Data Privacy with Red Hat Insights and More

Jay Ryan
Account Solutions Architect

Red Hat

Red Hat Insights

PREDICT RISK. GET GUIDANCE. STAY SECURE.

PREDICTIVE I.T. ANALYTICS

AUTOMATED EXPERT ASSESSMENT

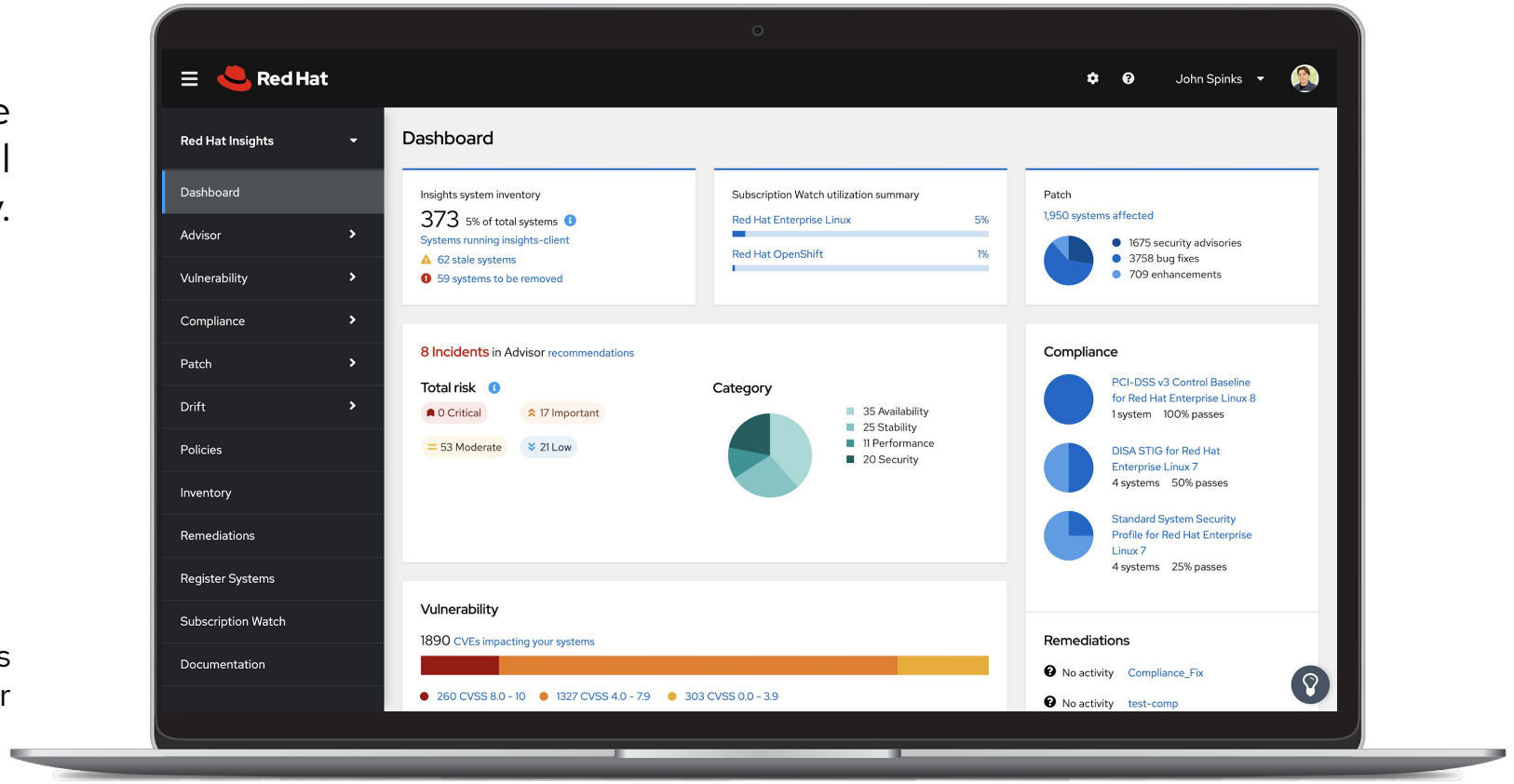
SIMPLE REMEDIATION

Red Hat

Red Hat Insights

Included with Red Hat Enterprise Linux subscription, now with more value

New and expanded services provide additional security and operational efficiency.



*Active RHEL subscriptions versions 6.4 & higher

Red Hat

Red Hat Insights Services

Advisor

Availability, performance, stability, and security risk analysis

Vulnerability

Assess Common Vulnerabilities and Exposures (CVEs) with advisories

Compliance

Assess and monitor compliance, built on OpenSCAP

Subscriptions

Track progress of your Red Hat subscription usage efficiently and confidently

Drift

Create baselines and compare system profiles

Policies

Define and monitor against your own policies to identify misalignment

Patch

Analyze for Red Hat product advisory applicability to stay up to date

Red Hat

Hey Jay, That's great, but....

- We don't allow that....
- I'd have to get an exception...
- My Security Team.....
- But we have firewalls...
- We are export controlled...
- But....GDPR/HIPAA/NIST/PCI-DSS/OMG/PDQ/XYZ....

- What's in it for Red Hat?
- How long do you keep it?
- Who do you share it with?

Forrest Gump - Paramount Pictures - 1994

Red Hat cares about your data privacy!

- Red Hat Privacy Statement
  https://www.redhat.com/en/about/privacy-policy
- Red Hat Polices and Guidelines
  https://www.redhat.com/en/about/all-policies-guidelines
- Trust Red Hat https://www.redhat.com/en/trust
  - trust@redhat.com
- If you see something, say something!
  - Product Security secalert@redhat.com
  - Information Security infosec@redhat.com

Data Processing Controls

- Insights runs in an OpenShift Dedicated Cluster running on the US East Coast
- Penetration testing is conducted by both internal and external parties
- Access to systems that handle customer data is controlled via multi-factor authentication and strict authorization controls
- Access is granted on a need to know basis and limited for required SaaS infrastructure operations.

Red Hat Insights, designed simple and secure

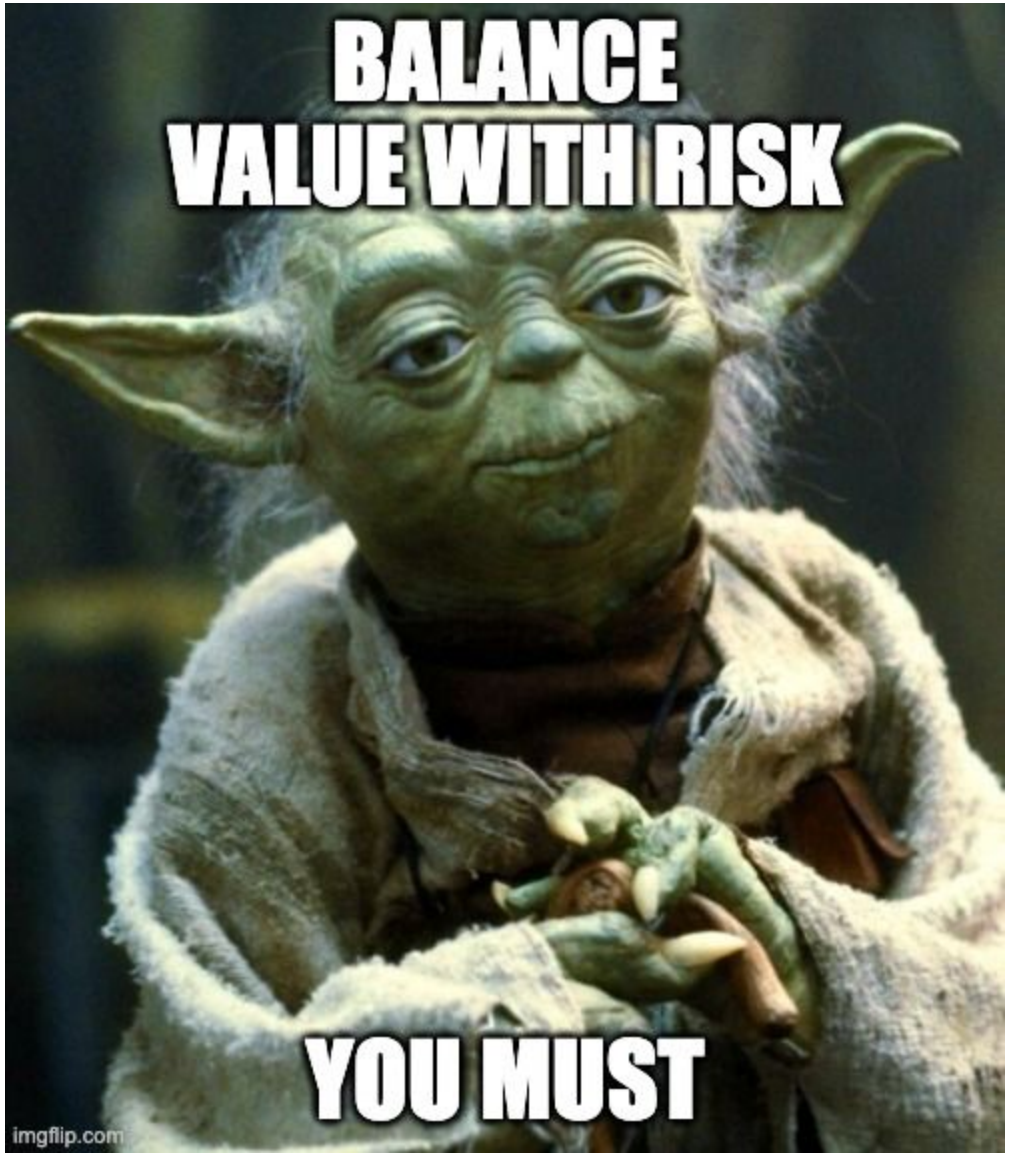
Insights is designed to work with minimal data.

