



# 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

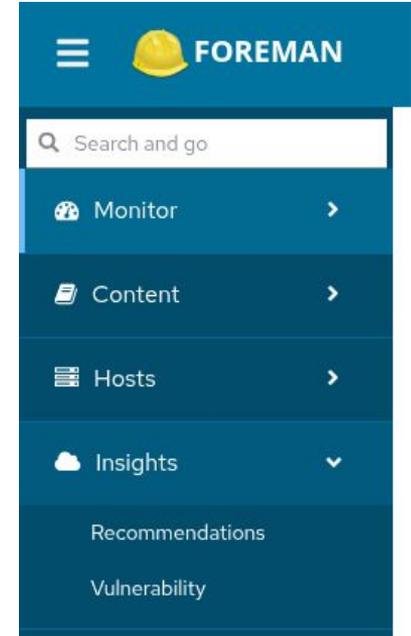
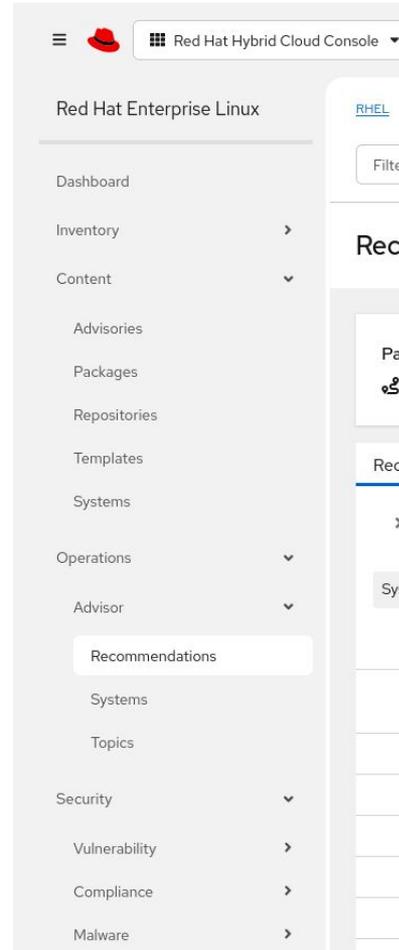
Viliam Krizan

- ➡ 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)

Recommendations > Incorrect permissions on sensitive files

## Incorrect permissions on sensitive files

Recommendation last modified on: 26 Jan 2025

[Security](#)

Permissions or ownership of authentication files are set incorrectly. This might allow processes or users to access the data of other users.

[Knowledgebase article](#)

Total risk

**Important**

High likelihood  
High impact



Risk of change

**High**

The risk of change is **high**, because the change takes a significant amount of time and planning to execute, and will impact the system and business operations of the host due to downtime.

System reboot is **not** required.

## Affected Systems

| Name                                  | OS       | Last seen | First impacted |
|---------------------------------------|----------|-----------|----------------|
| <input type="checkbox"/> fdf67c5ed28a | RHEL 9.5 | Just now  | Just now       |

1 - 1 of 1

<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

**FOREMAN** Default Organization Default Location 3 Admin User

Search and go

Monitor Content Hosts Insights Recommendations Vulnerability Configure Infrastructure Administer Toolbox

### Vulnerabilities

- CVEs with known exploits: 0
- CVEs with security rules: 0
- CVEs with critical severity: 1
- CVEs with important severity: 0

▼ CVE Search ID or description 1-1 of 1

Hosts 1 or more ✕

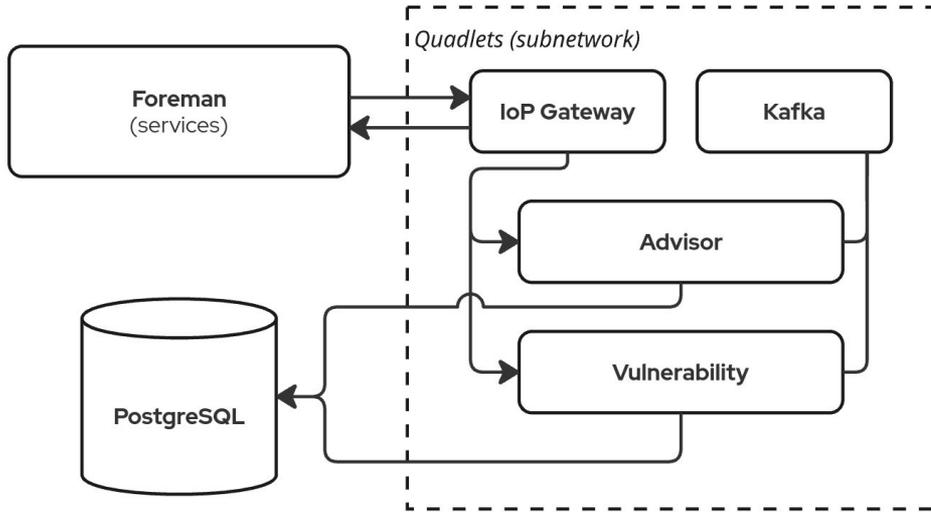
| CVE ID           | Publish date | Severity | CVSS base score | Affected hosts |
|------------------|--------------|----------|-----------------|----------------|
| ▼ CVE-2025-45582 | 11 July 2025 | Moderate | 5.6             | 1              |

**CVE description**  
A relative path traversal flaw was found in the gnu tar utility. When archives with relative paths are extracted without the '--keep-old-files' ('-k'), the extraction process may overwrite existing files that the current user has access to. The server may be impacted if these files are critical to the operation of some service.

1-1 of 1 1 of 1



# 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)





FOREMAN

# Questions?

<https://github.com/RedHatInsights/>



FOREMAN

# 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