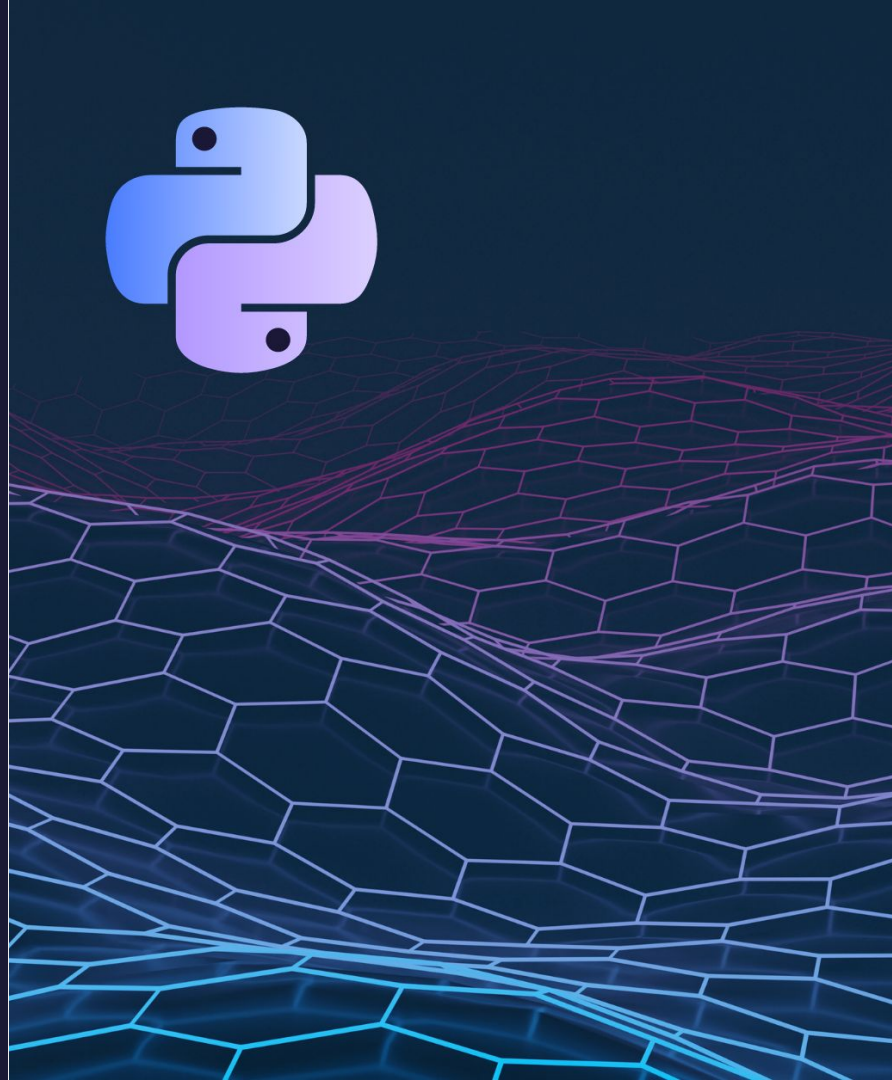
ActiveState

Snakes on the AI Plain:

Securing AI Applications From Supply Chain Attacks



Introductions

Evan Cole

Sr. Solutions Engineer
ActiveState

Dana Crane

Product Marketing Mgr
ActiveState

Why is ML open source?

- Involvement of academia in development
- Complex systems that are too risky/complex to build in house
- Inherently secure
- Composability

Industry Concerns

“Machine learning has accelerated so quickly and proliferated so widely largely because of this shared well of tools and data. But the trust that so many place in these common resources is a security weakness.”

Georgetown University’s Center for Security and Emerging Technology

The ML Open Source Supply Chain

What is the ML Supply Chain?

- **Training Data**
  - Data obtained from public repositories may pose a risk, especially if it's stored as non-human-readable blobs
- **Models**
  - Models are no more secure than the code from which they are built
- **Languages (Python, R, Julia, etc)**
  - Data Science packages are prime targets for compromise by bad actors due to the open nature of their ecosystems

Data Poisoning

Many AI models use input data to retrain their model, but:

- Studies have determined that corrupting as little as 0.01% of the data used by a model is enough to spoil it.
- Training data generated by AI (either synthetically on purpose, or inadvertently by using data generated by Mechanical Turk or Fivver users) will drive AI systems MAD after just 5 iterations.

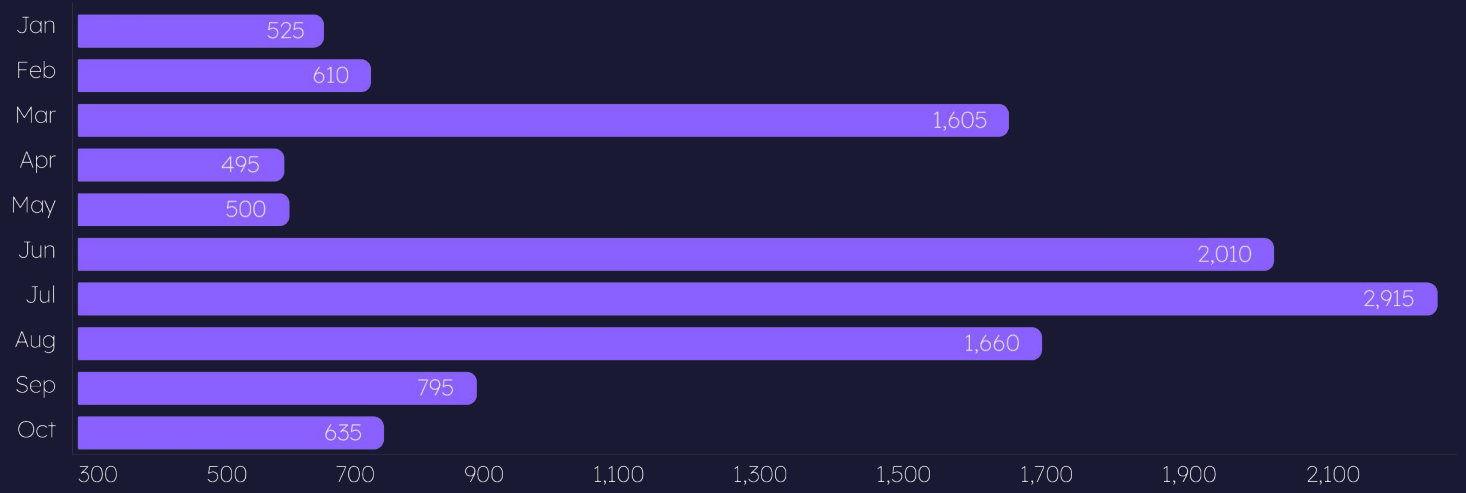
Model Poisoning

Models are really just code. It's common practice to:

- Pull models from a repository (like Hugging Face) that provides no guarantees as to security & integrity (unverified; unsigned, etc)
- Serialize models using Python's Pickle library whose docs state "The 'pickle' module is not secure."

Open Source Poisoning

Malicious Packages Published per Month, January-October 2022



Source: Mend Supply Chain Defender

Squeaky Wheels: Understanding The Build Threat

Python Packaging: Wheels vs Dist

Sdist -> Source Distribution
Wheel -> Binary Distribution

But Python is an interpreted language? Why would we need a binary distribution for a Python package?

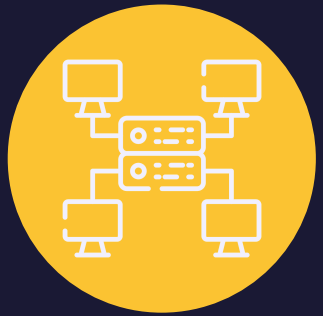
From Source To Binary

Tensorflow Source

Tensorflow Binary Artifact (Wheel)

Community Built Binary Artifacts

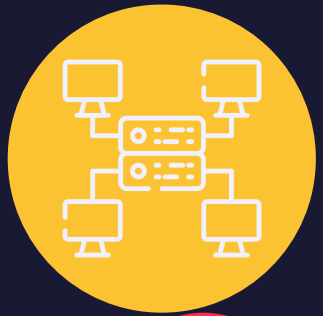
Tensorflow Source



Tensorflow Binary Artifact (Wheel)

Community Built Binary Artifacts

Tensorflow Source



Tensorflow Binary Artifact (Wheel)

From Source To Binary

Tensorflow Source

```
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(("%s %d %s\r\n" %
                    (self.protocol_version, code, message)).encode(
                        'latin-1', 'strict'))

    def send_header(self, keyword, value):
        """Send a MIME header to the headers buffer."""
        if self.request_version != 'HTTP/0.9':
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(
                ("%s: %s\r\n" % (keyword, value)).encode('latin-1', 'strict'))

        if keyword.lower() == 'connection':
            if value.lower() == 'close':
                self.close_connection = True
            elif value.lower() == 'keep-alive':
                self.close_connection = False
```

Tensorflow Binary Artifact
(Wheel)

Community Built Binary Artifacts

Tensorflow Source

```
                message =
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(("%s %d %s\r\n" %
                    (self.protocol_version, code, message)).encode(
                        'latin-1', 'strict'))

    def send_header(self, keyword, value):
        """Send a MIME header to the headers buffer."""
        if self.request_version != 'HTTP/0.9':
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(
                ("%s: %s\r\n" % (keyword, value)).encode('latin-1', 'strict'))

        if keyword.lower() == 'connection':
            if value.lower() == 'close':
                self.close_connection = True
            elif value.lower() == 'keep-alive':
                self.close_connection = False
```

Tensorflow Binary Artifact (Wheel)

Community Built Binary Artifacts

Tensorflow Source

```
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(("%s %d %s\r\n" %
                    (self.protocol_version, code, message)).encode(
                        'latin-1', 'strict'))

    def send_header(self, keyword, value):
        """Send a MIME header to the headers buffer."""
        if self.request_version != 'HTTP/0.9':
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(
                ("%s: %s\r\n" % (keyword, value)).encode('latin-1', 'strict'))

        if keyword.lower() == 'connection':
            if value.lower() == 'close':
                self.close_connection = True
            elif value.lower() == 'keep-alive':
                self.close_connection = False
```

Tensorflow Binary Artifact (Wheel)

Compromised Build Systems

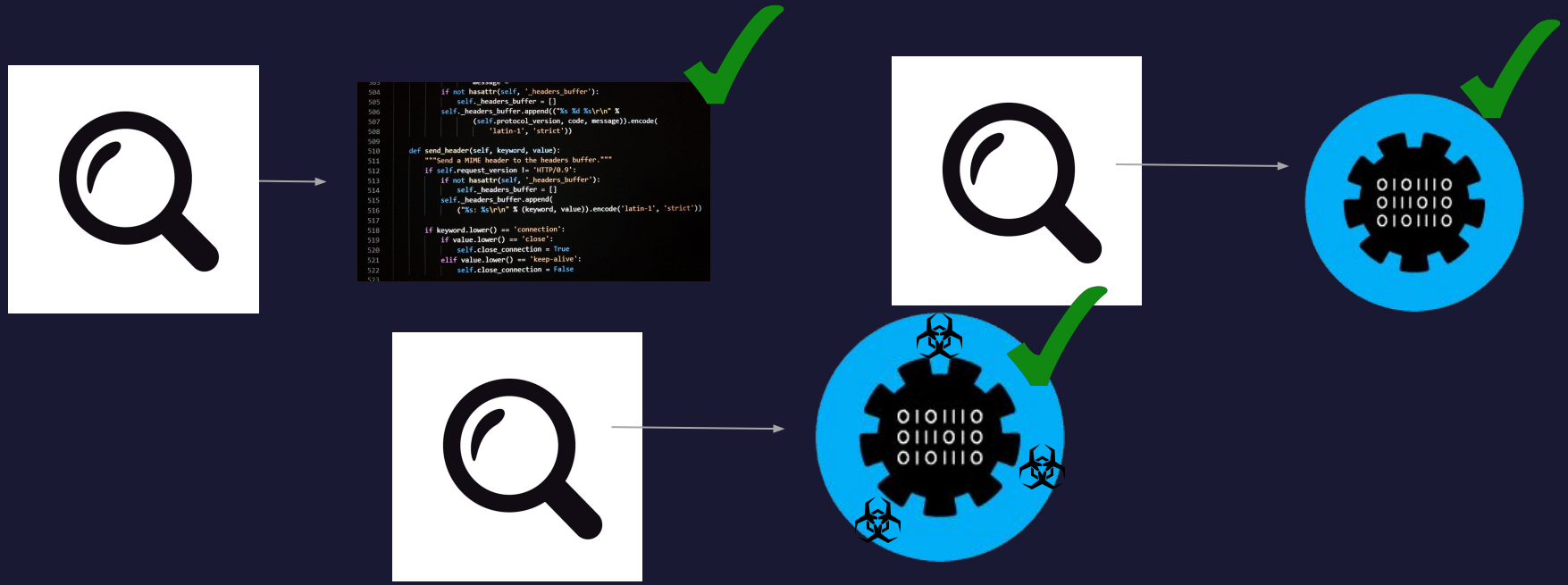
- Malware is purposely injected during the build process. Do you trust the publisher?
- The tools used in the factory contain malware and a trusted publisher inadvertently publishes infected binaries (Solarwinds)

Scan Tool Failure

- Scan tools cannot tell if a certain binary artifact was built to specification

Scan Tool Failure

- Scan tools cannot tell if a certain binary artifact was built to specification



Traditional AppSec Not Enough

74% of IT pros believe technologies like static and dynamic application security testing [SAST & DAST] are important, but feel that those technologies aren't enough to protect them from supply chain threats

Source: ReversingLabs Software Supply Chain Risk Survey

AcitveState Built Binary Artifacts

Tensorflow Source

AcitveState Built Binary Artifacts

Tensorflow Source

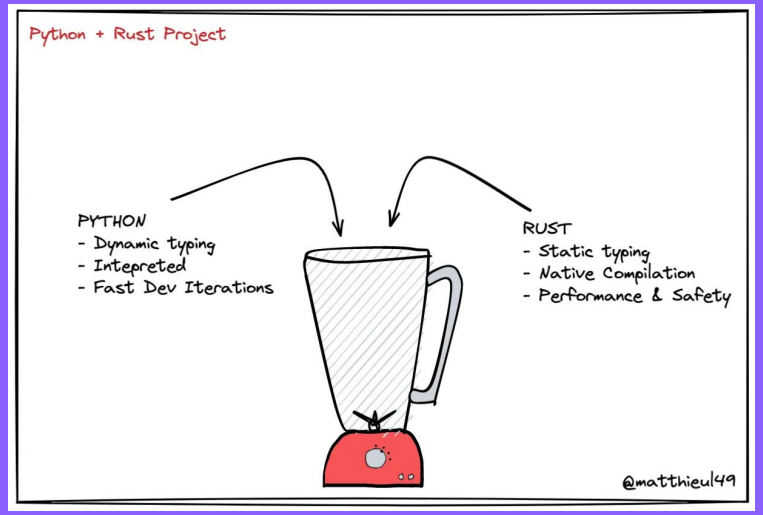
```
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(("%s %d %s\r\n" %
                    (self.protocol_version, code, message)).encode(
                        'latin-1', 'strict'))

    def send_header(self, keyword, value):
        """Send a MIME header to the headers buffer."""
        if self.request_version != 'HTTP/0.9':
            if not hasattr(self, '_headers_buffer'):
                self._headers_buffer = []
            self._headers_buffer.append(
                ("%s: %s\r\n" % (keyword, value)).encode('latin-1', 'strict'))

        if keyword.lower() == 'connection':
            if value.lower() == 'close':
                self.close_connection = True
            elif value.lower() == 'keep-alive':
                self.close_connection = False
```

Tensorflow Binary Artifact (Wheel)

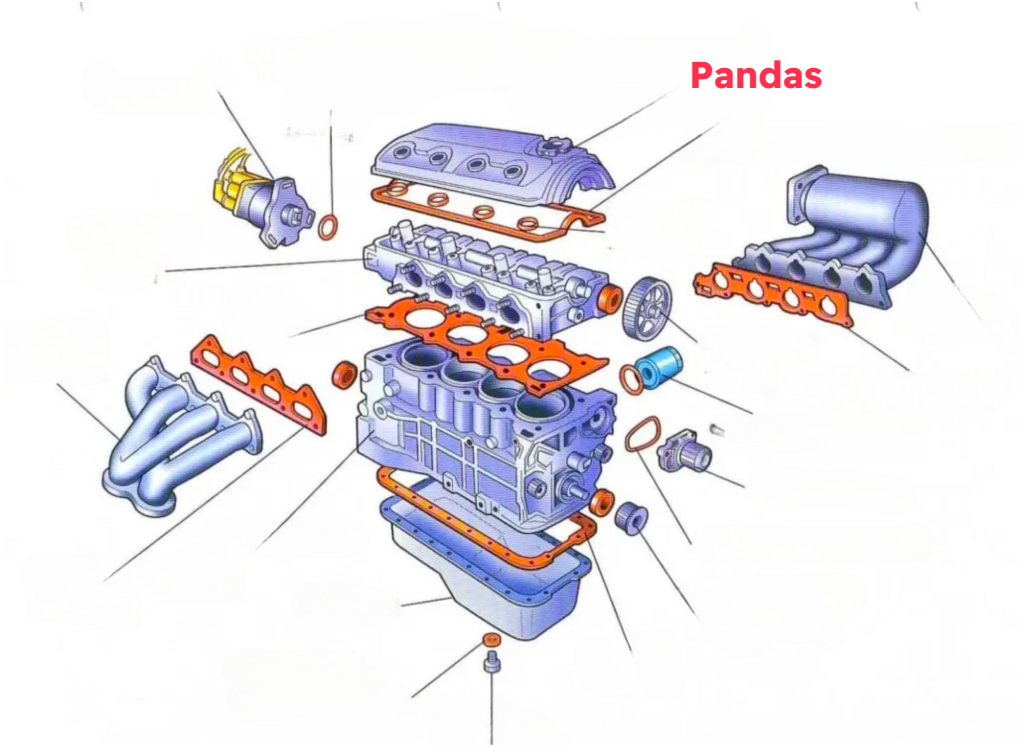
Rusty Wheels



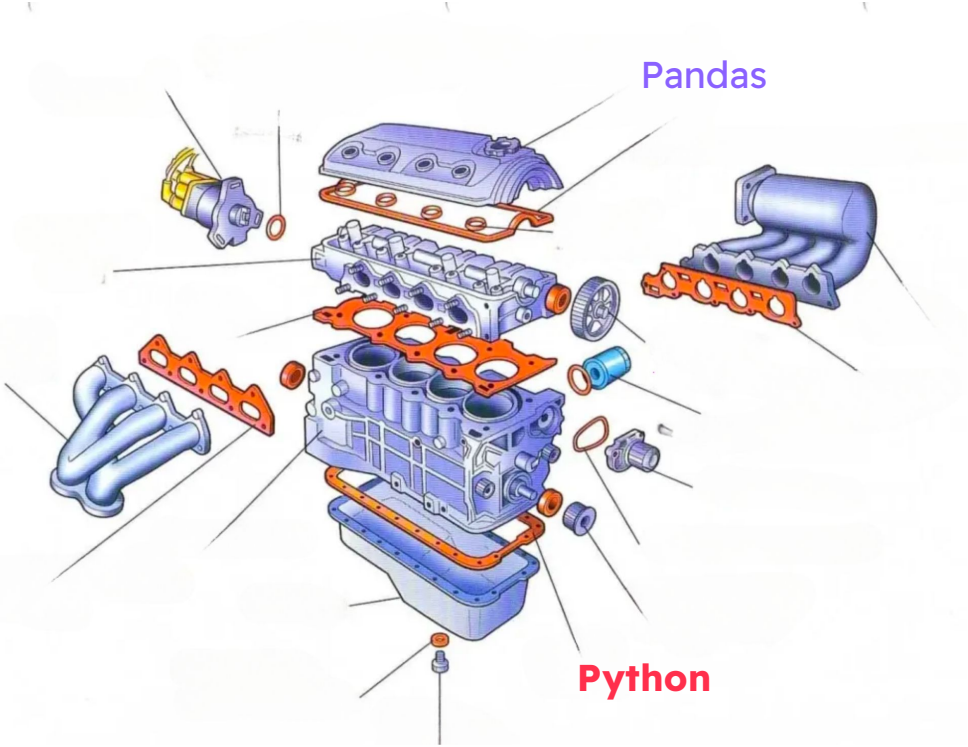
Rust is becoming increasingly popular choice for implementation ML business logic

Maturin is used to build wheels combining python and shared rust libraries

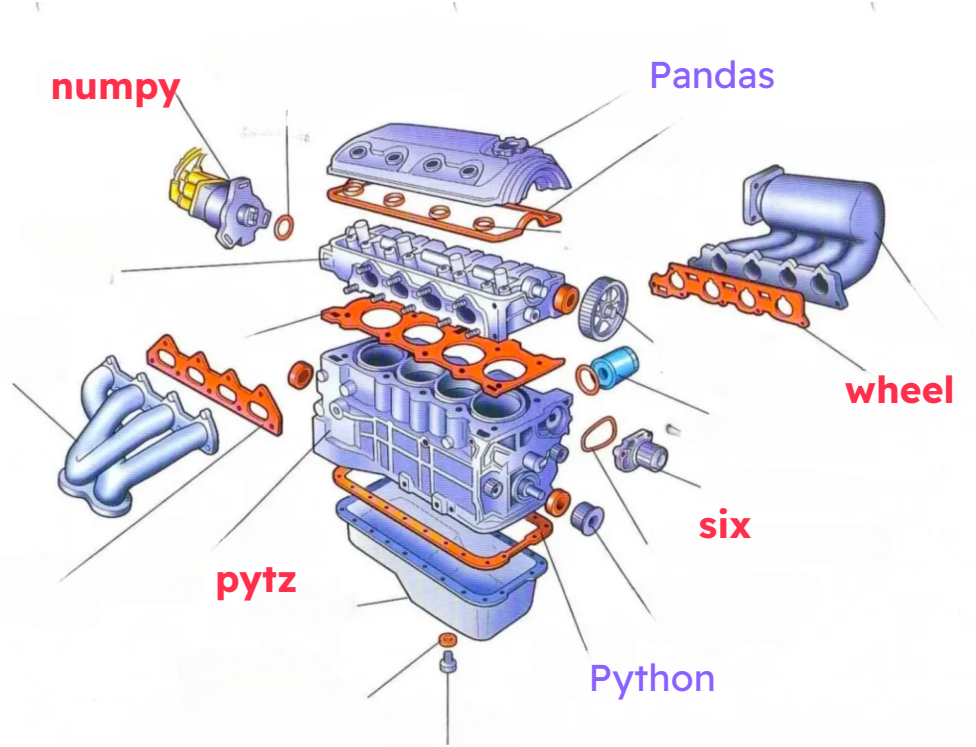
Open Source Runtime Observability



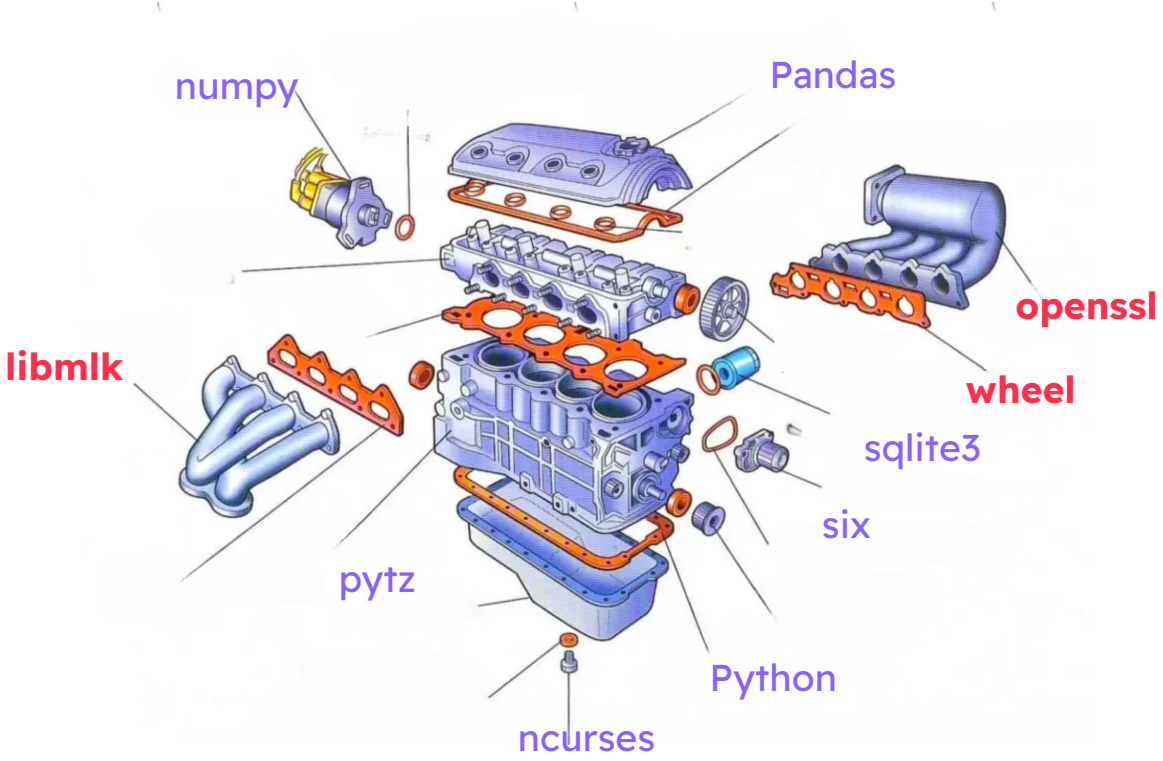
Open Source Runtime Observability



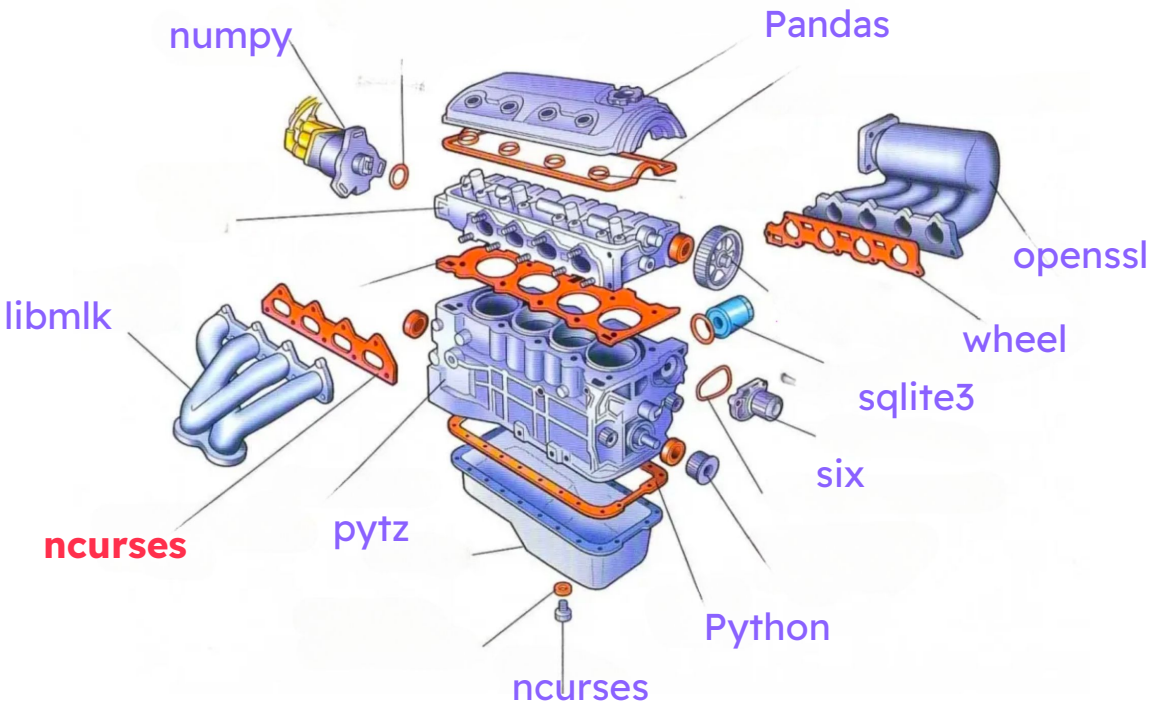
Open Source Runtime Observability



Open Source Runtime Observability



Open Source Runtime Observability



ActiveState Platform Demo

SLSA Standard

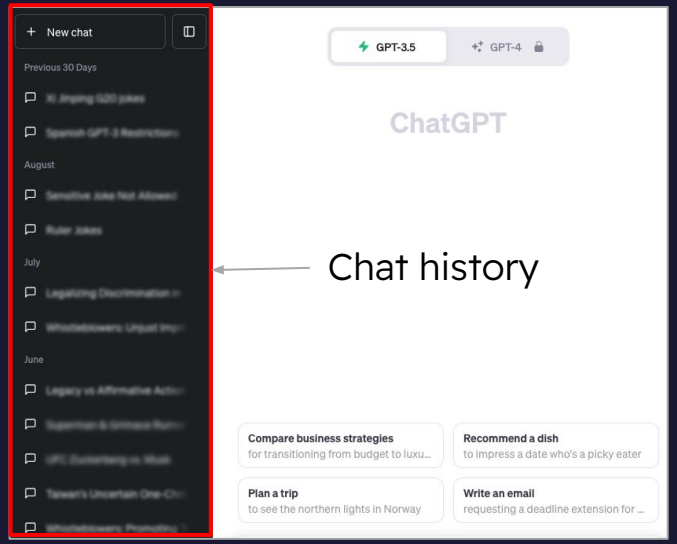
	ActiveState	**Conda Forge**
CI system	Declarative	Non-Declarative
Scripted builds	Yes	Maybe
Ephemeral containers	Yes	Maybe
Isolated processes	Yes	Unlikely
Hermetically sealed	Yes	Unlikely
Reproducible builds	Yes	No
Attestations	Yes	No

Avoidable Examples

Dec 5-22/2022 nightly builds installed a compromised dependency, torchtriton

```
2023-02-10 10:13:46 csikit-learn
2023-02-10 10:13:49 scikt-learn
2023-02-10 10:13:52 sikit-learn
2023-02-10 10:13:55 sciikt-learn
2023-02-10 10:13:58 scikit-leanr
2023-02-10 10:14:01 cikit-learn
2023-02-10 10:14:04 scikiit-learn
2023-02-10 10:14:07 scikit-earn
2023-02-10 10:14:11 sickit-learn
2023-02-10 10:14:16 scikit-leaarn
2023-02-10 10:14:21 scikit-lear
2023-02-10 10:14:25 sscikit-learn
2023-02-10 10:14:28 sciit-learn
2023-02-10 10:14:30 scikit-elarn
2023-02-10 10:14:34 scikit-llearn
2023-02-10 10:14:37 scikit-leran
2023-02-10 10:14:39 scikti-learn
2023-02-10 10:14:42 sccikit-learn
```

Typical typosquatting



redis-py bug exposed your Chat History to other users

Q&A

Next Steps

Schedule a demo with our product experts:
www.activestate.com/solutions/contact-sales/

Take our Supply Chain Security Survey & find out how you rate:
https://www.surveymonkey.com/r/BNGZPH6

Try the ActiveState Platform for free:
https://platform.activestate.com/

Get our Journey to Supply Chain Security eBook:
https://www.activestate.com/resources/white-papers/the-journey-to-software-supply-chain-security/