You control what data is sent to Red Hat for analysis

Only Certified engineers have access to insights data

Data is encrypted throughout the process, with a customizable collection schedule

Only one uploaded data set is stored at a time



https://www.egnyte.com/blog/2017/07/3-buzzfeed-inspired-memes-on-protecting-your-content/

What is Sensitive Data? (Examples)

- Personally identifiable information (e.g., Employee records, SSN, drivers license number, PIN, usernames, passwords)
- Proprietary Information / Company Secrets
- Classified / Controlled Data
- Email / Internal Documents & Data
- Application Data
- IP addresses
- MAC addresses
- Hostnames / FQDNs
- LUN WWIDs
- UUIDs
- File pathnames and mountpoints
- Serial numbers

Where is it found? (Examples)

- Logs
- Configuration files
- Command output
- Network diagrams
- Architecture diagrams
- Network packet captures
- Package version numbers
- Heap dumps
- Application code
- Data directories / Volumes

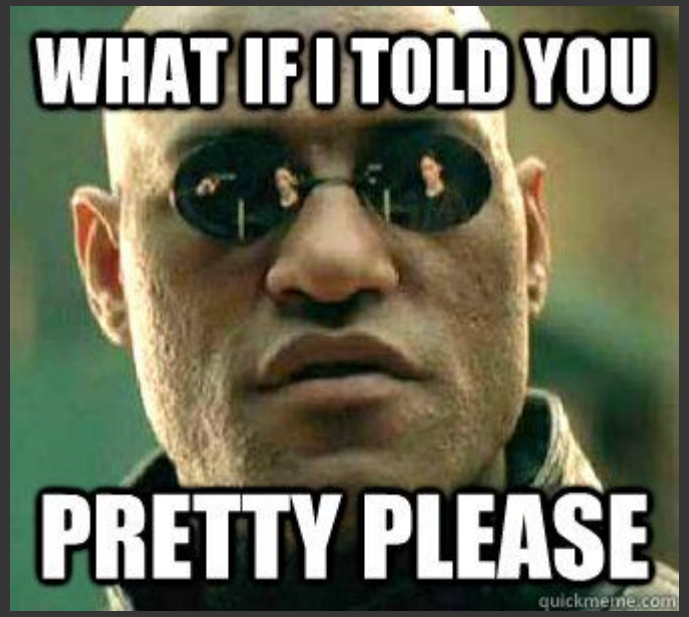
What tools may collect sensitive information? (Examples)

- ABRT
- kdump
- tcpdump
- Red Hat Labs
- redhat-support-tool
- sosreport
- sosreport Plugins
- soscleaner
- strace & ltrace
- logconv.pl
- satellite-debug
- foreman-debug
- rhevm-log-collector
- JBoss Diagnostic Reporter (JDR)
- oc adm must-gather

We Trust Red Hat....But

- We have rules
- We have regulatory bodies
- Some System Data / Information / metadata is considered sensitive
- Certain classification of sensitive data we can not / choose not to share with Red Hat or others.
- I have disconnected environments

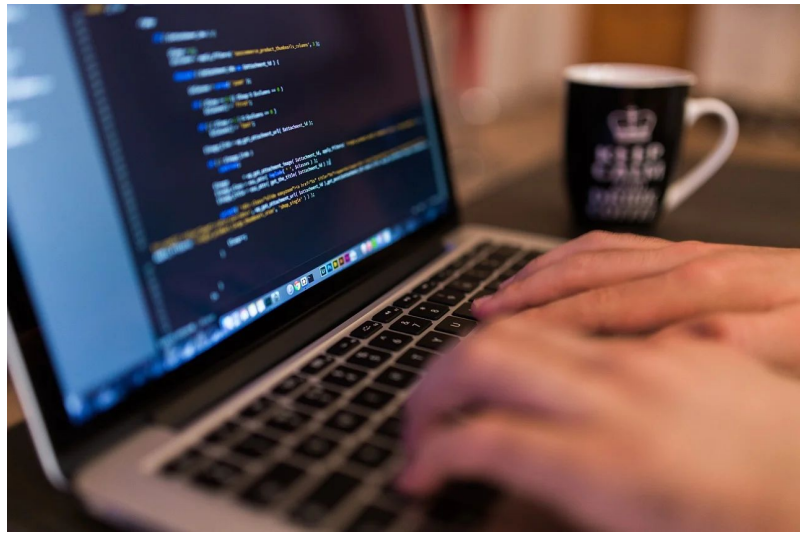
Now tell me how!



