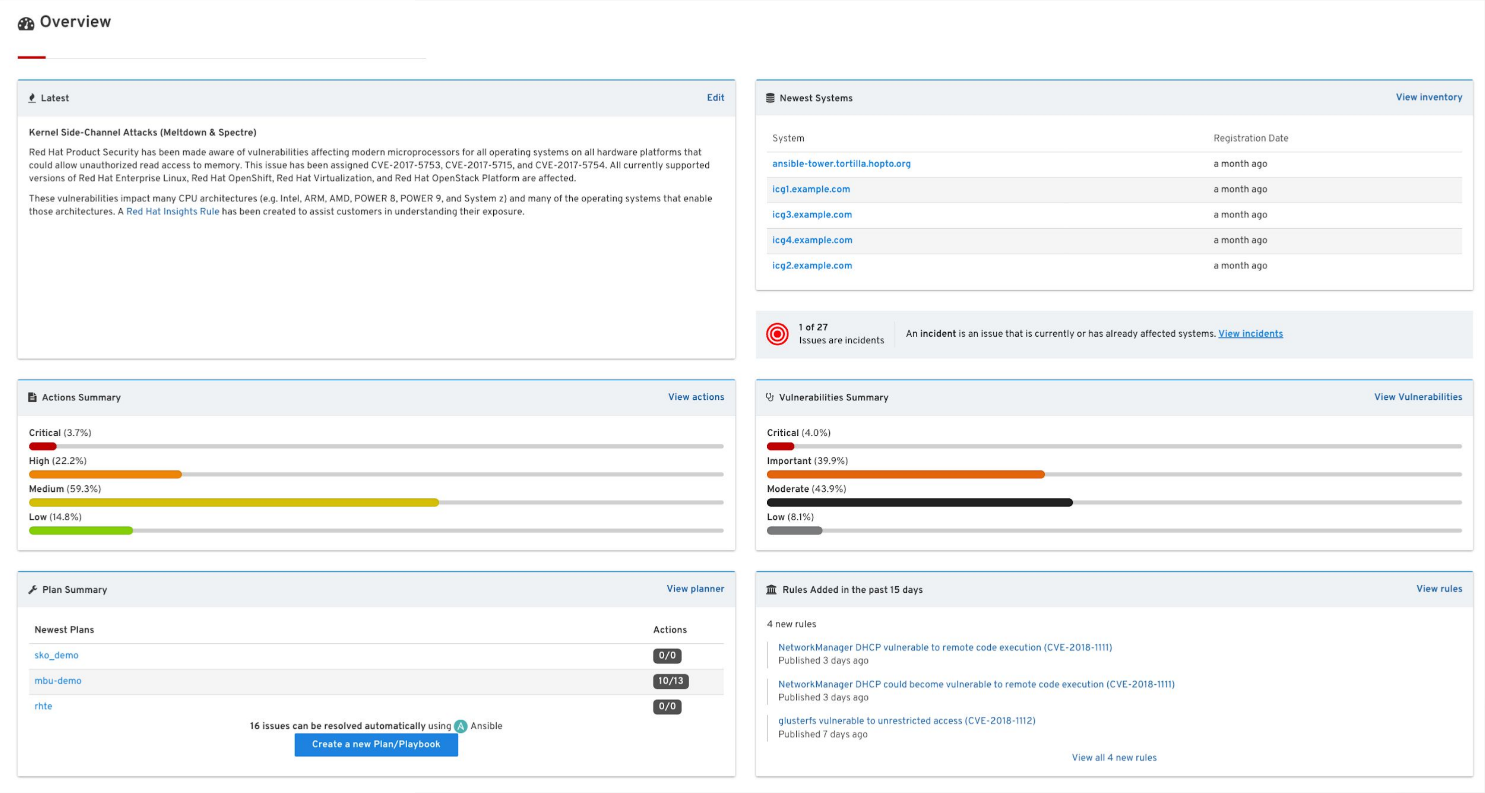
More information available at

https://access.redhat.com/articles/2025273



A DAY IN THE LIFE OF A RED HAT INSIGHTS ADMIN

RED HAT INSIGHTS DASHBOARD



Overview

Latest

Edit

Kernel Side-Channel Attacks (Meltdown & Spectre)

Red Hat Product Security has been made aware of vulnerabilities affecting modern microprocessors for all operating systems on all hardware platforms that could allow unauthorized read access to memory. This issue has been assigned CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754. All currently supported versions of Red Hat Enterprise Linux, Red Hat OpenShift, Red Hat Virtualization, and Red Hat OpenStack Platform are affected.

