Codenotary

Trusted Software Supply Chain

Trusted SBOMs

SDLC Evidence

Trusted Software

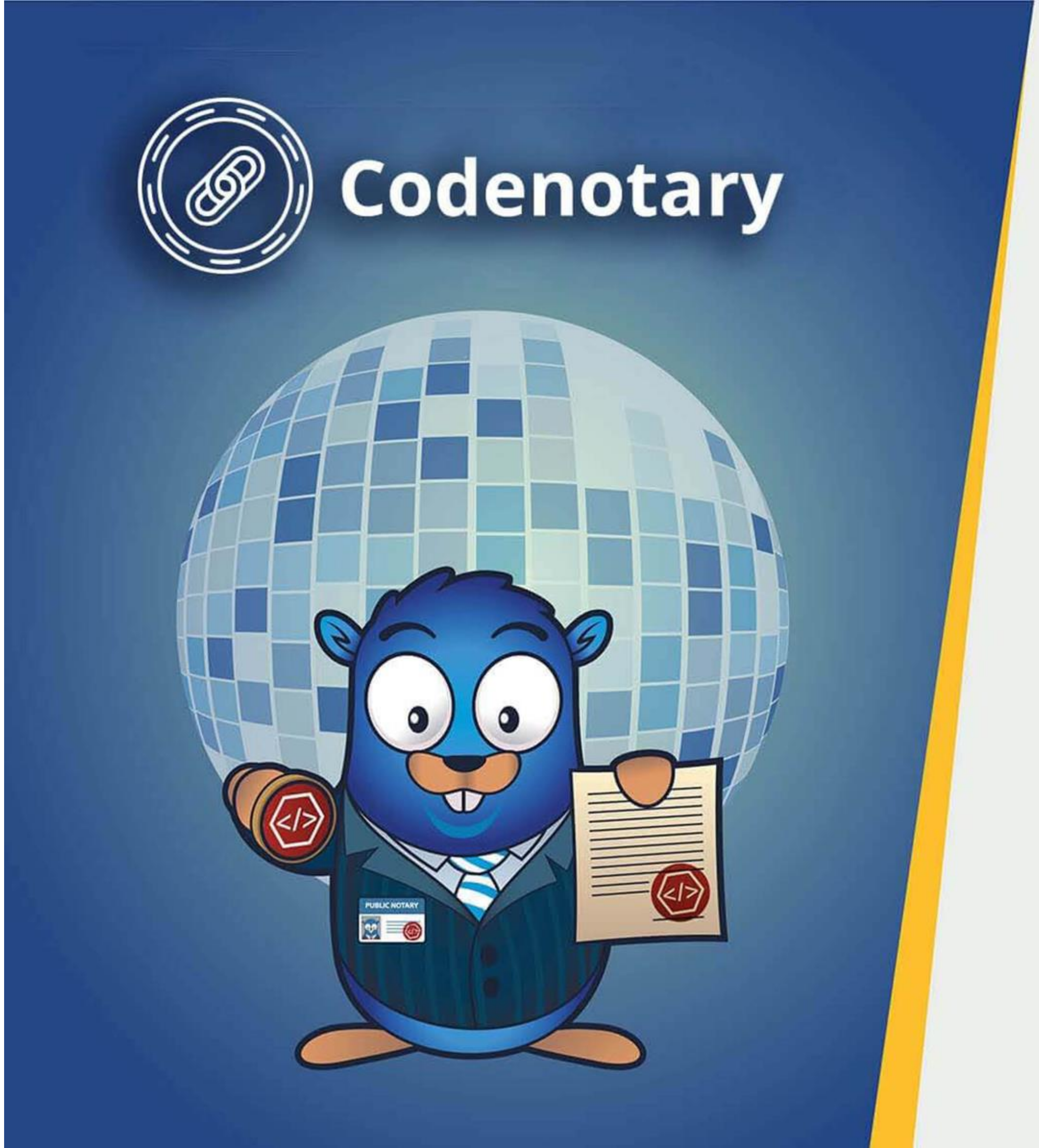
CI/CD Pipelines kontinuierlich schützen und Risiken senken

October, 2022

OSAD

IBM PartnerWorld

vmware PARTNER TECHNOLOGY ALLIANCE



Topics

- Software Supply Chain Attacks
- Executive Order
- Vulnerability Scanner
- SBOMs (Software Bill of Materials)
- SLSA and Attestation
- The Runtime problem
- Ways to protect CI/CD pipelines/applications

CYBER AND SUPPLY CHAIN ATTACKS

MANIPULATED CODE AND DATA CAUSES EVER INCREASING COSTS

01

SolarWinds

December 2020

Cyberattack affects over 18.000 companies and authorities. Estimated losses in the billions.

solarwinds

02

British Airways

August 2018

Details of about 500,000 customers were stolen resulting in a $329M penalty plus various claims.

BRITISH AIRWAYS

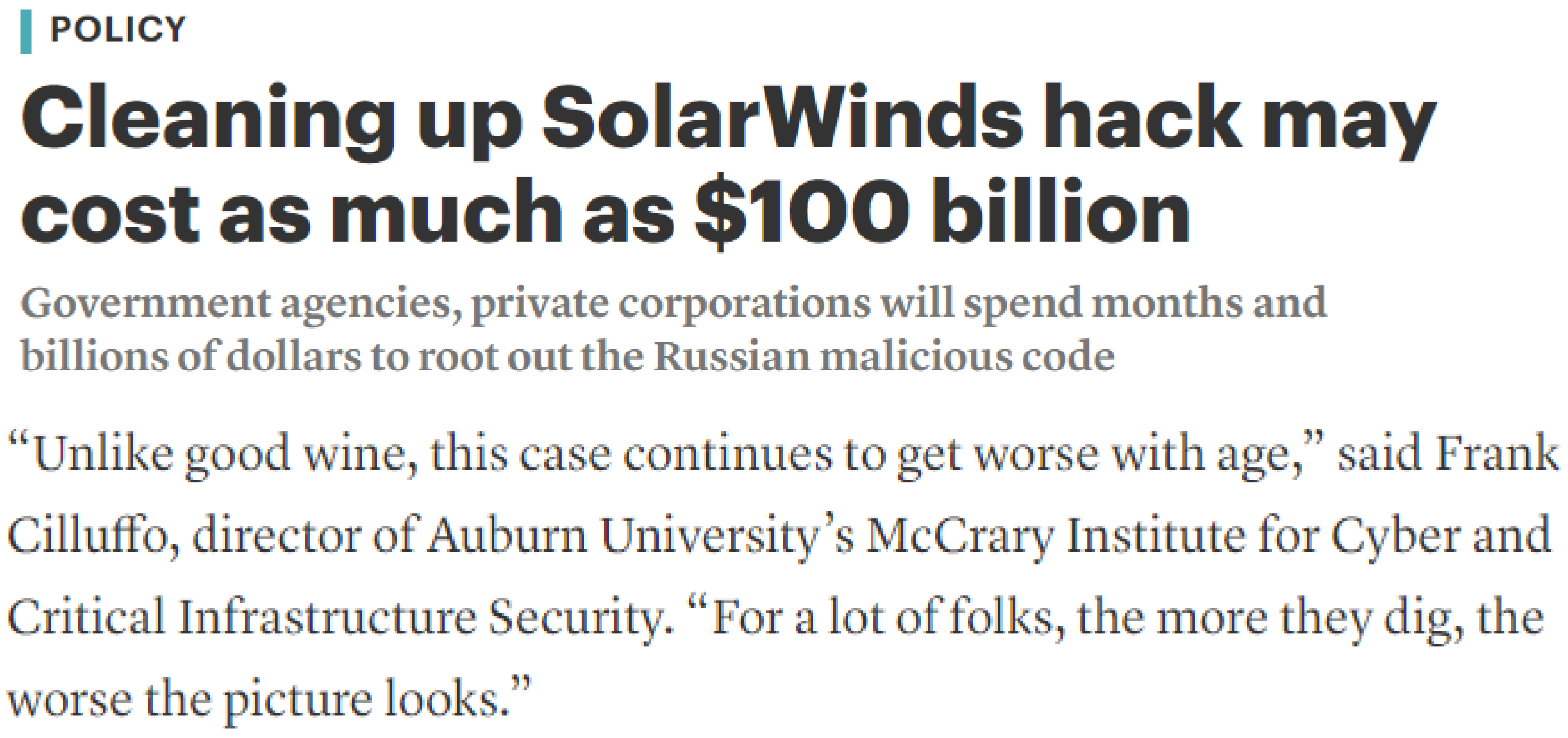
03

Codecov

JULY 2021

Malicious code gained access to customers' CICD environments.

