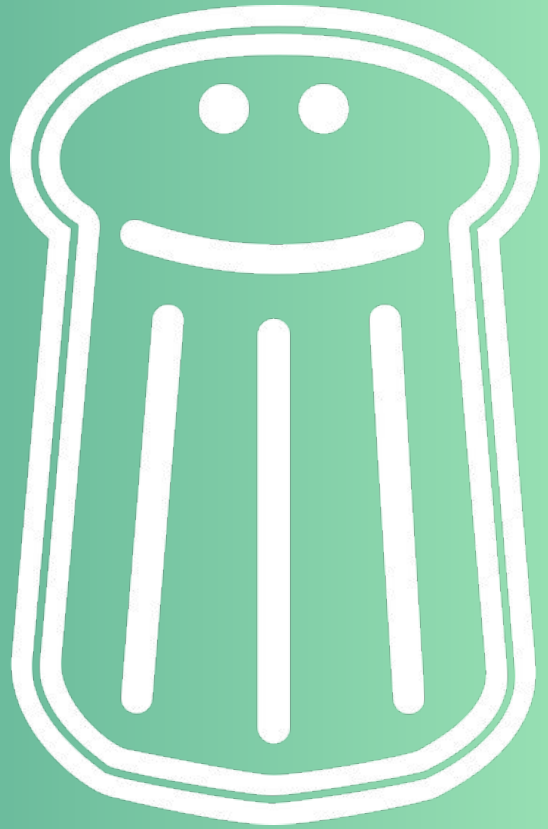
Configuration compliance in 2022

Pass The Salt 2022 - Ramps



alexandre@rudder.io

Who am I?

Alexandre BRIANCEAU

Cybersecurity university

Bull (French integrator) - Security and cloud project manager

French Polynesian Gov - Infrastructure Manager

Worteks - External Red Hat consultant

Rudder - Operations manager, then CEO

@abrianceau alexandre@rudder.io

Disclaimer: I may not be objective, feel free to discuss with me later!

Configuration audit are complexs

- Many different systems (RHEL-like, Debian-like, Windows, AIX…)
- Many standards (CIS, PCI-DSS, SecNumCloud, BSI C5, NIS, …)
- Many technologies and usage (servers, laptops, IoT, containers, …)
- Many heterogeneous configurations (many apps, many teams, …)
- Knowledge management is hard (*"You know nothing Jon Snow"*)

And finally, **many open source tools exists to audit configuration compliance !**

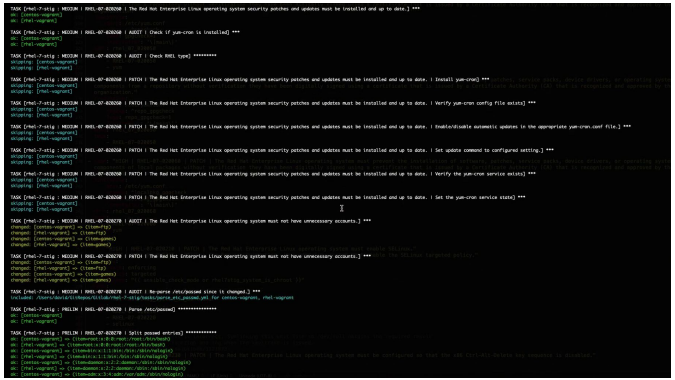
1 - Bash scripts and hardening deployment

Scripts or playbooks that enforce hardening. Auditing by erasing (is it auditing?).

[Ansible Lockdown collection](#) (MIT)

[OVH Debian-CIS](#) (Apache-2.0)

[Jsietch JShielder](#) (GPLv3)



2 - Scanning tool

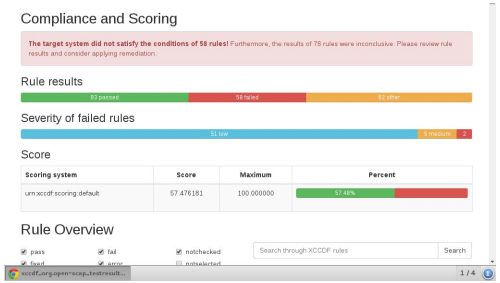
Focus on **scanning host by host based on templates** (such as CIS)

Some are generics:

OpenSCAP (LGLP-2.1), Cisofy Lynis (GPLv3) , Checkmarks KICS (Apache-2.0)

And other are specifics:

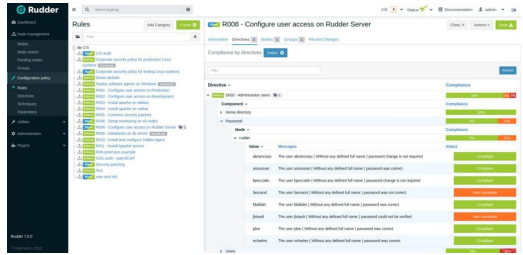
Rancher CIS-Operator (Apache-2.0), Aquasec Kub-Bench (Apache-2.0),
Alibaba Cloud Compliance (Apache-2.0), Neuvector Kubernetes CIS (Apache-2.0)



3 - Configuration management with dashboards

Auditing & enforcing all hosts with centralized dashboards

- Based on open-source project (but not open-source)
  - VMware Saltstack, Perforce Puppet Comply: dashboards and preset rules with enforcing
  - CFEngine Enterprise: dashboards only with enforcing
- Open-source projects
  - OpenSCAP Scap-Workbench (GPLv3): preset rules with enforcing on single host
  - Normation Rudder (GPLv3): dashboards, audit + enforcing
    (rules presets in 2023)



Conclusion

Choose your tools depending on your needs:

Small volumetry for sec team: OpenSCAP or Lynis

Small volumetry for ops team: Ansible lockdown or any configuration mgmt tool

Big volumetry for sec team: OpenSCAP + Satellite (for redhatters) or Rudder

Big volumetry for ops team: same

These tools are more versatile than specific tools (for Kubernetes for example).

Thank you!

Download these slides on Twitter @abrianceau or by scanning: