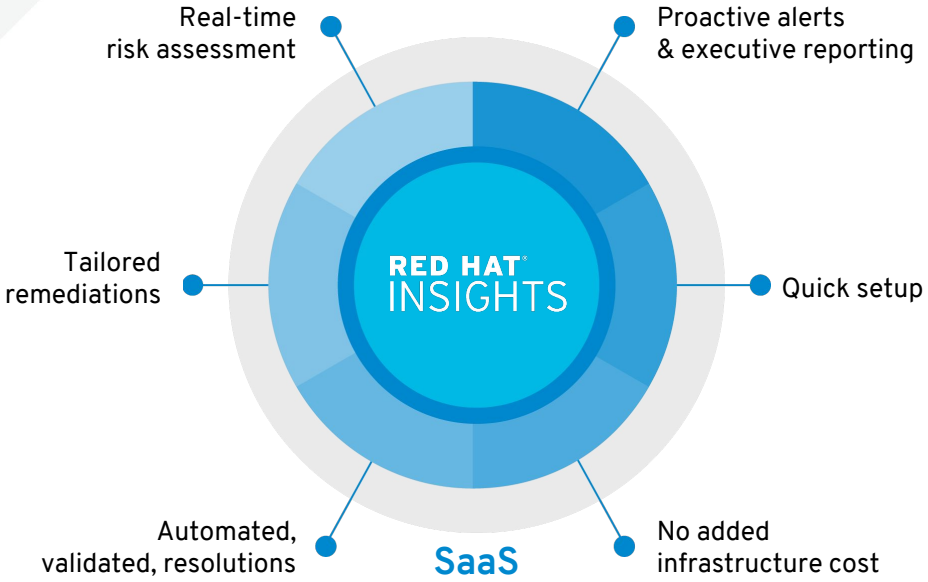
redhat®

Analytics-Driven Automation

with Insights and Ansible Integration

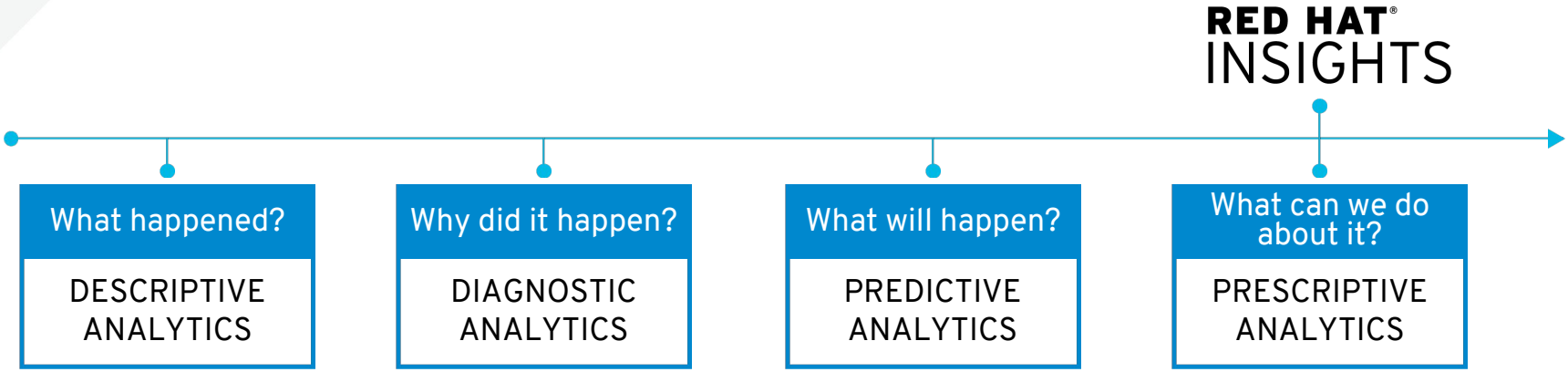
Fred van Zwieten
Senior Solution Architect Platform & Cloud

WHAT'S RED HAT® INSIGHTS



Red Hat Insights assesses your Red Hat infrastructure to help you proactively identify and remediate threats to security, performance, availability, and stability--avoiding issues, outages and unplanned downtime; and ensuring that your Red Hat environment is operating optimally.

I.T. OPERATIONAL ANALYTICS (ITOA)



" We have taken a position that, 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 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.