Codecov



POLICY

Cleaning up SolarWinds hack may cost as much as $100 billion

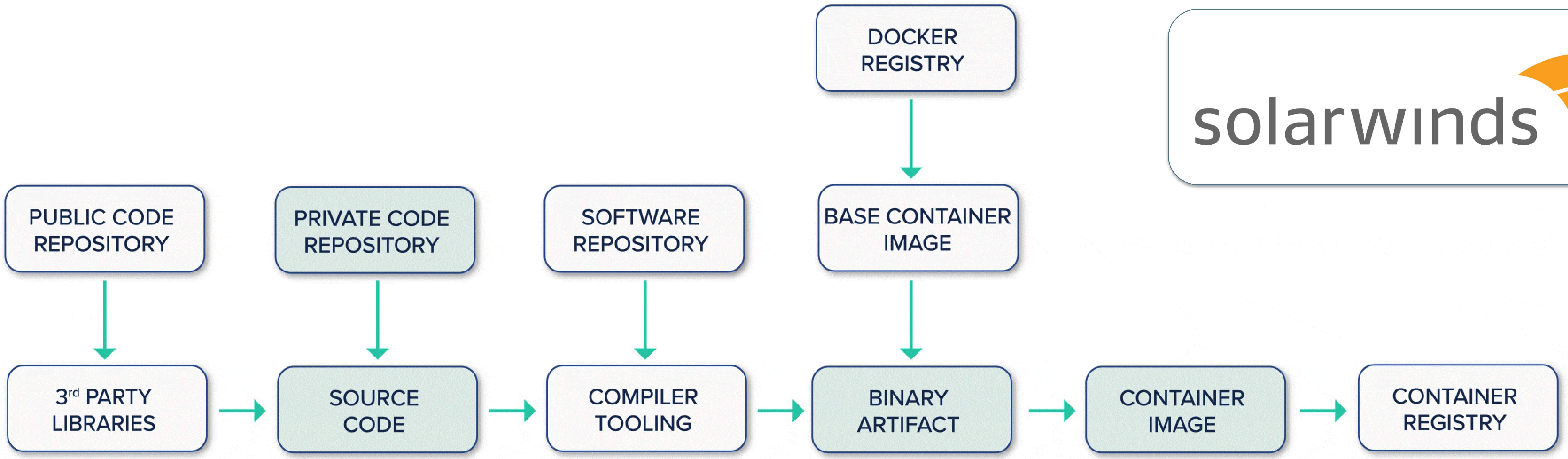
Government agencies, private corporations will spend months and billions of dollars to root out the Russian malicious code

"Unlike good wine, this case continues to get worse with age," said Frank Cilluffo, director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security. "For a lot of folks, the more they dig, the worse the picture looks."

INCREASE

IN SUPPLY CHAIN ATTACKS IN 2021

SOLARWINDS ATTACK APRIL 2021



solarwinds

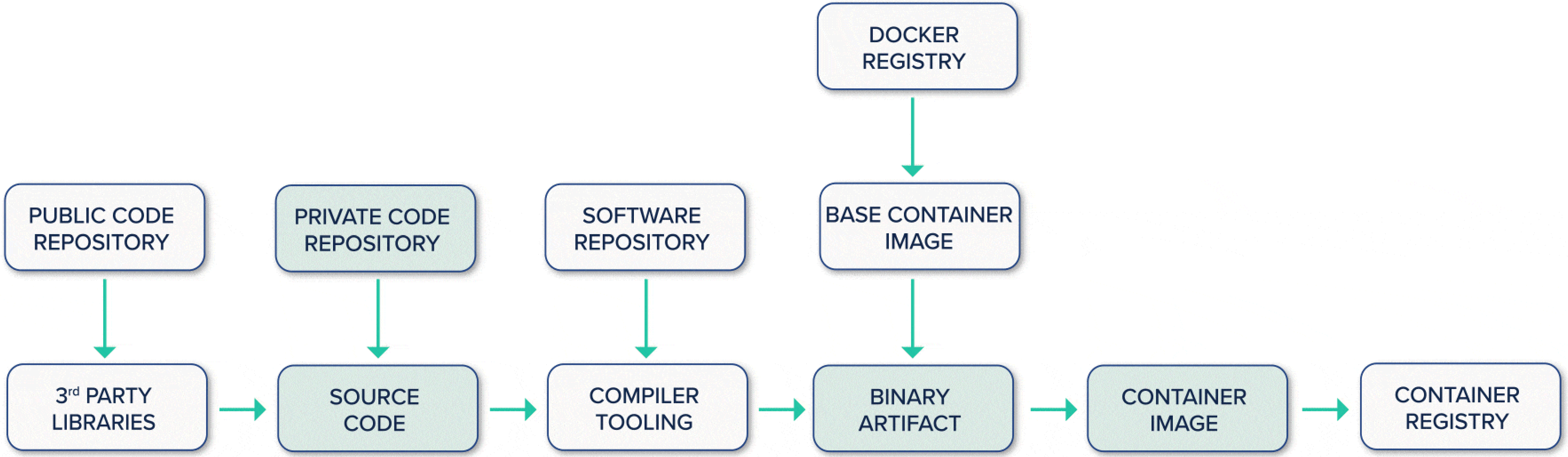
18,000 +Customers Have Been Affected!

vmware intel Microsoft NVIDIA cisco FireEye DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA belkin

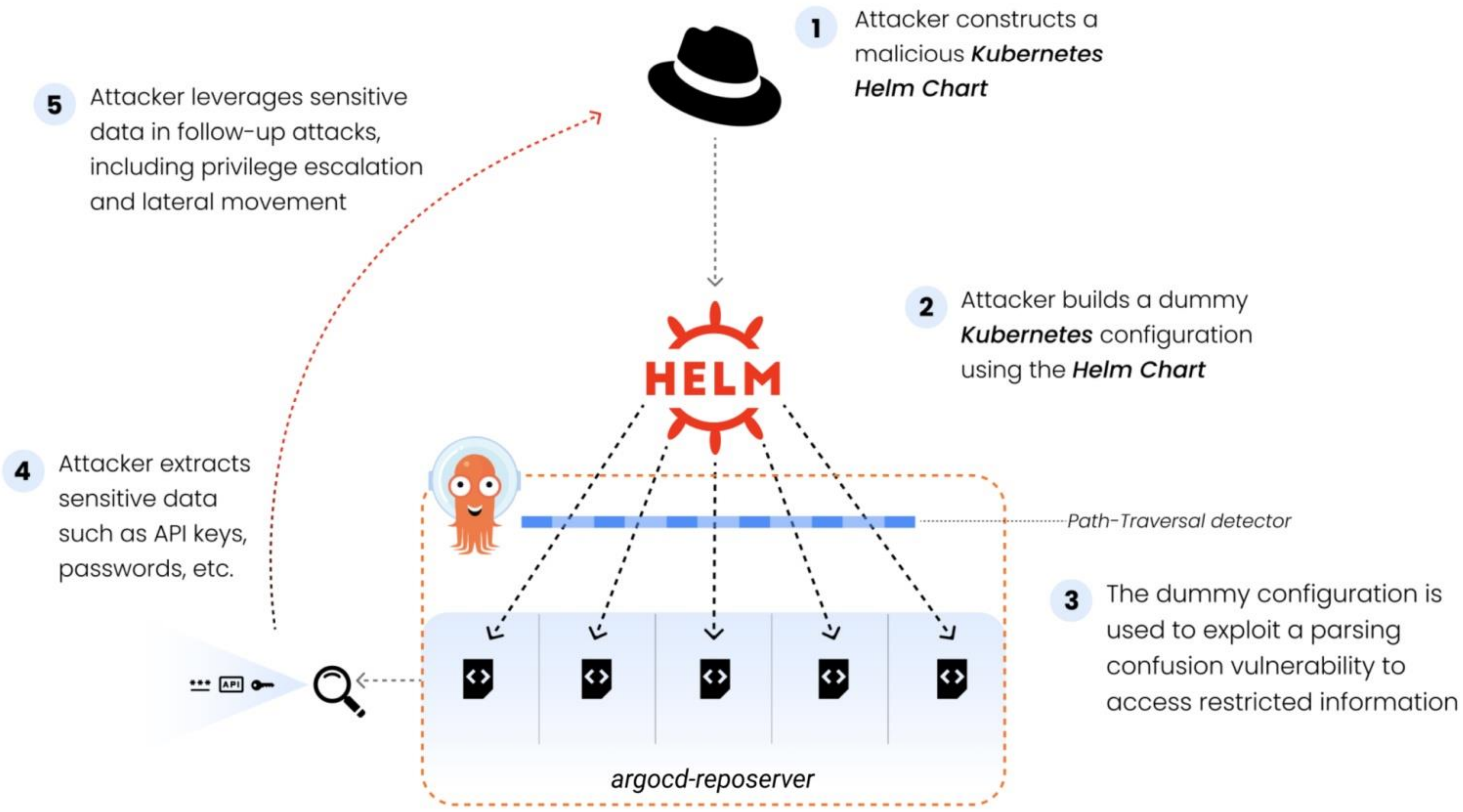
CODECOV ATTACK APRIL 2021

- Approximately 29,000 companies use Codecov's development tools according to the company's statement, including GoDaddy, Proctor & Gamble, Lululemon, RBC, Mozilla, Elastic, and others.
- According to federal investigators, the hackers compromised hundreds of networks following the supply chain attack and compare it to the SolarWinds attack.

Codecov



ARGO CD ATTACK JAN 2022



1 Attacker constructs a malicious ***Kubernetes Helm Chart***

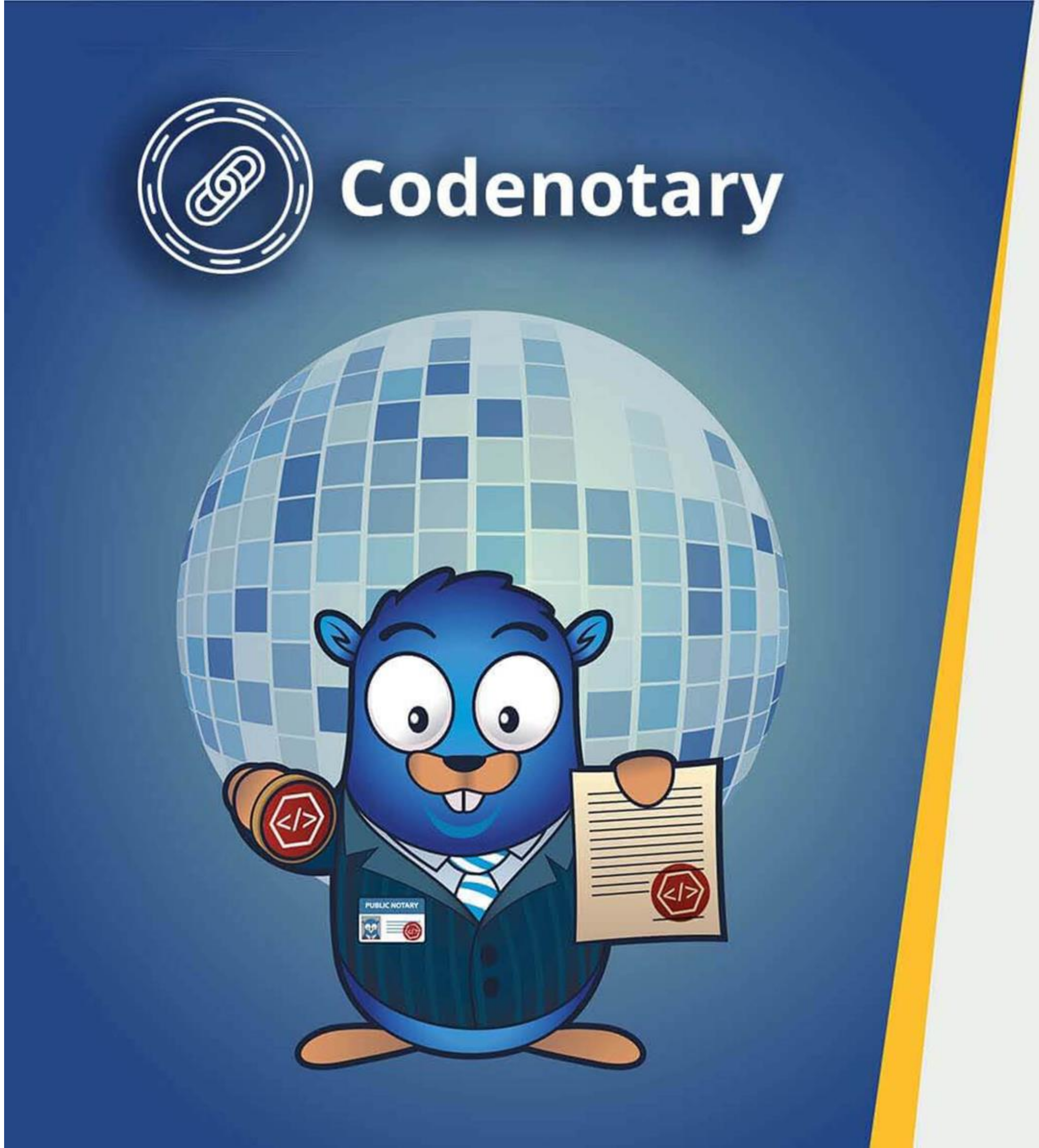
2 Attacker builds a dummy ***Kubernetes*** configuration using the ***Helm Chart***

3 The dummy configuration is used to exploit a parsing confusion vulnerability to access restricted information

4 Attacker extracts sensitive data such as API keys, passwords, etc.

5 Attacker leverages sensitive data in follow-up attacks, including privilege escalation and lateral movement

https://cloud7.news/security/zero-day-vulnerability-appeared-on-argo-cd-tool-for-kubernetes/

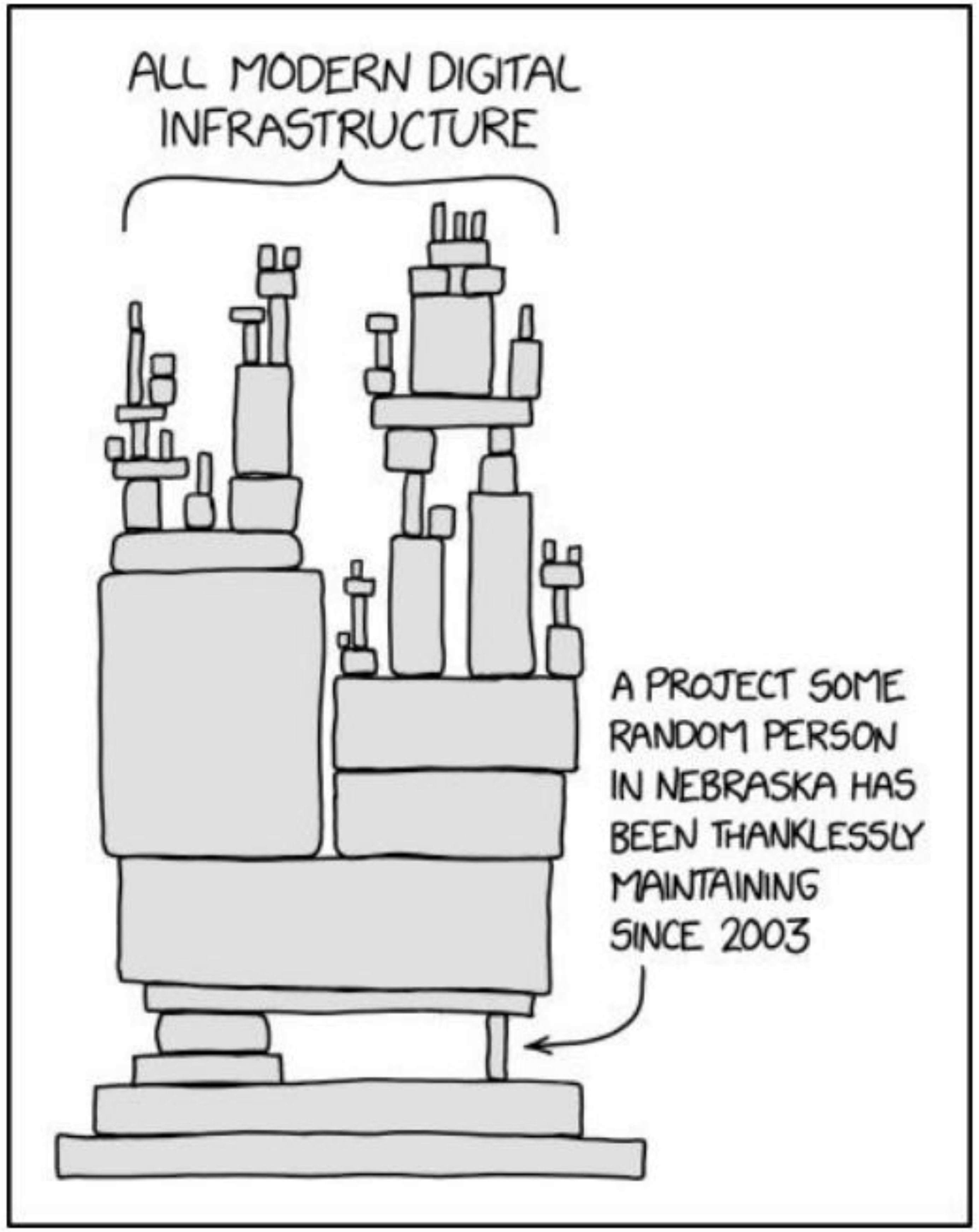


Topics

- Software Supply Chain Attacks
- Executive Order
- Vulnerability Scanner
- SBOMs (Software Bill of Materials)
- SLSA and Attestation
- The Runtime problem
- Ways to protect CI/CD pipelines/applications

HOW CAN THAT EVEN HAPPEN TO THESE BIG SW COMPANIES

MOST COMPANIES ARE NOT ABLE TO ACCURATELY SUMMARIZE THE SOFTWARE THAT IS RUNNING ON THEIR SYSTEMS.


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Source: https://xkcd.com/2347/ This work is licensed under a Creative Commons Attribution-NonCommercial 2.5 License.

MAJOR ATTACKS FORCED THE U.S. ADMINISTATION TO ACT

BRIEFING ROOM

Executive Order on Improving the Nation’s Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

REQUIREMENTS

- Software Bill of Materials (SBOM)
- Zero Trust & Immutable
- Forensic Proof

Codenotary

Topics

- Software Supply Chain Attacks
- Executive Order
- Vulnerability Scanner
- SBOMs (Software Bill of Materials)
- SLSA and Attestation
- The Runtime problem
- Ways to protect CI/CD pipelines/applications

Security Scanning Tools

Static Application Security Testing

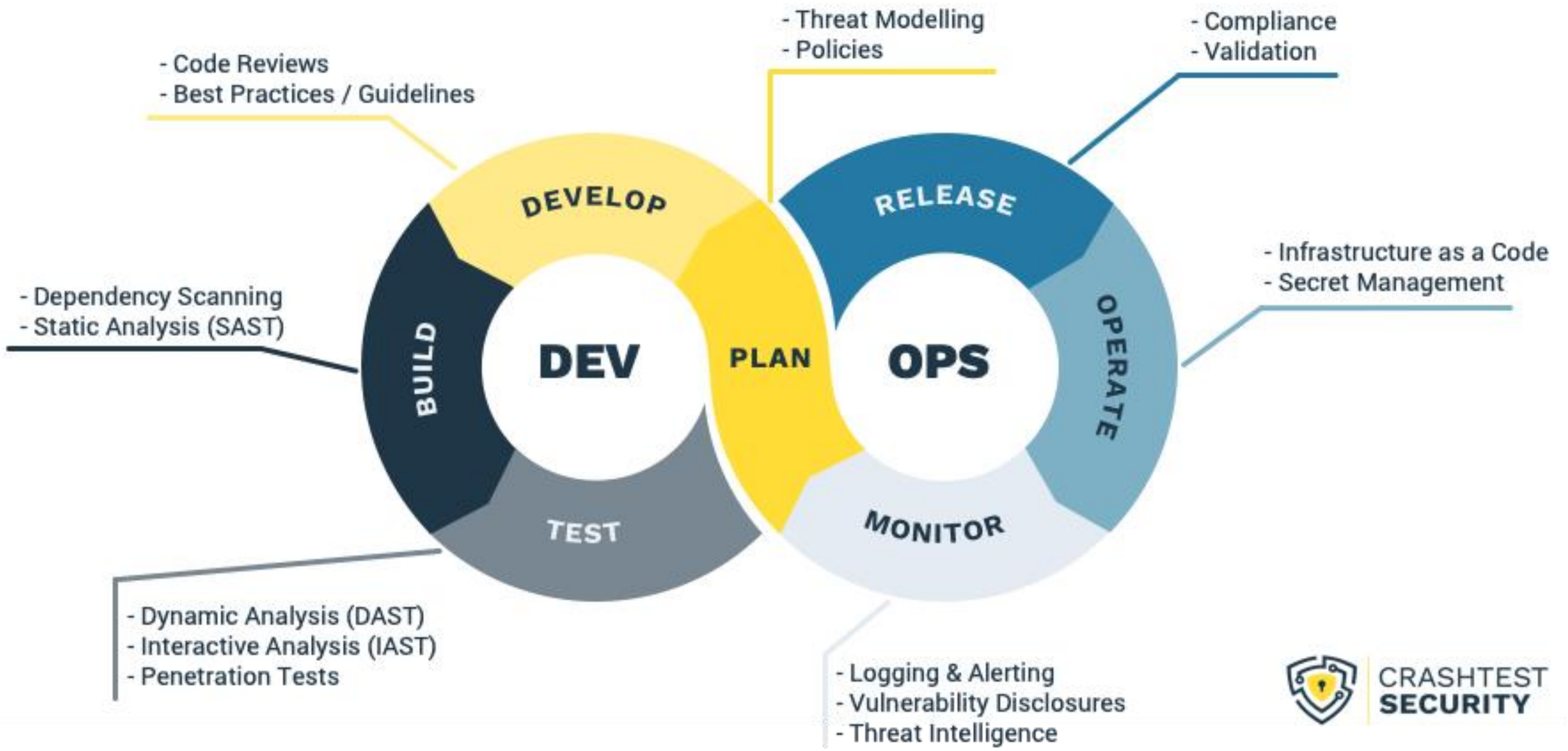
https://owasp.org/www-community/Source_Code_Analysis_Tools

