



HOW TO MANAGE THE

tangled web of dependencies

31st annual FIRST conference

Hello!



Lisa Bradley, PhD

NVIDIA Senior Manager – PSIRT
LBradley @ nvidia.com



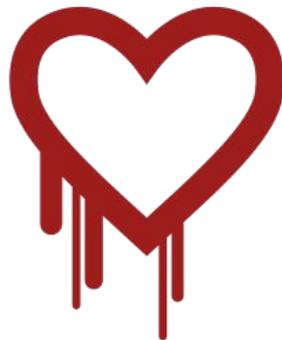
Jessica Butler

NVIDIA Security Tools Development Lead
Jessicab @ nvidia.com

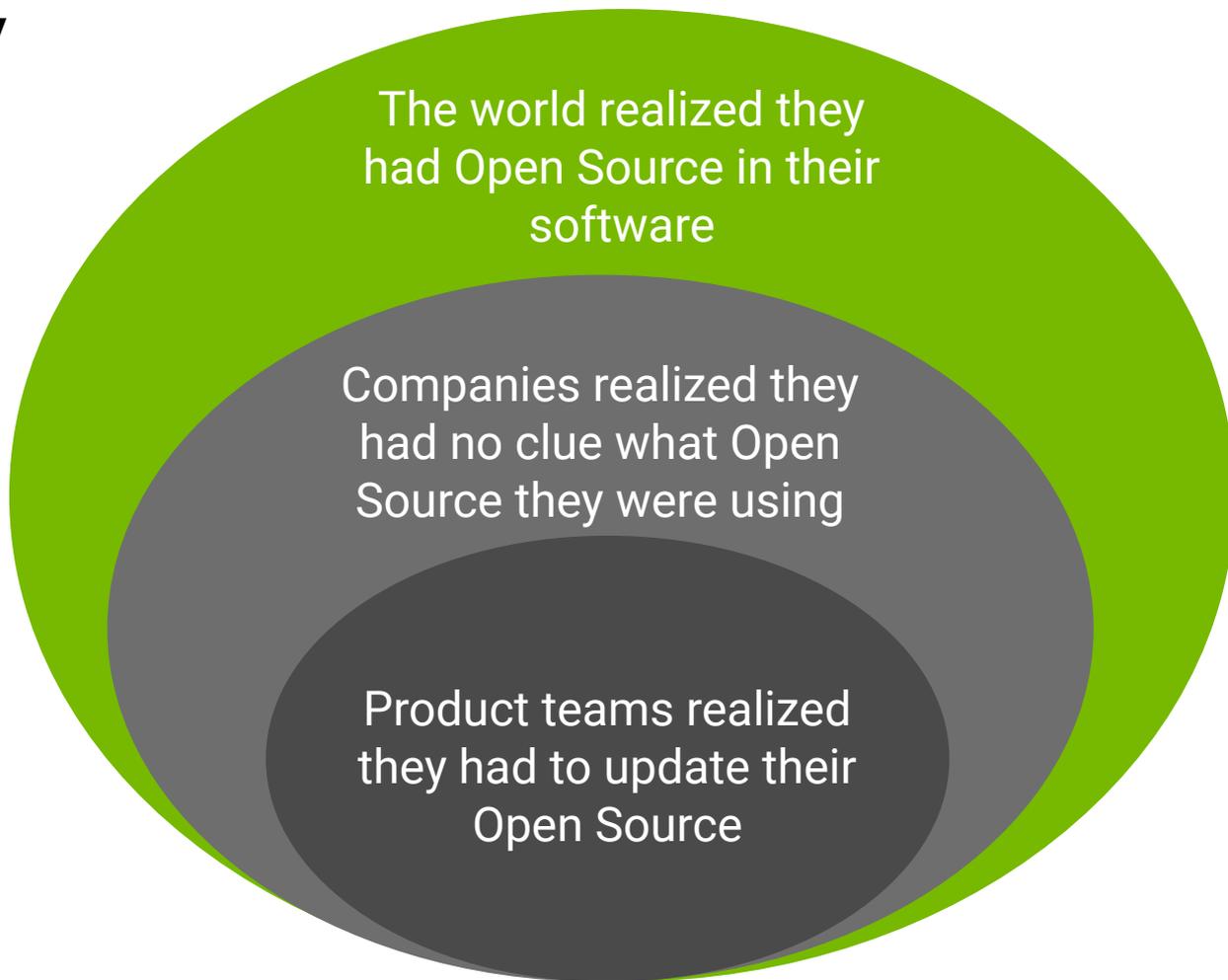


April 7, 2014

CVE-2014-0160



The day



FIGURING OUT WHAT YOU USE



OSS APPROVAL
TICKET



LICENSE
SCANNING



PSIRT
SPREADSHEETS



Let's get the right stuff
in the first place!!

Where to begin?

Customizability
Flexibility
Scaleability
Functionability

Selecting the right open source

Having the right security practices for internal components

Choosing the right vendors

Interoperability
Performance
Useability
Cost
WHAT ARE YOUR NEEDS?

What else do you need?



Project Development Model
Quality assurance
Documentation
Use open standards



Security evaluations
Reviewers
Cryptographic signatures
Way to report security issues

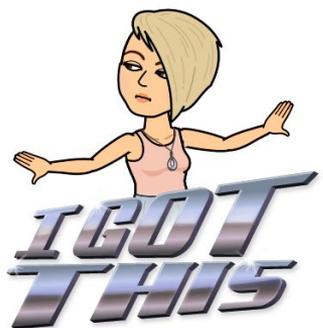


Maintainability
Stability
Active support
Community
Reputation

What are we using already?

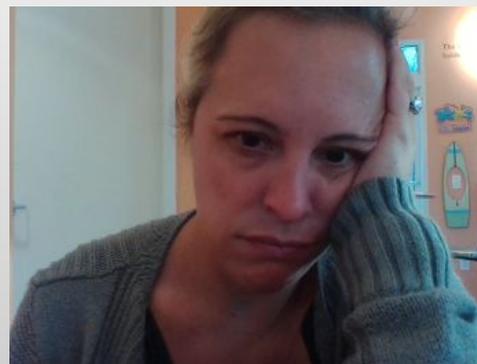


Do we actually know?



We thought we could use...

Content from our OSS approvals
Certificate of Originality
OSS licensing scanning tool results



The reality...

Emails and requests in bugs!
Non-consistent formats!
No mapping to product lines!
False positives!

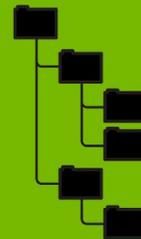
Save me from
the spreadsheet
nightmare!



open source scanning

VULNERABILITY DETECTION

MANUAL PROCESS



1

REQUEST
RECEIVED

2

GATHER
SOURCE
LOCATION

3

RUN
SCANNING
TOOL

4

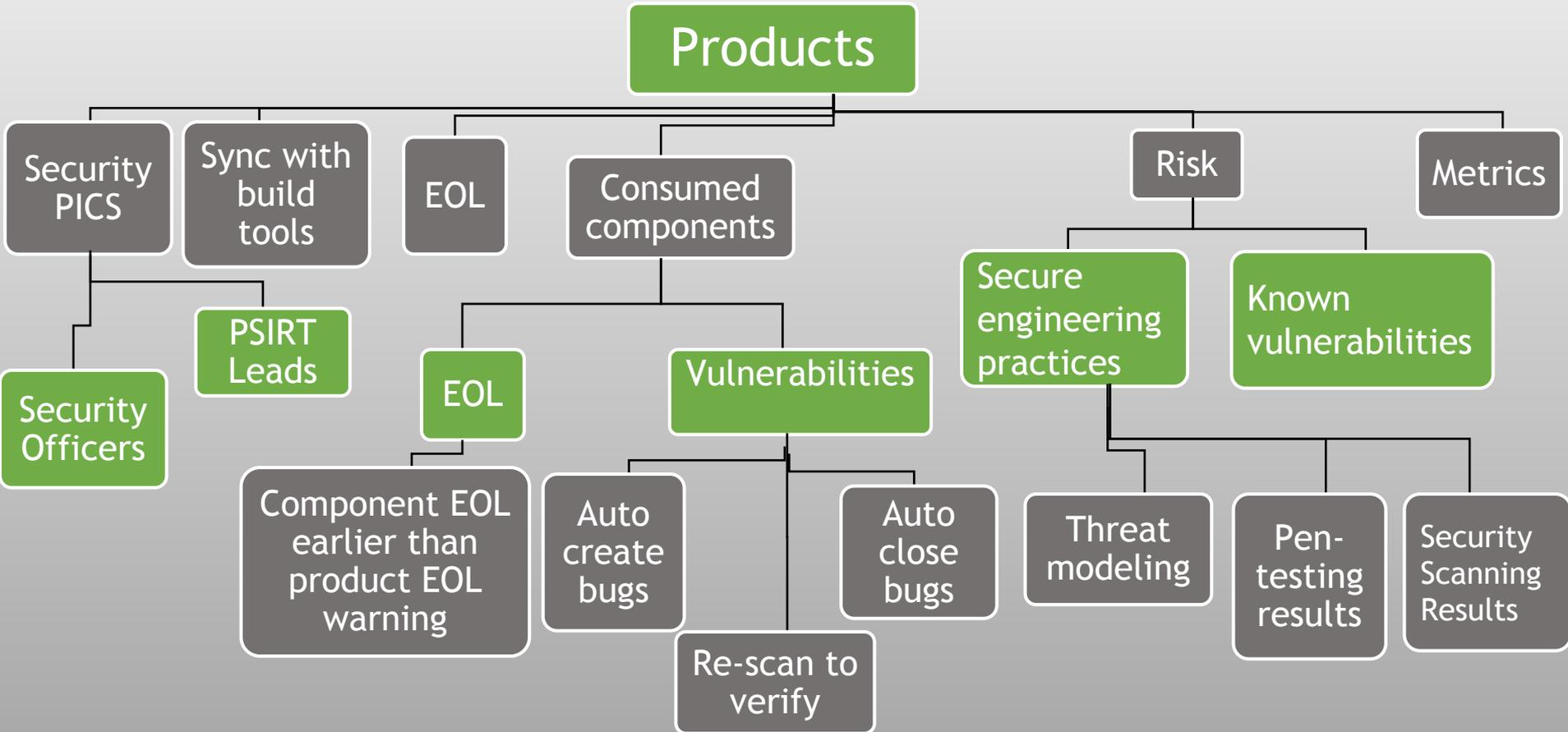
MANUALLY
GROUP DATA

5

SHIP REPORT TO
REQUESTER

WHAT I -
EVER
YOU'RE
THINK -
ING
THINK
BIGGER

Wants



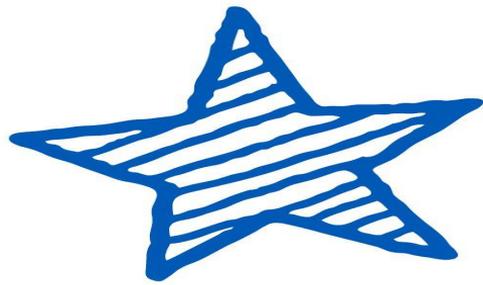
Did I forget to say I also want...

Everything needs to be automated!!

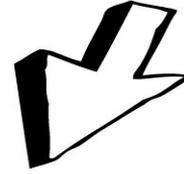
DevOps teams are 90% more likely to comply with open source governance when policies are automated.

-Sonatype's 2018 State of the Software Supply Chain

All parts plug and play :)

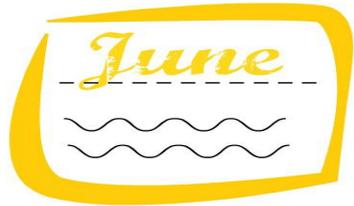


Big thing

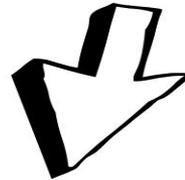


Break it down

- 1
- 2
- 3



Schedule time



Track progress



Step 1:

PRODUCTS

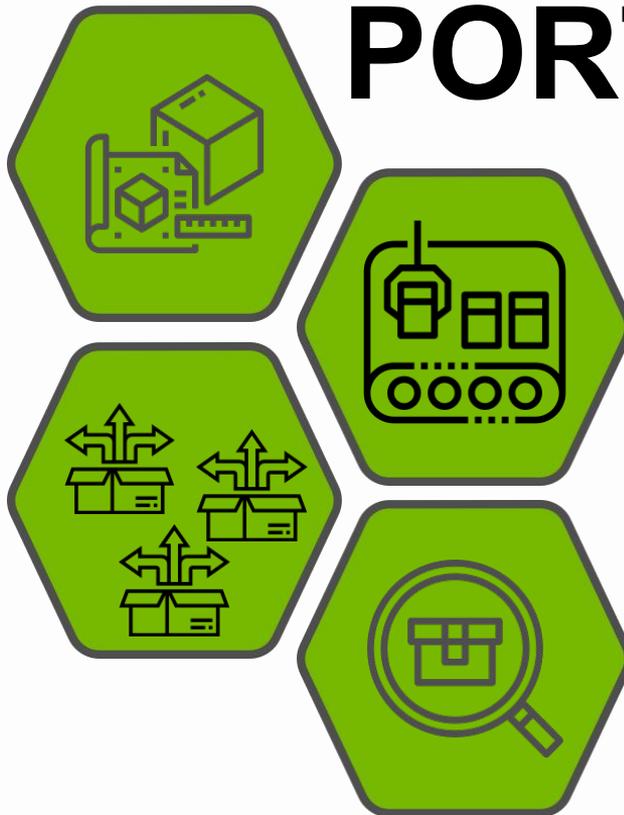
- Top level
- Shippable or deployable
- Executive ownership
- Versioning and EOL

DEPENDENCIES

- Internal components
- External open source software
- External third-party software
- Nestable

Defining the

PORTFOLIO



COMPONENTS

- Logical segregation of product
- 1:n source code projects
- n:n products
- Build level ownership
- 1:n developer teams

OPEN SOURCE SOFTWARE

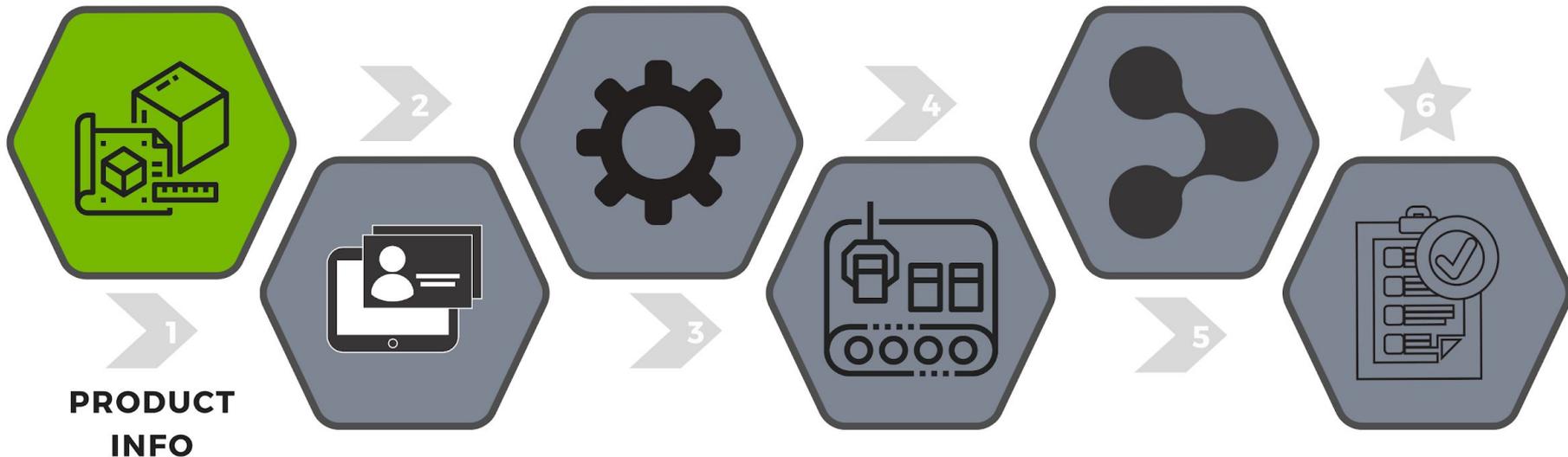
- Versioning detection
- Vulnerability mapping
- Fix recommendations
- Fix verification

Step 2:

Self Service

REGISTRATION

Automating component mapping via build tool synchronization

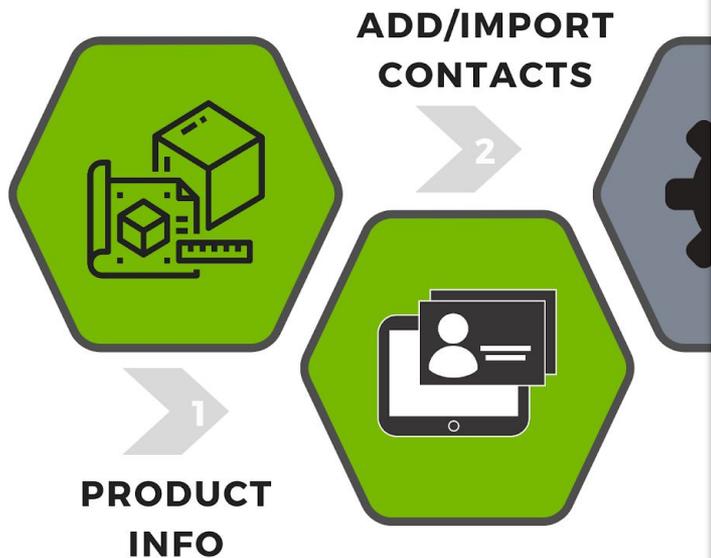


Step 2:

Self Service

REGISTRATION

Automating component mapping via build tool synchronization



Start — Select Product — Release Version — **4 Contacts** — 5 Build Components — 6 Source Code

Contacts

Import Contacts from...

Name	Email	Type	Delete
Jessica Butler	jessicab@nvidia.com	BU PSIRT Lead	<input type="button" value="Delete"/>
Lisa Bradley	lbradley@nvidia.com	Security Officer	<input type="button" value="Delete"/>

Active Directory Username * ESTAFF

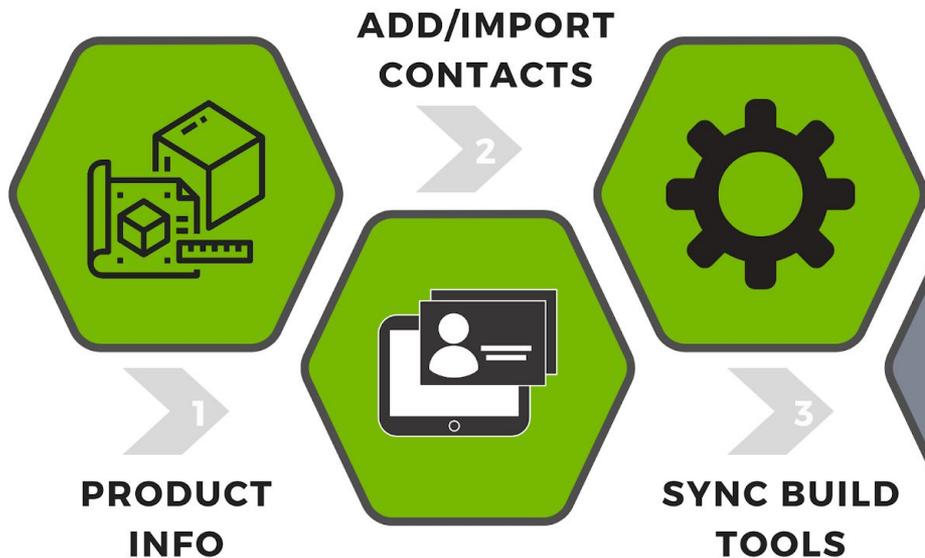
- Escalations
- Security Officer
- Security Reviewer
- QA Security PIC
- BU PSIRT Lead

Step 2:

Self Service

REGISTRATION

Automating component mapping via build tool synchronization



Start Select Product Release Version Contacts **5 Build Components** 6 Source Code

How is your project built?

We'll try to synch with manifests or build scripts so we can automatically create software components.

Android Manifest

Jenkins Project(s)

Jenkins Server	Job	Delete
http://grid-devops-jenkins.nvidia.com	DGX-Cloud-WebService-Deploy-Prod	
http://grid-devops-jenkins.nvidia.com	DGX-Cloud-WebService-Deploy-Prod	
http://grid-devops-jenkins.nvidia.com	NGN-GFN-Healthcheck-NGN-SEC	

server url * jobname *

DVS build script(s)

GVS build script(s)

Git CI/CD pipeline(s)

Step 2:

Self Service

REGISTRATION

Automating component mapping via build tool synchronization

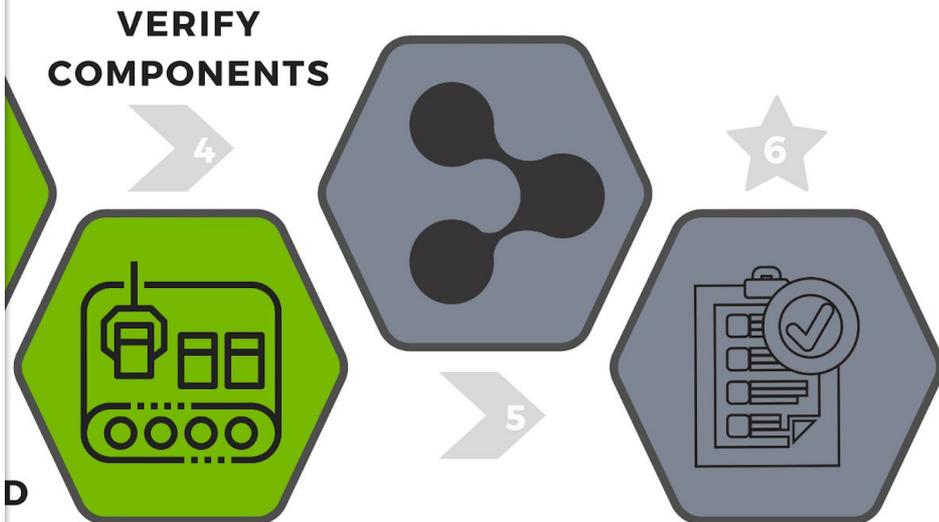
Start — Select Product — Release Version — Contacts — Build Components — **6 Source Code**

Components and Source Code Repositories

Great! You're almost done, just verify the results and add anything that we weren't able to pull.

shell #f6698fc-3ac5-11e9-a350-441ea1432ae0	Static Analysis Info
grid-devops-jenkins-DGX-Cloud-WebService-Depl 21ca49dd-beee-4373-a1cb-843bd4c4c65e	Static Analysis Info
grid-devops-jenkins-NGN-GFN-Healthcheck-NGN-S e2037886-1101-455c-8608-7be9d551db8b	Static Analysis Info

Back Next

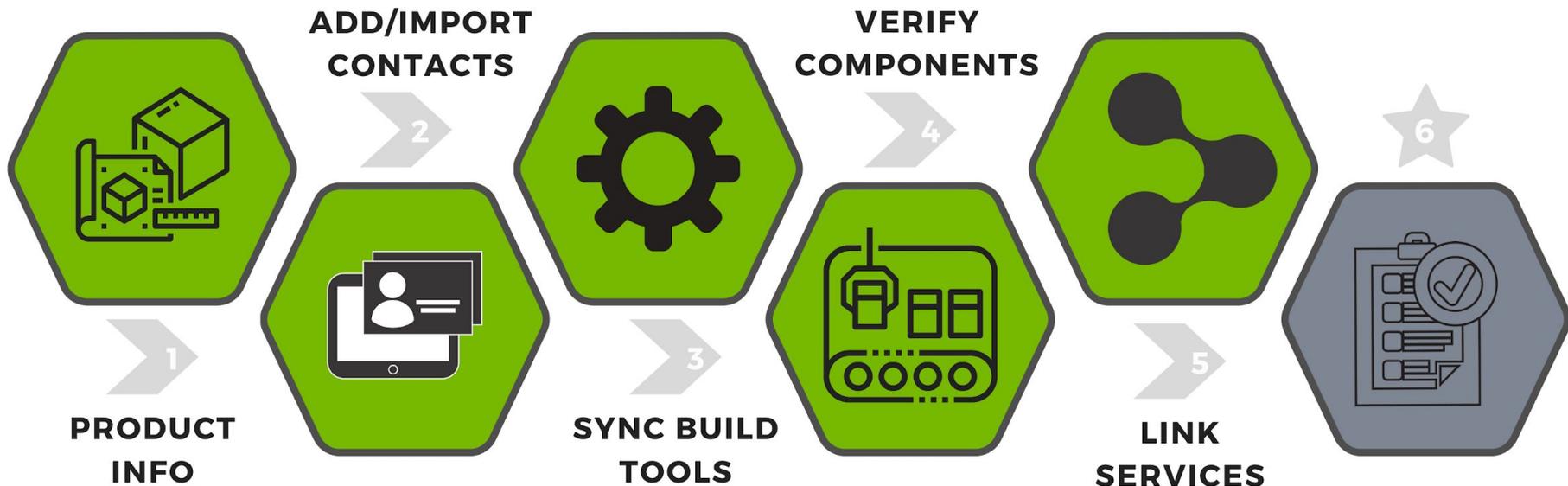


Step 2:

Self Service

REGISTRATION

Automating component mapping via build tool synchronization

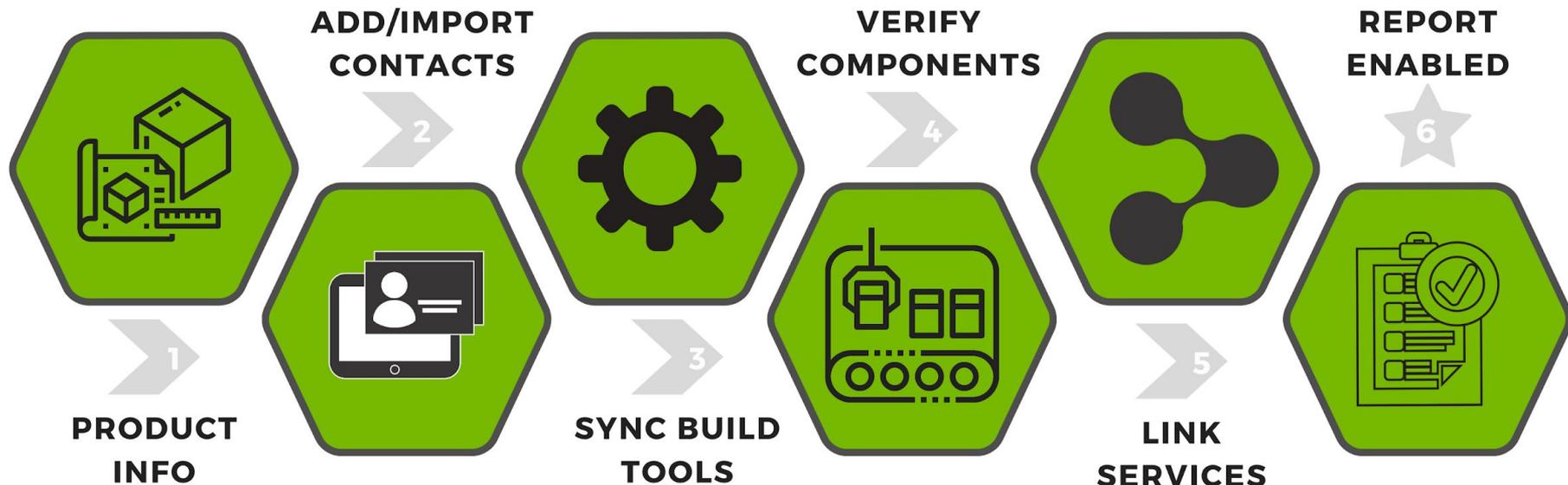


Step 2:

Self Service

REGISTRATION

Automating component mapping via build tool synchronization



Step 3:

DEPENDENCY DEVOPS

← Shift Left



Open Source
screening

Step 3:

DEPENDENCY DEVOPS

← Shift Left



Open Source
screening

Commit
triggered
scanning

Step 3:

DEPENDENCY DEVOPS

← Shift Left



Open Source screening

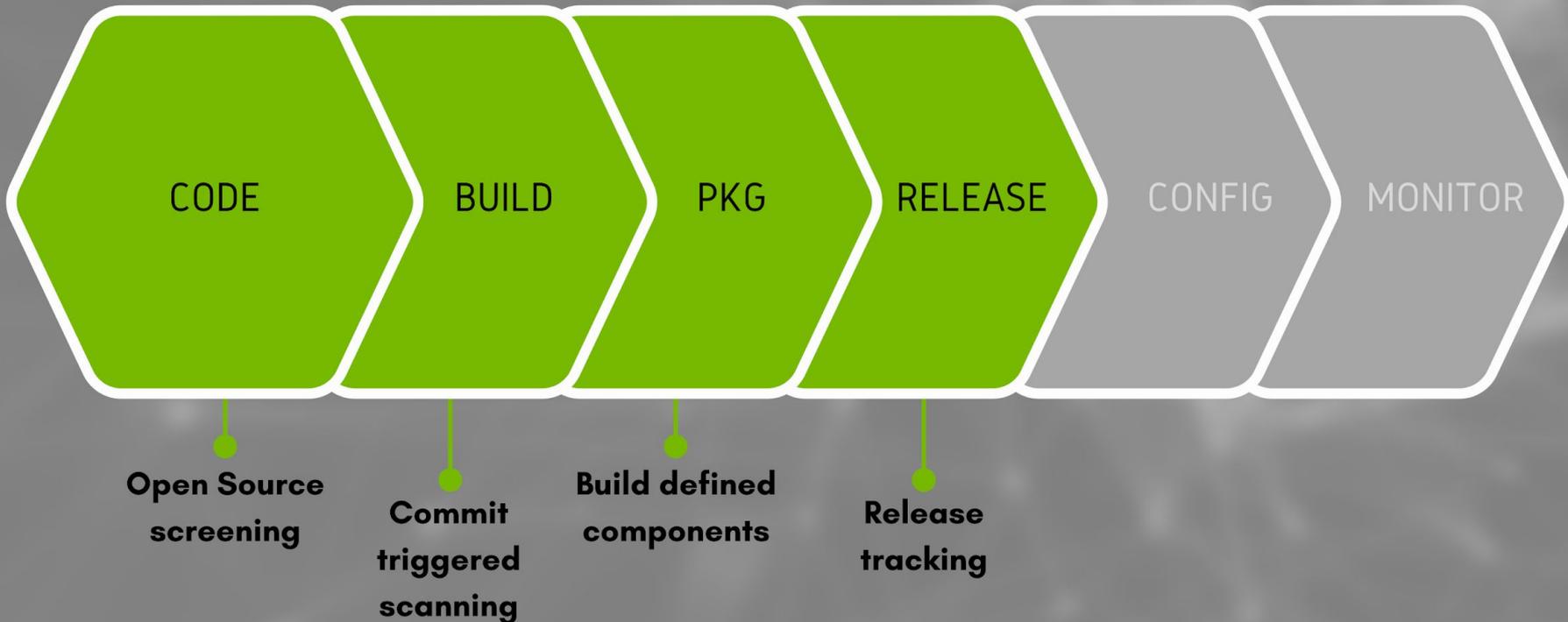
Commit triggered scanning

Build defined components

Step 3:

DEPENDENCY DEVOPS

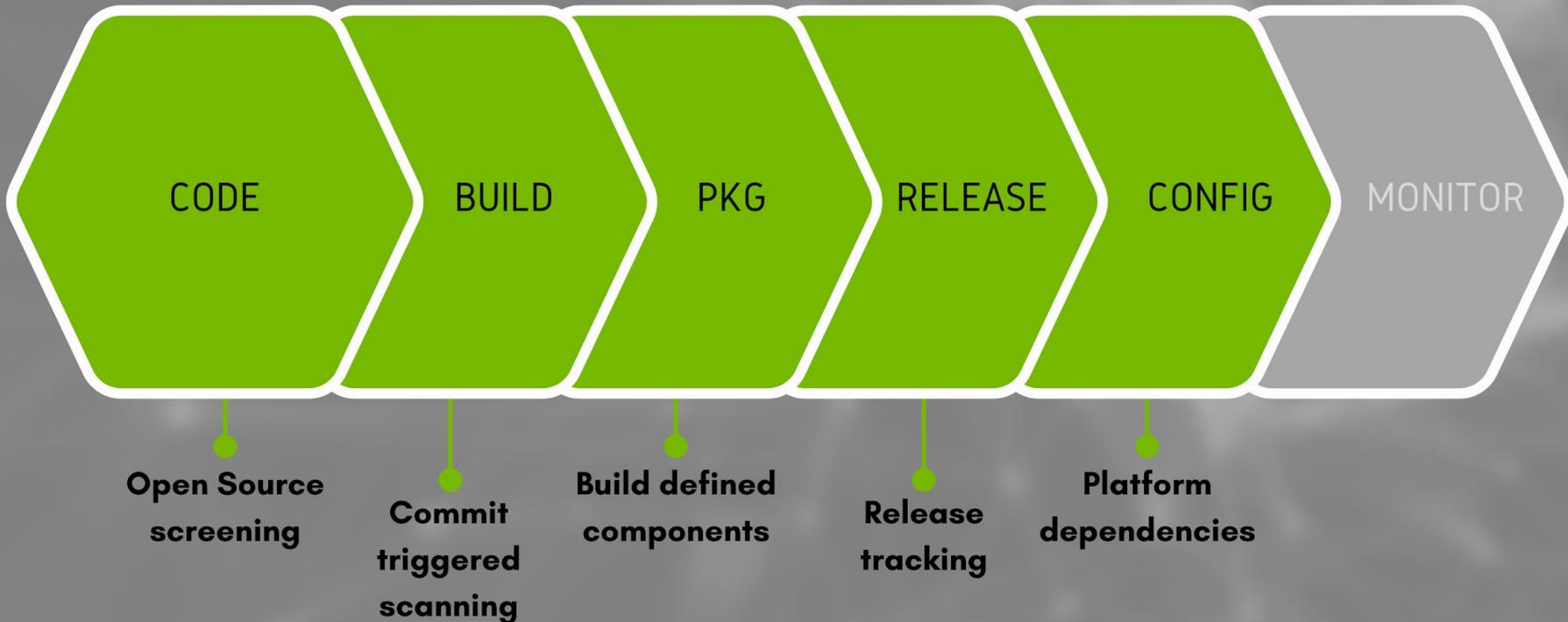
← Shift Left



Step 3:

DEPENDENCY DEVOPS

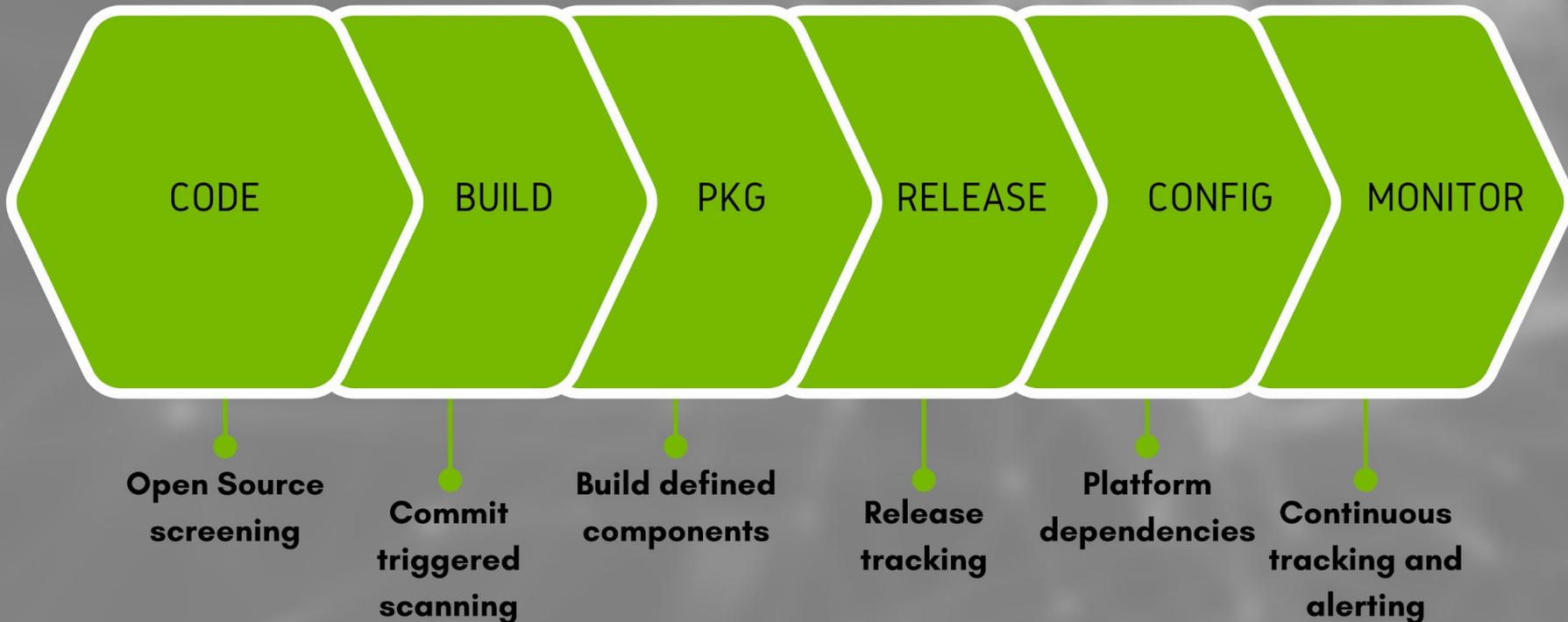
← Shift Left



Step 3:

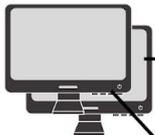
DEPENDENCY DEVOPS

← Shift Left



Step 4: Integrate for more data!

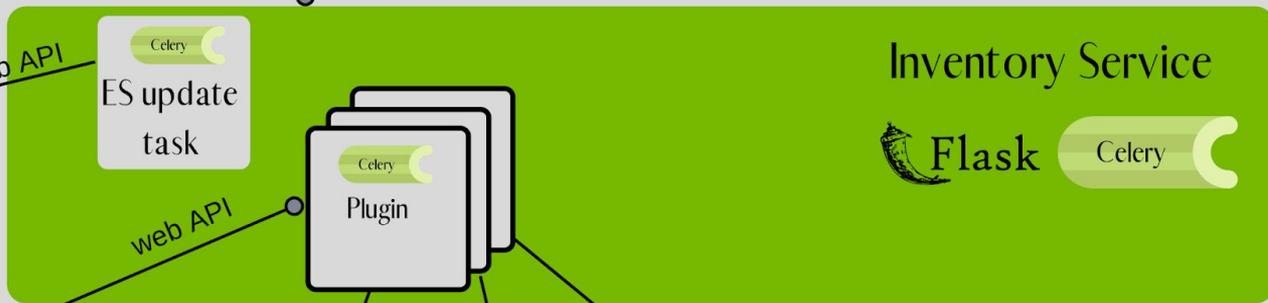
Users
(Web Browser)



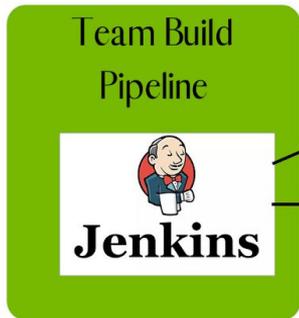
nspect



web API



web API



trigger



Internal security tool(s)



Static analysis

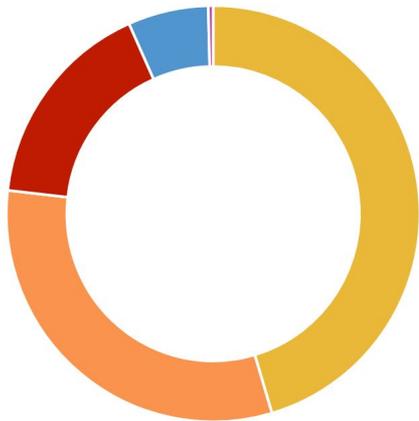


OSS scanning

Step 5:

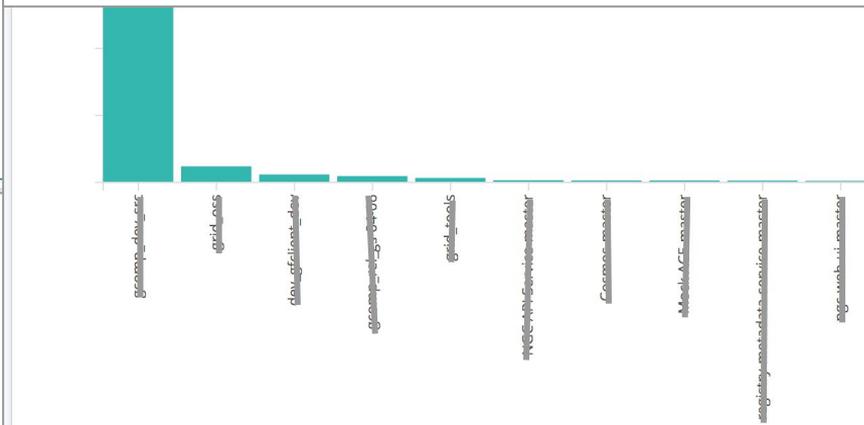
Metrics Drive Change

Severity Distribution for Vulnerabilities



- Medium
- High
- Critical
- Low
- None

Top 10 Repositories per Vulnerability Count



- Count

Managing YOUR WEB

Portfolio

Find the quickest way to populate and standardize.

Scope

Determine what is important and who owns it!

Automation

Integrate and automate. Meet developers where they are already working.

Value

Look for *more* interesting data. Entice your users with undeniable value. ;))

Leverage

Uncover the levers that control how your organization behaves with **metrics!**



