End-to-end post-quantum cryptography development in a dis/connected Nexus environment

DevOps World 2020

Austin Bradley
Enterprise Infrastructure Architect, Qrypt
austin@qrypt.com

Agenda

Cryptography today and in the quantum world of tomorrow

Protecting our sensitive software development in a dis/connected environment with Nexus

Secure C/C++ development with Conan and Nexus

Cryptography today,
quantum world tomorrow

Cryptography Today

mostly not end-to-end

zoom[1,2]

WhatsApp[3,4,5]

weak against seed attacks

ethereum[6]

RSA SecurID®[7]

mostly vulnerable to quantum threats[8,9,11]

RSA®

IPsec

ssh

TLS (https)

GPG, PGP

bitcoin

modern cryptography is vulnerable

Who Should Worry

today[10]

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

Bank of America

WELLS FARGO

CHASE

HIPAA

in ~5 years[11]

in ? years[11]

more people should be acting than are

Qrypt Solution

cryptographic software

Provably secure algorithms delivered through APIs

network architecture

Seamless distribution across private and public networks

custom hardware

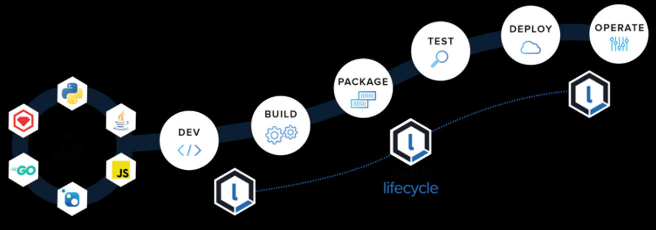
Revolutionary quantum random key generator

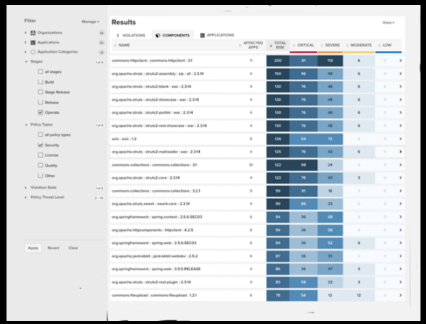
Everlasting Security™ for all data and network traffic

the future depends on something different

Nexus

Lifecycle




Filter Manage ▾

- ▸ Organizations 14
- ▸ Applications 51
- ▸ Application Categories 12
- ▾ Stages 1 of 4
  - □ all stages
  - □ Build
  - □ Stage Release
  - □ Release
  - ☑ Operate
- ▾ Policy Types 1 of 4
  - □ all policy types
  - ☑ Security
  - □ License
  - □ Quality
  - □ Other
- ▸ Violation State 1 of 2
- ▸ Policy Threat Level 2 – 10

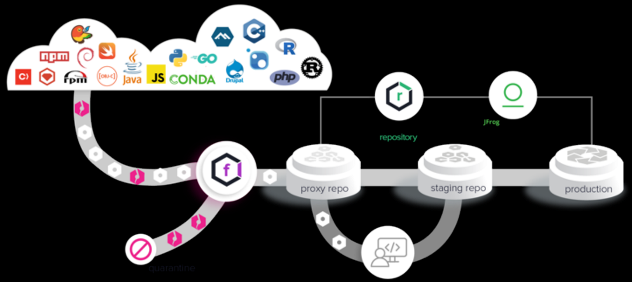
Apply Revert Clear

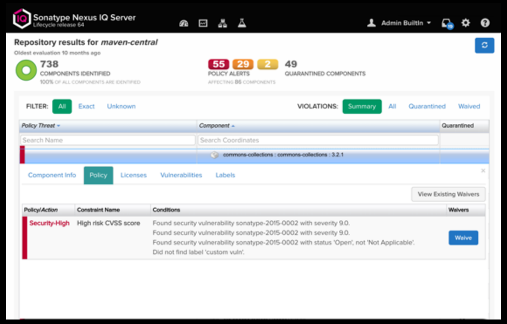
Results View ▾

VIOLATIONS COMPONENTS APPLICATIONS

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient : commons-httpclient : 3.1	11	200	81	113	6	0
org.apache.struts : struts2-assembly : zip : all : 2.3.14	4	150	96	48	6	0
org.apache.struts : struts2-blank : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-showcase : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-portlet : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-rest-showcase : war : 2.3.14	4	130	76	48	6	0
axis : axis : 1.2	6	126	54	72	0	0
org.apache.struts : struts2-mailreader : war : 2.3.14	4	125	76	43	6	0
commons-collections : commons-collections : 3.1	10	122	98	24	0	0
org.apache.struts : struts2-core : 2.3.14	4	122	76	43	3	0
commons-collections : commons-collections : 3.2.1	9	99	81	18	0	0
org.apache.struts.xwork : xwork-core : 2.3.14	4	99	66	33	0	0
org.springframework : spring-context : 2.5.6.SEC03	6	94	36	58	0	0
org.apache.httpcomponents : httpclient : 4.2.5	6	94	36	58	0	0
org.springframework : spring-web : 2.5.6.SEC03	6	94	36	52	6	0
org.apache.jackrabbit : jackrabbit-webdav : 2.5.2	6	87	36	51	0	0
org.springframework : spring-web : 3.0.5.RELEASE	4	86	36	47	3	0
org.apache.struts : struts2-rest-plugin : 2.3.14	4	83	58	22	3	0
commons-fileupload : commons-fileupload : 1.2.1	6	78	54	12	12	0

Firewall




Sonatype Nexus IQ Server
Lifecycle release 64

Admin BuiltIn ▾

Repository results for *maven-central*
Oldest evaluation 10 months ago

738 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE IDENTIFIED

55 29 2 POLICY ALERTS
AFFECTING 86 COMPONENTS

49 QUARANTINED COMPONENTS

FILTER: All Exact Unknown VIOLATIONS: Summary All Quarantined Waived

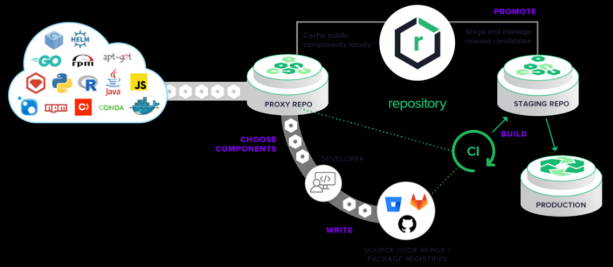
Policy Threat ▾	Component ▴	Quarantined
Search Name	Search Coordinates	
	commons-collections : commons-collections : 3.2.1	

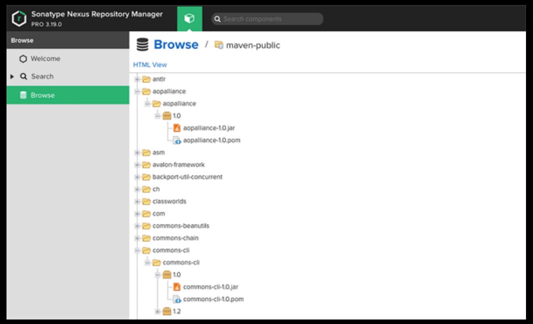
Component Info Policy Licenses Vulnerabilities Labels

View Existing Waivers

Policy/Action	Constraint Name	Conditions	Waivers
Security-High	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with status 'Open', not 'Not Applicable'. Did not find label 'custom vuln'.	Waive

Repository Pro




Sonatype Nexus Repository Manager
PRO 3.19.0

Search components

Browse
- Welcome
- ▸ Search
- Browse

Browse / maven-public

HTML View

- antlr
- aopalliance
  - aopalliance
    - 1.0
      - aopalliance-1.0.jar
      - aopalliance-1.0.pom
- asm
- avalon-framework
- backport-util-concurrent
- ch
- classworlds
- com
- commons-beanutils
- commons-chain
- commons-cli
  - commons-cli
    - 1.0
      - commons-cli-1.0.jar
      - commons-cli-1.0.pom
    - 1.2

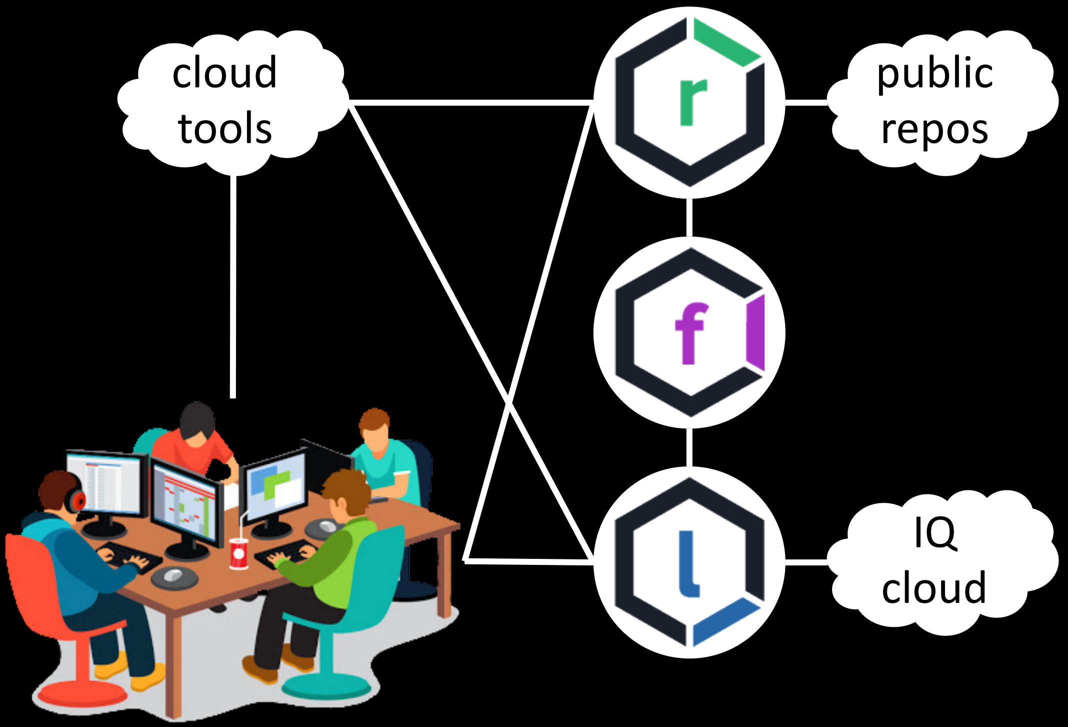
application protection built into CI/CD

images borrowed from sonatype.com

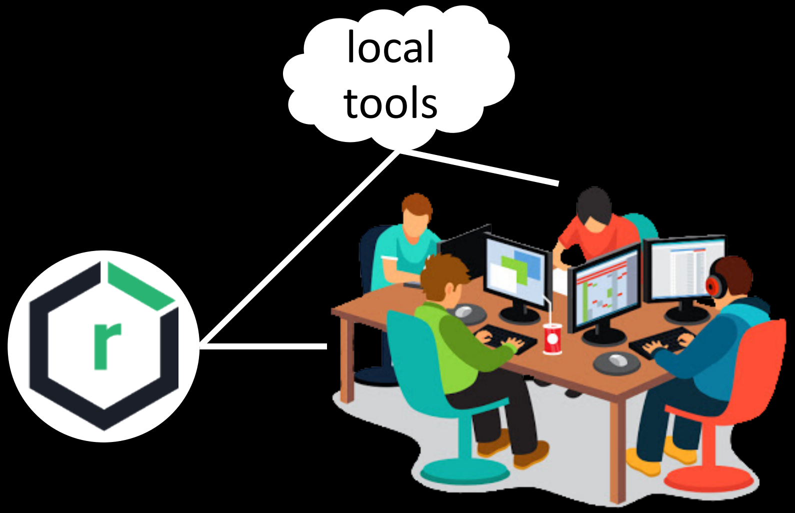
Dis/connected environment with Nexus

Dis/connected Development

internet-connected

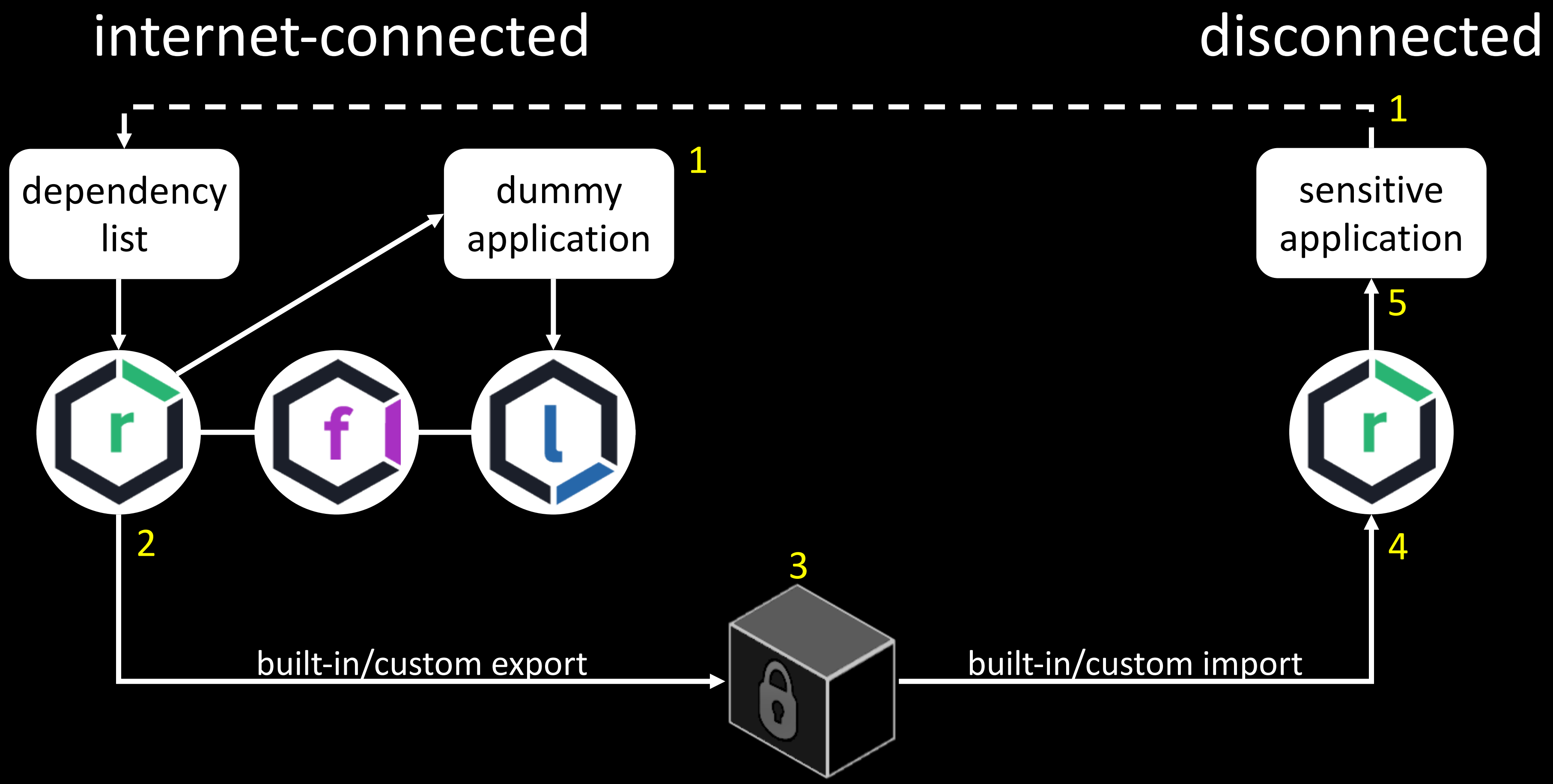


disconnected



sensitivity of applications necessitates extra protections

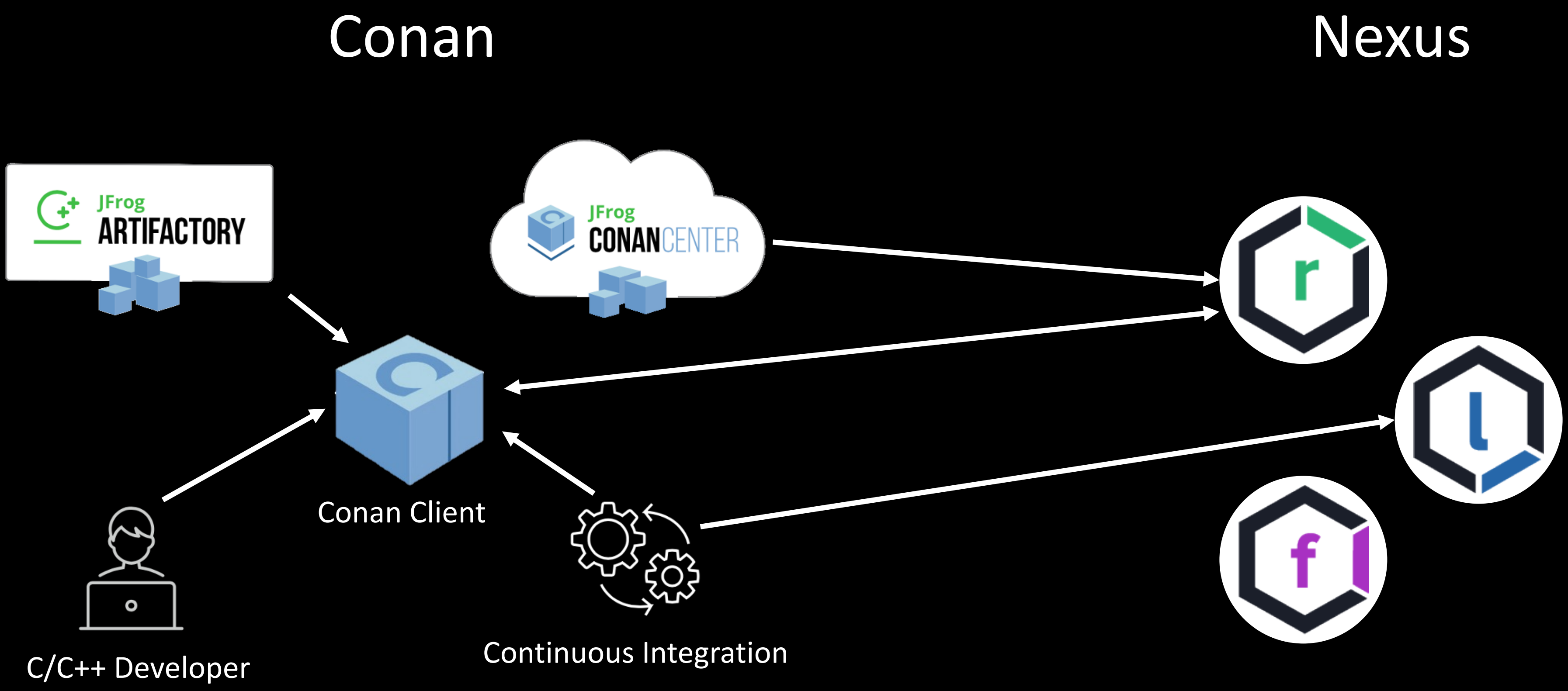
Disconnected Nexus



sensitive applications protected by connected-Lifecycle/Firewall

Secure C/C++ development with Conan and Nexus

Nexus and C/C++ Development

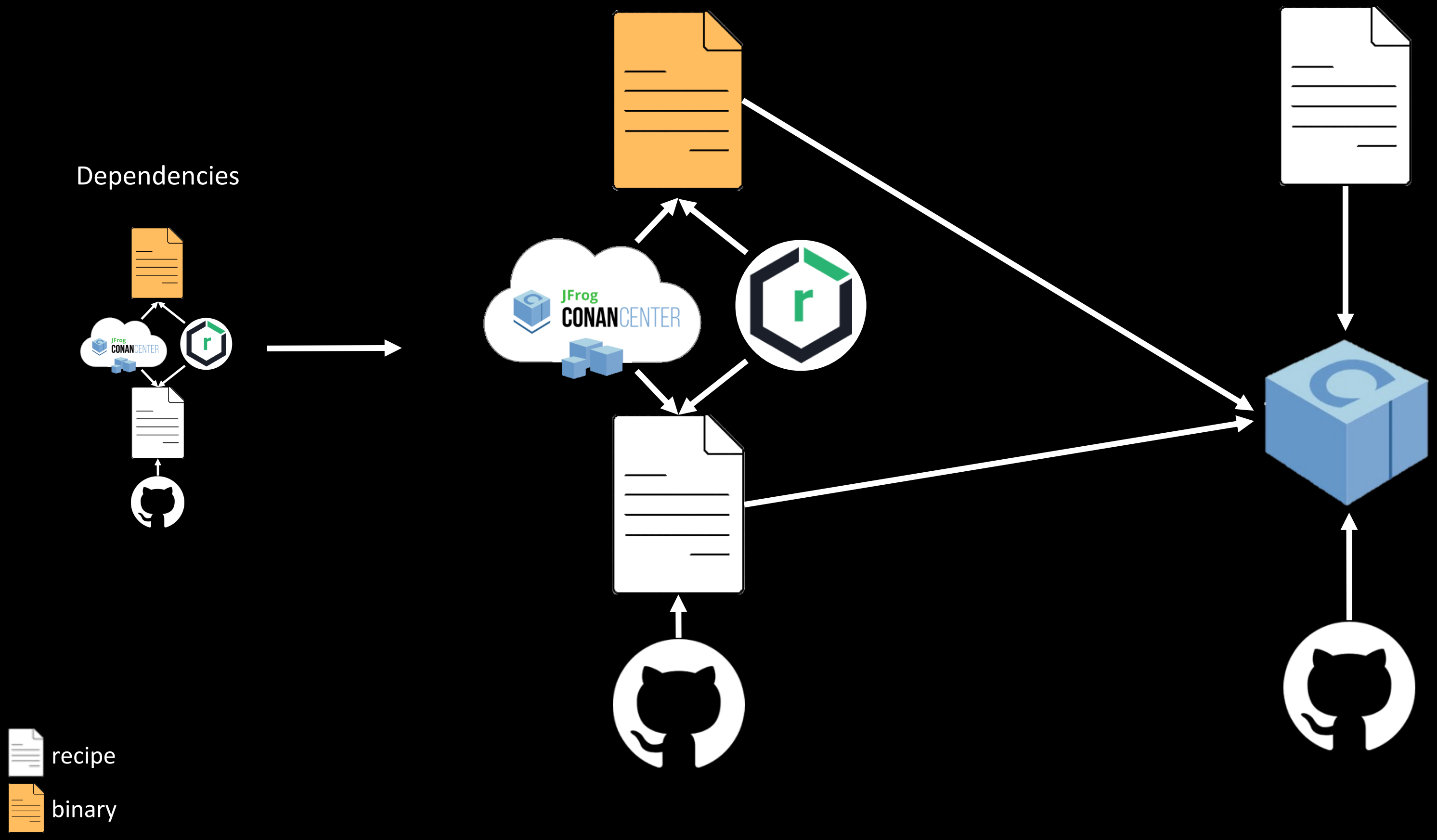


should be easy, but the truth is in the details

Conan Overview

Dependencies

Dev/Build Environment



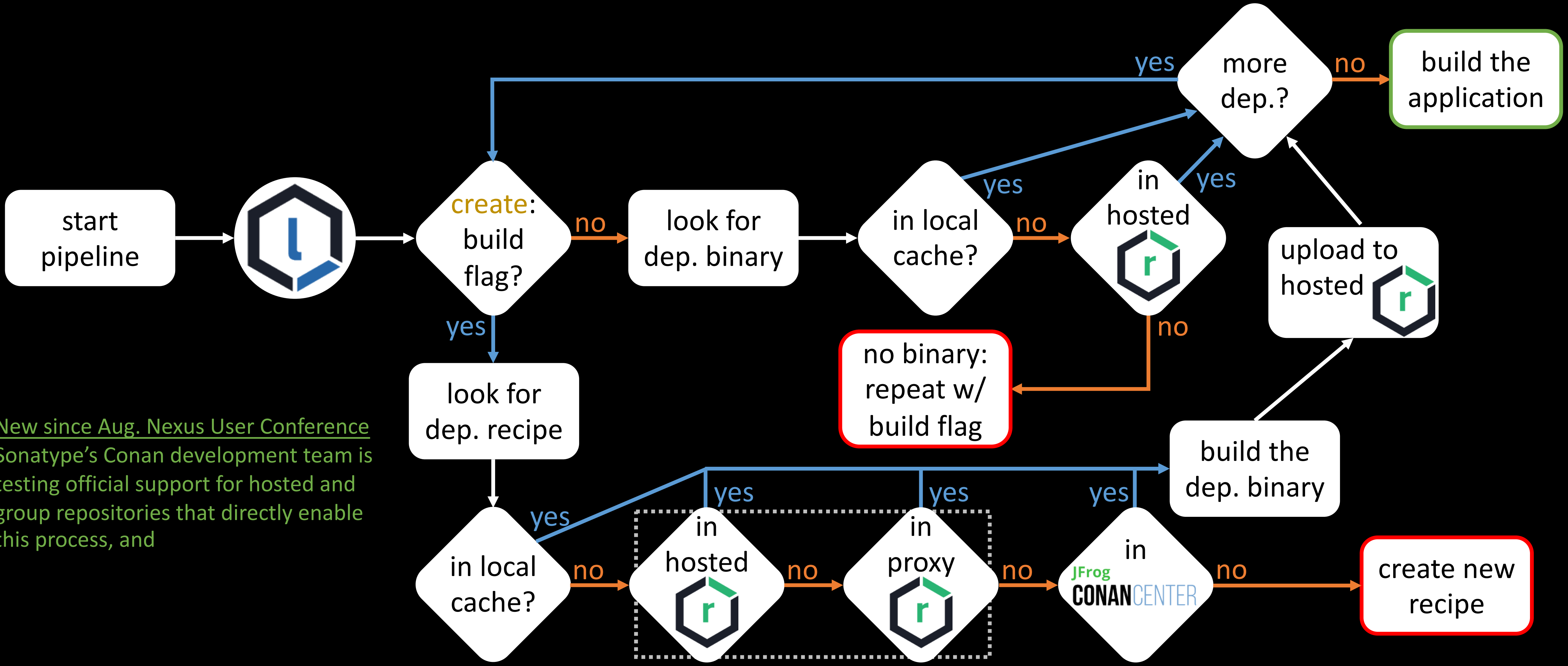
recipe – Python code build instructions

- list of dependencies
- logic like:
    - if this build env, use this
    - if this target env, do this

Conan Client – execute Conan commands

- create from recipe (including downloading source)
- export a package
- upload to a repository (including the built binary)

Secure Conan Development Process



start pipeline

create: build flag?

no

look for dep. binary

in local cache?

no

in hosted

yes

yes

more dep.?

no

build the application

yes

no

no binary: repeat w/ build flag

upload to hosted

yes

look for dep. recipe

in local cache?

yes

no

in hosted

yes

no

in proxy

yes

no

in JFrog CONANCENTER

yes

build the dep. binary

no

create new recipe

New since Aug. Nexus User Conference
Sonatype's Conan development team is testing official support for hosted and group repositories that directly enable this process, and

Conan command

Step-through not automatic, intended limitation of Conan

use only binaries we compile for IQ-scanned dependencies

Challenges with Conan

- by design, looks for binaries and recipes only in the first defined remote (can `add-ref` for packages in other remotes)
- no Conan group repositories (now in development)
- learning curve is steep
- some/many recipes in the Conan Center Index don't support all build/target environments
- building on Windows for Windows, other environments with recipes focused on *nix has had unique challenges
- Nexus Conan capabilities still in development, like the API and certain Conan commands have limitations (e.g., official Conan hosted repositories support in development)

Sonatype is very responsible and adding capabilities quickly

References

1. https://blog.zoom.us/zoom-acquires-keybase-and-announces-goal-of-developing-the-most-broadly-used-enterprise-end-to-end-encryption-offering
2. https://blog.zoom.us/end-to-end-encryption-update
3. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf
4. https://www.forbes.com/sites/kalevleetaru/2019/03/23/could-facebook-start-mining-decrypted-whatsapp-messages-for-ads-and-counter-terrorism
5. https://www.forbes.com/sites/zakdoffman/2020/05/23/why-this-new-facebook-update-suddenly-gives-whatsapp-users-a-powerful-boost
6. https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys
7. https://arstechnica.com/information-technology/2011/06/rsa-finally-comes-clean-securid-is-compromised
8. https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat
9. Well-known information, taught and found in any number of university cryptography courses and textbooks
10. https://www.wired.com/story/quantum-computing-is-coming-for-your-data
11. https://www.csiac.org/journal-article/staying-ahead-of-the-race-quantum-computing-and-cybersecurity

Qrypt

Questions?

Our team is growing! Check out our open positions at

https://www.qrypt.com/careers