ANACONDA®

Develop and Deploy Secure Python Solutions, Faster

AGENDA

- Anaconda Overview
- What We Heard
- The Solution
- Business On Prem Features
- Infosec & CVEs
- Business Case: Build vs. Buy
- Key Takeaways

ANACONDA OVERVIEW

- The leading provider of enterprise-grade Python & R
- We build OSS packages from source code in house giving DISA
- the certainty that you're getting packages that are:
  - Securely built from source on our systems
  - Tested for interoperability
  - Analyzed by the builders for all CVE claims leading to accurate vulnerability information
- Clients include Goldman Sachs, JP Morgan, Citigroup, SMBC, BNY Mellon, ICBC, Bank of America, and American Express and many gov entities

Anaconda supports a wide variety of use cases for some of the largest companies in these industries

Oil & Gas

ExxonMobil

Chevron

Manufacturing

3M NEC

LOCKHEED MARTIN

Panasonic cisco

Transportation

PORSCHE TOYOTA gm

Audi BOEING

Healthcare

CVSHealth.

LabCorp Laboratory Corporation of America

Roche

Finance

Goldman Sachs JPMorgan Chase & Co.

synchrony citi

Banking

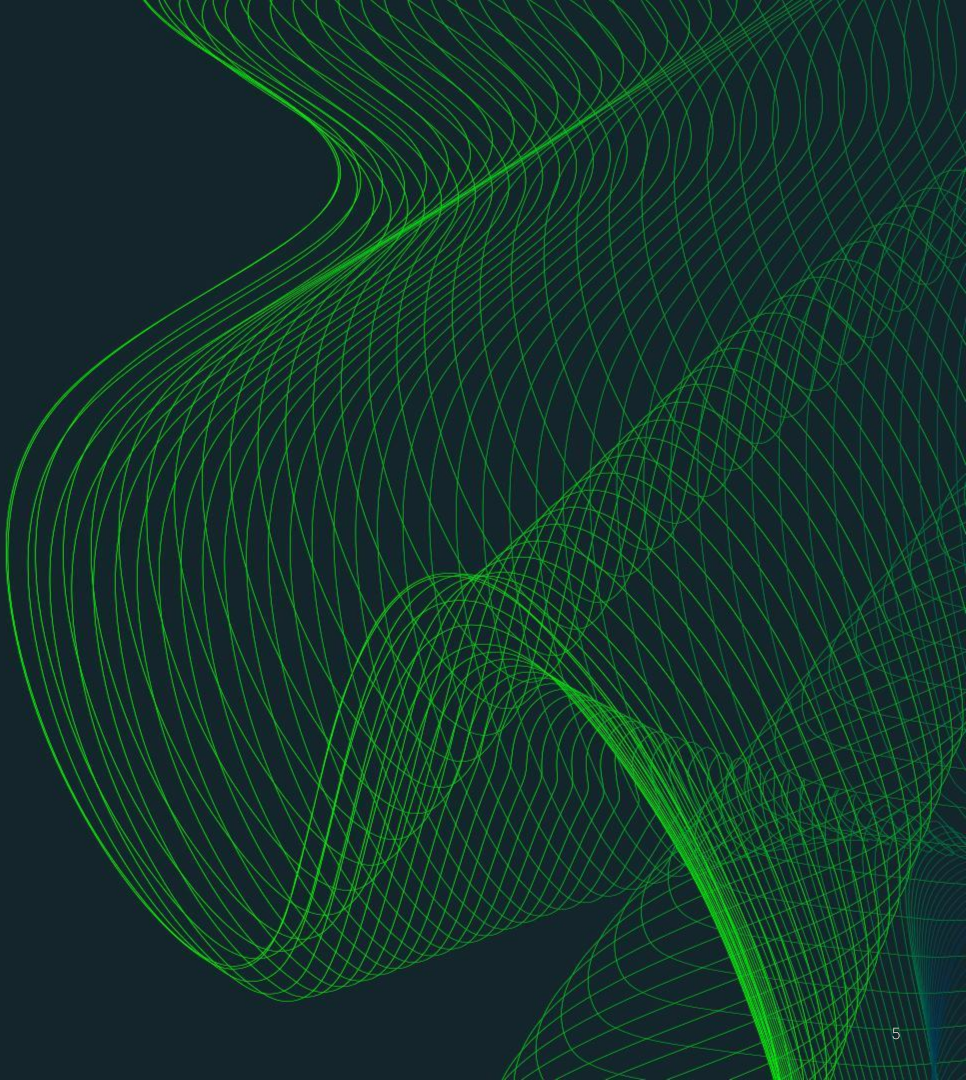
USAA® TRUIST

BANK OF AMERICA

WELLS FARGO

Anaconda Business

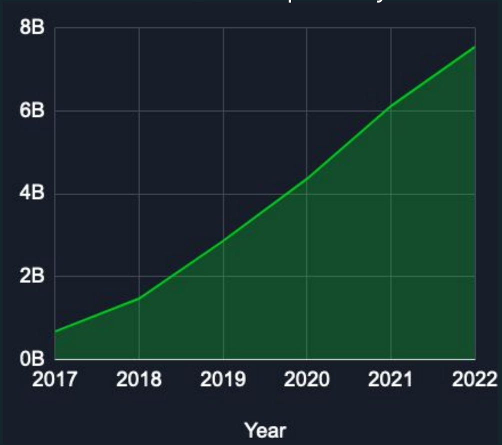
Centrally manage packages and CVEs



State of Python and data science today

Python adoption is increasing

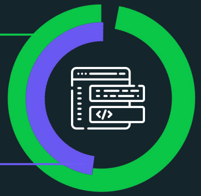
Package downloads from Anaconda's repository



Open-source software risks are multiplying

96% codebases contain OSS

48% codebases contain high-risk packages



Synopsys 2023 OSS Risk Analysis Report

633% increase

in malicious software supply chain attacks last year

Sonatype 2023 State of Software Supply Chain

Putting models into production takes too long

Over 1/4

of data scientists' time is taken up by deployment roadblocks, like meeting IT and InfoSec standards or refactoring models to other languages

Anaconda 2022 SODS

Less Than 1/2

of data teams effectively provide value to the organization

Gartner '23 CDO survey

Anaconda Business

Secure your software supply chain

Centralize

Enable access to the packages your team needs from a central customized repository.

Manage

Control access and distribution with custom channels and user access controls.

Secure

Keep vulnerabilities and unreliable software out of your pipeline with our security policy engine.

Secure your software supply chain

Leverage built-in security to stop risks without stopping workflows

Centralize

Pre Approved and Secure Access to Packages the Enterprise is willing to Support

Manage

Centrally Manage Python and R Packages while Enforcing Policies and Access Control

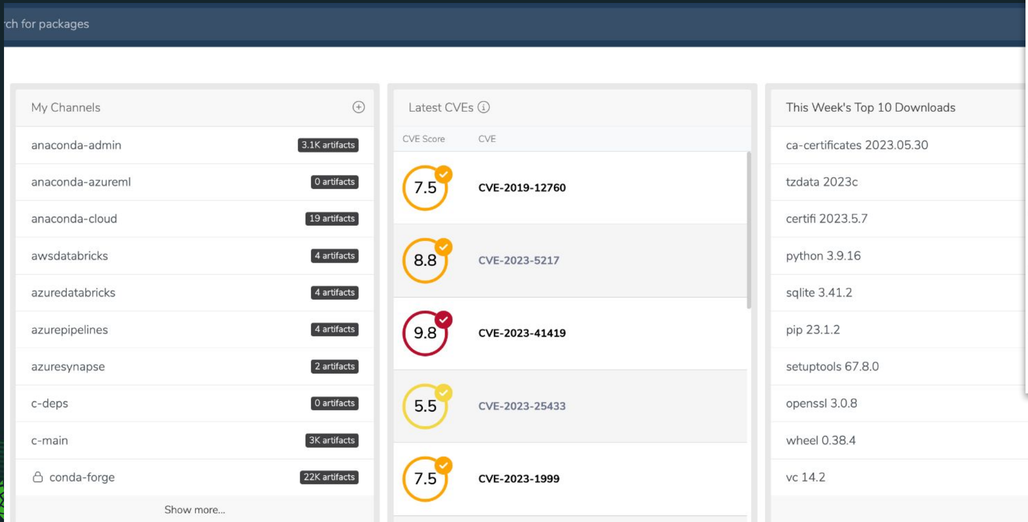
Secure

Enterprise Grade Repository with Vulnerability Curation from the experts

Centralize

Centralize access to open-source software through your dedicated repository

- Mirror our conda-curated repository as well as public repos including conda, CRAN, and standard Python.
- Centralize access to artifacts:
    - Packages, dependents, metadata
- Easily search and distribute consumable artifacts to end users and workflows



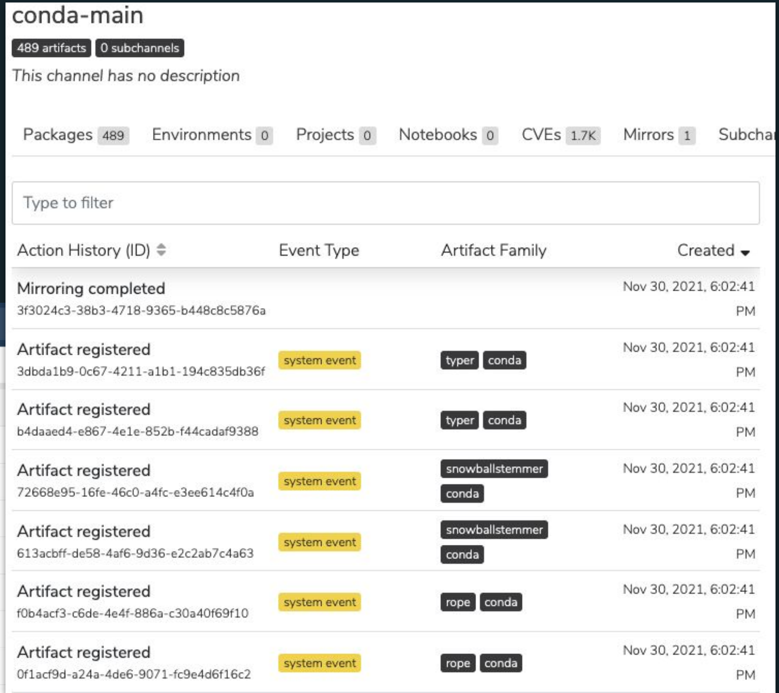
My Channels	
anaconda-admin	3.1K artifacts
anaconda-azureml	0 artifacts
anaconda-cloud	19 artifacts
awsdatabricks	4 artifacts
azuredatabricks	4 artifacts
azurepipelines	4 artifacts
azuresynapse	2 artifacts
c-deps	0 artifacts
c-main	3K artifacts
conda-forge	22K artifacts

Show more...

