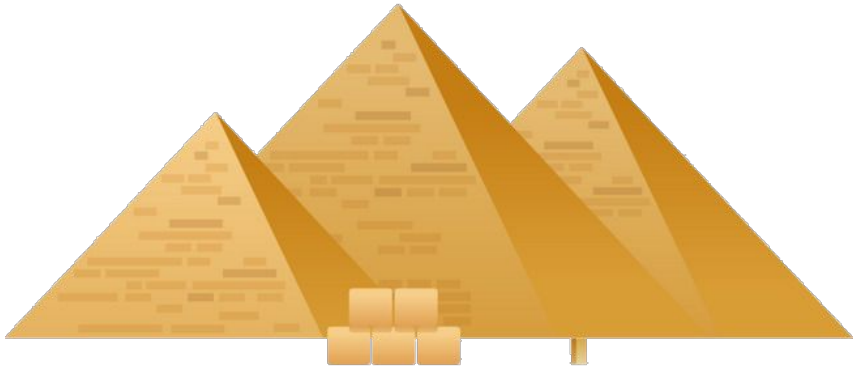


Discover project Thoth

Thoth team - https://thoth-station.ninja

Presented by:

Maya Costantini <mcostant@redhat.com>
Fridolin Pokorny <fridolin@redthat.com>

Red Hat

$ whoarewe

- Thoth - AIDevSecOps
  - Started (2018) as a research project in AICoE team, Office of the CTO
  - https://thoth-station.ninja
- Current members:
  - Christoph Goern, Dominik Tuchyna, Francesco Murdaca, Frido Pokorny, Gage Krumbach, Gregory Pereira, Harshad Reddy Nalla, Kevin Postlethwait, Maya Costantini, Pep Turro Mauri, Viliam Podhajecky
- See our linked YouTube channel for more information
- Follow us on Twitter - @ThothStation

Our mission

- Help Python developers and data scientists create healthy applications

- Project has multiple parts:
  - AICoE-CI - a CI that builds container images
  - Thoth resolver - a recommendation engine for Python applications
    - AIDevSecOps
  - Dependency Monkey - a service that can validate software in a cluster
  - jupyterlab-requirements extension for managing dependencies
  - Bots maintaining GitHub repositories
  - A self hosted Python package index using Pulp available to all Red Hatters
  - Container image analysis and containerized Python applications

Red Hat

Agenda

1. Introducing Python cloud based resolver
2. Benefits of resolving application dependencies in the cloud
   a. Know your runtime environment
   b. Know your Python dependencies
3. A CLI for the Python cloud based resolver
4. Demo

Thoth: The cloud Python resolver

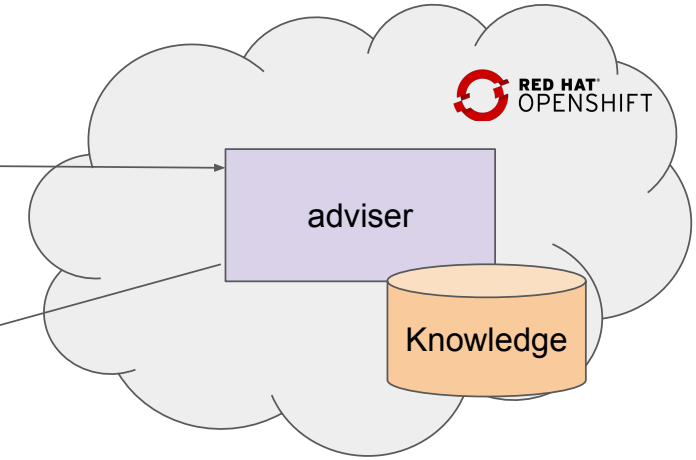
Red Hat

The Python resolver run in cloud

- Recommendation engine for Python applications
- Publicly available to the community
- Stochastic resolver implementing gradient-free reinforcement learning methods
  - Temporal difference learning is used in production
- See documentation for more information:
  - https://thoth-station.ninja/docs/developers/adviser