These vulnerabilities impact many CPU architectures (e.g. Intel, ARM, AMD, POWER 8, POWER 9, and System z) and many of the operating systems that enable those architectures. A Red Hat Insights Rule has been created to assist customers in understanding their exposure.

Newest Systems

View inventory

System	Registration Date
ansible-tower.tortilla.hopto.org	a month ago
icg1.example.com	a month ago
icg3.example.com	a month ago
icg4.example.com	a month ago
icg2.example.com	a month ago

1 of 27
Issues are incidents

An **incident** is an issue that is currently or has already affected systems. View incidents

Actions Summary

View actions

Critical (3.7%)

High (22.2%)

Medium (59.3%)

Low (14.8%)

Vulnerabilities Summary

View Vulnerabilities

Critical (4.0%)

Important (39.9%)

Moderate (43.9%)

Low (8.1%)

Plan Summary

View planner

Newest Plans	Actions
sko_demo	0/0
mbu-demo	10/13
rhte	0/0

16 issues can be resolved automatically using Ansible

Create a new Plan/Playbook

Rules Added in the past 15 days

View rules

4 new rules

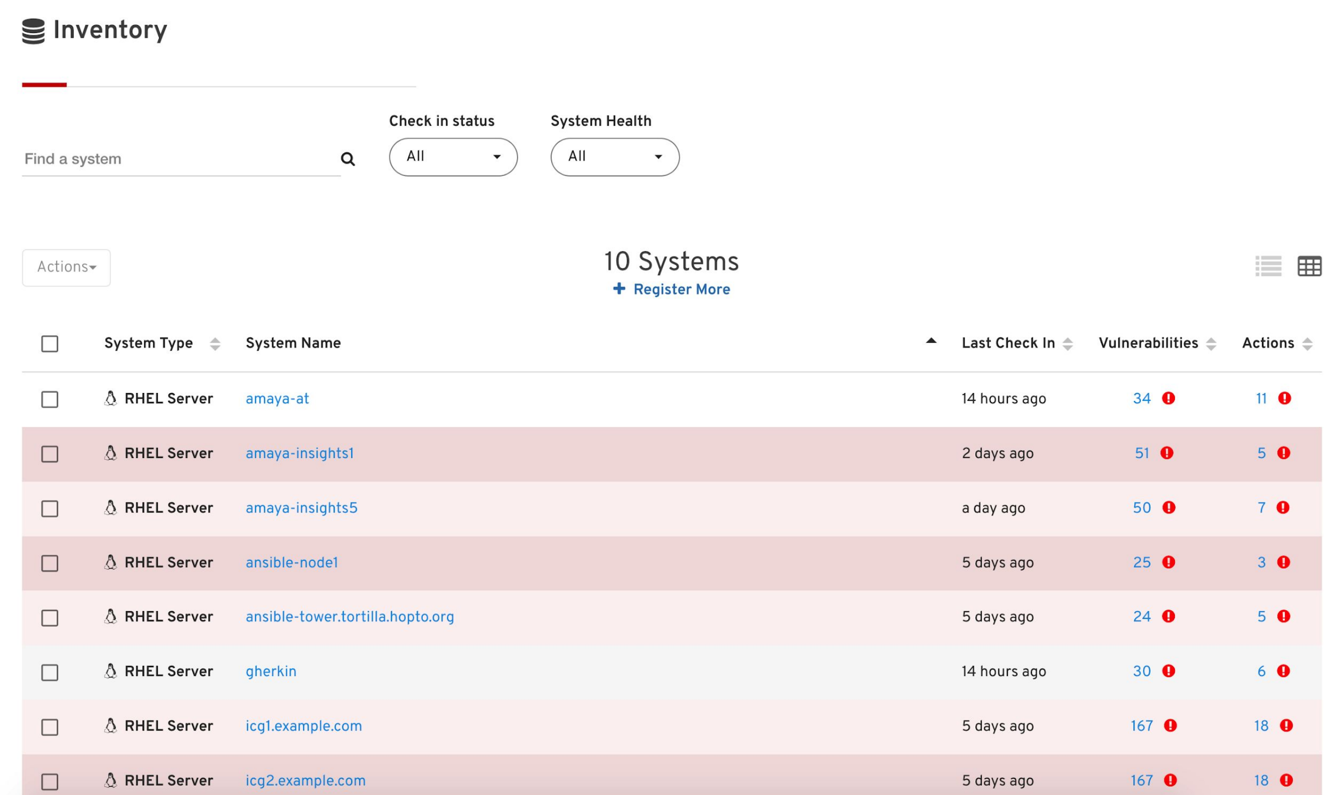
NetworkManager DHCP vulnerable to remote code execution (CVE-2018-1111)
Published 3 days ago

NetworkManager DHCP could become vulnerable to remote code execution (CVE-2018-1111)
Published 3 days ago

glusterfs vulnerable to unrestricted access (CVE-2018-1112)
Published 7 days ago

View all 4 new rules

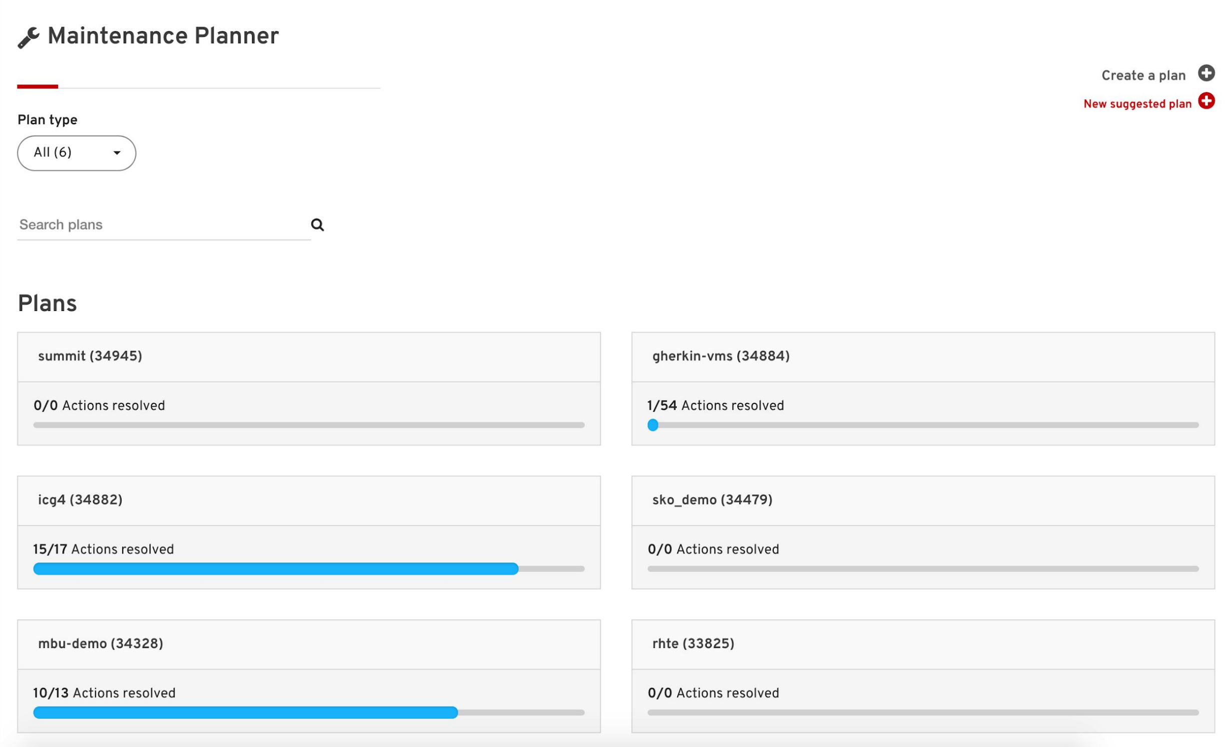
RED HAT INSIGHTS INVENTORY



10 Systems

□	System Type	System Name	Last Check In	Vulnerabilities	Actions
□	RHEL Server	amaya-at	14 hours ago	34 !	11 !
□	RHEL Server	amaya-insights1	2 days ago	51 !	5 !
□	RHEL Server	amaya-insights5	a day ago	50 !	7 !
□	RHEL Server	ansible-node1	5 days ago	25 !	3 !
□	RHEL Server	ansible-tower.tortilla.hopto.org	5 days ago	24 !	5 !
□	RHEL Server	gherkin	14 hours ago	30 !	6 !
□	RHEL Server	icg1.example.com	5 days ago	167 !	18 !
□	RHEL Server	icg2.example.com	5 days ago	167 !	18 !