Latest CVEs

CVE Score	CVE
7.5	CVE-2019-12760
8.8	CVE-2023-5217
9.8	CVE-2023-41419
5.5	CVE-2023-25433
7.5	CVE-2023-1999

This Week's Top 10 Downloads	
ca-certificates 2023.05.30	
tzdata 2023c	
certifi 2023.5.7	
python 3.9.16	
sqlite 3.41.2	
pip 23.1.2	
setuptools 67.8.0	
openssl 3.0.8	266
wheel 0.38.4	188
vc 14.2	168



conda-main

489 artifacts 0 subchannels

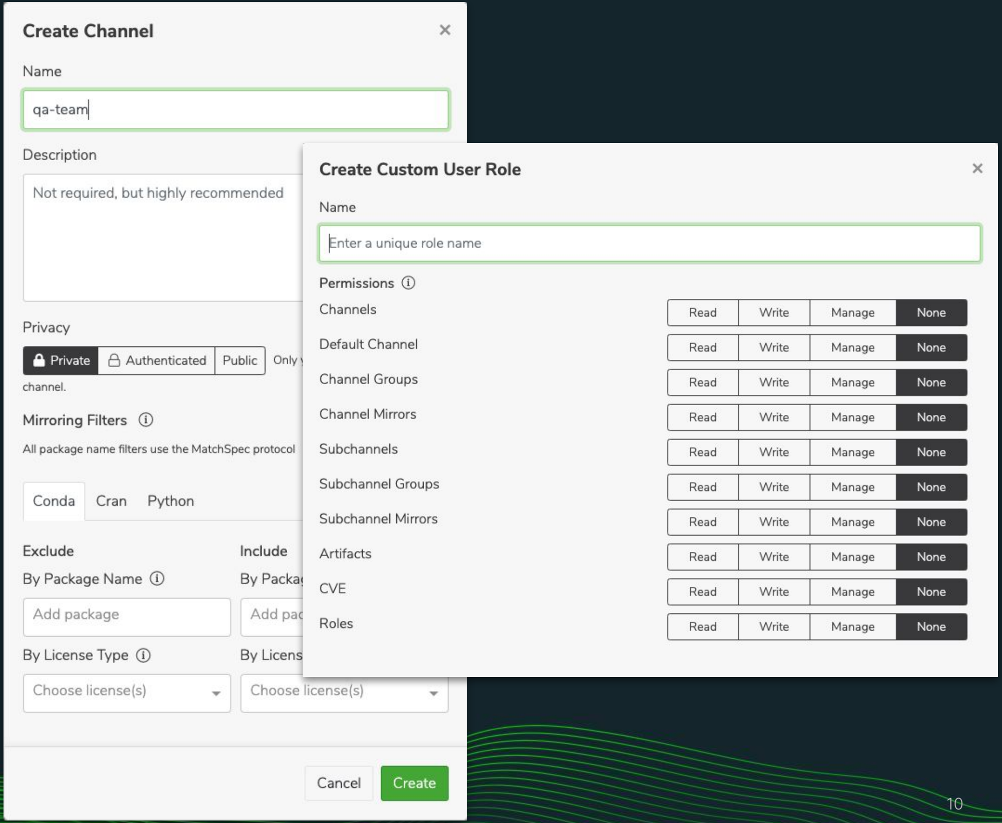
This channel has no description

Action History (ID)	Event Type	Artifact Family	Created
Mirroring completed 3f3024c3-38b3-4718-9365-b448c8c5876a			Nov 30, 2021, 6:02:41 PM
Artifact registered 3dbda1b9-0c67-4211-a1b1-194c835db36f	system event	typer conda	Nov 30, 2021, 6:02:41 PM
Artifact registered b4daaed4-e867-4e1e-852b-f44cadaf9388	system event	typer conda	Nov 30, 2021, 6:02:41 PM
Artifact registered 72668e95-16fe-46c0-a4fc-e3ee614c4f0a	system event	snowballstemmer conda	Nov 30, 2021, 6:02:41 PM
Artifact registered 613acbff-de58-4af6-9d36-e2c2ab7c4a63	system event	snowballstemmer conda	Nov 30, 2021, 6:02:41 PM
Artifact registered f0b4acf3-c6de-4e4f-886a-c30a40f69f10	system event	rope conda	Nov 30, 2021, 6:02:41 PM
Artifact registered 0f1acf9d-a24a-4de6-9071-fc9e4d6f16c2	system event	rope conda	Nov 30, 2021, 6:02:41 PM

Manage

Control access and distribution with custom channels and user access controls

- Enable open-source innovation from your on-premises and private cloud environments
- Manage permissions across channels with group-wide or user-specific access controls
- Track artifact history with platform reporting and monitoring
- Manage vulnerabilities with Anaconda-curated CVEs



Create Channel

Name: qa-team

Description: Not required, but highly recommended

Privacy: [✓ Private] Authenticated Public Only

channel.

Mirroring Filters ⓘ

All package name filters use the MatchSpec protocol

Exclude

By Package Name ⓘ

Add package

By License Type ⓘ

Choose license(s)

Include

By Packa

Add pac

By Licens

Choose license(s)

Create Custom User Role

Name: Enter a unique role name

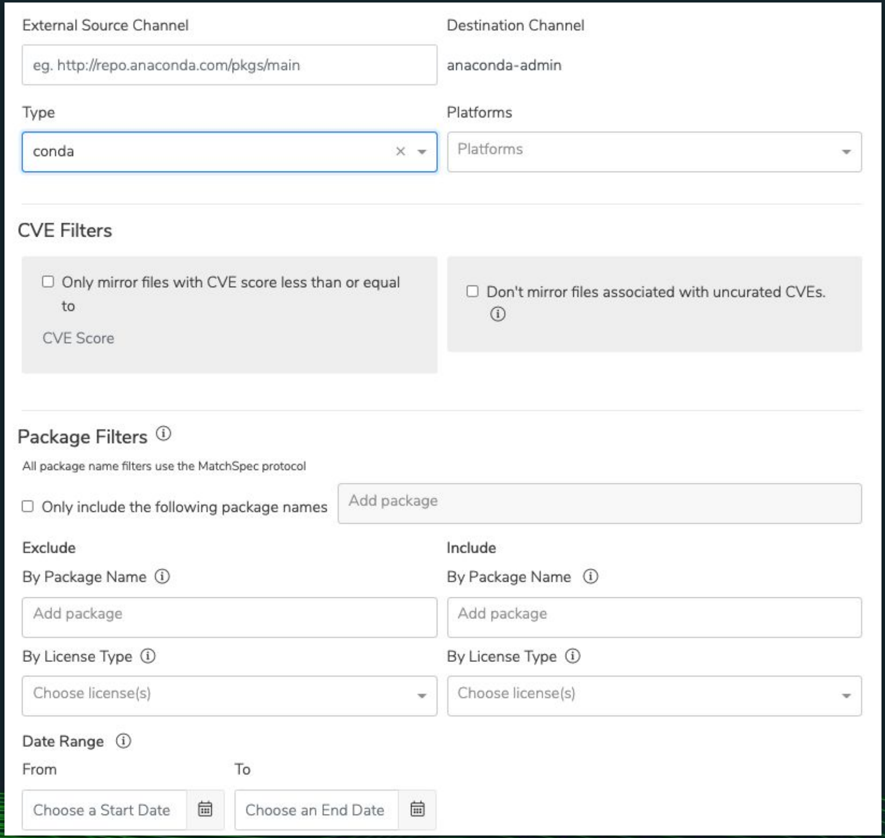
Permissions ⓘ

Channels	Read	Write	Manage	[✓ None]
Default Channel	Read	Write	Manage	[✓ None]
Channel Groups	Read	Write	Manage	[✓ None]
Channel Mirrors	Read	Write	Manage	[✓ None]
Subchannels	Read	Write	Manage	[✓ None]
Subchannel Groups	Read	Write	Manage	[✓ None]
Subchannel Mirrors	Read	Write	Manage	[✓ None]
Artifacts	Read	Write	Manage	[✓ None]
CVE	Read	Write	Manage	[✓ None]
Roles	Read	Write	Manage	[✓ None]

Secure

Keep vulnerabilities out of your software supply chain

- Proactively implement enterprise-grade security policies with CVSS and license filtering
- Secure access through approval path and private channels
- Ensure packages meet security requirements with Anaconda-curated vulnerability data
- Support for air-gapped environments
- Schedule pkg updates at your own frequency



External Source Channel: eg. http://repo.anaconda.com/pkgs/main

Destination Channel: anaconda-admin

Type: conda

Platforms: Platforms

CVE Filters

□ Only mirror files with CVE score less than or equal to

CVE Score

□ Don't mirror files associated with uncurated CVEs.

Package Filters

All package name filters use the MatchSpec protocol

□ Only include the following package names: Add package

Exclude

By Package Name: Add package

By License Type: Choose license(s)

Include

By Package Name: Add package

By License Type: Choose license(s)

Date Range

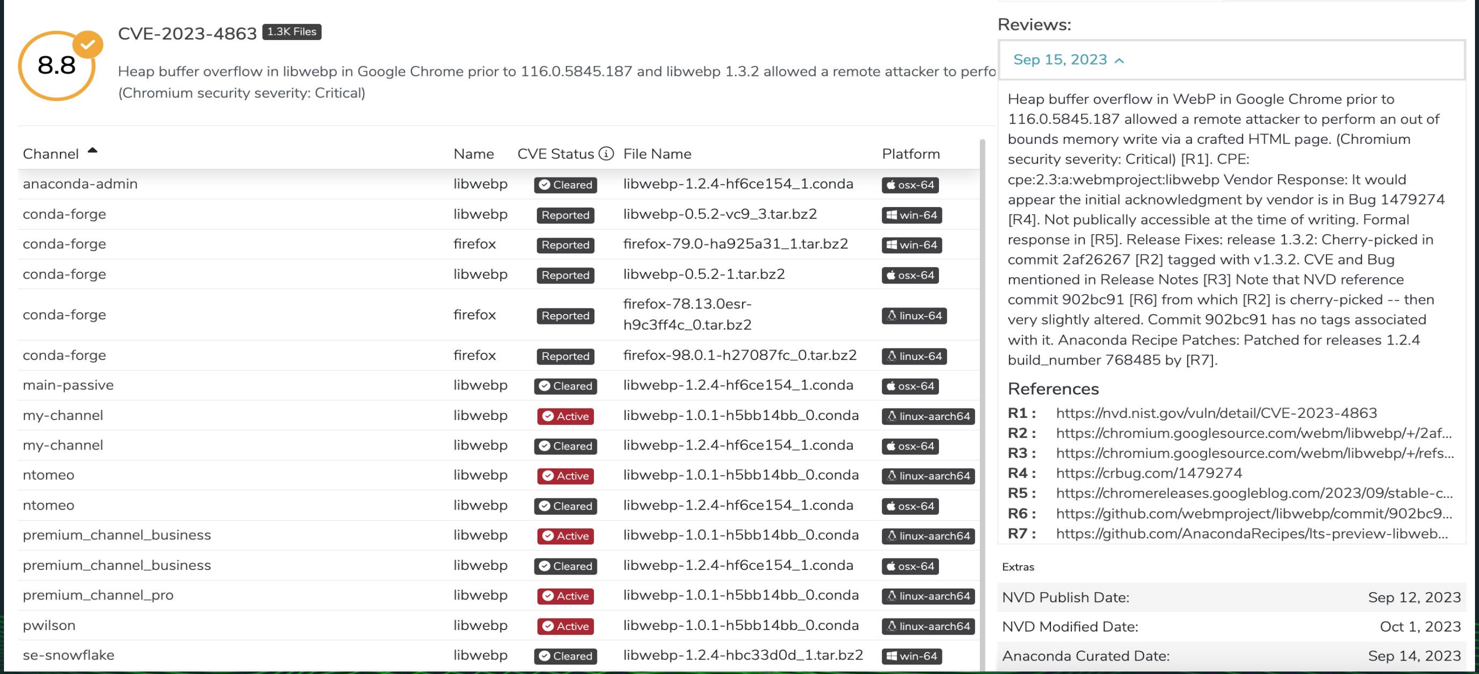
From: Choose a Start Date

To: Choose an End Date

Secure

Review Vulnerability Information

- Have ongoing visibility to new CVEs
- Dashboard of impacted versions
- CVE Commentary w references



8.8 CVE-2023-4863 1.3K Files

Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perfo
(Chromium security severity: Critical)

Channel	Name	CVE Status	File Name	Platform
anaconda-admin	libwebp	Cleared	libwebp-1.2.4-hf6ce154_1.conda	osx-64
conda-forge	libwebp	Reported	libwebp-0.5.2-vc9_3.tar.bz2	win-64
conda-forge	firefox	Reported	firefox-79.0-ha925a31_1.tar.bz2	win-64
conda-forge	libwebp	Reported	libwebp-0.5.2-1.tar.bz2	osx-64
conda-forge	firefox	Reported	firefox-78.13.0esr-h9c3ff4c_0.tar.bz2	linux-64
conda-forge	firefox	Reported	firefox-98.0.1-h27087fc_0.tar.bz2	linux-64
main-passive	libwebp	Cleared	libwebp-1.2.4-hf6ce154_1.conda	osx-64
my-channel	libwebp	Active	libwebp-1.0.1-h5bb14bb_0.conda	linux-aarch64
my-channel	libwebp	Cleared	libwebp-1.2.4-hf6ce154_1.conda	osx-64
ntomeo	libwebp	Active	libwebp-1.0.1-h5bb14bb_0.conda	linux-aarch64
ntomeo	libwebp	Cleared	libwebp-1.2.4-hf6ce154_1.conda	osx-64
premium_channel_business	libwebp	Active	libwebp-1.0.1-h5bb14bb_0.conda	linux-aarch64
premium_channel_business	libwebp	Cleared	libwebp-1.2.4-hf6ce154_1.conda	osx-64
premium_channel_pro	libwebp	Active	libwebp-1.0.1-h5bb14bb_0.conda	linux-aarch64
pwilson	libwebp	Active	libwebp-1.0.1-h5bb14bb_0.conda	linux-aarch64
se-snowflake	libwebp	Cleared	libwebp-1.2.4-hbc33d0d_1.tar.bz2	win-64

Reviews:

Sep 15, 2023

Heap buffer overflow in WebP in Google Chrome prior to 116.0.5845.187 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical) [R1]. CPE: cpe:2.3:a:webmproject:libwebp Vendor Response: It would appear the initial acknowledgment by vendor is in Bug 1479274 [R4]. Not publically accessible at the time of writing. Formal response in [R5]. Release Fixes: release 1.3.2: Cherry-picked in commit 2af26267 [R2] tagged with v1.3.2. CVE and Bug mentioned in Release Notes [R3] Note that NVD reference commit 902bc91 [R6] from which [R2] is cherry-picked -- then very slightly altered. Commit 902bc91 has no tags associated with it. Anaconda Recipe Patches: Patched for releases 1.2.4 build_number 768485 by [R7].

References

R1 :	https://nvd.nist.gov/vuln/detail/CVE-2023-4863
R2 :	https://chromium.googlesource.com/webm/libwebp/+/2af...
R3 :	https://chromium.googlesource.com/webm/libwebp/+/refs...
R4 :	https://crbug.com/1479274
R5 :	https://chromereleases.googleblog.com/2023/09/stable-c...
R6 :	https://github.com/webmproject/libwebp/commit/902bc9...
R7 :	https://github.com/AnacondaRecipes/lts-preview-libweb...

Extras

NVD Publish Date:	Sep 12, 2023
NVD Modified Date:	Oct 1, 2023
Anaconda Curated Date:	Sep 14, 2023

Anaconda CVE curation process

High-quality, accurate, and dependable CVE information

CVE Data Source

The National Institute of Standards and Technology(NIST) National Vulnerability Database (NVD)

Automated Matching

Associating NVD CVE data with packages in the Anaconda Repository

Human Curation

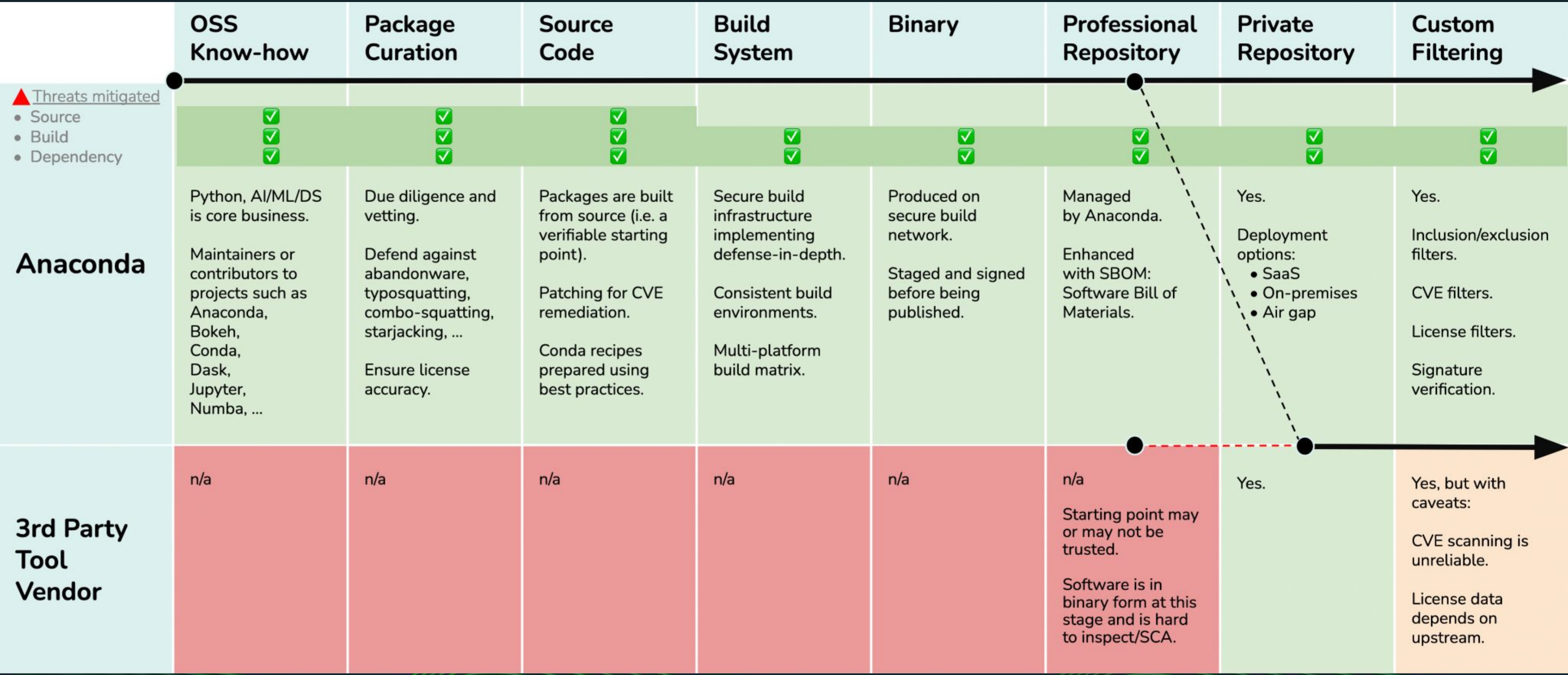
Anaconda engineers review NVD CVE data for accuracy and then categorize, refine, and augment the reported information

Refined CVE Metadata

Accurate CVE metadata allows organizations to filter out OSS packages that don't meet their security requirements

Performed By Anaconda Distribution Team

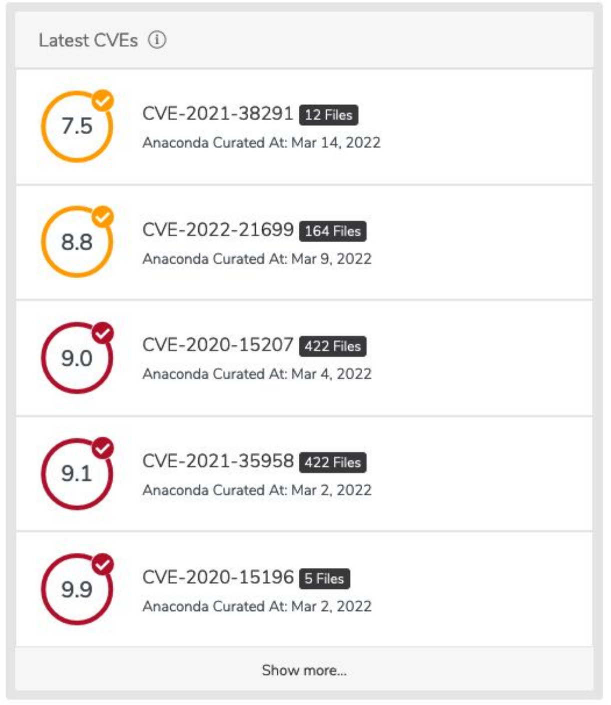
Holistic approach to securing the supply chain



	OSS Know-how	Package Curation	Source Code	Build System	Binary	Professional Repository	Private Repository	Custom Filtering
▲ Threats mitigated								
• Source	✓	✓	✓					
• Build	✓	✓	✓	✓	✓	✓	✓	✓
• Dependency	✓	✓	✓	✓	✓	✓	✓	✓
Anaconda	Python, AI/ML/DS is core business. Maintainers or contributors to projects such as Anaconda, Bokeh, Conda, Dask, Jupyter, Numba, ...	Due diligence and vetting. Defend against abandonware, typosquatting, combo-squatting, starjacking, ... Ensure license accuracy.	Packages are built from source (i.e. a verifiable starting point). Patching for CVE remediation. Conda recipes prepared using best practices.	Secure build infrastructure implementing defense-in-depth. Consistent build environments. Multi-platform build matrix.	Produced on secure build network. Staged and signed before being published.	Managed by Anaconda. Enhanced with SBOM: Software Bill of Materials.	Yes. Deployment options: • SaaS • On-premises • Air gap	Yes. Inclusion/exclusion filters. CVE filters. License filters. Signature verification.
3rd Party Tool Vendor	n/a	n/a	n/a	n/a	n/a	n/a Starting point may or may not be trusted. Software is in binary form at this stage and is hard to inspect/SCA.	Yes.	Yes, but with caveats: CVE scanning is unreliable. License data depends on upstream.

Filter out vulnerabilities

- Ensure developers are empowered with secure packages



Latest CVEs ⓘ

7.5 CVE-2021-38291 12 Files
Anaconda Curated At: Mar 14, 2022

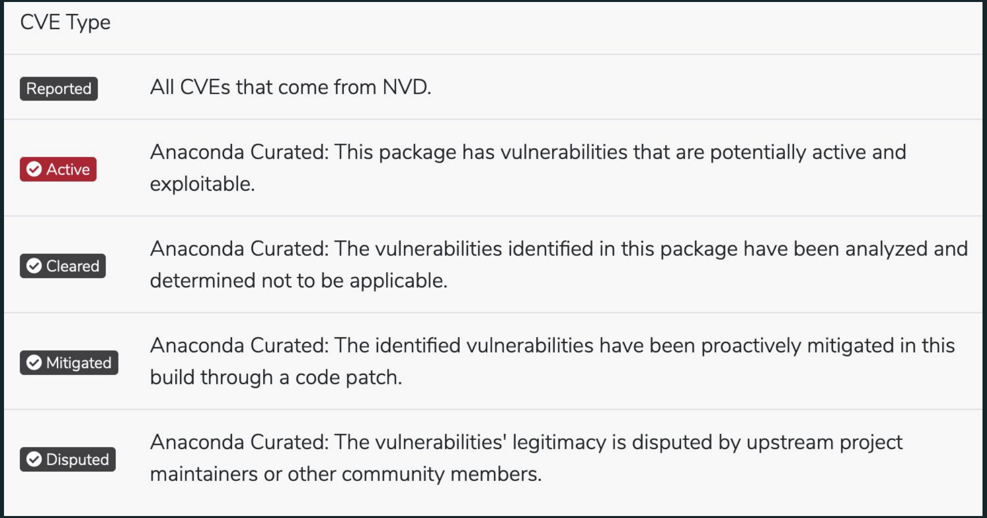
8.8 CVE-2022-21699 164 Files
Anaconda Curated At: Mar 9, 2022

9.0 CVE-2020-15207 422 Files
Anaconda Curated At: Mar 4, 2022

9.1 CVE-2021-35958 422 Files
Anaconda Curated At: Mar 2, 2022

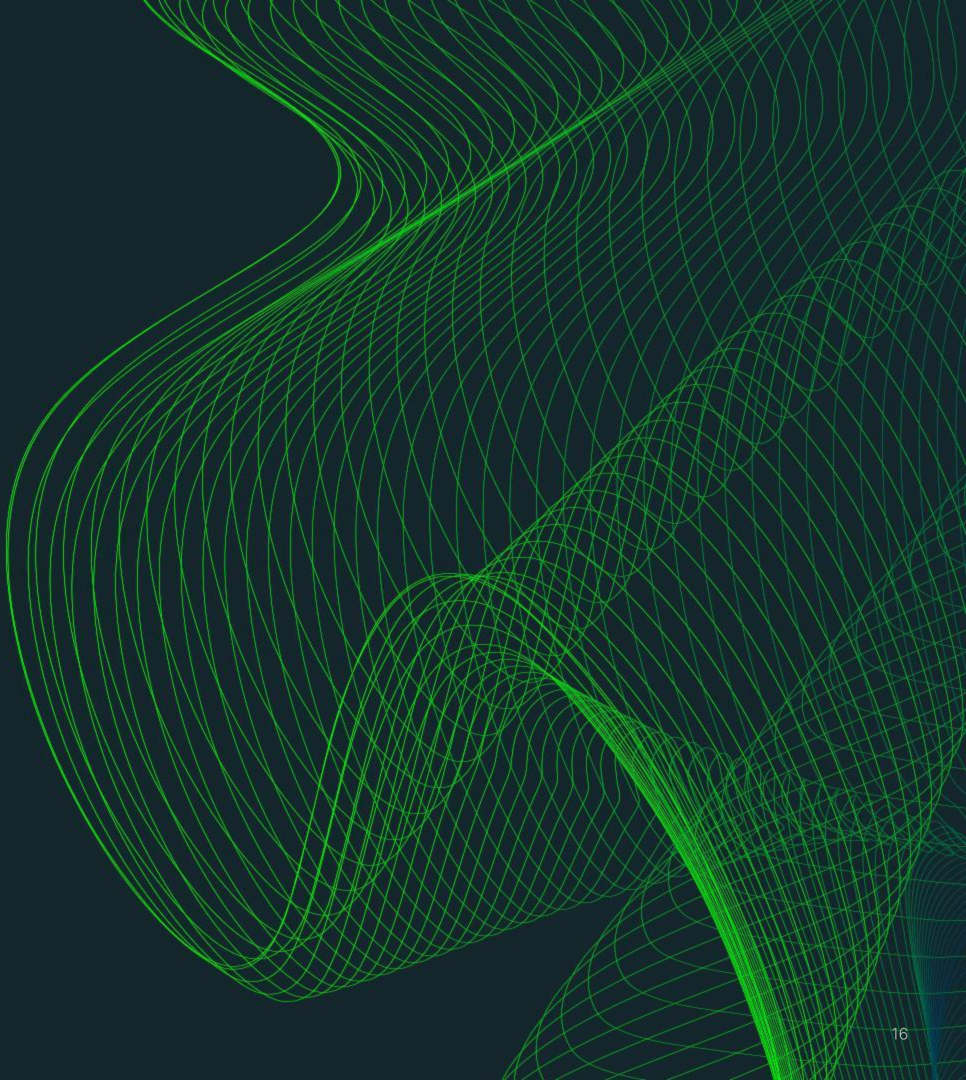
9.9 CVE-2020-15196 5 Files
Anaconda Curated At: Mar 2, 2022

Show more...



CVE Type	
Reported	All CVEs that come from NVD.
✓ Active	Anaconda Curated: This package has vulnerabilities that are potentially active and exploitable.
✓ Cleared	Anaconda Curated: The vulnerabilities identified in this package have been analyzed and determined not to be applicable.
✓ Mitigated	Anaconda Curated: The identified vulnerabilities have been proactively mitigated in this build through a code patch.
✓ Disputed	Anaconda Curated: The vulnerabilities' legitimacy is disputed by upstream project maintainers or other community members.

See it in action



Supply Chain Security

The challenges with community repositories

Community Repositories:
great resource, but with caveats

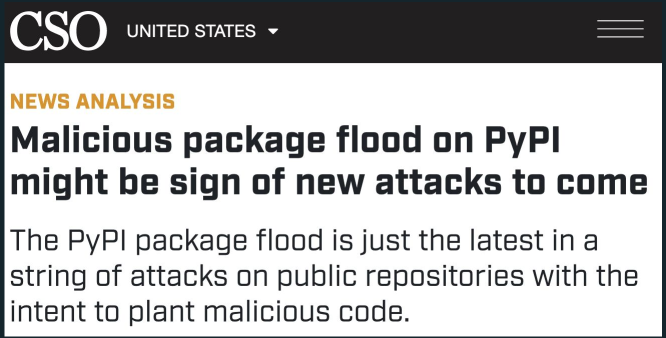
Low barrier of entry

- This is good – encourages participation and innovation
- Huge selection of packages:
  PyPI ~479,000, conda-forge ~22,000 (as of Sept. 2023)

Significant issues to consider

- Minimal quality control
- Entirely author-driven
- Wide range of code and metadata quality
- Potential interoperability conflicts
- Voluntary support
- May or may not have a build system
- Do not implement enterprise-grade security

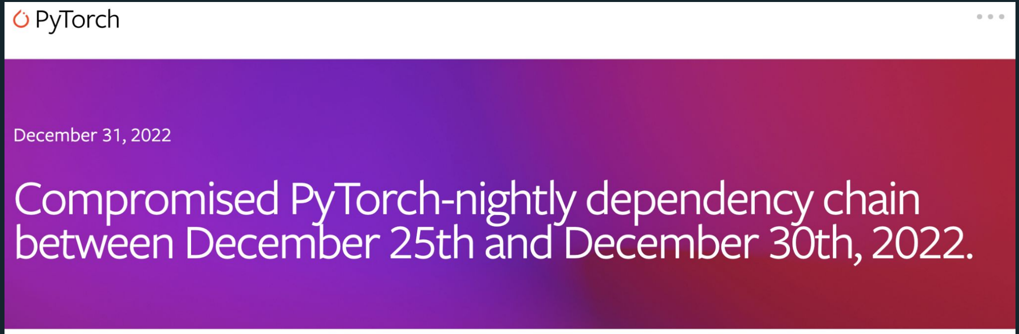
Numerous security incidents in the ecosystem



NEWS ANALYSIS

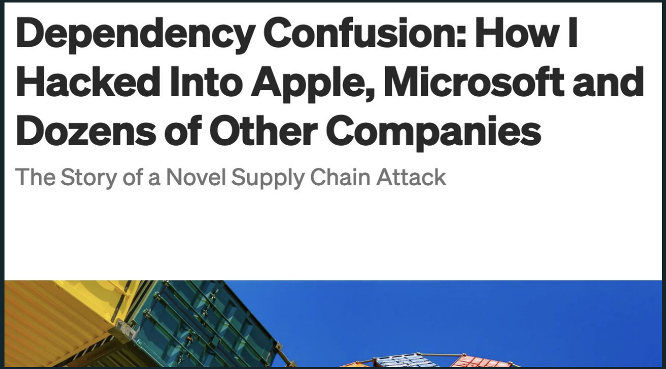
Malicious package flood on PyPI might be sign of new attacks to come

The PyPI package flood is just the latest in a string of attacks on public repositories with the intent to plant malicious code.



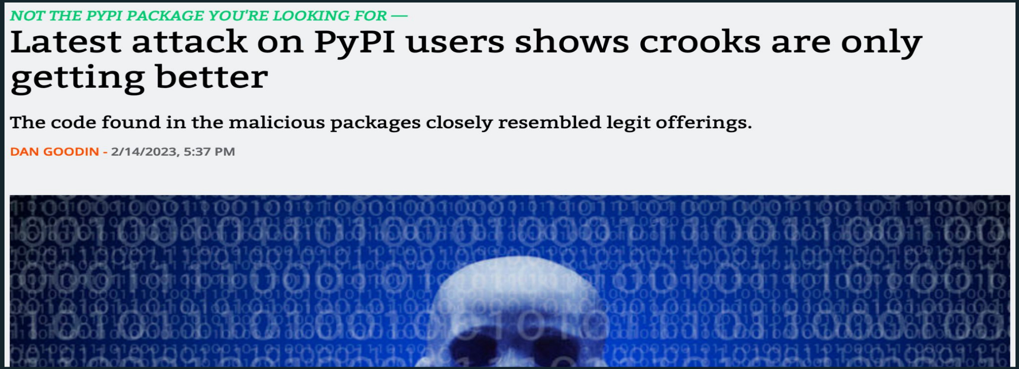
December 31, 2022

Compromised PyTorch-nightly dependency chain between December 25th and December 30th, 2022.



Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack



NOT THE PYPI PACKAGE YOU'RE LOOKING FOR —

Latest attack on PyPI users shows crooks are only getting better

The code found in the malicious packages closely resembled legit offerings.

DAN GOODIN - 2/14/2023, 5:37 PM

Community repositories struggle with security

PyPI overwhelmed by malicious packages

“PyPI new user and new project registrations temporarily suspended.”

“New user and new project name registration on PyPI is temporarily suspended. The volume of malicious users and malicious projects being created on the index in the past week has outpaced our ability to respond to it in a timely fashion…”

~ PyPI Incident Report (May 2023)

conda-forge core dev team issues caveat

“As a reminder, we do not recommend that you use conda-forge in environments with sensitive information. conda-forge’s software is built by our users and the core dev team cannot verify or guarantee that this software is not malicious or has not been tampered with.”

“If you use conda-forge in very sensitive environments (which we do not recommend!), please remove these artifacts from your system.”

~ conda-forge core dev team (March 2023)

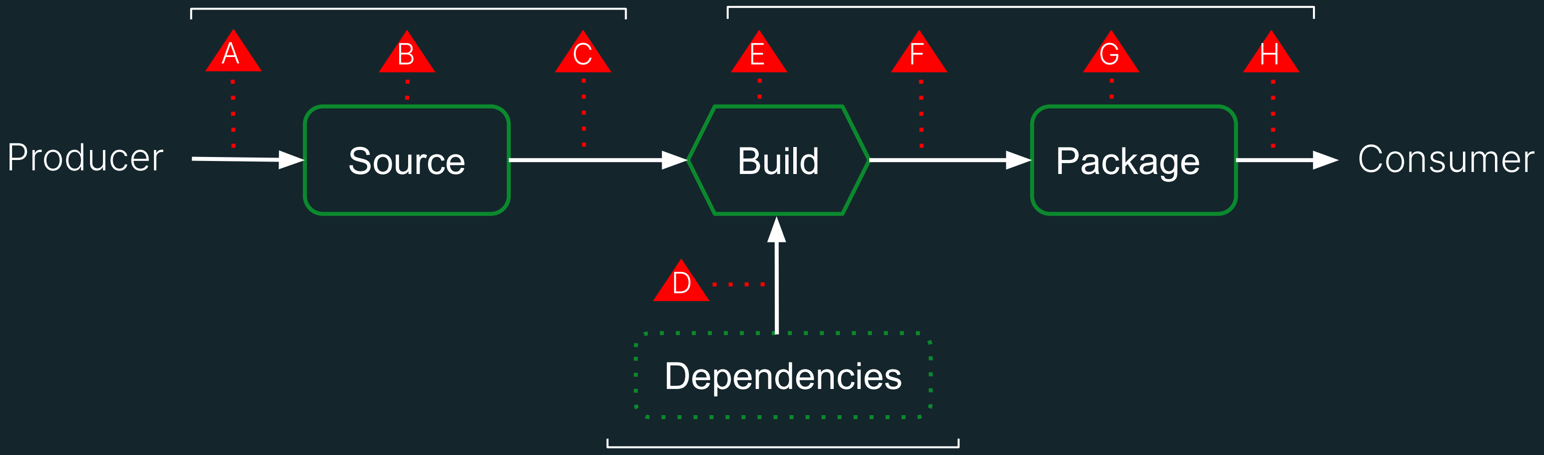
A package faces many pitfalls on its journey

SOURCE THREATS

A Submit unauthorized changes
B Compromise source repo
C Build from modified source

BUILD THREATS

E Compromise build process
F Upload modified package
G Compromise package repo
H Use compromised packages



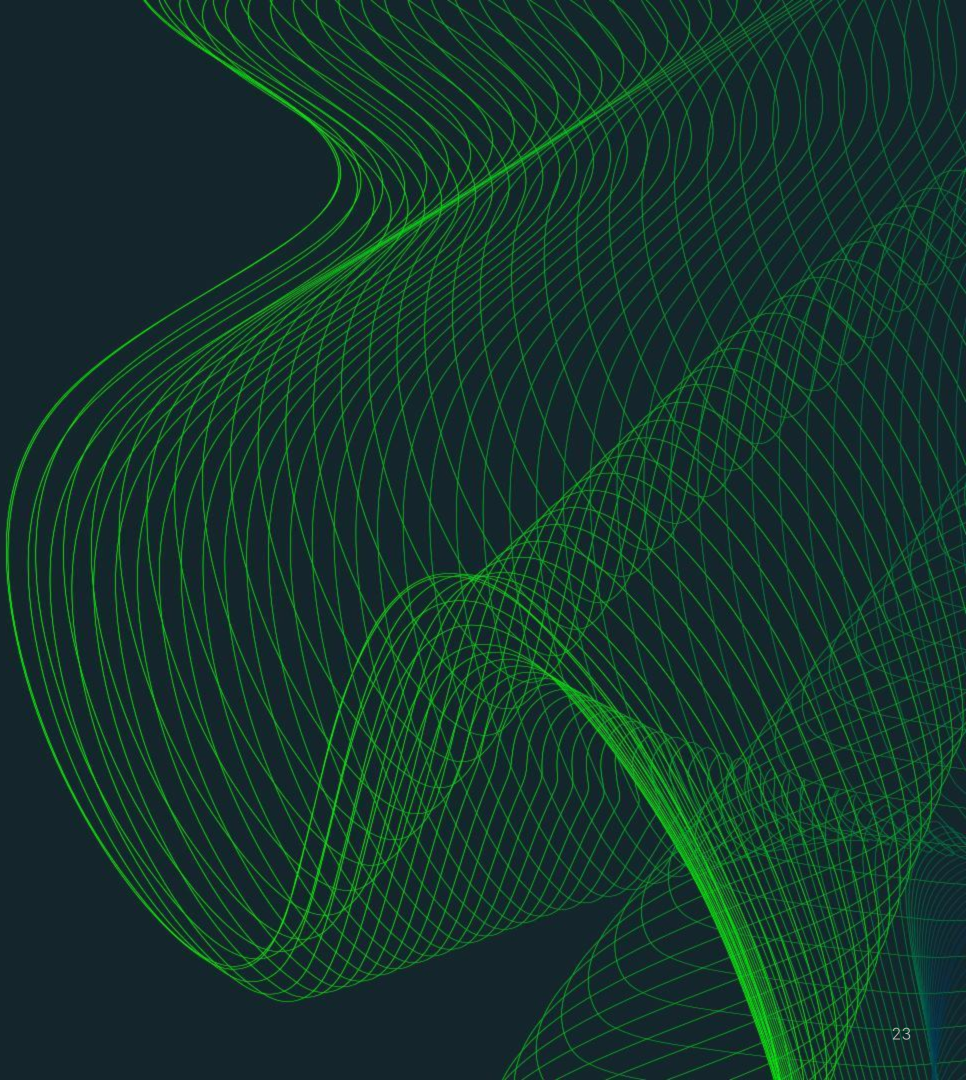
DEPENDENCY THREATS

D Use compromised dependency

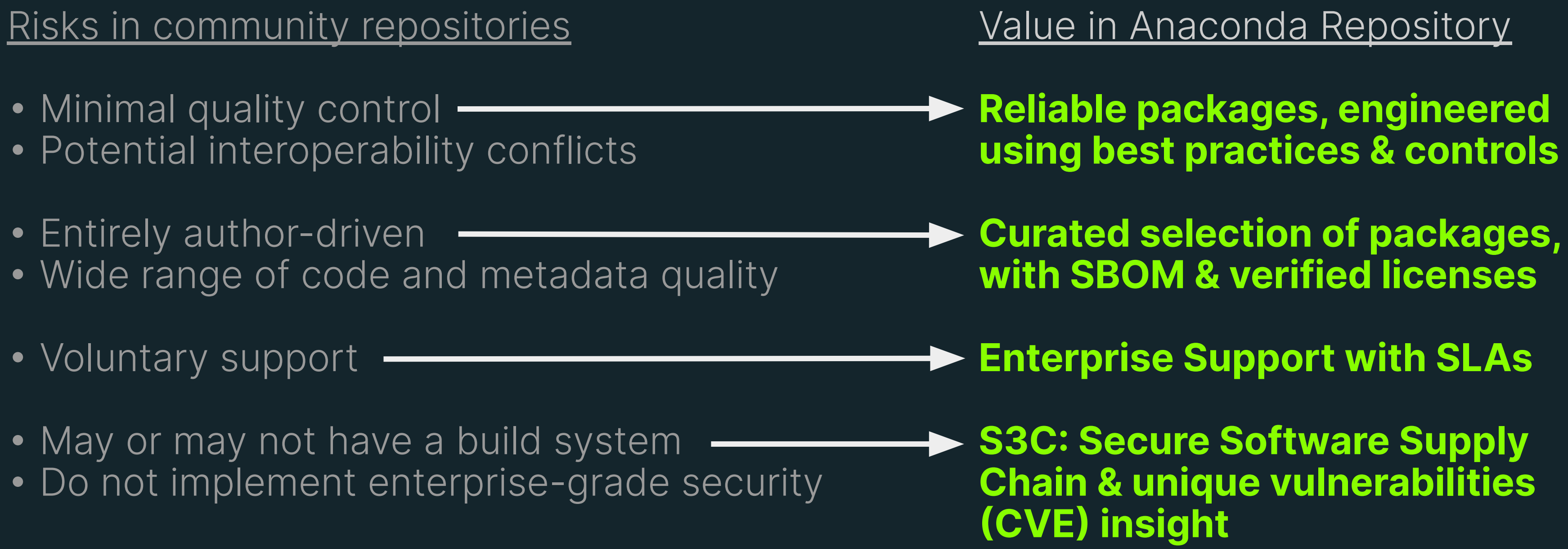
Adapted from slsa.dev

Anaconda:

Innovation + Security



Anaconda Repository:
built for professionals, by professionals



Risks in community repositories

Value in Anaconda Repository

- Minimal quality control
- Potential interoperability conflicts

→ **Reliable packages, engineered using best practices & controls**

- Entirely author-driven
- Wide range of code and metadata quality

→ **Curated selection of packages, with SBOM & verified licenses**

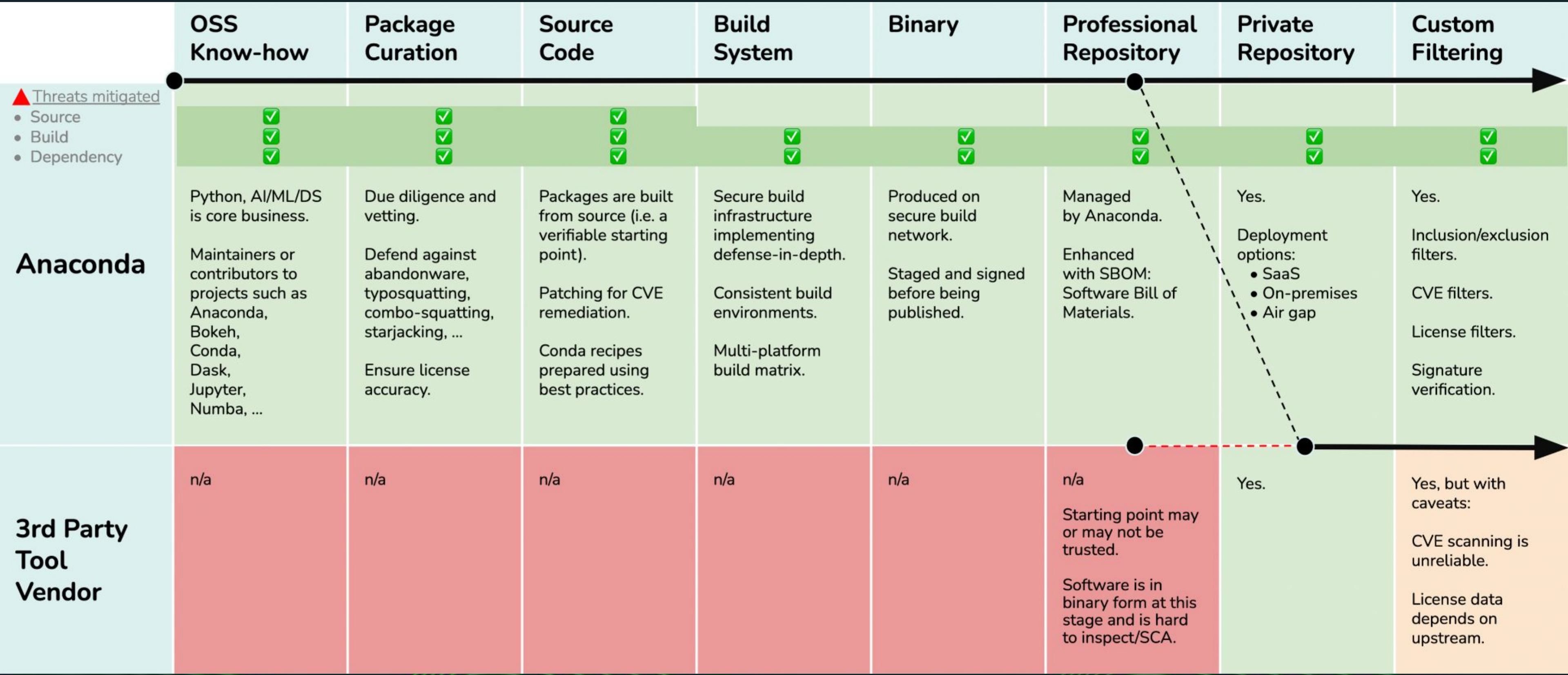
- Voluntary support

→ **Enterprise Support with SLAs**

- May or may not have a build system
- Do not implement enterprise-grade security

→ **S3C: Secure Software Supply Chain & unique vulnerabilities (CVE) insight**

Holistic approach to securing the supply chain



	OSS Know-how	Package Curation	Source Code	Build System	Binary	Professional Repository	Private Repository	Custom Filtering
▲ Threats mitigated								
• Source	✅	✅	✅					
• Build	✅	✅	✅	✅	✅	✅	✅	✅
• Dependency	✅	✅	✅	✅	✅	✅	✅	✅
Anaconda	Python, AI/ML/DS is core business. Maintainers or contributors to projects such as Anaconda, Bokeh, Conda, Dask, Jupyter, Numba, …	Due diligence and vetting. Defend against abandonware, typosquatting, combo-squatting, starjacking, … Ensure license accuracy.	Packages are built from source (i.e. a verifiable starting point). Patching for CVE remediation. Conda recipes prepared using best practices.	Secure build infrastructure implementing defense-in-depth. Consistent build environments. Multi-platform build matrix.	Produced on secure build network. Staged and signed before being published.	Managed by Anaconda. Enhanced with SBOM: Software Bill of Materials.	Yes. Deployment options: • SaaS • On-premises • Air gap	Yes. Inclusion/exclusion filters. CVE filters. License filters. Signature verification.
3rd Party Tool Vendor	n/a	n/a	n/a	n/a	n/a	n/a Starting point may or may not be trusted. Software is in binary form at this stage and is hard to inspect/SCA.	Yes.	Yes, but with caveats: CVE scanning is unreliable. License data depends on upstream.

Anaconda CVE curation process

High-quality, accurate, and dependable CVE information

CVE Data Source

The National Institute of Standards and Technology(NIST) National Vulnerability Database (NVD)

Automated Matching

Associating NVD CVE data with packages in the Anaconda Repository

Human Curation

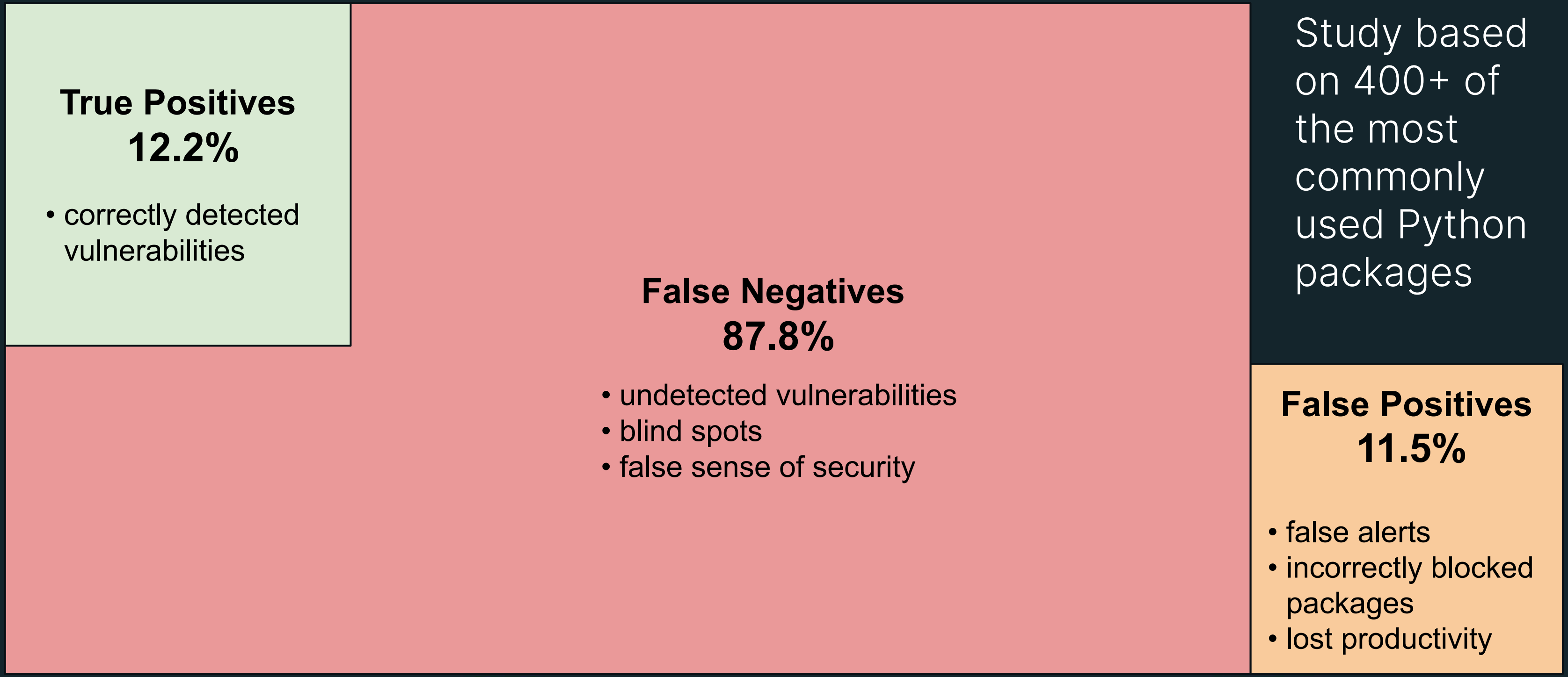
Anaconda engineers review NVD CVE data for accuracy and then categorize, refine, and augment the reported information

Refined CVE Metadata

Accurate CVE metadata allows organizations to filter out OSS packages that don’t meet their security requirements

Performed By Anaconda Distribution Team

Quantitative profile of a popular 3rd party CVE tool



True Positives
12.2%

- correctly detected vulnerabilities

False Negatives
87.8%

- undetected vulnerabilities
- blind spots
- false sense of security

False Positives
11.5%

- false alerts
- incorrectly blocked packages
- lost productivity

Study based on 400+ of the most commonly used Python packages

N = 439 packages, 133 CVEs

False positives:
real-world consequences

- Sample customer repository: 3600 fully approved, CVE scanned packages
- 89% of those packages were initially flagged with potential CVE vulnerabilities with standard open-source CVE scanning software:
  8000 false positives
- Reviewing false positives takes a lot of time
  - 8000 false positives * 10 minutes = 1333 hours = 33 weeks
- Anaconda's CVE curation eliminates these burdens for you
  - Reclaim productivity
  - Focus on your strategic differentiators

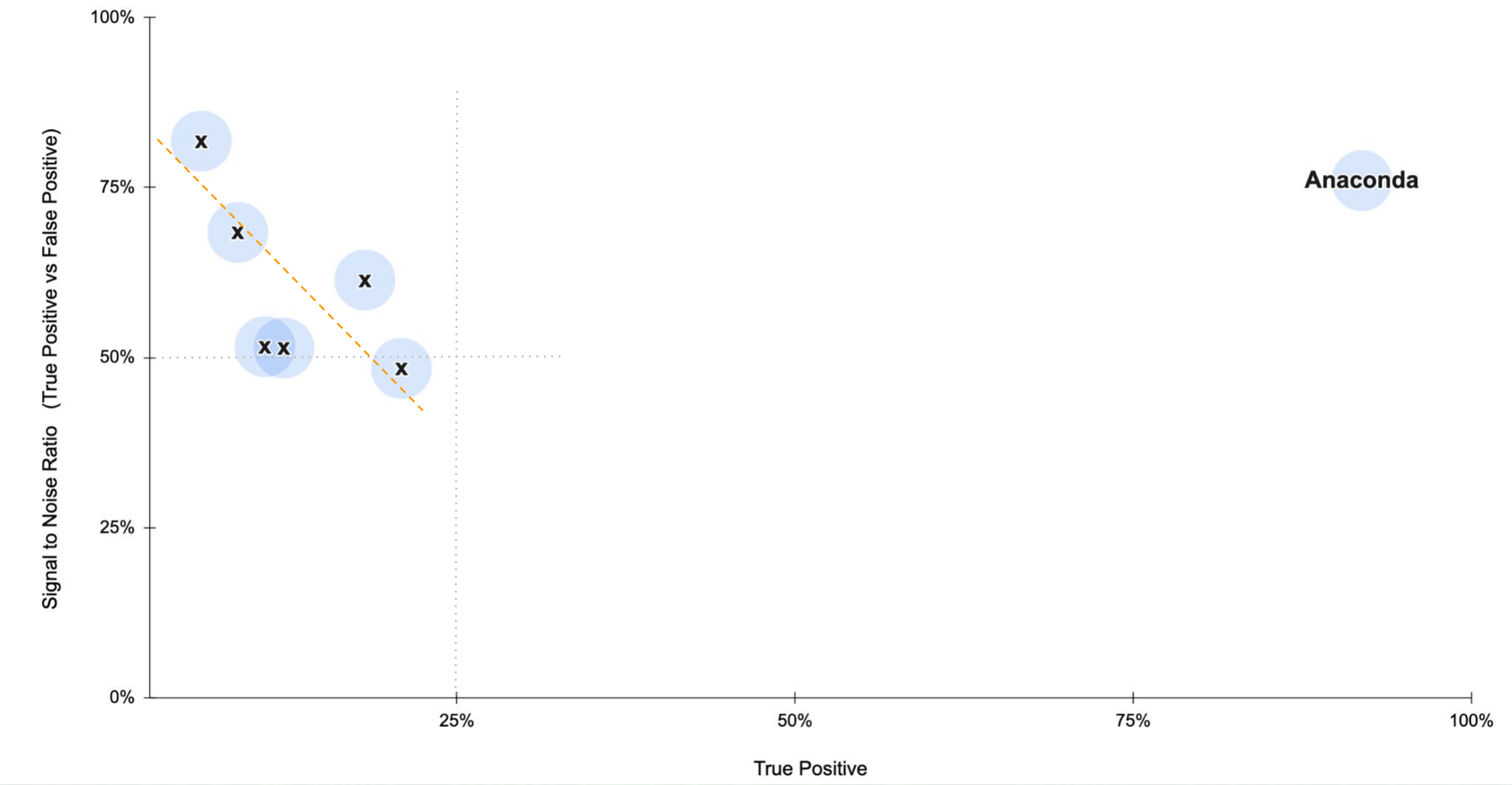
Alert fatigue, aka The Boy Who Cried "Wolf!"

Qualitative Survey of CVE tools

					3rd party tools									
	Package	Category	CVE	Anaconda	*****	*****	*****	*****	*****	*****	*****	*****	*****	*****
pure Python packages	urllib3=1.25.9	Pure Python	CVE-2021-33503	TP	TP	TP	TP	TP	TP	TP	TP	FN	FN	FN
	urllib3=1.26.6	Pure Python	~~CVE-2021-33503~~	TN	TN	TN	TN	TN	TN	TN	TN	n/a	n/a	n/a
compiled aka **binary** packages (e.g. C, C++, Fortran)	python=3.10.8	Language binary	CVE-2022-45061	TP	FN	FN	FN	FN	TP *	FN	TP	FN	FN	FN
	python=3.10.9	Language binary	~~CVE-2022-45061~~	TN	n/a	n/a	n/a	n/a	TN *	n/a	TN	n/a	n/a	n/a
	libxml2=2.9.10=he19cac6_1	Binary package	CVE-2020-7595	TP	FN	FN	FN	FN	FN	FN	FN	FN	FN	FN
	libxml2=2.9.10=hb55368b_3	Binary package • Anaconda remediated	~~CVE-2020-7595~~	TN	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

* Shallow scan that only inspects the name, but not the actual file content

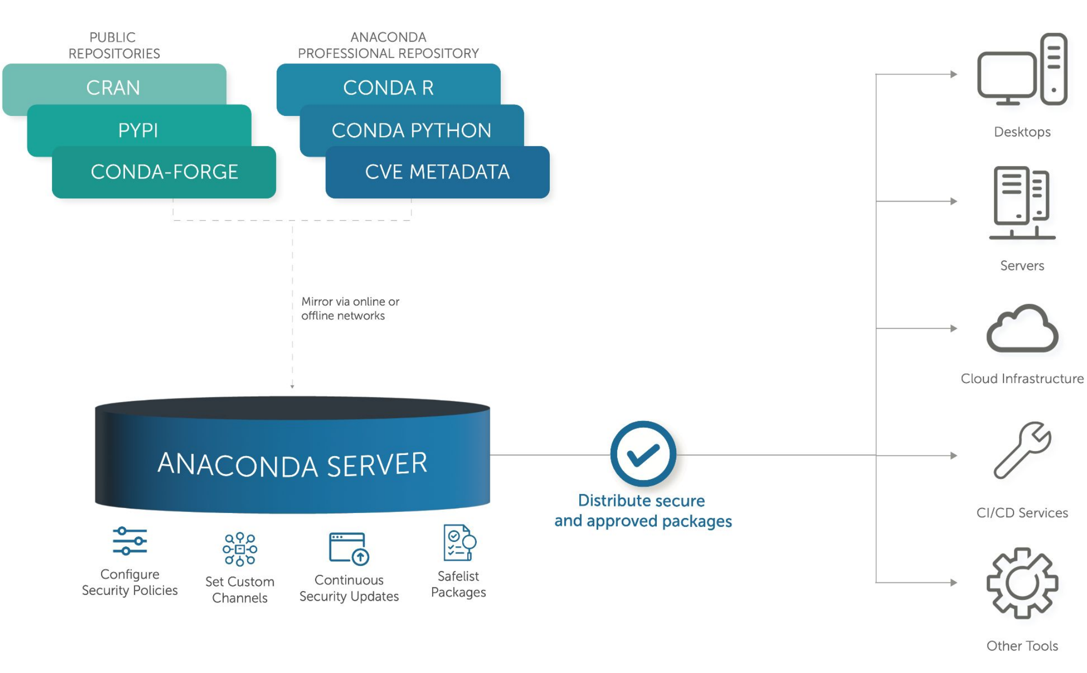
Industry-leading performance



Implementation

Implementation

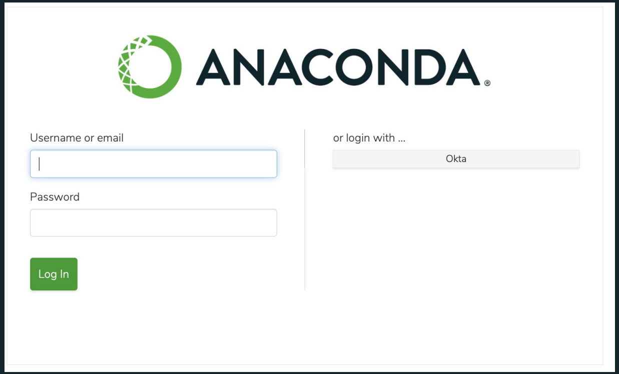
- Installation and configuration on your choice of infrastructure: bare metal, VMware vSphere, AWS, Microsoft Azure or Google Cloud
- Integration with an enterprise directory service for a single set of users using LDAP
- Advanced platform configurations and integrations including but not limited to CI/CD
- Can be installed locally or in the cloud
- 4 cores, 8 gb ram 1.5TB Storage
- K8s or linux?



Moving to 8 but 7.9 is fine for now
Linux based install - 1 VM
LDAP

Integration w SSO

- Part of implementation
- AD/LDAP/SAML/ODIC supported
- Users redirected to browser when token expires



ANACONDA.

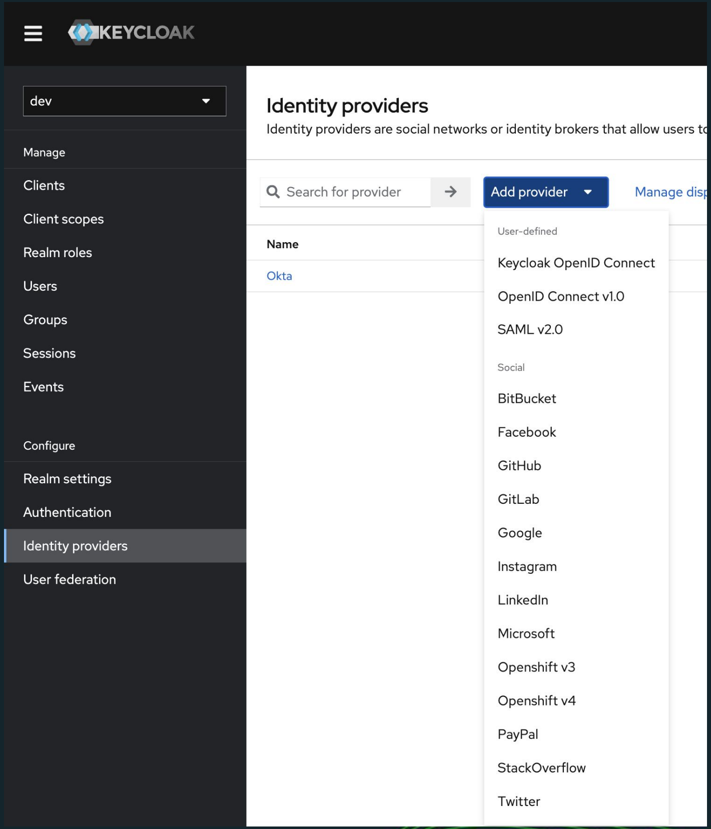
Username or email

Password

Log In

or login with ...

Okta



KEYCLOAK

dev

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Identity providers

Identity providers are social networks or identity brokers that allow users t

Search for provider

Add provider

Manage disp

Name
Okta

User-defined

Keycloak OpenID Connect

OpenID Connect v1.0

SAML v2.0

Social

BitBucket

Facebook

GitHub

GitLab

Google

Instagram

LinkedIn

Microsoft

Openshift v3

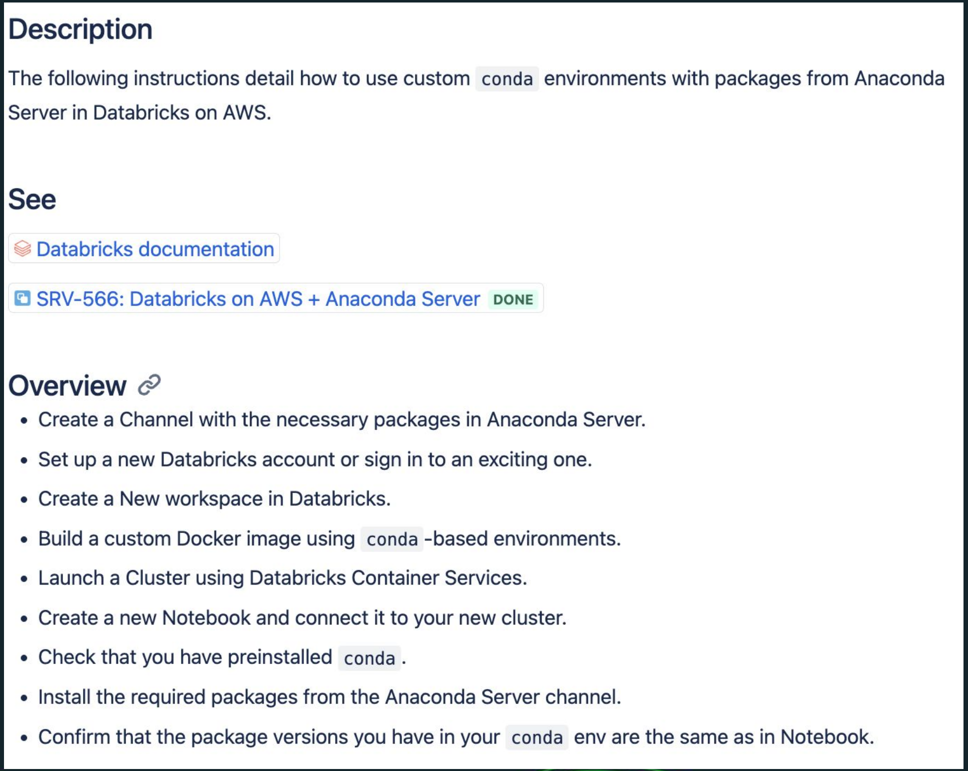
Openshift v4

PayPal

StackOverflow

Twitter

Conda & DataBricks



Description

The following instructions detail how to use custom `conda` environments with packages from Anaconda Server in Databricks on AWS.

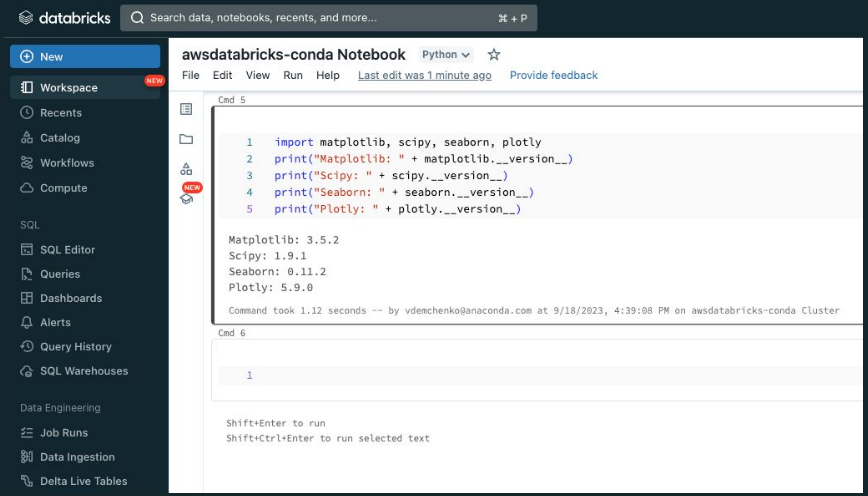
See

Databricks documentation

SRV-566: Databricks on AWS + Anaconda Server DONE

Overview

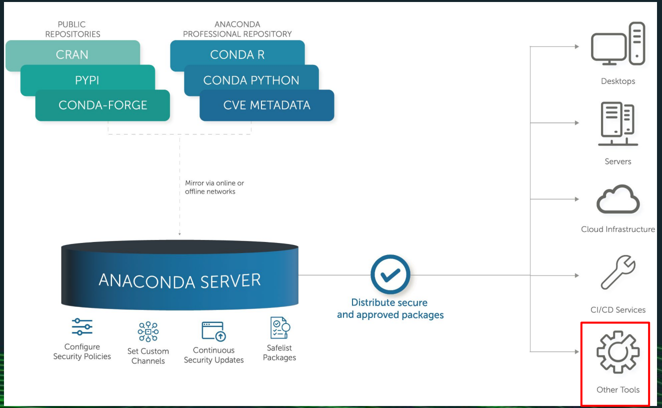
- Create a Channel with the necessary packages in Anaconda Server.
- Set up a new Databricks account or sign in to an exciting one.
- Create a New workspace in Databricks.
- Build a custom Docker image using `conda`-based environments.
- Launch a Cluster using Databricks Container Services.
- Create a new Notebook and connect it to your new cluster.
- Check that you have preinstalled `conda`.
- Install the required packages from the Anaconda Server channel.
- Confirm that the package versions you have in your `conda` env are the same as in Notebook.



```python
import matplotlib, scipy, seaborn, plotly
print("Matplotlib: " + matplotlib.__version__)
print("Scipy: " + scipy.__version__)
print("Seaborn: " + seaborn.__version__)
print("Plotly: " + plotly.__version__)
```

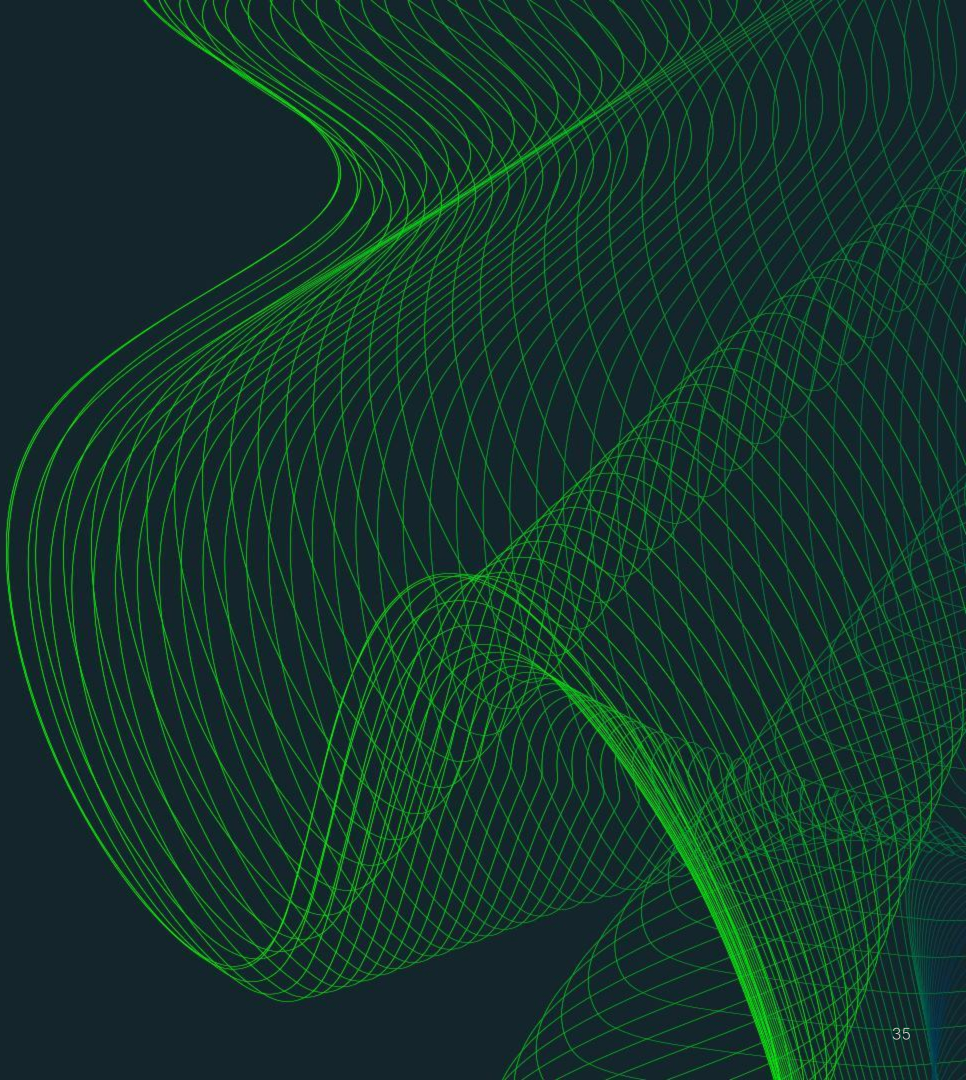
```
Matplotlib: 3.5.2
Scipy: 1.9.1
Seaborn: 0.11.2
Plotly: 5.9.0

Command took 1.12 seconds -- by vdemchenko@anaconda.com at 9/18/2023, 4:39:08 PM on awsdatabricks-conda Cluster
```

```
Shift+Enter to run
Shift+Ctrl+Enter to run selected text
```



Business Case:

Better,
Faster,
Cost-Effective



Better: industry-leading security

- Anaconda secures the software supply chain from end-to-end; this holistic solution provides value that cannot be achieved by cobbling together 3rd party tools.

Industry-leading Python security that is objectively the best-in-class:

7.2X

more True Positives vs **average** 3rd party scanner

4.4X

more True Positives vs **best** 3rd party scanner

Catch blind-spot vulnerabilities that 3rd party scanners miss:

13%

average 3rd party scanner's True Positive Rate

21%

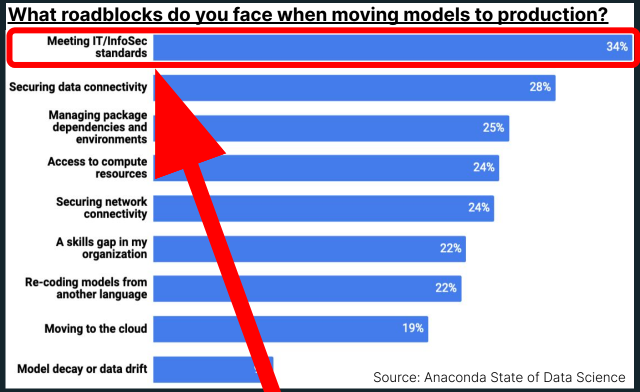
best 3rd party scanner's True Positive Rate

- Note: Anaconda's specialty is Python and AI/ML/DS, but we realize that your scope may extend beyond that. We complement your existing workflows and tools.

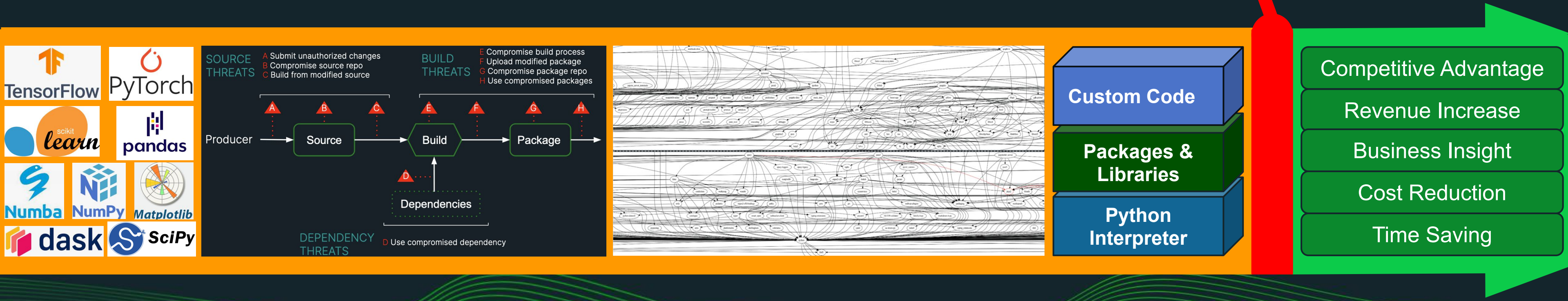
Faster: accelerate the path to value

- Empower your data science community with ongoing package and security updates

- Accelerate time to market by leveraging Anaconda's trusted building blocks:
  - Save time reviewing false alerts and licenses
  - Avert technical debt
  - Mitigate risk



Source: Anaconda State of Data Science



Cost-Effective

- Python packages are more heterogeneous and complex than other languages. The cost of DIY building, maintaining, and supporting a Python distribution will exceed the cost of buying.
- Economy of scale. Anaconda is able to price competitively because cost is amortized across many customers. If you build from scratch, you would bear the entire cost of a one-customer solution.
- Anaconda is an investment in innovation, and trusted by world-class organizations. Leverage the best-of-breed tools, so that you can focus on your key differentiators.
- Buy vs build can be on a spectrum and not binary. Anaconda provides a solid foundation and a head start for building additional packages, and at only an incremental cost. (Similar to building custom containers — you leverage an existing image and do not need to build Linux from scratch.)

Leverage the best-of-breed tools

"Open-source packages have been the biggest enabler for data science we've seen in recent years. Being able to offer a set of ***trusted tools from Anaconda will empower our customers*** *through every stage of the data science journey on Microsoft Azure."*

~

Mark Russinovich
Chief Technology Officer and Technical Fellow
Microsoft Azure
https://www.anaconda.com/press/anaconda-announces-collaboration-with-microsoft

"As a reminder, we do not recommend that you use conda-forge in environments with sensitive information. conda-forge's software is built by our users and the core dev team ***cannot verify or guarantee that this software is not malicious or has not been tampered with****."*

"If you use conda-forge in very sensitive environments (which we do not recommend!), please remove these artifacts from your system."

~

conda-forge core dev team
https://conda-forge.org/blog/posts/2023-03-12-circle-ci-security-breach/

Microsoft specializes in software, has invented 39 languages, and employs several core Python developers.
They considered building their own Python distribution & tools, but the conclusion of their careful analysis is that **Anaconda is the way to go**.

The Return on Investment

- Automation - Whenever anaconda rebuilds packages it automatically appears in our repository. There's no need for anyone in the program office to patch or deploy. It will lessen your workload and let your team focus on the strategic work while solving the top two needs of your data science community.

- Acceleration - Anaconda rebuilds the most popular packages in days not weeks. We provide Infosec with the policy and governance tools to fastrack safe packages. The result will be increased productivity and end user engagement.

- Opportunity Cost - Data Science is the hottest thing in business. Enabling your data scientists with the tooling they need to generative AI, LLMs, fraud detection, earn and retain customer, maximizing customer value. It's hard to overstate how important this is or to put a ceiling on that dollar figure.

- Security - Average ransomware attack in $5.12 million according to IBM

Cost of remediation

Every piece of software at one time or another needs to be fixed. When you take on the burden and responsibility of maintaining open source software yourself, software development cost increases.

With Anaconda Repository Maintenance and Support, you receive prioritization for compiling and updating packages with new community releases which may be triggered by new functionality and/or addressing new common vulnerabilities and exposures (CVEs).

Continued maintenance, regular updates, and support from Anaconda are essential

- Cost to fix a bug:
  - If it takes a developer on average half a day to fix a bug.
  - Software developer's average daily salary is ~$575
  - If most key projects have around 20K lines of code and for every 1000 lines of code there is an average of 20 bugs
  - Cost =
    - (20K Lines of code * 20 bugs for every 1000 lines of code) = 400 bugs
    - (400 ∗ 0.5 days for a developer to fix the bug) * ($575 Average daily salary of a developer) = $115,000
  - Multiply that by multiple projects....

This math does not include costs to remediate a vulnerability:

- Cost to remediate a vulnerability/ransomware attack: $5.12 million according to IBM

Key Takeaways

Key Takeaways

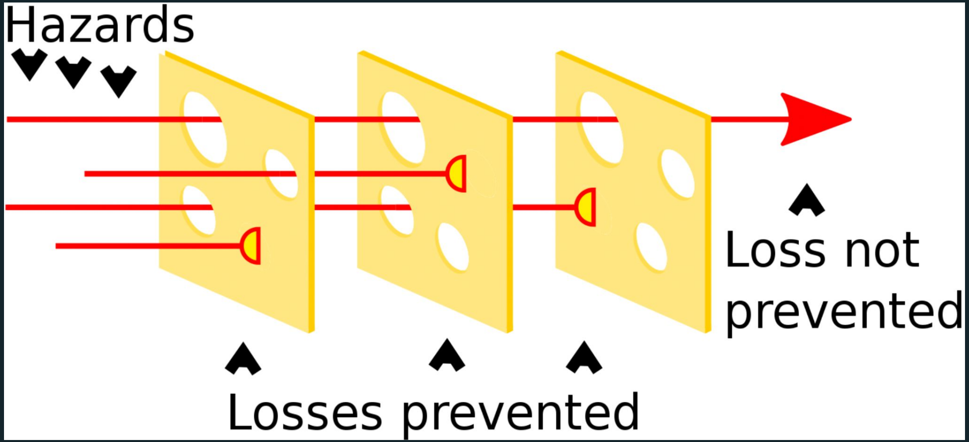
- Leverage the best-of-breed tools, so that you can focus on your strategic differentiators. Anaconda is an investment in innovation, and trusted by world-class organizations.
- There is clear and compelling evidence, including direct statement from conda-forge’s core team, that community repositories should not be treated as a trusted source.
- 3rd party scanner tools can be useful but have material shortcomings. A strategy reliant on free repositories and 3rd party tools will have significant blind spots that compromise security.
- Anaconda secures the software supply chain by taking care of the package lifecycle end-to-end; this holistic solution provides value that cannot be achieved by cobbling together 3rd party tools.
- Repositories are only as good as the packages they serve. Enhance the value you get from 3rd party repo tools by using Anaconda’s professional-grade packages.
- Anaconda will increase package velocity and improve cyber security.

Contact Information

Government Sales- Grant Samples
e: gsamples@anaconda.com
c: 724-562-9036

Counter imperfection with defense-in-depth

- The reality is that security tools have holes
- Mitigate risk by assembling complementary tools (aka the Swiss Cheese Model)



Discerning Security Tools

- Is the CVE scanner general or specialized?
- What universe of packages are supported?
- What does “scan” actually mean? Is it shallow or deep?
- How does the scanner know what is in the binaries?
- How is patching handled?
- What is the vendor’s role and effective scope in the supply chain?