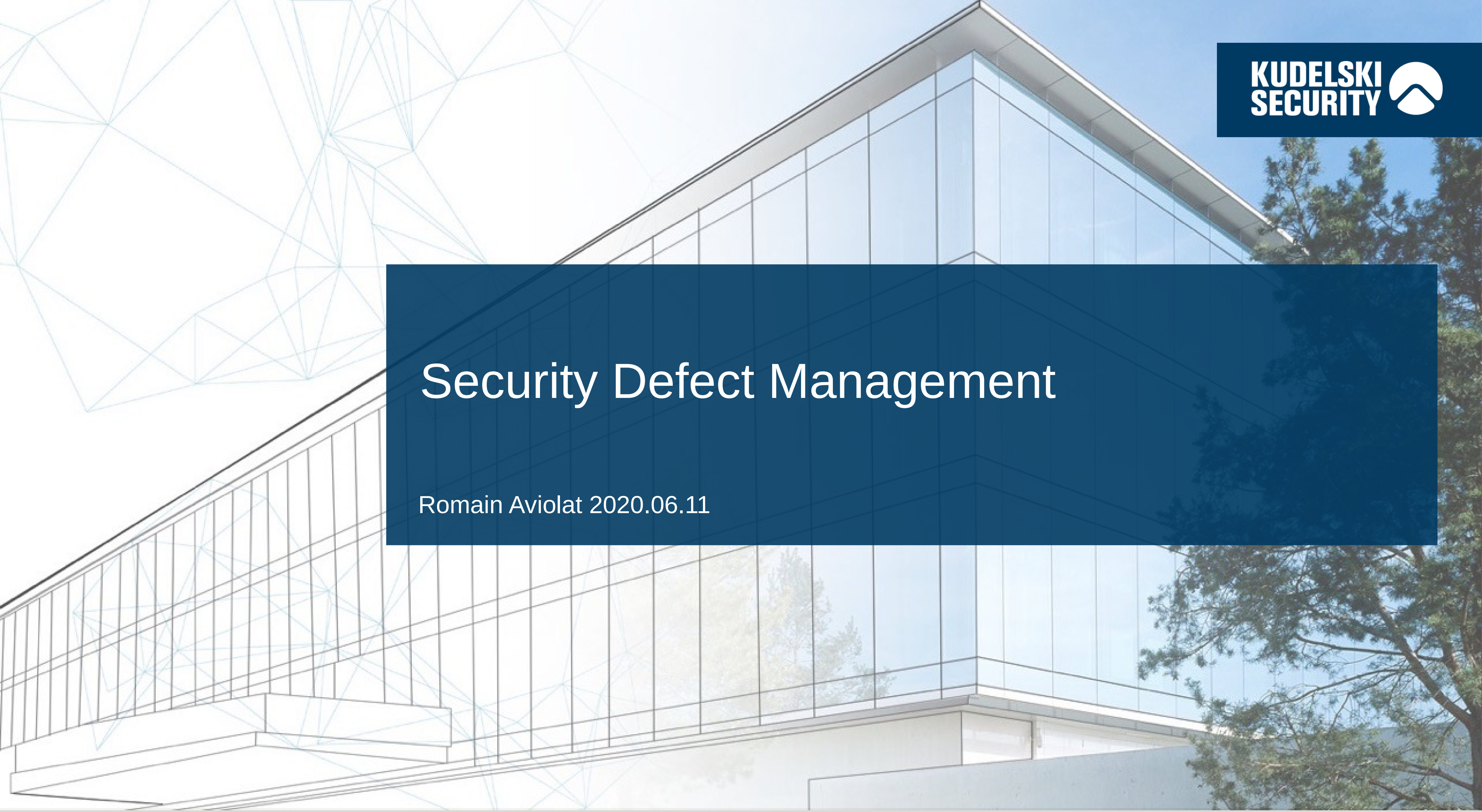


Security Defect Management

Romain Aviolat 2020.06.11

Me

Cloud and Security enthusiast

Love automation, infrastructure-as-code, DevSecOps

SME for security related question / architecture (Network, IAM, Cloud, BeyondCorp, SSDLC, …), security champions / guild.

Thanks Giulio for setting this up !

Today’s talk is about

Discussing the complexity of collecting intelligence about the security issues of a product / infrastructure, and the challenges that are facing DevSecOps teams in prioritizing fixes.

Based on my personal experience.

Spoiler: I don’t have all the answers
(feedback welcome)

KUDELSKI SECURITY

Systems security

There’s no such thing as a secure software, or a secure operating system.

- Systems can be patched against known vulnerabilities (NVD, OSVDB, …)
- What about unknown vulnerabilities ? (0day, darknets, …)
- Vulnerabilities that have not been found yet

KUDELSKI SECURITY

One line of defense is to collect as much information as possible about our products

Information can come at different stages

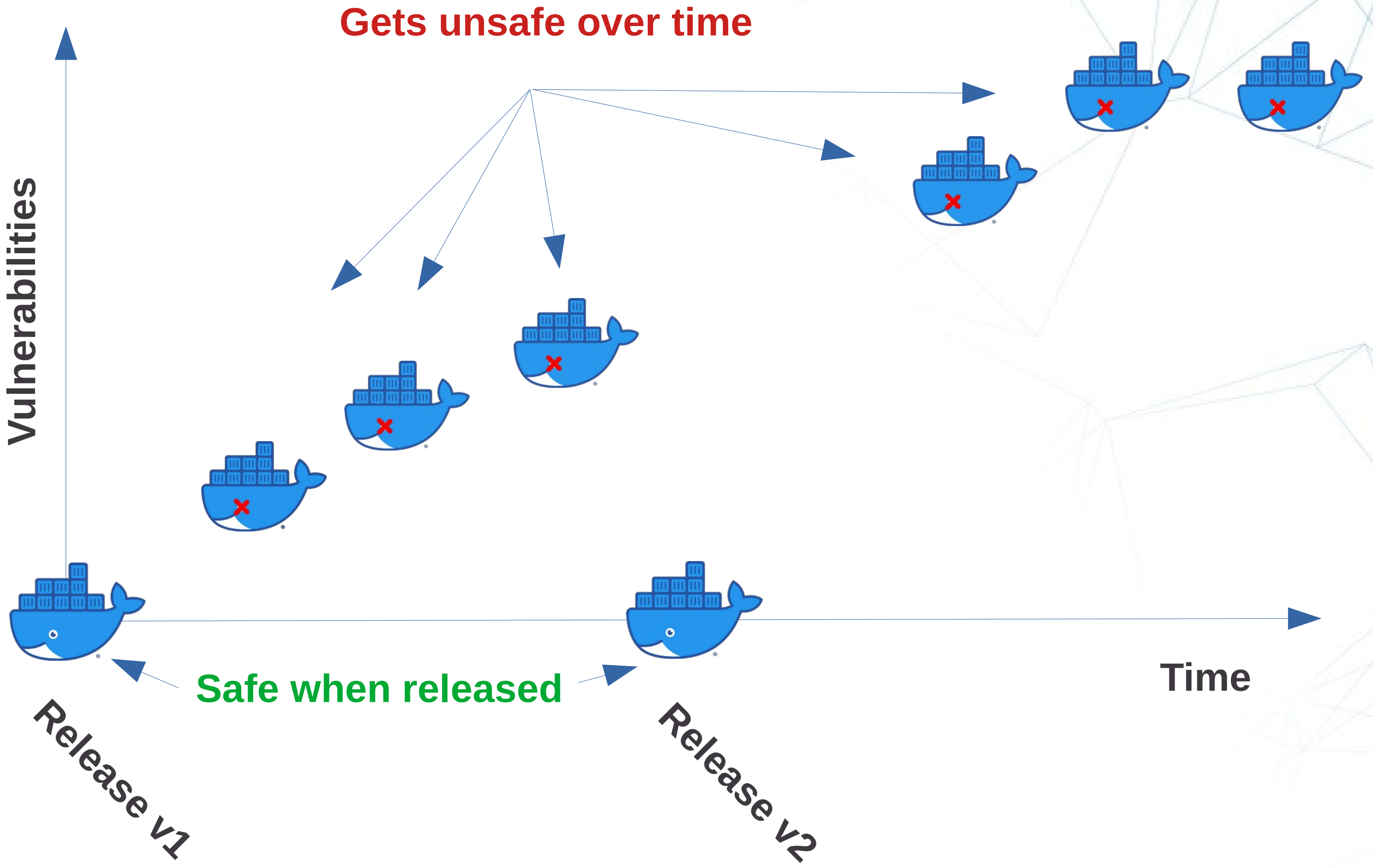
1) At Build / Release time
2) At scan-time (daily, weekly, …)
3) At Pen-test-time (yearly / ISO27001)
4) (When your data are available on paste-bin)