Dynamic Application Security Testing

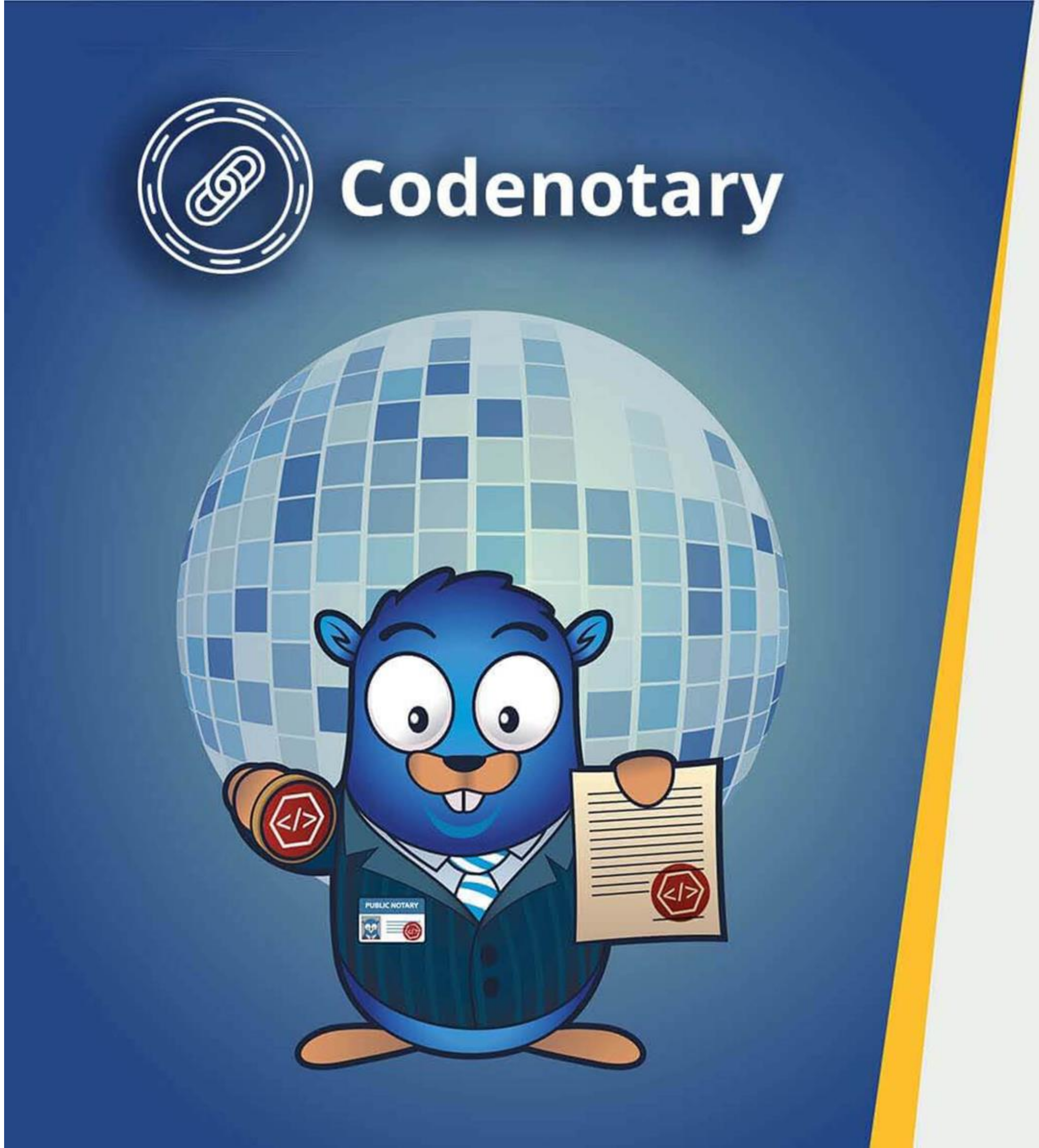
https://owasp.org/www-community/Vulnerability_Scanning_Tools

Container Security Testing

https://techbeacon.com/security/17-open-source-container-security-tools



Many, many tools, but: You can’t scan the way out of a problem!



Topics

- Software Supply Chain Attacks
- Executive Order
- Vulnerability Scanner
- SBOMs (Software Bill of Materials)
- SLSA and Attestation
- The Runtime problem
- Ways to protect CI/CD pipelines/applications

The first question after discovering a new security advisory

ARE WE AFFECTED? AND IF YES, HOW, WHERE AND SINCE WHEN?

New Security Advisory release

Spot affected components by name, version and checksum

Understand what software is at risk, what deployments are based on and if its still running

LAST DEPLOYMENT:
2 DAYS AGO

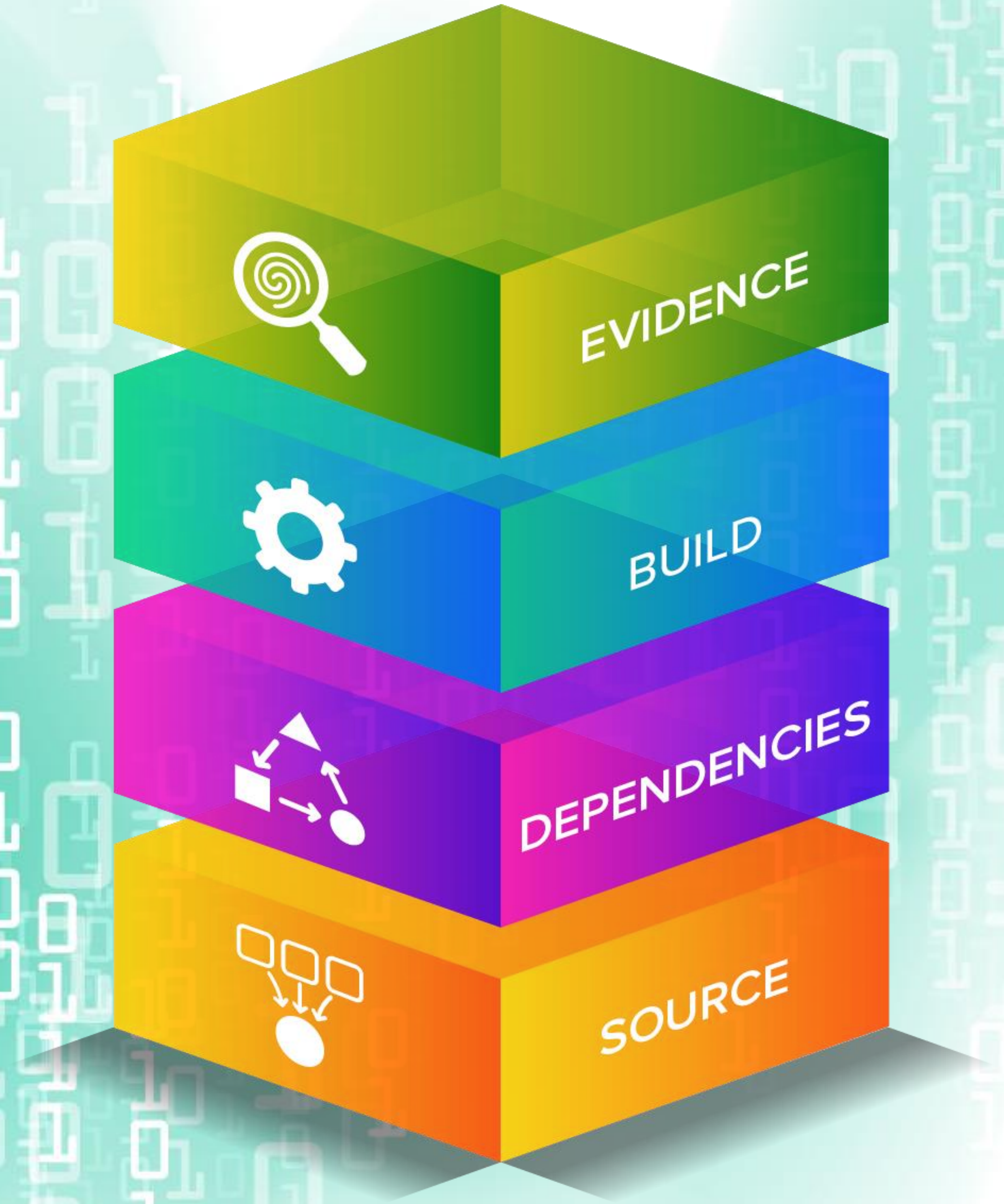
4 ACTIVE
DEPLOYMENTS

30 X
USED IN BUILDS

ACTION: UNSUPPORT CONTAINER IMAGES USING THESE BUILDS

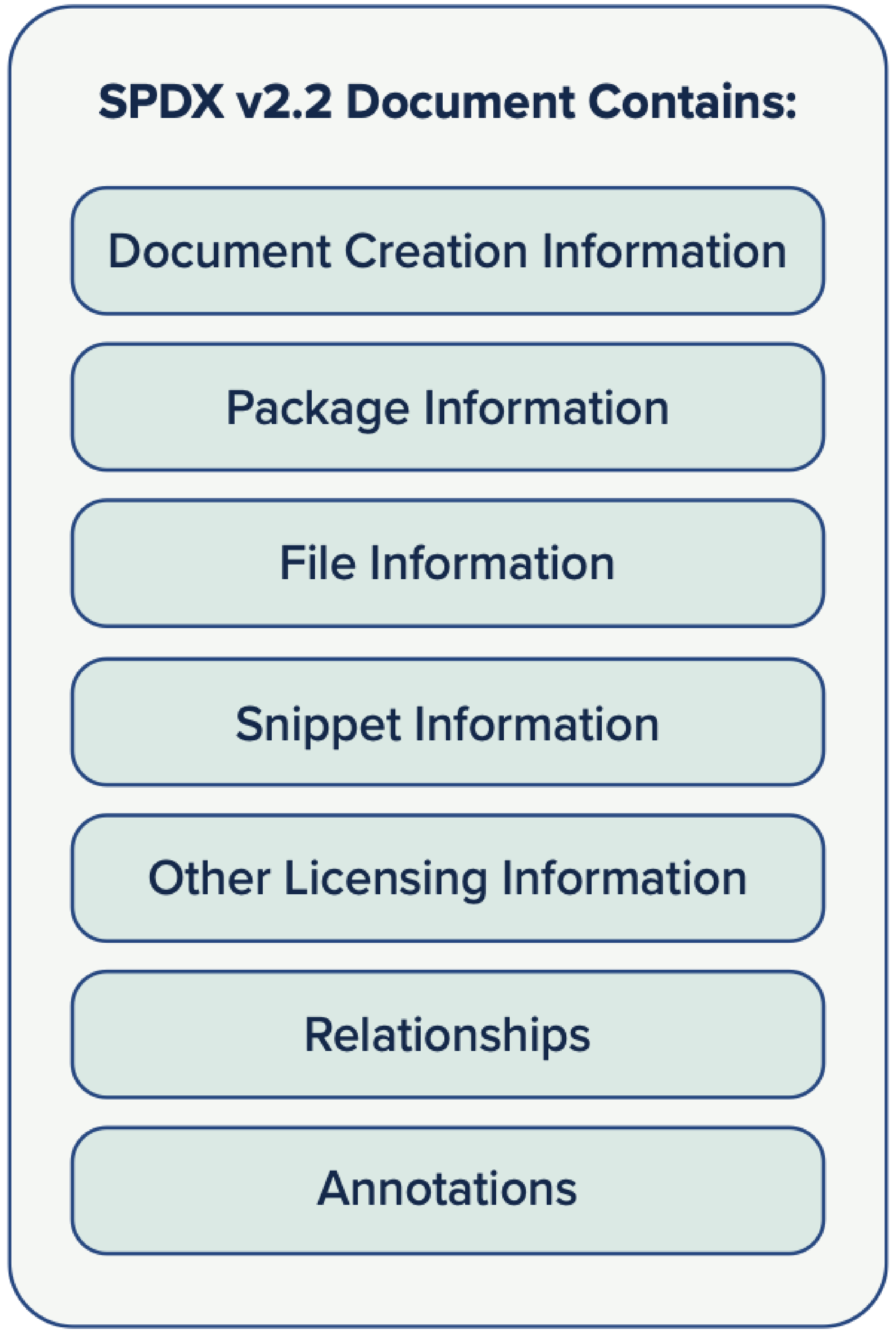
WHAT IS A SOFTWARE BILL OF MATERIALS (SBOM)

- SBOM is a list of components in a piece of software.
- SBOMs help companies avoid use of harmful software & locate affected products in case of defects.
- Standards in progress: SPDX, CycloneDX



SOFTWARE BILL OF MATERIALS

THE STATE OF SBOM STANDARDS



SPDX v2.2 Document Contains:

- Document Creation Information
- Package Information
- File Information
- Snippet Information
- Other Licensing Information
- Relationships
- Annotations

SPDX

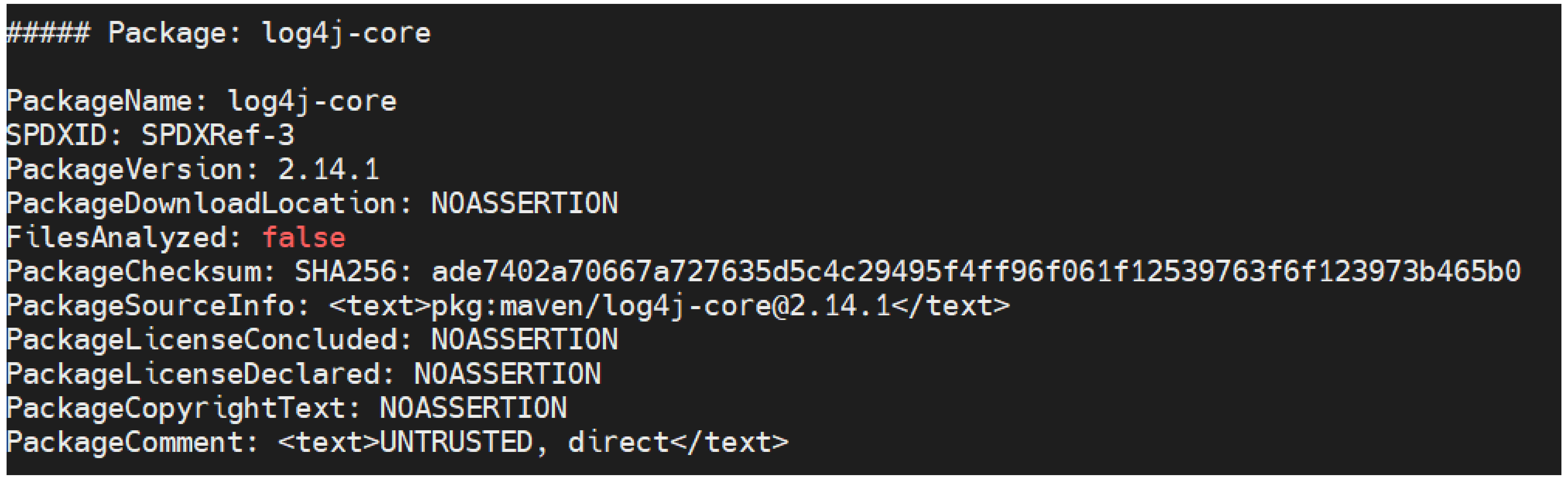
https://spdx.dev/

https://github.com/orgs/spdx/repositories
https://github.com/opensbom-generator/spdx-sbom-generator

CycloneDX

https://cyclonedx.org/

https://github.com/orgs/CycloneDX/repositories



```
##### Package: log4j-core

PackageName: log4j-core
SPDXID: SPDXRef-3
PackageVersion: 2.14.1
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageChecksum: SHA256: ade7402a70667a727635d5c4c29495f4ff96f061f12539763f6f123973b465b0
PackageSourceInfo: <text>pkg:maven/log4j-core@2.14.1</text>
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageComment: <text>UNTRUSTED, direct</text>
```

Codenotary Trustcenter command: vcn a --bom vulnerable-application --bom-spdx vulnapp.spdx

