Risk and Vulnerability Management on Premise in Foreman

Viliam Krizan
GitHub: vkrizan
vkrizan @ Matrix

Agenda

- About me
- Introduction of Insights services
- Architecture
- Stack
- Considerations and the possibilities
- Questions

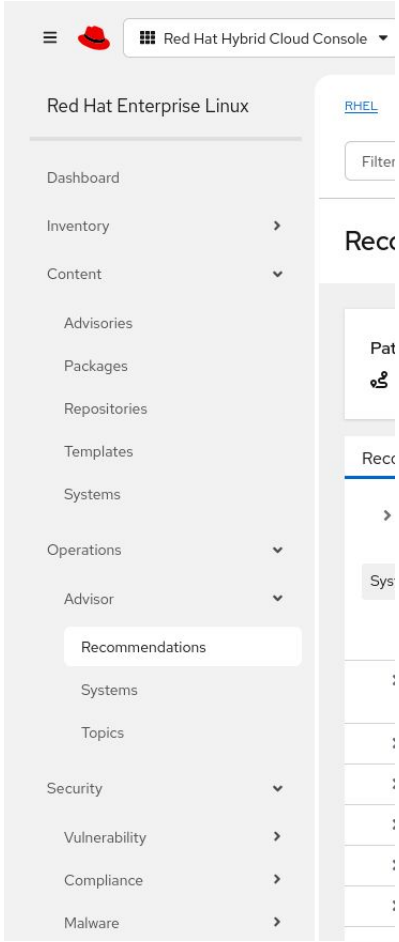
About me

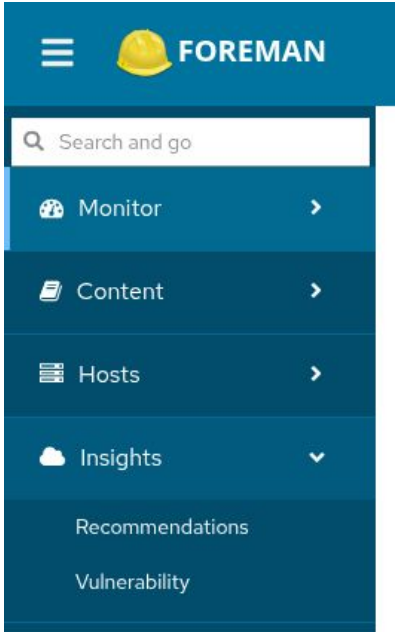
Viliam Krizan

- Principal Software Engineer @ Red Hat
- Over a decade experience with management tool development
- Open Source devotee
- Relatively new to Foreman Community
- FlightSim enthusiast

Introduction

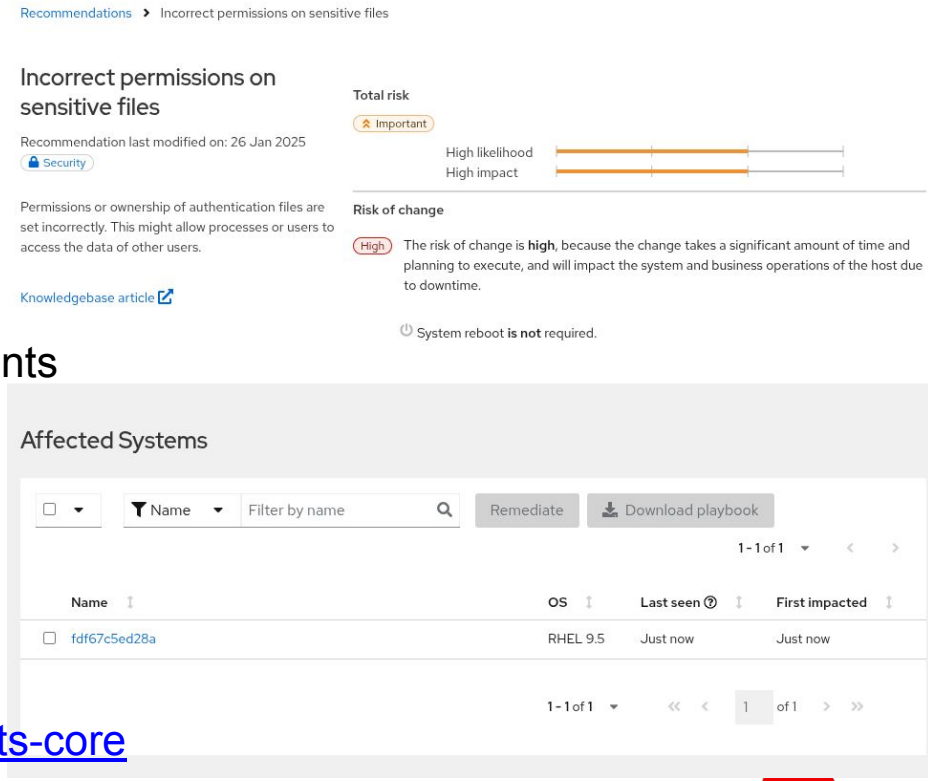
- Insights, Red Hat Lightspeed
- Analytical services
- SaaS available on Hybrid Console
  - https://console.redhat.com/
  - running on k8s/OpenShift
- Source Code
  - https://github.com/RedHatInsights/
- Insights Client providing facts
- Transformation to on premise





Recommendations w/ Advisor

- Proactive risk identification
- Host facts diagnosis
- Detection of misconfiguration
  - security hardening
  - performance and stability improvements
  - availability
- Rules in Python
- Remediations with Ansible w/ Remote Execution (REX)

