# Building Secure and Reproducible Open Source Runtimes

Machine Learning with Pets

DevOps.com
POWERED BY Techstrong | Learning

ActiveState

# ActiveState Workshop: Building Secure and Reproducible Open Source Runtimes

June 8, 1 pm ET

**Nicole Schwartz**
Security Product Manager
ActiveState

**Evan Cole**
Sr. Solutions Engineer
ActiveState

**Mitch Ashley**
CTO, Techstrong Group Principal
Techstrong Research

# Setup

1. Ensure you have Docker installed on your machine and running
2. Pull the docker image to your machine with
   docker pull ecole5/tensorflow-ml-demo:latest
3. Make an ActiveState account
   https://platform.activestate.com/

# Overview

# Goals

1. Run data experiments in Jupyter Notebook with open source ML libraries
2. Operationalize a system that identifies different breeds of dogs using a pre trained Tensorflow model

# Constraints

1. Ensure the security and integrity of all the components in the runtime (environment)
2. Ensure the runtime is reproducible cross platform
3. Ensure the runtime is portable enough to integrate into any DevOps pipeline

# Let’s Dive In

https://github.com/ActiveState/tensorflow_ml_demo

All instructions for this tutorial can be found here

# Key Takeaways

# Great open source observability is essential for both functionality and security.

Bundling the Jupyter IDE and the ML libraries in the runtime make the experiments portable and reproducible cross platform.

ML models are amazing compression systems. They take a lot of data and compute resource to train but are more efficient to run.

A lightweight command line tool can efficiently and securely integrate open source runtimes into your DevOps pipelines.

ActiveState

# Q&A

# Next Steps

- Create a free ActiveState account: https://platform.activestate.com/
- Review the tutorial on GitHub: https://github.com/ActiveState/tensorflow_ml_demo

# ActiveState Platform - Team Tier

Get reproducible runtimes, open source observability and satisfy your company’s security requirements:

- Up to 75 runtimes and older language versions
- Organization-level CVE reports and more security insights
- SBOMs, attestations and secure artifact repository support if you sign up by June 30!

**Get started with Team Tier for just $1k USD/year:** https://www.activestate.com/solutions/pricing/

ActiveState

# Thank You!