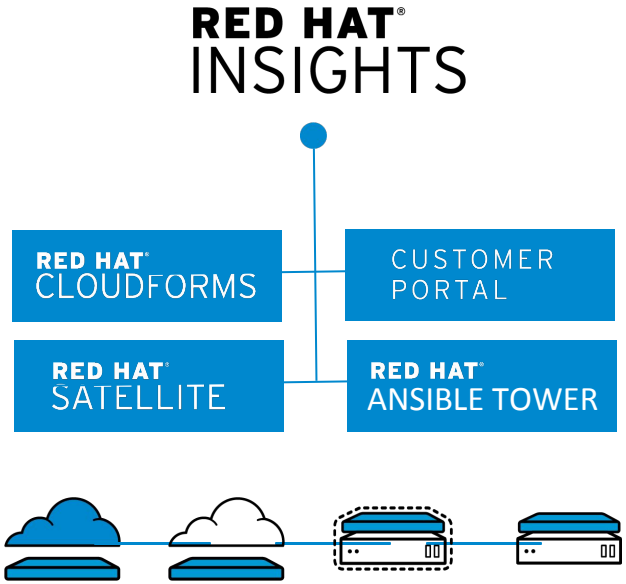
INCREASED VISIBILITY TO SECURITY RISKS

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.

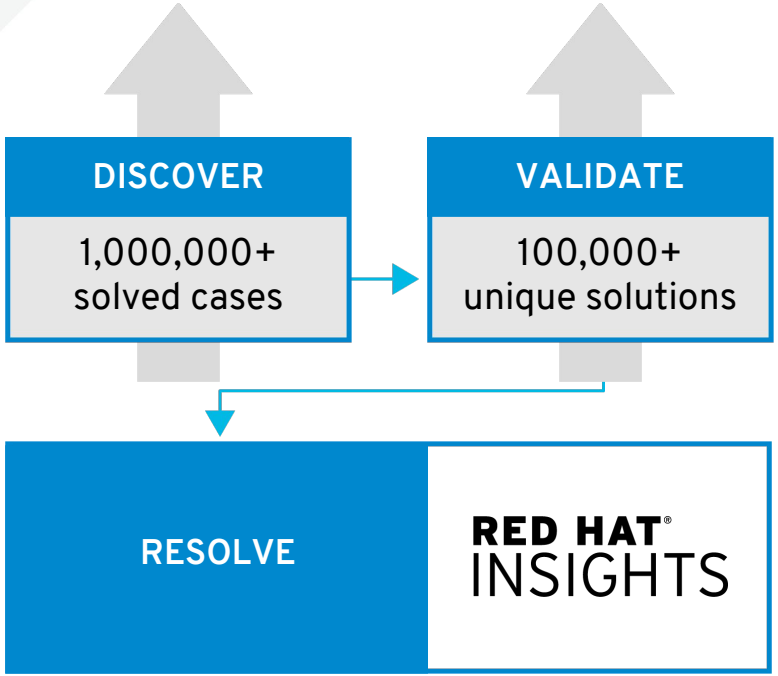
INTEGRATED INTO TOOLS YOU ALREADY USE



- **Integrated into**
  - Red Hat Satellite 5.7+ and 6.1+
  - Red Hat CloudForms 4.0+
  - Red Hat Ansible Tower 3.1+
  - Red Hat Customer Portal
- Works on physical, virtual, cloud, and container-based workloads
- API available for custom integration
- **Current Supported Platforms:**
  - Red Hat Enterprise Linux 6.4+ & 7+
  - Red Hat OpenStack 7+
  - Red Hat Virtualization 4+
  - Red Hat OpenShift Container Platform

RED HAT INSIGHTS CAPABILITIES

PROACTIVE & CONTINUOUS ASSESSMENT

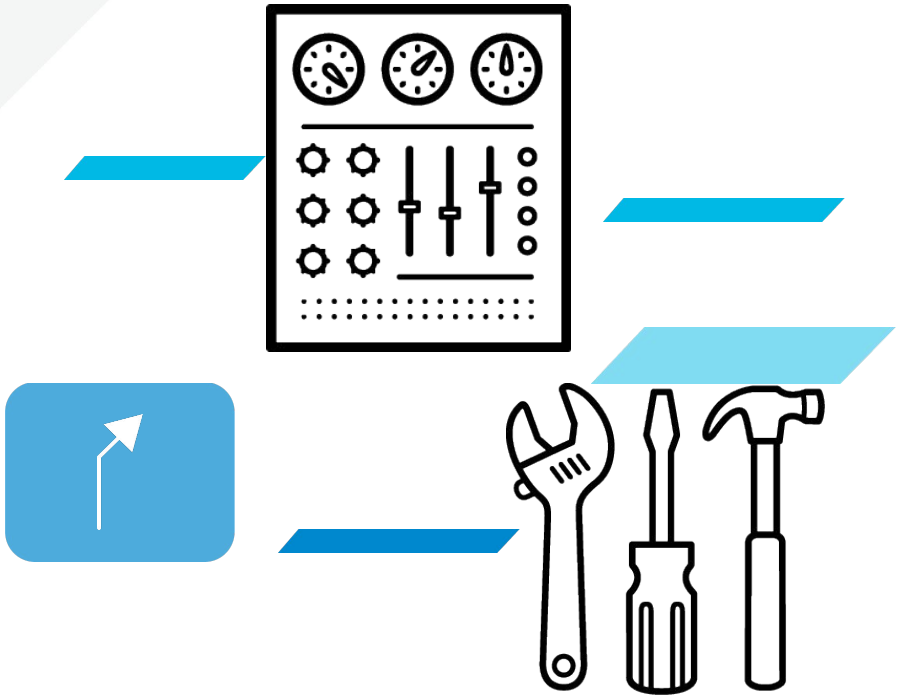


- Continuous identification of new risks driven by unique industry data
- Based on real-world results from millions of enterprise deployments

“ 85% of critical issues raised to Red Hat® support are already known to Red Hat or our partners.”

— RED HAT GLOBAL SUPPORT SERVICES

REMEDIATION MADE SIMPLE



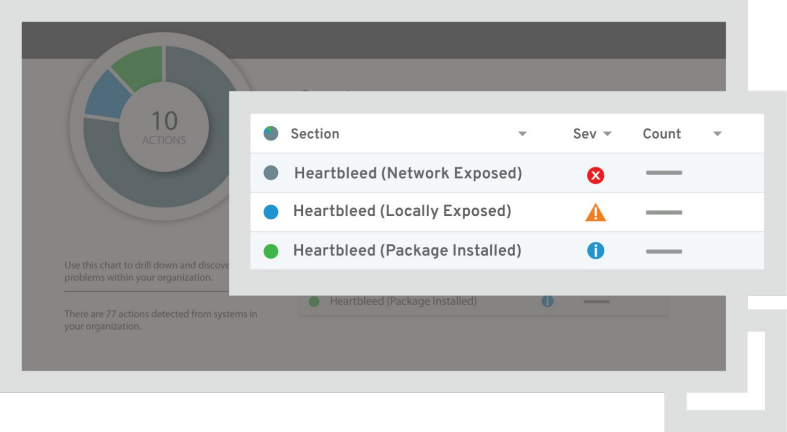
- Automatically tailored recommendations and remediation down to the per-host level
- Ansible playbook generation provides remediation automation
- Create and share maintenance plans to better coordinate responses within your team
- Avoid complexity with easy-to-follow issue resolution.

“ 22% of disasters are caused by human error.”

– QUORUM DISASTER RECOVERY REPORT

GET AHEAD OF KEY SECURITY RISKS

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



- Prioritizes security response by analyzing runtime configuration and usage
- Automates security analysis for customers, beyond just CVEs

“ In the first year 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 existing vulnerabilities.”

— KENNA SECURITY GROUP

redhat.

WHAT IS YOUR TOTAL RISK?

And furthermore, are you willing to take it?

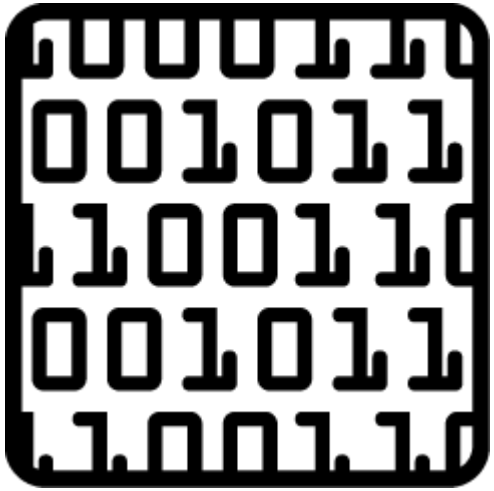
- Clear concepts to help you understand your risk

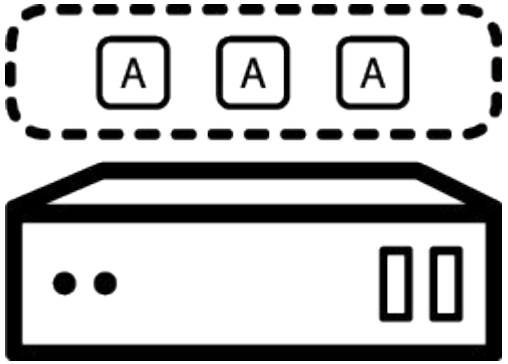
- Likelihood
- Impact
- Total Risk

- Tailored for your environment

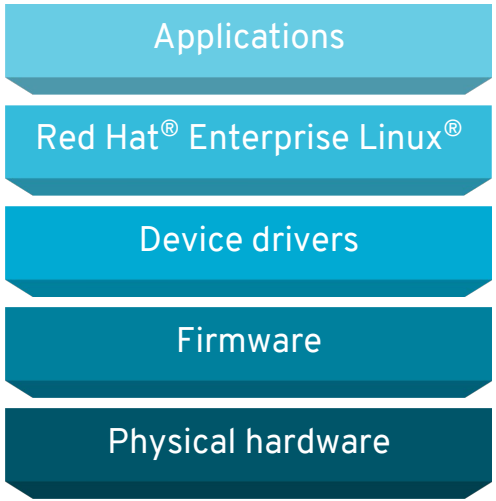
INSIGHTS ON PREMISE

Back end engine resides at Red Hat





FULL STACK ANALYSIS



INSIGHTS vs SATELLITE / CLOUDFORMS / TOWER

Do I really need them all?

RED HAT
INSIGHTS

RED HAT
CLOUDFORMS

RED HAT
ANSIBLE TOWER

RED HAT
SATELLITE

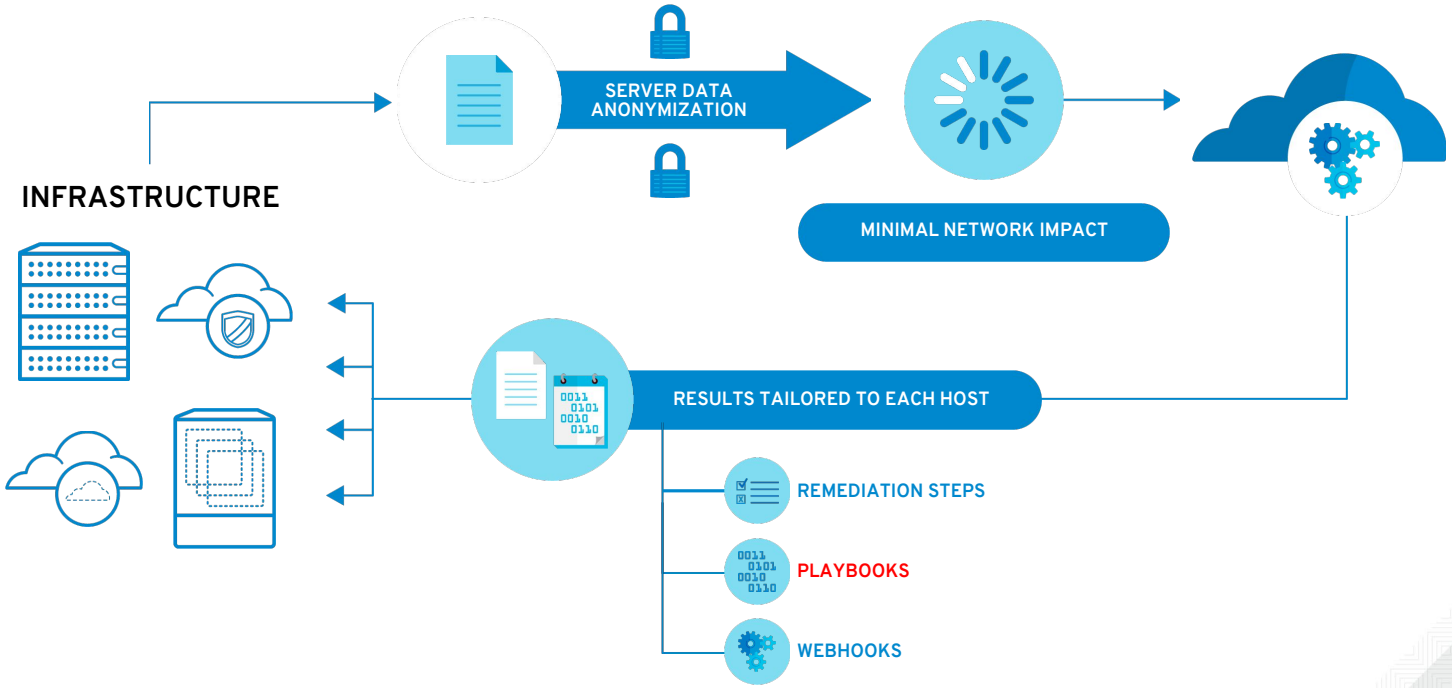
INSIGHTS AND SATELLITE

Smart Management

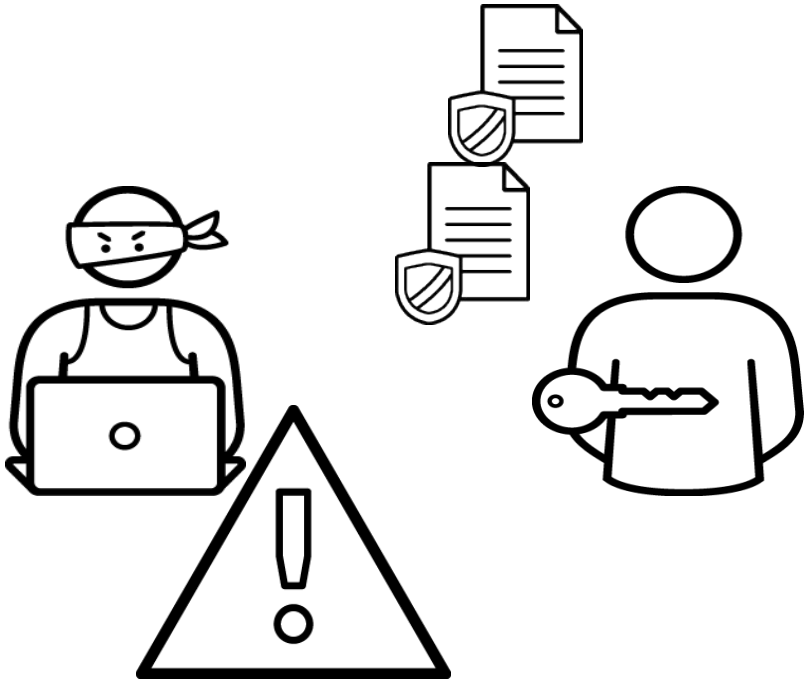
BETTER TOGETHER!

HOW INSIGHTS WORKS

ARCHITECTURE



CONCERNED ABOUT SECURITY?

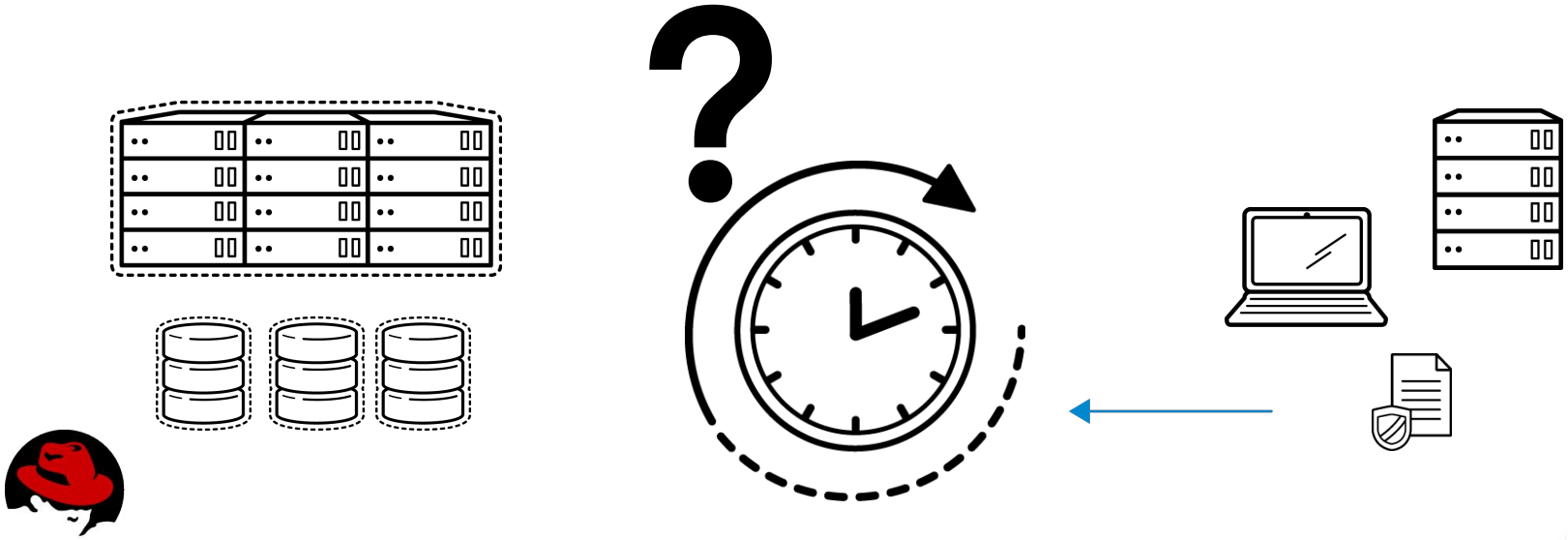


DATA SECURITY ASSUED

- 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 store permanently your data



HOW TO DEPLOY INSIGHTS

INSTALLATION AND REGISTRATION

CONFIRMING A GOOD INSTALLATION

To install, run (as root) `# yum install insights-client`

- Installs systemd service and timer unit's

Other options:

- Pre-made Ansible, Puppet and Chef resources available
- Automatic installation using Satellite
  - Ansible Role
  - Puppet Class
  - Bootstrap

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`

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`

DATA COLLECTION DETAILS

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 the entire messages file, 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`

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 from yourself what we are collecting!

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

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 is sent to us and how it is sent!

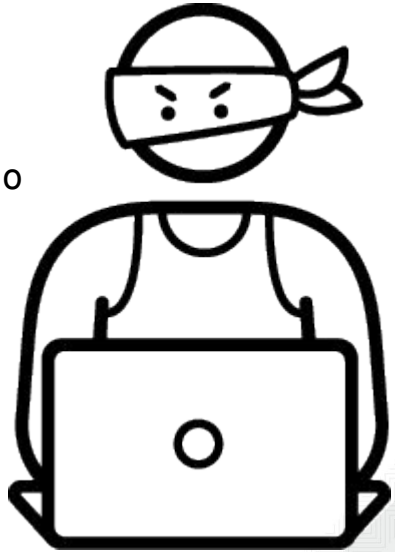
DATA COLLECTION

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 a encrypted data store)

More information available at

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



Demo Time..

GETTING STARTED

ALREADY A RED HAT® ENTERPRISE LINUX® CUSTOMER?

Try Insights at no cost:

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

INTERESTED IN A MANAGEMENT SUITE?

Insights is included in:

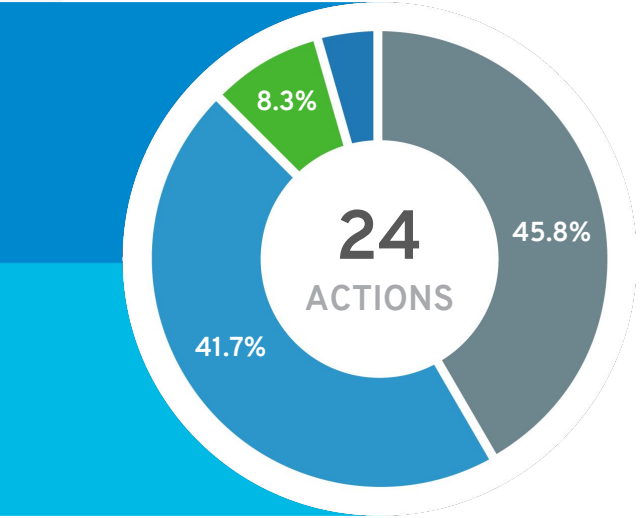
Red Hat Cloud Infrastructure, Red Hat Cloud Suite & Red Hat Smart Management

WOULD YOU LIKE TO LEARN MORE ABOUT INSIGHTS?

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

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

YOUR NO-COST INSIGHTS ASSESSMENT



Run an Insights assessment for 30 days:

1. Work with your account team to get an Insights eval subscription.
2. Install the Red Hat Insights RPM.
3. Register 50+ systems for best view.
4. See results immediately.
5. Schedule a best practices workshop.

See valuable insights in minutes:

1. Activate eval: https://access.redhat.com/insights/evaluation.
2. Installation: https://access.redhat.com/insights/getting-started.

QUESTIONS?

insights@redhat.com

Links

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

Insights portal:
https://access.redhat.com/insights

Insights blog:
https://access.redhat.com/blogs/insights

QUESTIONS ?

RATE THE SESSION

Please don't forget to rate this session in the Red Hat Events App

- Open the Agenda
- Select the session you have followed
- Rate the session

THANK YOU