Python cloud resolver

Requirements
Constraints
Information about software in runtime environment
 - OS, Python version, base image, CUDA, ...
Information about hardware in runtime environment
 - CPU, GPU, ...
Static source-code analysis
Recommendation type



Lockfile + justification

```
$ pip install thamos
$ thamos config
$ thamos advise
```


Red Hat

Declarative interface for the resolver to resolve Python packages following prescribed rules

Prescriptions - declarative interface to the cloud based resolver

- Provide a way to declaratively state how the resolution process should look like
- Community driven open database used by the resolver to resolve high quality software - you can contribute!
  - https://github.com/thoth-station/prescriptions/
- A set of YAML files that are automatically consumed by the resolver in a deployment
- See documentation for more information:
  - https://thoth-station.ninja/docs/developers/adviser/prescription.html

Prescriptions - Example

- Pillow in version 8.3.0 does not work with NumPy

  https://github.com/python-pillow/Pillow/issues/5571

```
with PIL.Image.open(filepath) as img:
      numpy.array(img, dtype=numpy.float32)
```

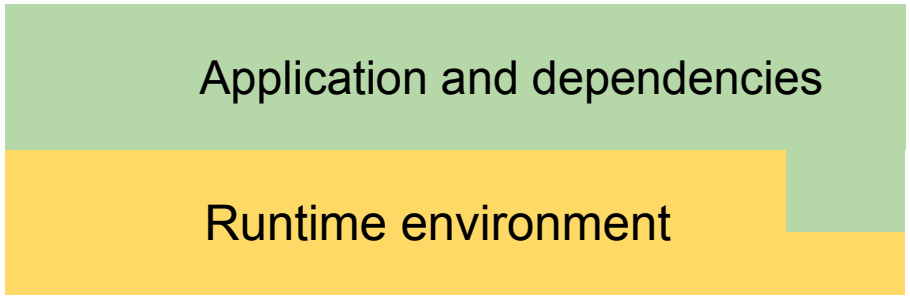
```
>           frame_paletted = np.array(im, np.uint8)
E           TypeError: __array__() takes 1 positional argument but 2 were given

/lib/python3.9/site-packages/imageio/plugins/pillow.py:745: TypeError
```

```
units:
 steps:
 - name: Pillow830TypeErrorStep
   type: step
   should_include:
     adviser_pipeline: true
   match:
     package_version:
       name: pillow
       version: ==8.3.0
       index_url: https://pypi.org/simple
     state:
       resolved_dependencies:
       - name: numpy
   run:
     not_acceptable: Pillow in version 8.3.0 does not work with NumPy
     stack_info:
     - type: WARNING
       message: Pillow in version 8.3.0 does not work with NumPy
       link: https://github.com/python-pillow/Pillow/issues/5571
```

Fitting the runtime environment

- Checking RPM, Python packages, ABI, CUDA, cuDNN, OpenMKL, ...
- One central place to declare requirements
  - Prescriptions (packages)
  - User's runtime environment (Pipfile, .thoth.yaml file)
- Still optional, the resolution might be "generic", like pip, Pipenv, ...



Red Hat

Security - AIDevSecOps

- Docs: Thoth security advises
- Recommendations based on static source code analysis
  - See recommendations from the Python standard library (example)
- PyPA - advisory-db
  - A database of known vulnerabilities in Python ecosystem
  - https://github.com/pypa/advisory-db
- Security Scorecards by Open Source Security Foundation
  - https://openssf.org/blog/2020/11/06/security-scorecards-for-open-source-projects/
  - Example: see scorecards_prefixed prescriptions for TensorFlow
- + additional information about Python packages not strictly related to security

🖥 Demo

```
pip install thamos
thamos config
thamos add “flask~=0.12”
thamos advise
```

Look at the tutorial documentation to reproduce the demo

https://redhat-scholars.github.io/managing-vulnerabilities-with-thoth

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat