

```
1
2
3
4 match pycon_talk:
5     case "Python Security":
6         print(
7             "Because "
8             "\"Nobody Would Hack my Project\" "
9             "is not a Security Strategy"
10        )
11
12
13 # Benjamin Müllner + Pamphile T. Roy
14
```

Pamphile Roy {

- Senior Engineer @ Bitpanda
- SciPy and SALib maintainer
- Scientific Python SPEC Steering Committee
- Stellar Community Fund Pilot

}

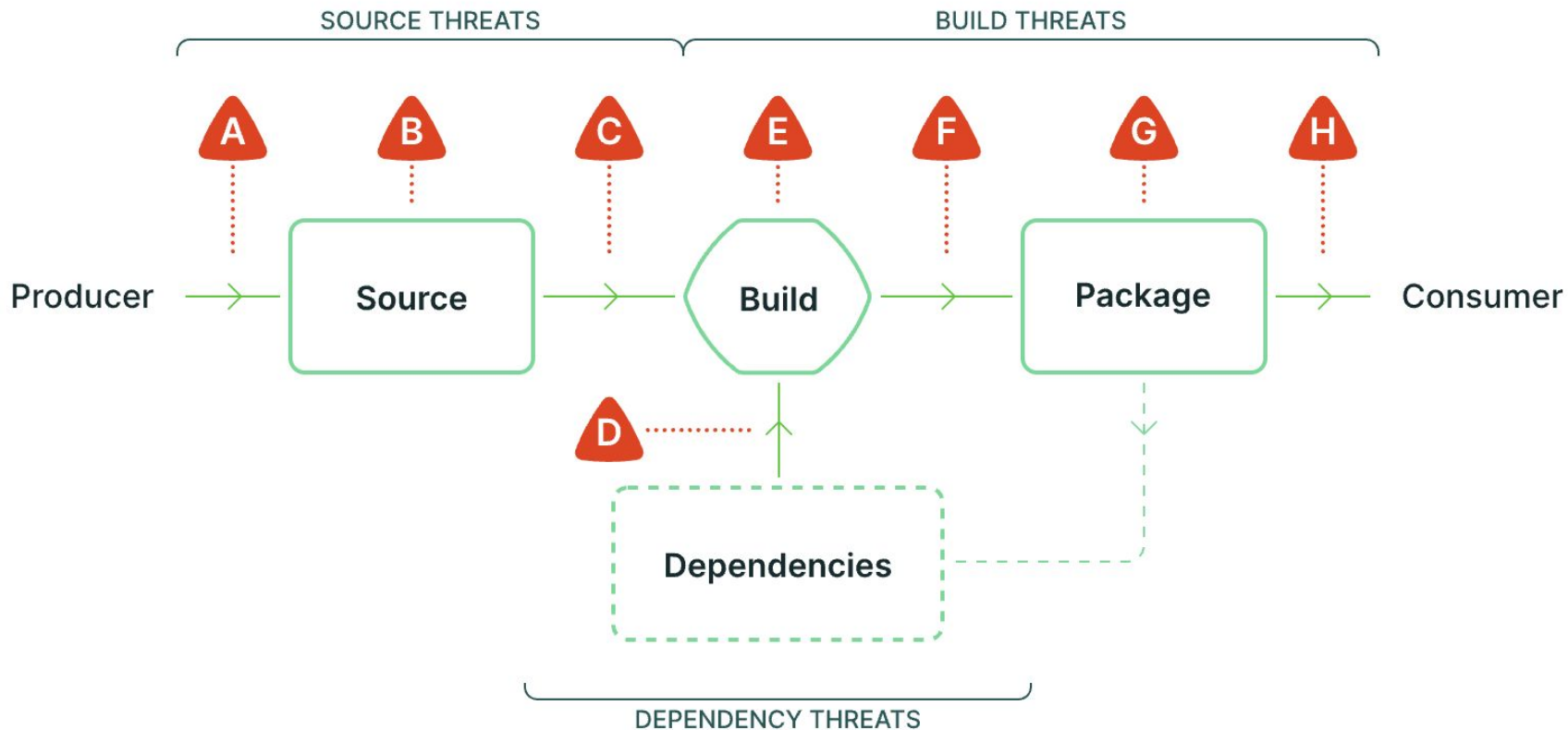


Benjamin Müllner {

- Staff IT Security Engineer @ Bitpanda
- (Former) Golang Engineer
- Building Dev(Sec)Ops Tooling

}





Solarwinds 'the Hack' {

09.2019 "Nobelium Group" get access

10.2019 Code Injection Test into Orion

02.2020 "Sunburst" Injected into Orion

03.2020 Solarwinds Ships out Malicious Software

}

```
1 PyTorch 'dependency injection' {
```

```
2 |  
3 |  
4 | 12.2022 torchtriton uploaded to PyPi
```

```
5 |  
6 | 5 days SSH, /etc, configs...
```

```
7 |  
8 |  
9 | Happy New Year
```

```
PyPi notified and PyTorch team  
removed the internal dependency
```

```
10 |  
11 | }  
12 |  
13 |  
14 |
```

Name Confusion Attacks

'OSS-RISK-3' {

Synonym

Typosquatting

Example

Colo(u)rama (PyPI, 2018)

AI Helpers

Make it Easier (for the Attacker)

}

```
1  tj-actions/changed-files {
2
3      Attack      Compromised PAT of Renovate Bot
4      Vector      (@tj-actions-bot)
5
6      Issue       Overprovisioned access for Bot
7
8
9      Attack      Memory Dump via Python Script
10
11
12      Avoid       Check Actions and Dependabot Config
13
14 }
```


1
2
3
4
5
6
7
8
9
10
11
12
13
14

Verify Your Dependencies

Python Packaging Authority 'PyPA' {

Transparency

Disclosure and impact assessment

Analysis

Security incident analysis

Features

2FA, OIDC, attestations,
quarantine, ...

Collaboration

PEP, security support, SPEC

}

release-1.0-py3-none-any.whl

action.yaml

Trusted Publisher 'attestations' }

Works on my machine, ship it!

Making a release:

- * CI
- * Build sdist and wheels
- * Sign
- * Push it! The CD part

}

The screenshot displays the GitHub repository page for 'soroban-cli'. The 'Verified details' section indicates that the release was verified by PyT. The 'Project links' section includes links to documentation, homepage, and source. The 'GitHub Statistics' section shows repository information, stars, forks, and open issues. The 'Maintainers' section lists the maintainer 'tupui'. The 'Unverified details' section shows details that have not been verified by PyT. The 'Meta' section includes license, author, maintainer, contributors, and other metadata. The 'Classifiers' section shows the development status. The 'File hashes' section displays a table of hashes for the release, including SHA256, MD5, and BLAKE2b-256. The 'Provenance' section shows the attestation bundles for the release.

Algorithm	Hash digest	Copy
SHA256	1a9aa2535683942486bbadf19aca95816af480221cc888575c68cb48b4c2e621	Copy
MD5	6add22b70e4e52e5c6818bfccdf247b	Copy
BLAKE2b-256	722e5fa9600340773d516c3a88831a1fa414bfbc5404fb524eafbb19bb71144	Copy

```
1  PyPI 'organization' {
2
3      # We can now create organizations! But why?
4
5
6      >>>      * Branding
7                * Logical grouping for your community
8                * Permissions management
9
10     >>>      * Support PyPI
11                * Organization plans with maybe extras ;)
12
13 }
14
```

PEP 751 'The Standard' {

File Name

`r"^pylock\.([\^.]+)\.toml$"`

Global

Not depending on pip, uv, poetry,
etc.

Standard

Makes life easier for Security Tools.

}

Scientific Python 'SPEC' {

SLSA



Validation of
software artifacts

OIDC



Use mechanism such
as TrustedPublisher
from PyPi

Permissions



Hardening workflow
environment; especially
for releases

Dependencies



Pin dependencies
with full hashes

<https://scientific-python.org/specs/spec-0008>

<https://scientific-python.org/specs/spec-0006>

}

Open Source 'Maintainer' {

Your pipeline has access to secrets, artifacts, and deploy targets.



Know your Maintainers



Treat workflow files like application code – review, audit, and lock them down.



Attest your Builds

}

Open Source 'User' {

Trust

Use Trusted Sources (Github, PyPI, ...)

Size

Prefer Well Maintained Projects

Review

Spend some time on checking what you are using and installing

Stay
Alert

Lock and continuously monitor dependencies

}


```
1 Thanks 'Now go check your dependencies' {
2
3
4
5
6
7
8
9
10
11
12
13
14 }
```



<https://github.com/tupui>

<https://github.com/prempador>

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**