You need to have visibility on all these stages (incl 4… / collecting intelligence)

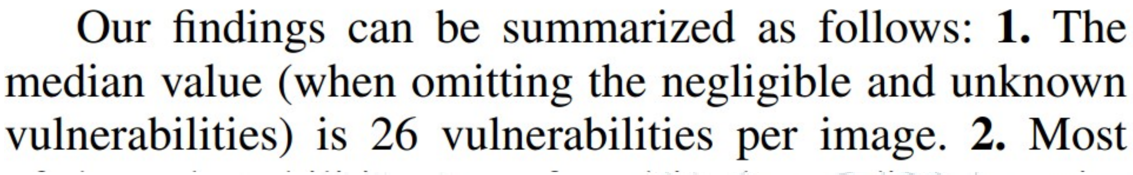
KUDELSKI SECURITY

Security of products is often linked to product releases

- Even with modern CI/CD workflows, security is assessed during the release stage.
- If you don't re-release often then the security posture of your products = security at release-time + all the vulnerabilities found in the meantime.
- Container-scanning usually don't make a lot of sense if you use latest versions at build-time.



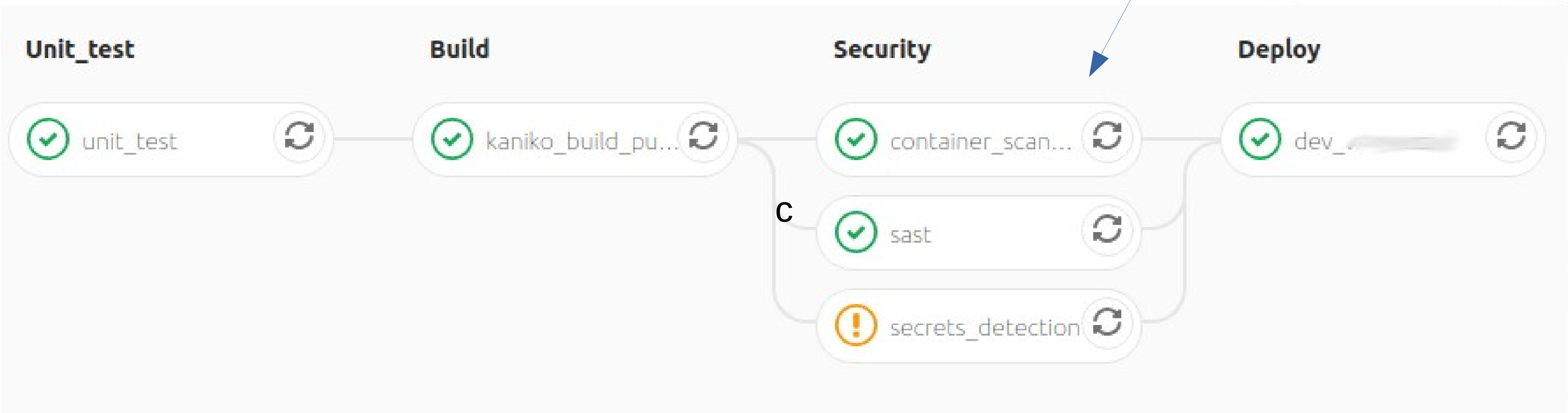
At Build / Release time



Our findings can be summarized as follows: **1.** The median value (when omitting the negligible and unknown vulnerabilities) is 26 vulnerabilities per image. **2.** Most

Vulnerability Analysis of 2500 Docker Hub Images https://arxiv.org/pdf/2006.02932.pdf

- Check your code (SAST, code quality)
- Ensure you’re not leaking secrets in your commits (git-secrets)
- Scan you containers
- Make sure that your releases are as clean as possible



Pros / Cons

+ Catch issues early in the release-cycle

+ Context around the issue (problem with a library introduced with the new feature)

- Can slow down pipelines, sometimes needs to be moved to QA pipelines (Fuzzing, Deep container scanning, ...)
- Not always easy to handle false-positives
- Hard to get “always green” jobs (fatigue)