RED HAT INSIGHTS MAINTENANCE PLANNER



Maintenance Planner

Create a plan

New suggested plan

Plan type

All (6)

Search plans

Plans

summit (34945)

0/0 Actions resolved

gherkin-vms (34884)

1/54 Actions resolved

icg4 (34882)

15/17 Actions resolved

sko_demo (34479)

0/0 Actions resolved

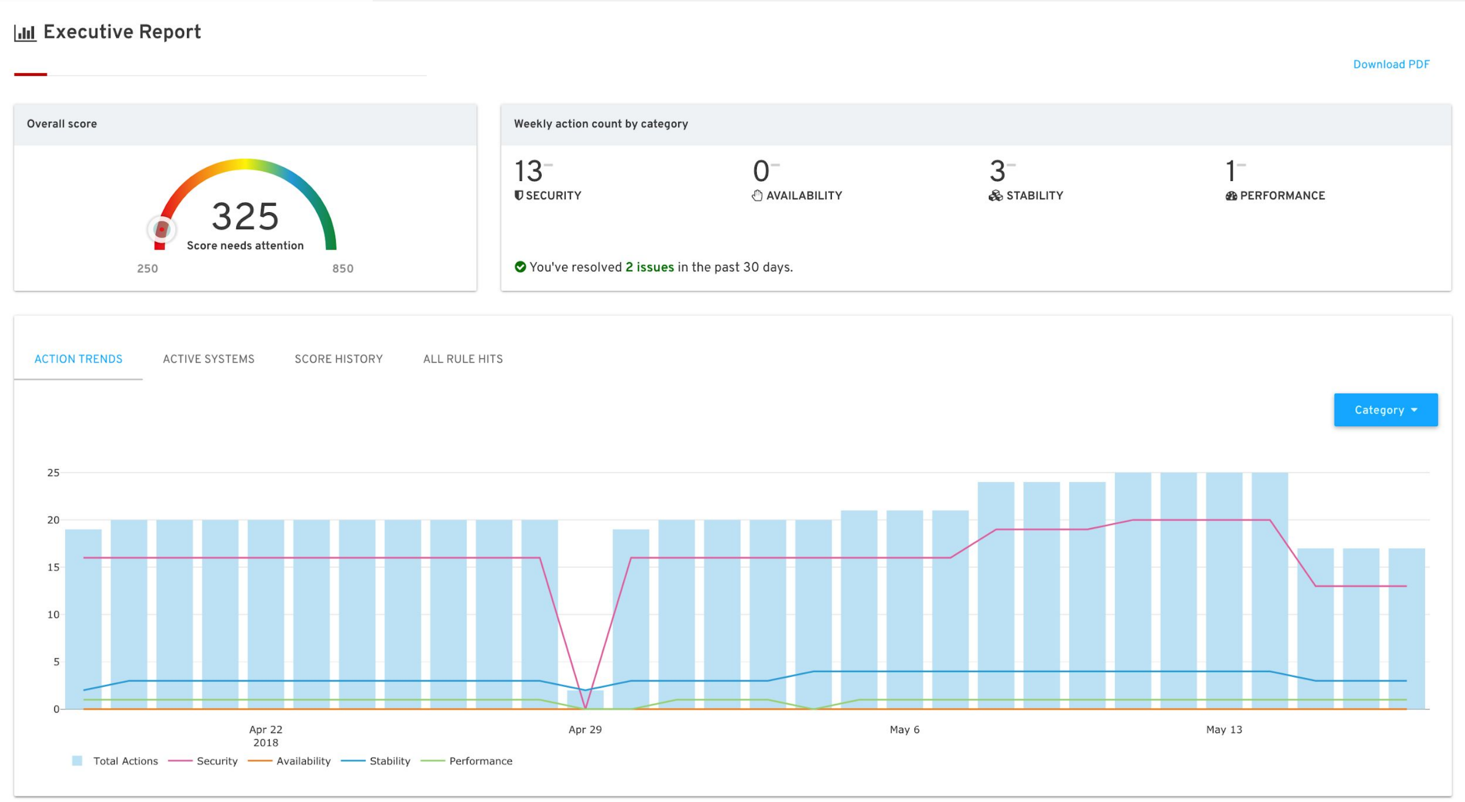
mbu-demo (34328)

10/13 Actions resolved

rhte (33825)

0/0 Actions resolved

RED HAT INSIGHTS EXECUTIVE REPORTING



Executive Report

Download PDF

Overall score

325

Score needs attention

250 850

Weekly action count by category

13	0	3	1
SECURITY	AVAILABILITY	STABILITY	PERFORMANCE

✓ You've resolved **2 issues** in the past 30 days.

GIVE IT A GO FOR FREE!!!

GETTING STARTED

ALREADY A RED HAT® ENTERPRISE LINUX® CUSTOMER?

Try Red Hat Insights at no cost:

https://access.redhat.com/insights/getting-started

INTERESTED IN A MANAGEMENT SUITE?

Red Hat Insights is included in:

Red Hat Cloud Infrastructure + Red Hat Cloud Suite

Red Hat Smart Management

WOULD YOU LIKE TO LEARN MORE ABOUT RED HAT INSIGHTS?

https://www.redhat.com/en/technologies/management/insights

For more info, visit: https://access.redhat.com/insights/info

redhat

THANK YOU

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