ActiveState

Securing Python & Open Source Ecosystems

Safeguarding Trust in Public Repositories

Housekeeping

- We will host polls throughout the webinar
- We will be emailing everyone the slides after the webinar
- Submit your questions in the Q&A tab and we will answer at the end

ActiveState

Agenda

<table>
<tr><td>1.</td><td>Introduction to Supply Chain Security</td></tr>
<tr><td>2.</td><td>Current Initiatives in Public Ecosystems</td></tr>
<tr><td>3.</td><td>The Future of Repository Security</td></tr>
<tr><td>4.</td><td>Technical Demonstration of Trusted Publishing</td></tr>
<tr><td>5.</td><td>Q&A</td></tr>
</table>

ActiveState

Introductions

Pete Garcin

Director of Product
ActiveState

Dustin Ingram

 Fellow, Python Software
Foundation

Poll

Does your organization allow packages pulled directly from public repositories?

Choose one:

- ■ Yes, there are no restrictions.
- ■ We have some restrictions and rules about what is in place.
- ■ No, we don't allow any packages from public repositories.
- ■ I don't know.

Poll

What best describes your interest in securing public repos?

Choose one or more:

- Concerned about software supply chain attacks
- How this relates to our company policies
- How can I contribute to making open source safer
- General interest in community initiatives
- Other (let us know in the chat!)

ActiveState

Trusted Publishing Demo

Q&A

Learn More

Publishing to PyPI with a Trusted Publisher

https://docs.pypi.org/trusted-publishers/

Expanding Trusted Publisher Support

- https://blog.pypi.org/posts/2024-04-17-expanding-trusted-publisher-support/

Trusted publishing: a new benchmark for packaging security

- https://blog.trailofbits.com/2023/05/23/trusted-publishing-a-new-benchmark-for-packaging-security/

Securing your Package Ecosystem with Trusted Publishing – William Woodruff | PackagingCon 2023

- https://www.youtube.com/watch?v=Fa9cI2Rf2qc

Trusted Publishing: Lessons from PyPI - William Woodruff, Trail of Bits

- https://www.youtube.com/watch?v=Cc7hl_tyKWE

ActiveState

Next Steps

Schedule a call with our technical experts:

https://www.activestate.com/get-demo/

Try out Trusted Publishing:

https://docs.activestate.com/platform/start/pypi

Try the ActiveState Platform for free:

https://platform.activestate.com/