KUDELSKI SECURITY

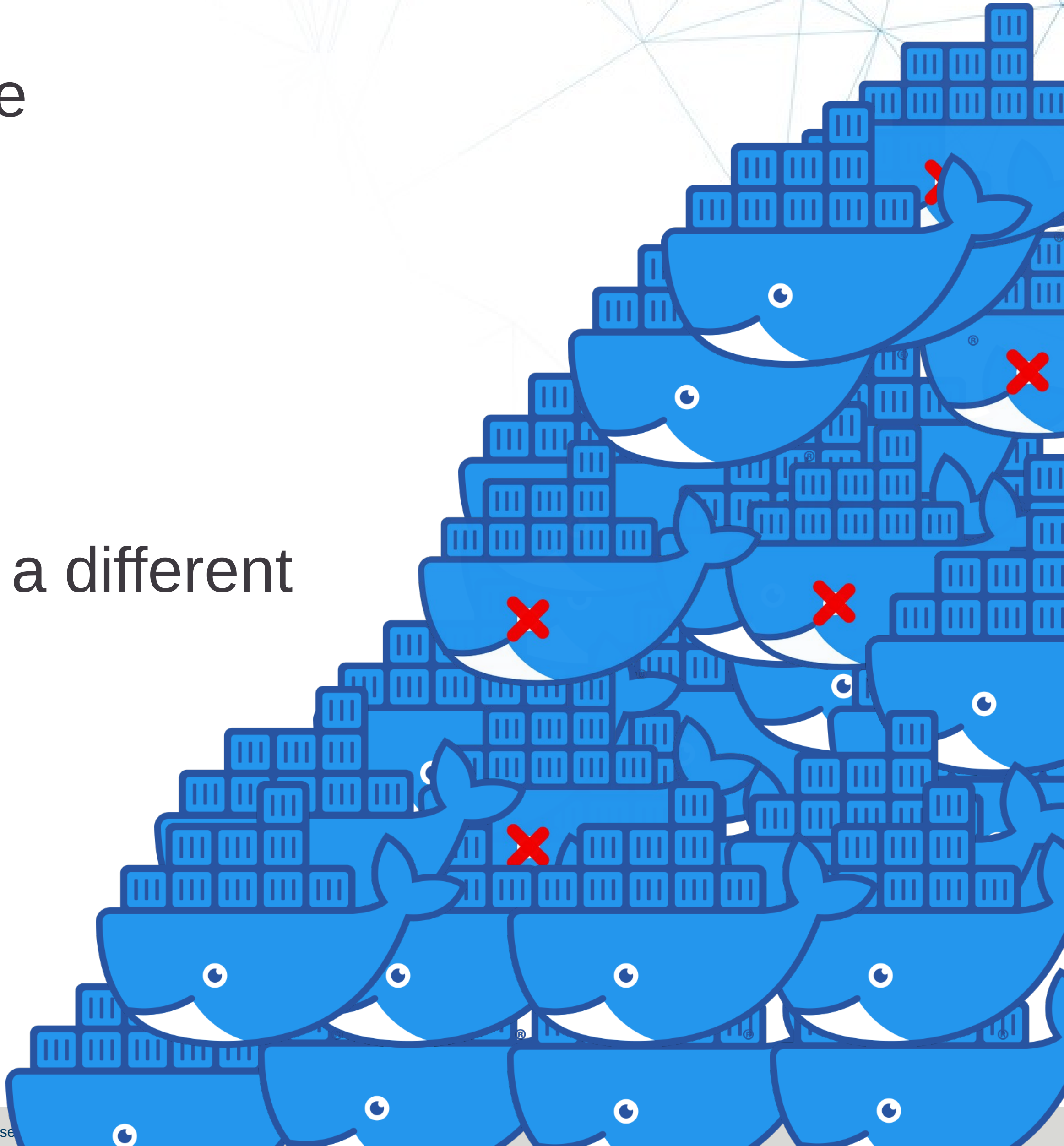
At scan-time

- Daily or weekly perimeter / vulnerability scan
- Daily container-registry-scans
- Daily web-app scans (OWASP top ten connected scans, ...)

Pros / Cons

+ Catch issues outside of the release-cycle

- Context is usually lost:
  - To whom does it belong ?
  - Is it running in production ?
  - Is it business-critical ?
- Perimeter scans are usually operated by a different team. (or company).



KUDELSKI SECURITY

At pen-test-time

+ Catch issues that automated tools would have missed
+ Things that computers can hardly do (yet)
  - Social-engineering
  - identify weak processes

- Frequency is not great
- Process is often painful (legal / mgmt, PR/PO, scoping, reports, ...)

Clean releases + continuous assessment over time + context

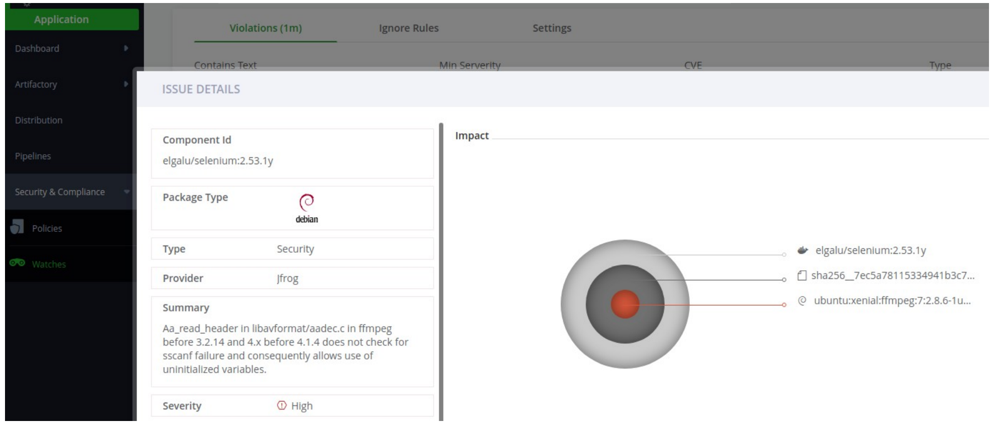
Defect-Management

KUDELSKI SECURITY

Security Defect Management

- Usually all inside their own silo
  - Container scanning, perimeter scans, webapp testing, sast, K8s, … .
- Loss of context

WebUIs, emails



Component Id
elgalu/selenium:2.53.1y

Package Type: debian

Type: Security

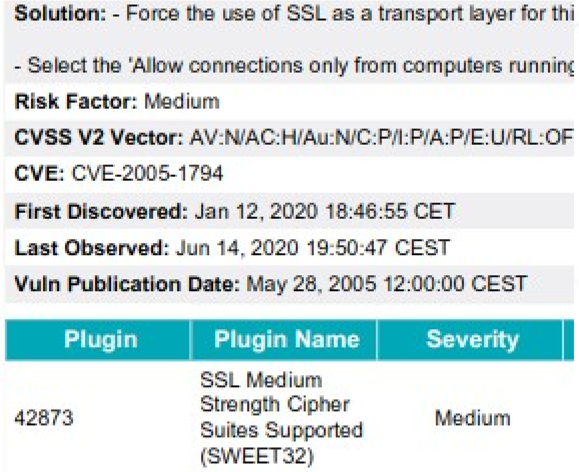
Provider: Jfrog

Summary
Aa_read_header in libavformat/aadec.c in ffmpeg before 3.2.14 and 4.x before 4.1.4 does not check for sscanf failure and consequently allows use of uninitialized variables.

Severity: High

Impact
elgalu/selenium:2.53.1y
sha256__7ec5a78115334941b3c7...
ubuntu:xenial:ffmpeg:7:2.8.6-1u...

700 pages PDF reports



Solution: - Force the use of SSL as a transport layer for thi

- Select the 'Allow connections only from computers running

Risk Factor: Medium

CVSS V2 Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P/E:U/RL:OF

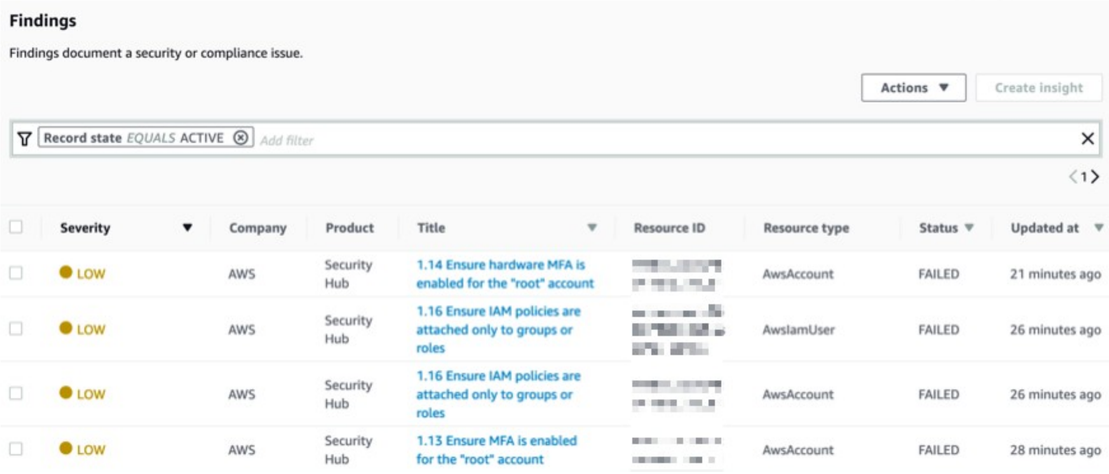
CVE: CVE-2005-1794

First Discovered: Jan 12, 2020 18:46:55 CET

Last Observed: Jun 14, 2020 19:50:47 CEST

Vuln Publication Date: May 28, 2005 12:00:00 CEST

Plugin	Plugin Name	Severity
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium



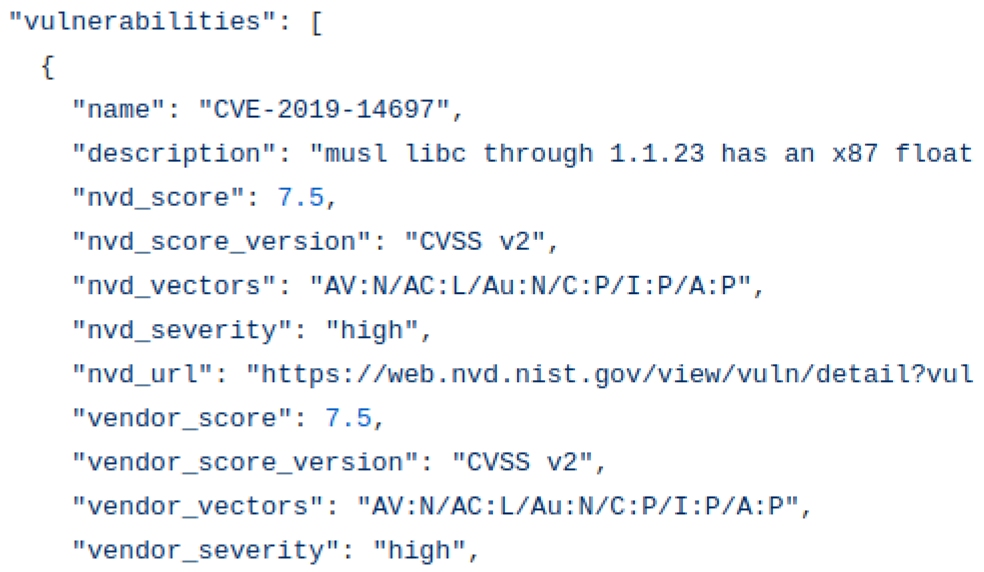
Findings

Findings document a security or compliance issue.

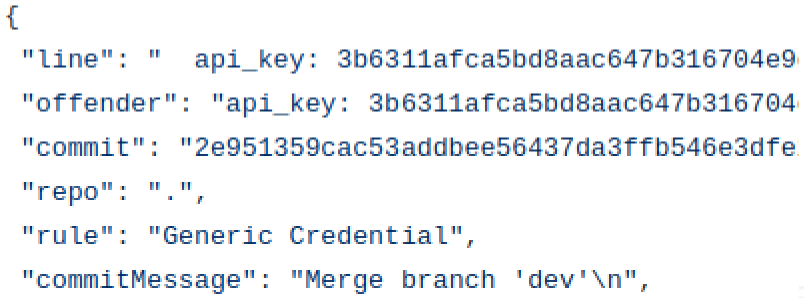
□	Severity ▼	Company	Product	Title ▼	Resource ID	Resource type	Status ▼	Updated at ▼
□	● LOW	AWS	Security Hub	1.14 Ensure hardware MFA is enabled for the "root" account	[redacted]	AwsAccount	FAILED	21 minutes ago
□	● LOW	AWS	Security Hub	1.16 Ensure IAM policies are attached only to groups or roles	[redacted]	AwsIamUser	FAILED	26 minutes ago
□	● LOW	AWS	Security Hub	1.16 Ensure IAM policies are attached only to groups or roles	[redacted]	AwsAccount	FAILED	26 minutes ago
□	● LOW	AWS	Security Hub	1.13 Ensure MFA is enabled for the "root" account	[redacted]	AwsAccount	FAILED	28 minutes ago

Security Defect Management

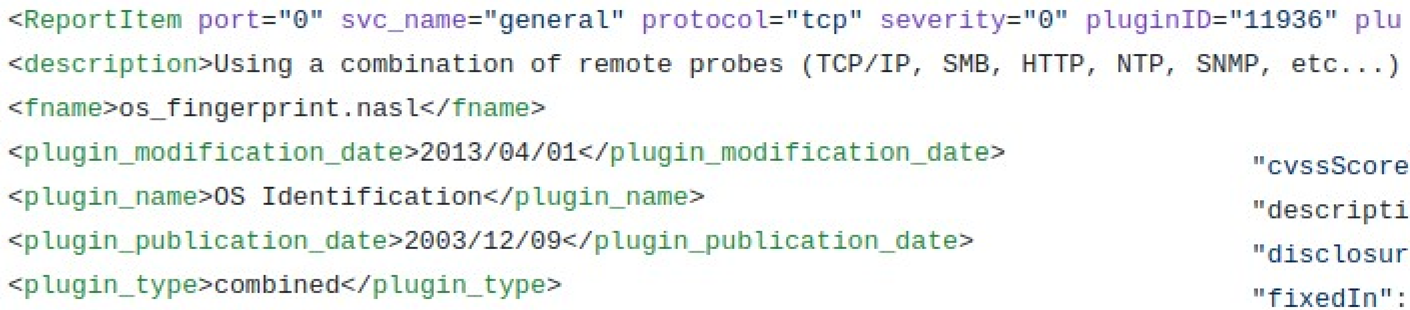
All these tools are usually generating computer-readable information.



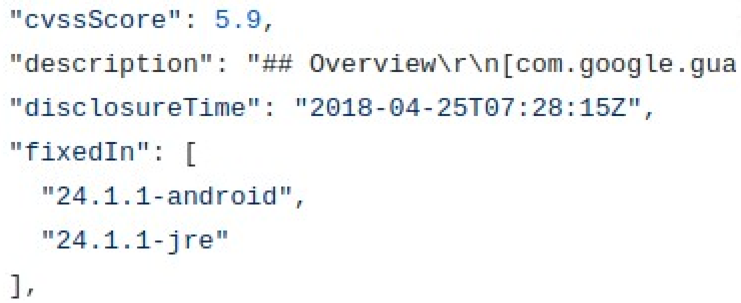
```
"vulnerabilities": [
  {
    "name": "CVE-2019-14697",
    "description": "musl libc through 1.1.23 has an x87 float
    "nvd_score": 7.5,
    "nvd_score_version": "CVSS v2",
    "nvd_vectors": "AV:N/AC:L/Au:N/C:P/I:P/A:P",
    "nvd_severity": "high",
    "nvd_url": "https://web.nvd.nist.gov/view/vuln/detail?vul
    "vendor_score": 7.5,
    "vendor_score_version": "CVSS v2",
    "vendor_vectors": "AV:N/AC:L/Au:N/C:P/I:P/A:P",
    "vendor_severity": "high",
```



```
{
 "line": "  api_key: 3b6311afca5bd8aac647b316704e9
 "offender": "api_key: 3b6311afca5bd8aac647b316704
 "commit": "2e951359cac53addbee56437da3ffb546e3dfe
 "repo": ".",
 "rule": "Generic Credential",
 "commitMessage": "Merge branch 'dev'\n",
```

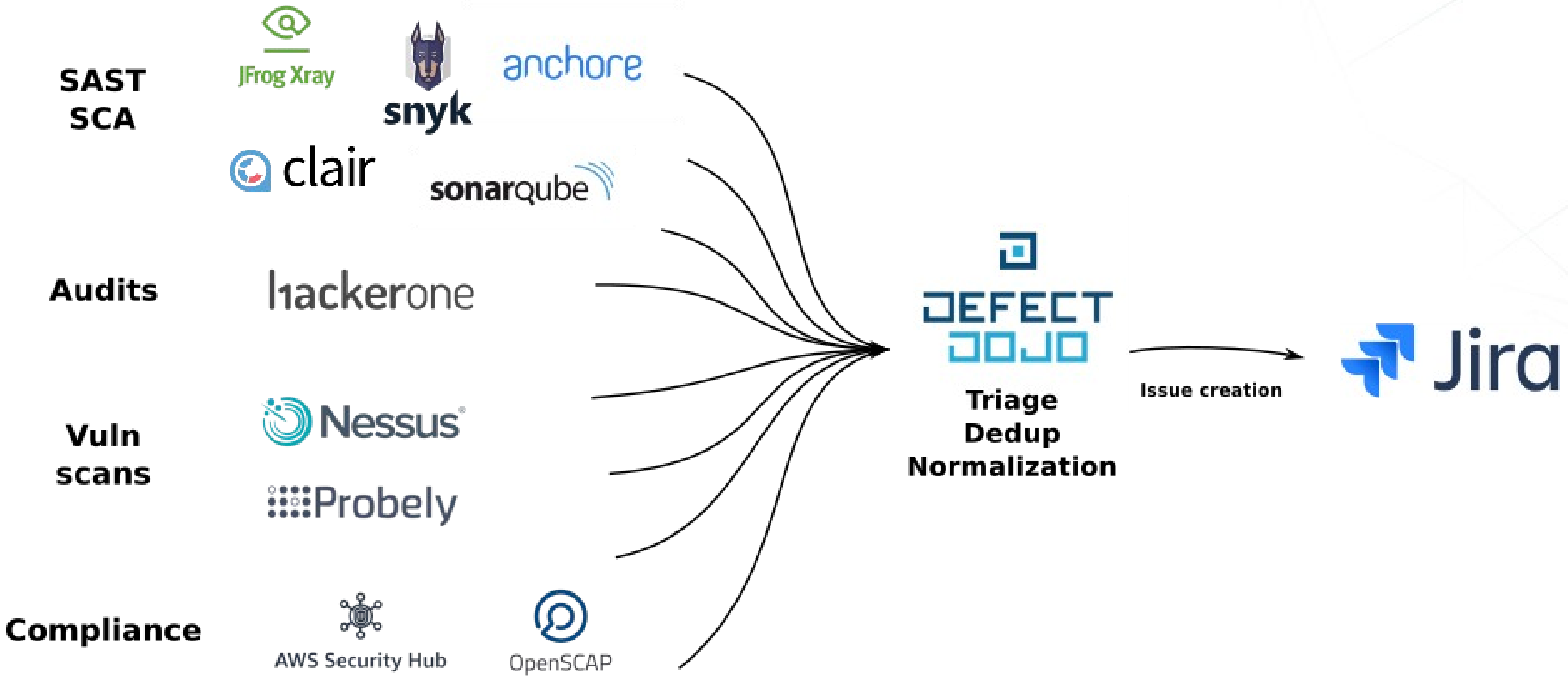


```
<ReportItem port="0" svc_name="general" protocol="tcp" severity="0" pluginID="11936" plu
<description>Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...)
<fname>os_fingerprint.nasl</fname>
<plugin_modification_date>2013/04/01</plugin_modification_date>
<plugin_name>OS Identification</plugin_name>
<plugin_publication_date>2003/12/09</plugin_publication_date>
<plugin_type>combined</plugin_type>
```



```
"cvssScore": 5.9,
"description": "## Overview\r\n[com.google.gua
"disclosureTime": "2018-04-25T07:28:15Z",
"fixedIn": [
  "24.1.1-android",
  "24.1.1-jre"
],
```

Security Defect Management (with Defect Dojo a proposal)



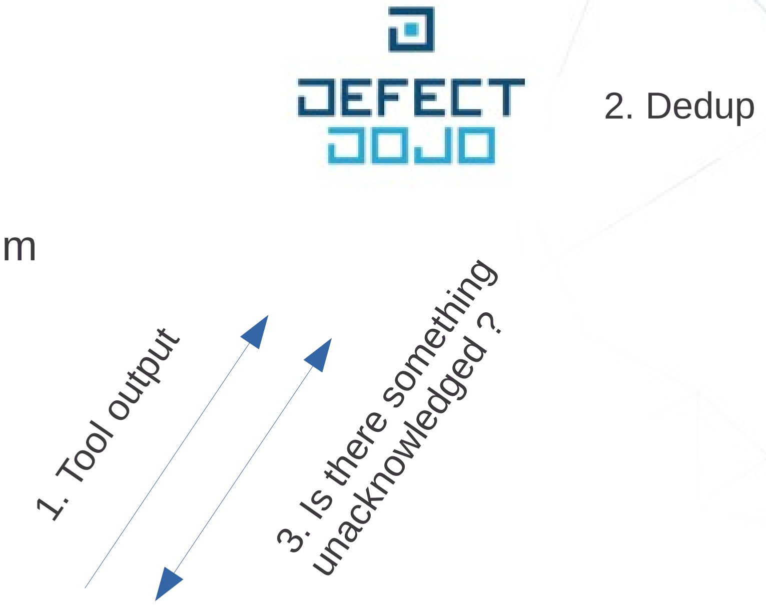
Defect Management at release-time

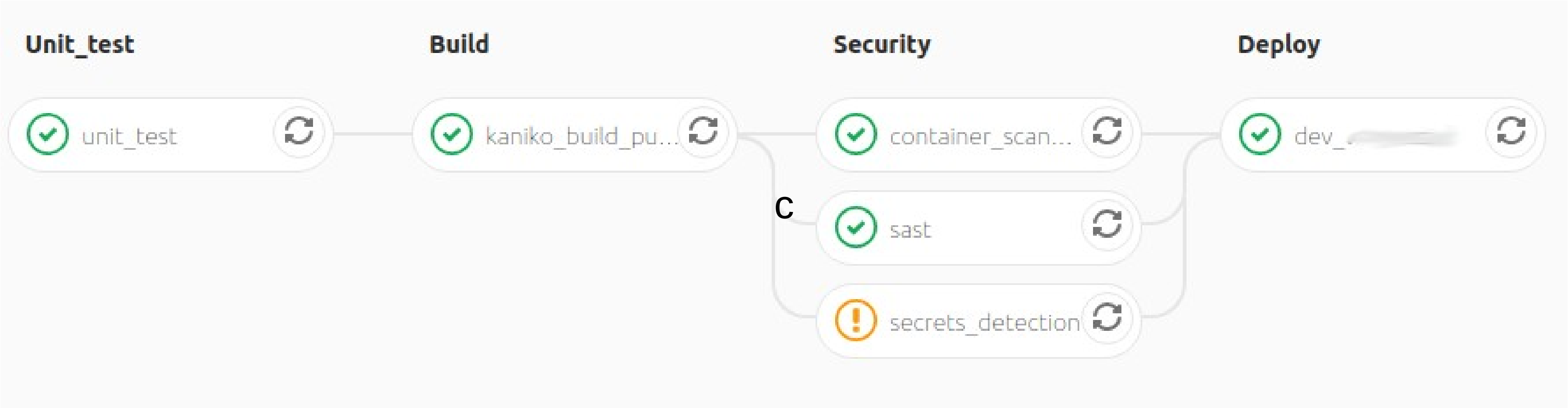
Proposal: track the defects outside the CI/CD pipelines.

Both can now be flagged, inside the defect-management system

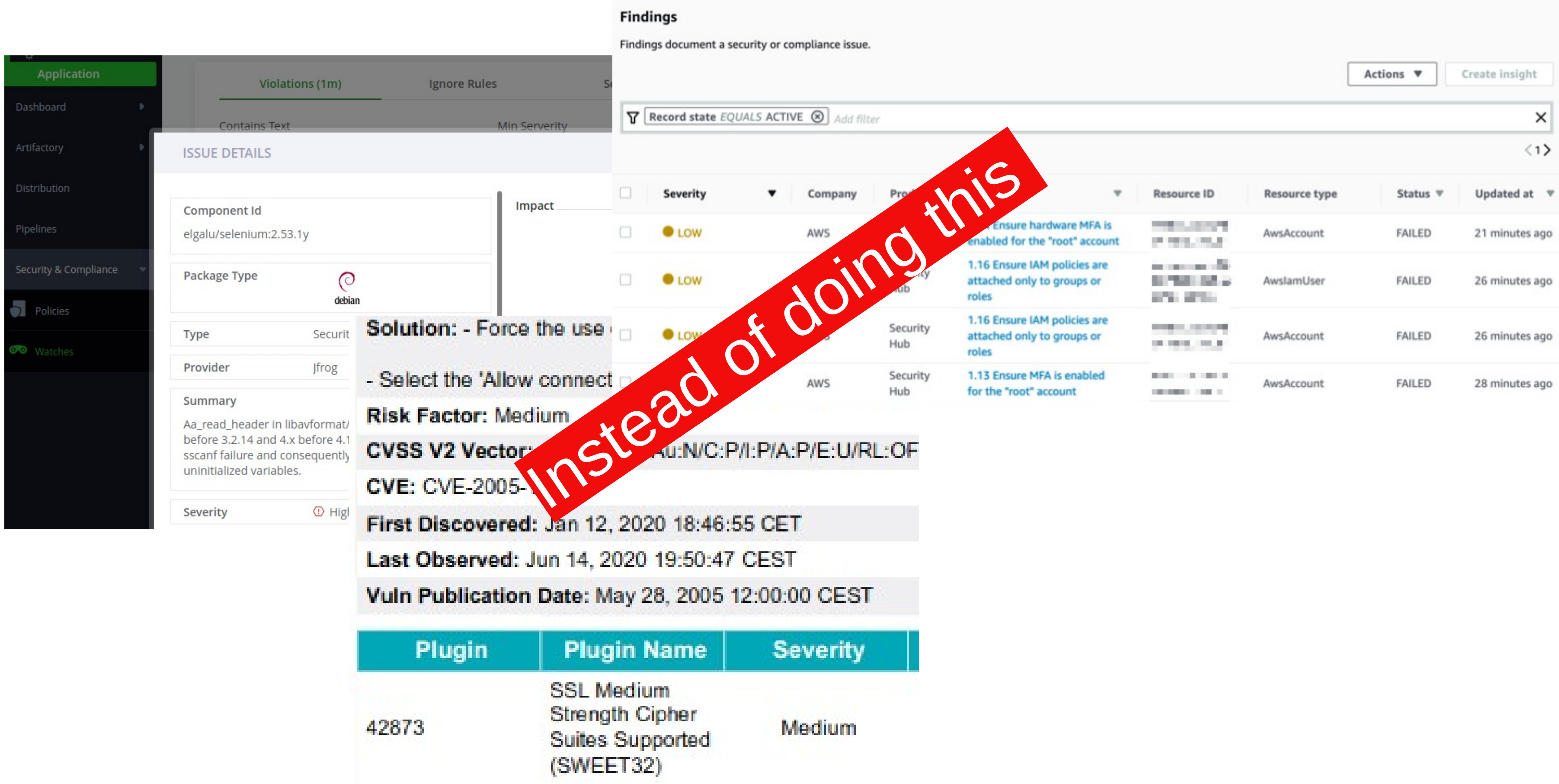
~~- Not always easy to handle false-positives~~

~~- Hard to get “always green” jobs (fatigue)~~





Defect Management at scan-time



Instead of doing this

Component Id	elgalu/selenium:2.53.1y
Package Type	debian
Type	Securit
Provider	Jfrog
Summary	Aa_read_header in libavformat/ before 3.2.14 and 4.x before 4.1 sscanf failure and consequently uninitialized variables.
Severity	Higl

Solution: - Force the use

- Select the 'Allow connect

Risk Factor: Medium

CVSS V2 Vector: Au:N/C:P/I:P/A:P/E:U/RL:OF

CVE: CVE-2005-

First Discovered: Jan 12, 2020 18:46:55 CET

Last Observed: Jun 14, 2020 19:50:47 CEST

Vuln Publication Date: May 28, 2005 12:00:00 CEST

Plugin	Plugin Name	Severity
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium

Findings

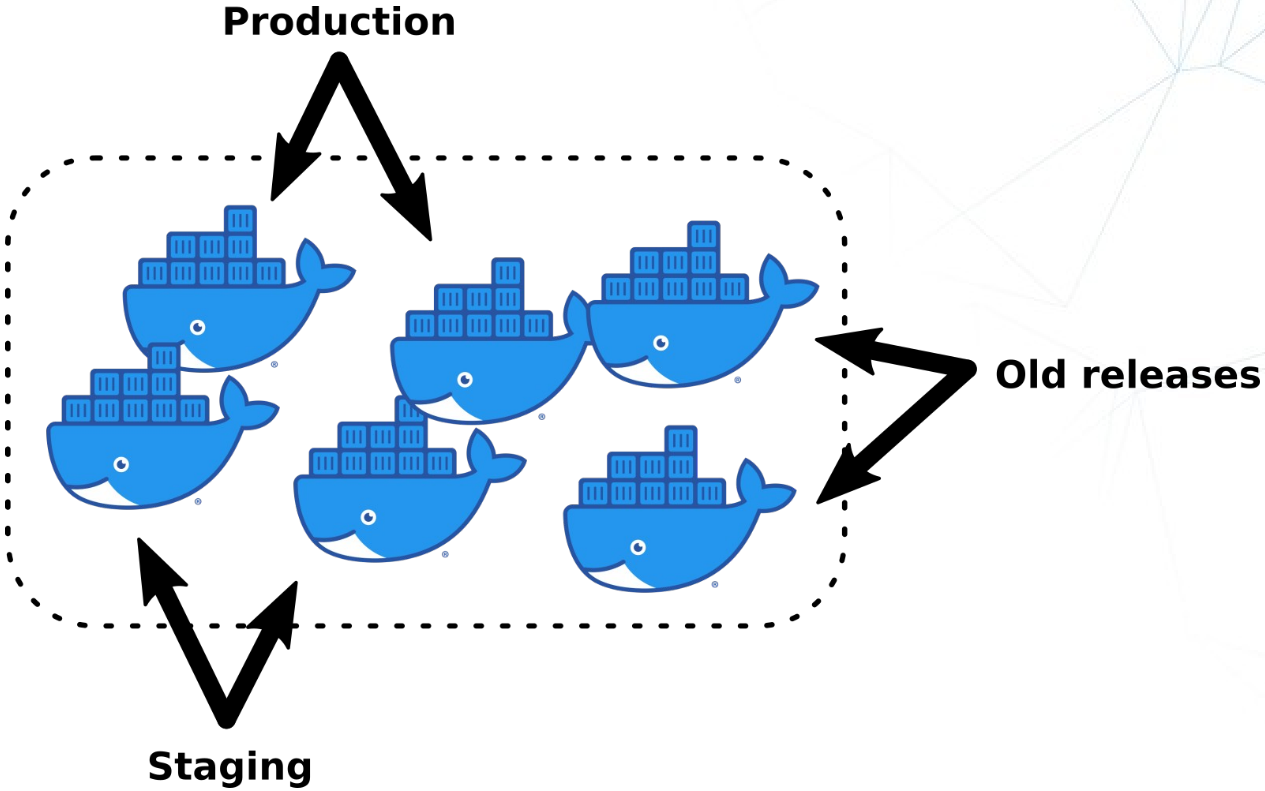
Findings document a security or compliance issue.

□	Severity ▼	Company	Pro	▼	Resource ID	Resource type	Status ▼	Updated at ▼
□	● LOW	AWS		Ensure hardware MFA is enabled for the "root" account	[redacted]	AwsAccount	FAILED	21 minutes ago
□	● LOW		ty Hub	1.16 Ensure IAM policies are attached only to groups or roles	[redacted]	AwsIamUser	FAILED	26 minutes ago
□	● LOW		Security Hub	1.16 Ensure IAM policies are attached only to groups or roles	[redacted]	AwsAccount	FAILED	26 minutes ago
		AWS	Security Hub	1.13 Ensure MFA is enabled for the "root" account	[redacted]	AwsAccount	FAILED	28 minutes ago

Defect Management at scan-time

Proposal:

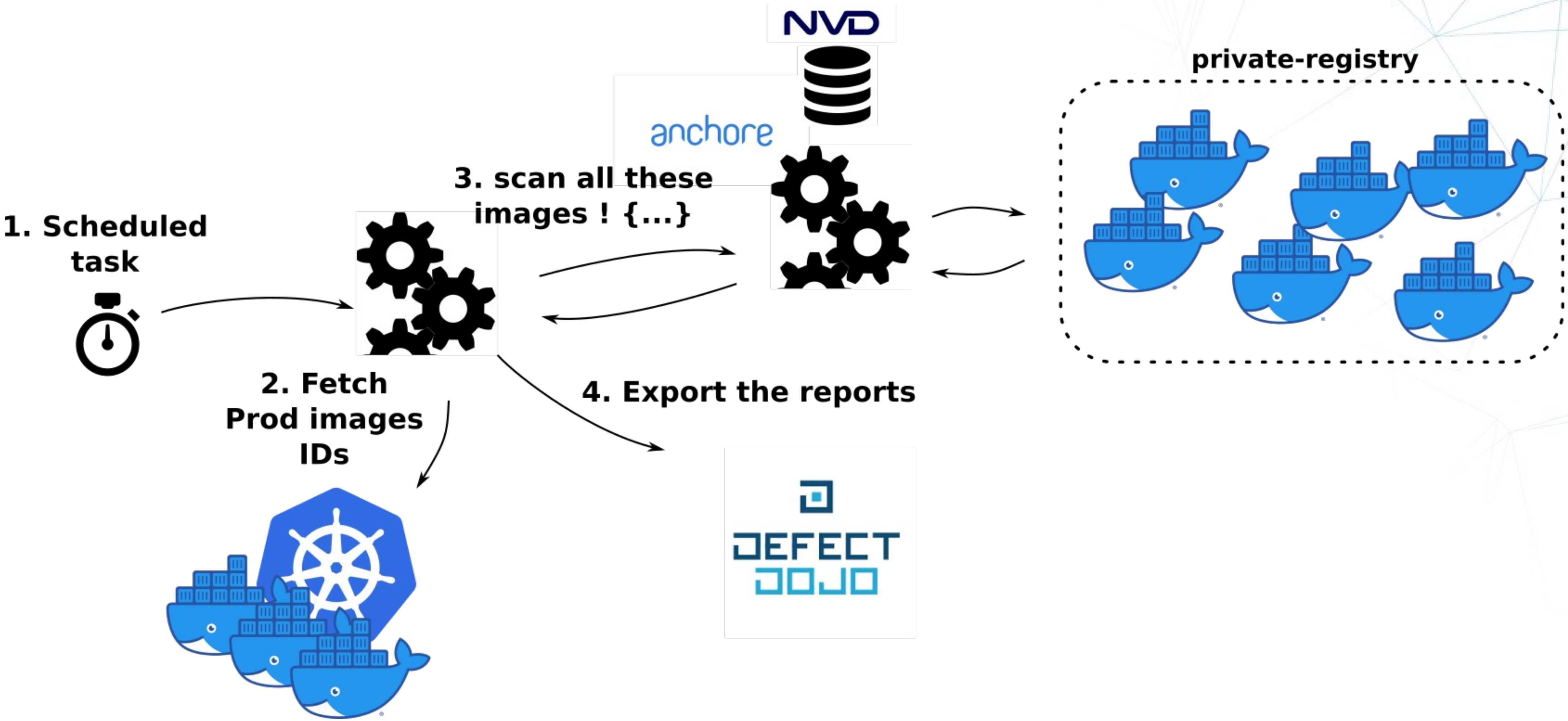
1. Give context to your security defects
2. Scan what make sense
3. Aggregate data close to the defects that are coming from CI/CD pipelines



Ex for containers:

- Scan only containers that are running in production.

Defect contextualization example (K8s + Docker)



1. Scheduled task

2. Fetch Prod images IDs

3. scan all these images ! {...}

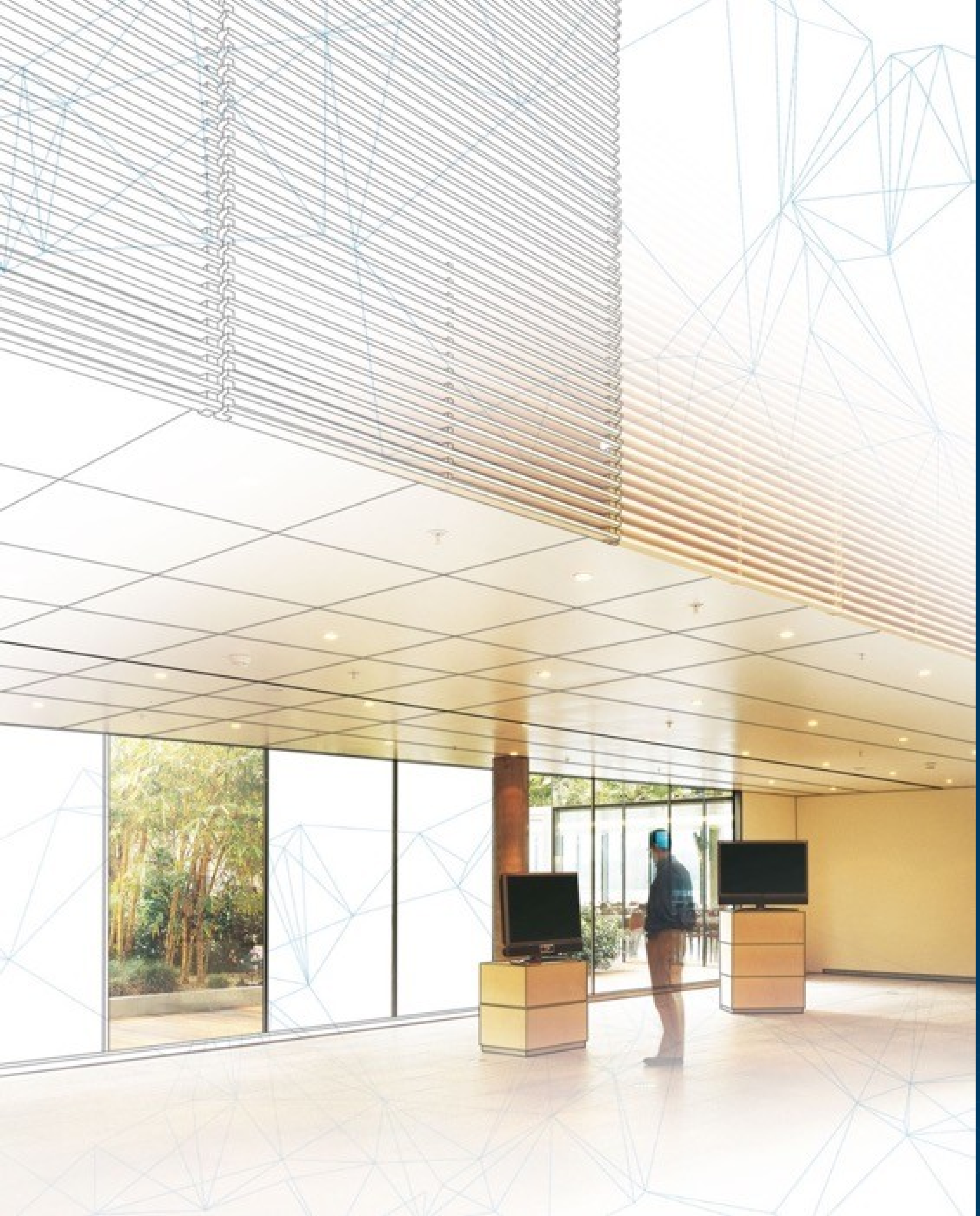
4. Export the reports

Ultimately we should have

- A system that aggregates all the information about our products
- That is easy to integrate inside existing teams tools:
  - Gitlab, Jenkins, Jira, ...
- That can give visibility to a broad category of users (devs, po, ciso, …)
- That is easy to use

KUDELSKI SECURITY

Questions, Ideas ?



KUDELSKI SECURITY