SBOM Open Source Tools

Open Source SBOM Tools

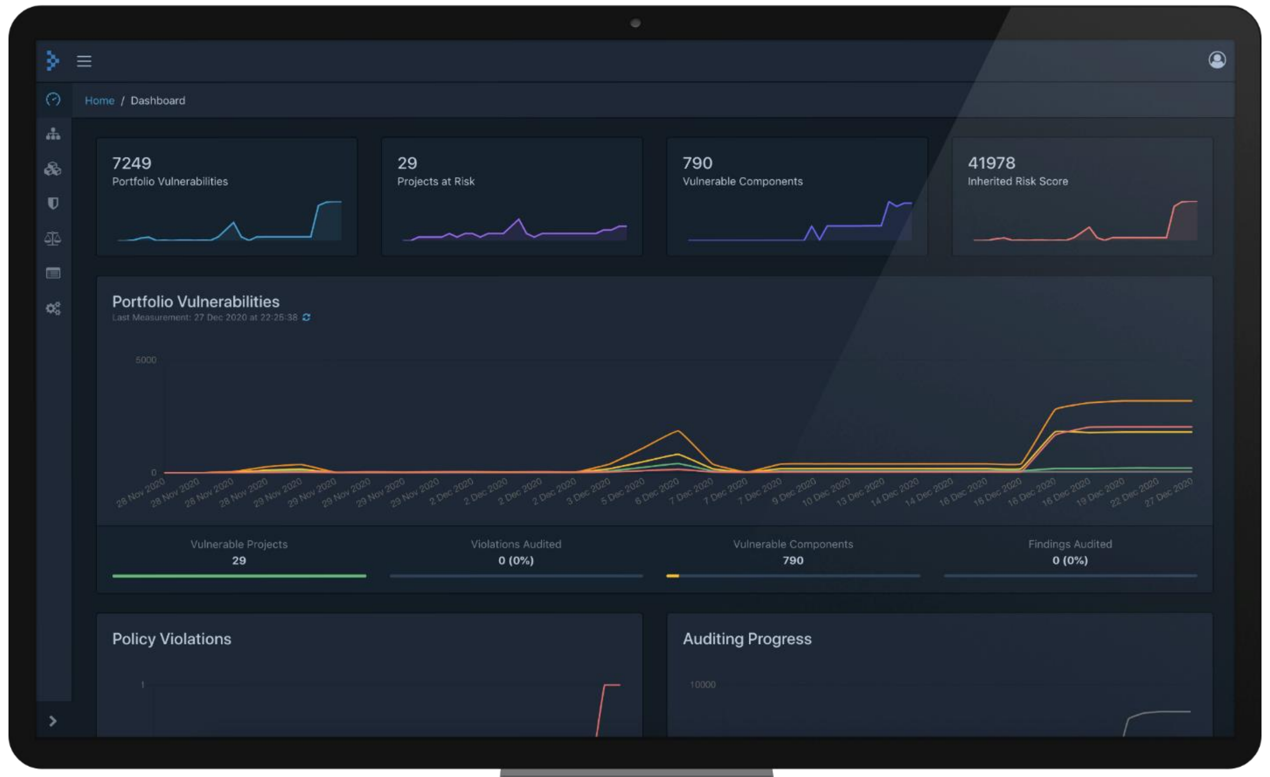
https://github.com/microsoft/sbom-tool
https://github.com/kubernetes-sigs/bom
https://github.com/anchore/syft

Open Source SBOM Integrated tooling

https://github.com/ckotzbauer/sbom-operator

Integrated SBOM and Vulnerability Open Source Tools

dependency track



Home / Dashboard

7249 Portfolio Vulnerabilities

29 Projects at Risk

790 Vulnerable Components

41978 Inherited Risk Score

Portfolio Vulnerabilities

Vulnerable Projects 29

Violations Audited 0 (0%)

Vulnerable Components 790

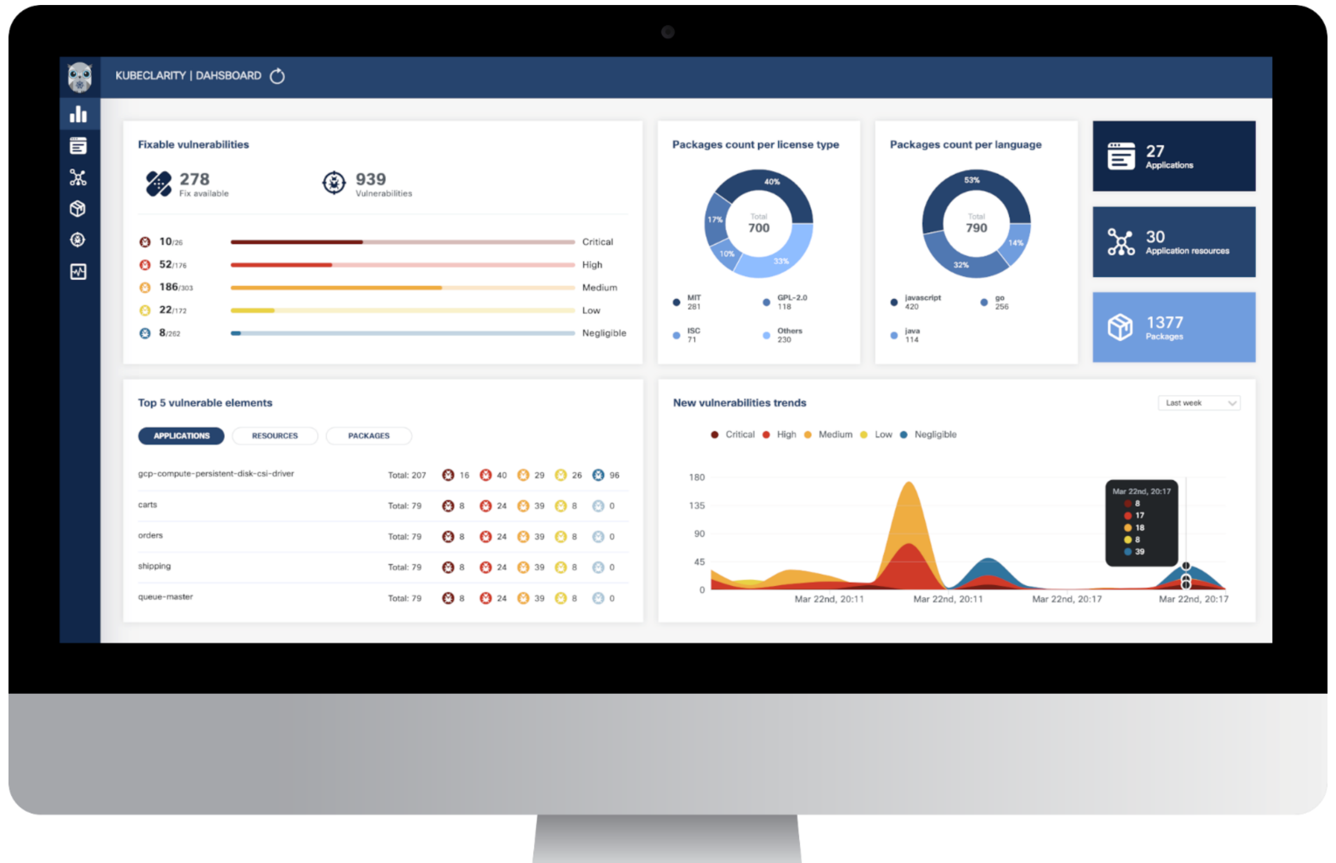
Findings Audited 0 (0%)