How to Roll Red Hat Insights out safely and securely

1. Start with a known system, without company workload (You've got an ansible pipeline to churn them out in a few minutes right?)
2. Analyze the data insights produces (insights-client --no-upload)
3. Check your internal company policies and documentation around data classifications and 3rd parties
4. Determine the value that Red Hat Insights has for your organization
5. Obfuscate / Remove any data that could potentially be in breach of a company policy from being uploaded
6. **`ansible all -i inventory -m command -a insights-client`**

The Details



- Gather data but don't send
  - `insights-client --no-upload`
- Obfuscate IP Addresses and/or Host Names
  - `/etc/insights-client/insights-client.conf`
    - `obfuscate=True`
    - `obfuscate_hostname=True`
- Deny certain commands to be ran
- Deny access to certain files
- Deny content with pattern or regex matching
  - `/etc/insights-client/remove.conf (old)`
  - `/etc/insights-client/file-redaction.yaml`
  - `/etc/insights-client/file-content-redaction.yaml`

Demo!

- Install insights-client
- Explore cli & config files
- Review & Adhere to Security Policy
- Ansible Automation
- Information Security Officer review
- Action Items! (Clean the data!)

What About sosreports?

- soscleaner - it's actually what Insights appears to use under the covers
- redhat-support-tool has soscleaner built into it (supported)
  - Please ensure this tool is up to date!
- `redhat-support-tool addattachment -c <CASE NUMBER> -o /path/to/sosreport`

Resources

- Red Hat Trust Promise https://www.redhat.com/en/trust
- Red Hat Privacy Policy https://www.redhat.com/en/about/privacy-policy
- Red Hat Insights Technical Q&A https://access.redhat.com/articles/4602981
- Where do I start? https://cloud.redhat.com/security/insights
- System Information Collected by Red Hat Insights https://access.redhat.com/articles/1598863
- Opting Out of Sending Metadata from Red Hat Insights Client https://access.redhat.com/articles/2025273
- Red Hat Insights Client Core Collection Description https://access.redhat.com/articles/5699071
- How do I protect my information when sending data to Red Hat? https://access.redhat.com/articles/1329063
- Red Hat Insights guidelines for deployment at scale https://access.redhat.com/blogs/2184921/posts/3606531
- Red Hat Personal Data Request - https://www.redhat.com/en/about/personal-data-request

Resources

- Obfuscating IP Addresses and Host Names in Red Hat Insights - https://access.redhat.com/articles/2047593
- YAML-style denylist configuration for Red Hat Insights Client - https://access.redhat.com/articles/4511681
- How to remove potentially sensitive data from a sosreport https://access.redhat.com/solutions/902563
- Personal Data Request Form https://www.redhat.com/en/about/personal-data-request
- Simple Content Access https://access.redhat.com/articles/4903191
- Insights - Basic Authentication for Cloud Access https://access.redhat.com/articles/4038251
- Subscribe a disconnected system https://access.redhat.com/solutions/3121571
- Accessing Red Hat Insights Through a Firewall/Proxy https://access.redhat.com/solutions/1583183
- Our Code is Open!
  - https://github.com/RedHatInsights/insights-core
  - https://github.com/sosreport/sos

Thank You!

April 27-28, 2021

Red Hat Summit is the premier open source technology event for thousands of IT professionals to innovate and focus on high-performing Linux, cloud, automation and management, container, and Kubernetes technologies.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat

Data Transfer

- Data is encrypted in three key ways:
  - On the host system at the point of collection
  - In transit across the network
  - When it is at rest on Red Hat the infrastructure
- Red Hat signs its data collection rules and will abort if the signature cannot be verified

Data Processing Controls

- Insights runs in an OpenShift Dedicated Cluster running on the US East Coast
- Penetration testing is conducted by both internal and external parties
- Access to systems that handle customer data is controlled via multi-factor authentication and strict authorization controls
- Access is granted on a need to know basis and limited for required SaaS infrastructure operations.

Data Retention

- Only one uploaded dataset is stored at a time
- When a new dataset is transmitted, the older raw dataset is deleted and replaced with the new dataset
- You can unregister Insights clients at any time
- If you stop sending us data, the last set will be kept for 15 days then it will be deleted
- Data is encrypted with LUKS on the Red Hat servers