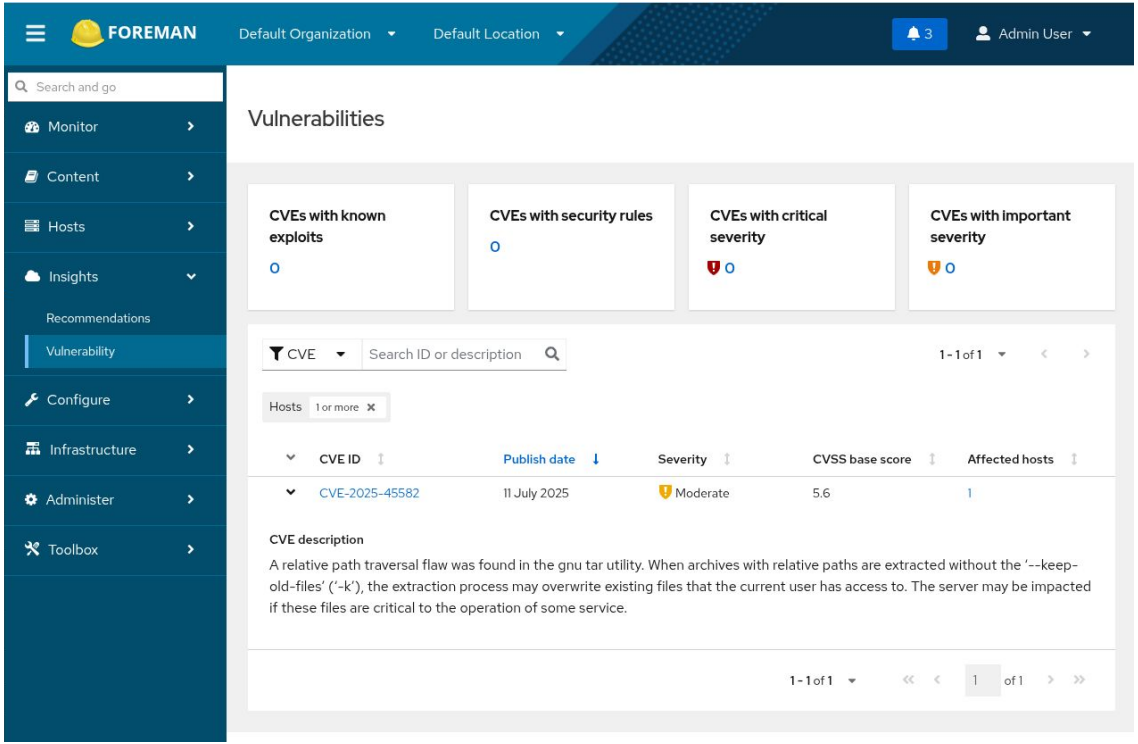


https://github.com/RedHatInsights/insights-core

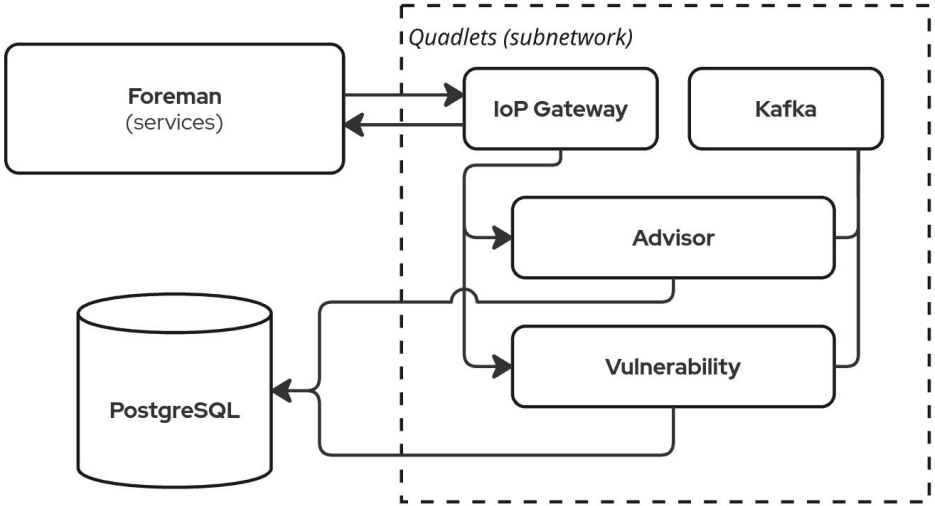
Vulnerability

https://github.com/RedHatInsights/vulnerability-engine/
https://github.com/RedHatInsights/vmaas/

- Security management for RHEL systems on Katello environments
- Introduced in Foreman 3.16
- Detection of CVEs
- Data from RPM repositories provided by Pulp
- Security Rules



Architecture



- Containers (Containerfile)
- Podman
- Quadlets (systemd)
- Subnetwork
- Shared PostgreSQL database
- Kafka
- IoP Gateway (bidirectional)
- Foreman Request Forwarder

Stack

- Python (Django, Connexion)
- Golang
- React, Patternfly
- Federated frontends

Considerations

- Microservice granularity
- RBAC
- RHEL systems
- System facts collection by Insights Client
- Security data
- No separation by locations (Forman organizations only)

Community and the possibilities

- Documentation
- Community recommendation rules (for Advisor)
- Standardization of a facts archive
- Support for other operating systems
- New services
  - Compliance (OpenSCAP)

Questions?

https://github.com/RedHatInsights/

Thank you!

https://community.theforeman.org/
https://matrix.to/#/#theforeman:matrix.org
https://matrix.to/#/#theforeman-dev:matrix.org

Stop by the Forman booth, provide feedback through a magic jar