Policy Violations

Auditing Progress

https://github.com/DependencyTrack

KUBEClarity



KUBECLARITY | DAHSBOARD

Fixable vulnerabilities

278 Fix available

939 Vulnerabilities

10/26	Critical
52/176	High
186/303	Medium
22/172	Low
8/262	Negligible

Packages count per license type

Total 700

MIT 281, GPL-2.0 118, ISC 71, Others 230

Packages count per language

Total 790

javascript 420, go 256, java 114

27 Applications

30 Application resources

1377 Packages

Top 5 vulnerable elements

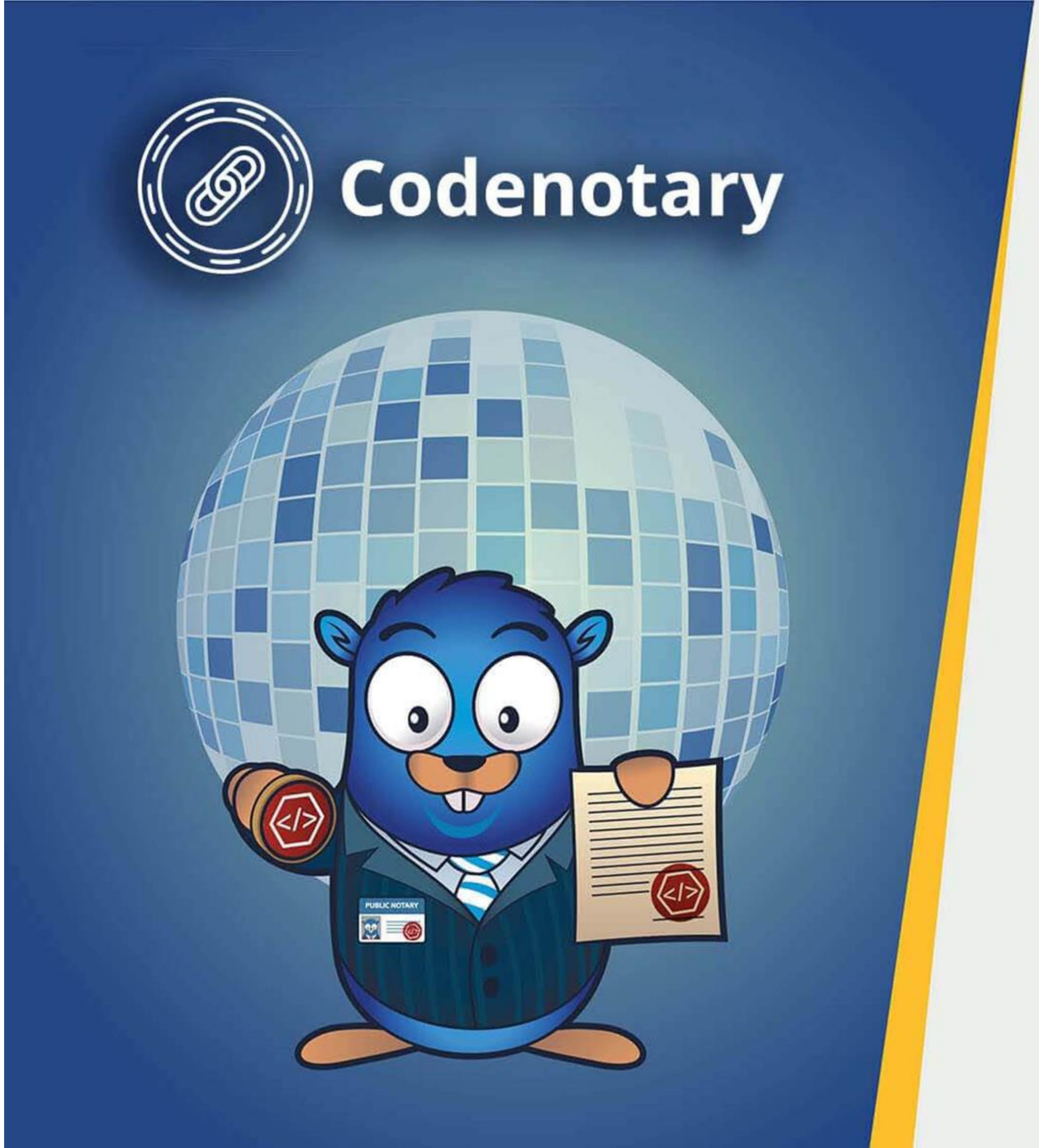
APPLICATIONS RESOURCES PACKAGES

gcp-compute-persistent-disk-csi-driver	Total: 207	16	40	29	26	96
carts	Total: 79	8	24	39	8	0
orders	Total: 79	8	24	39	8	0
shipping	Total: 79	8	24	39	8	0
queue-master	Total: 79	8	24	39	8	0

New vulnerabilities trends

Last week

https://github.com/openclarity/kubeclarity



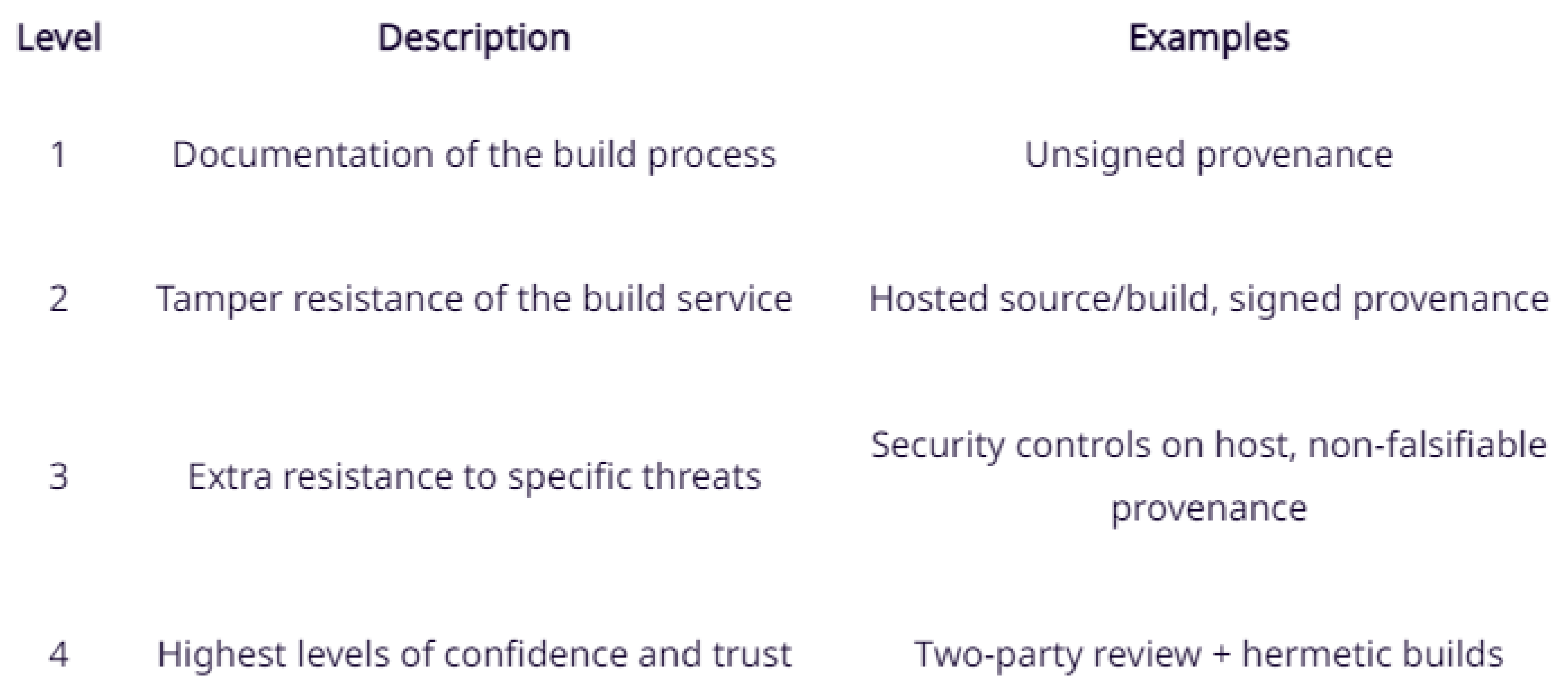
Topics

- Software Supply Chain Attacks
- Executive Order
- Vulnerability Scanner
- SBOMs (Software Bill of Materials)
- SLSA and Attestation
- The Runtime problem
- Ways to protect CI/CD pipelines/applications

SLSA and Attestation

SLSA ("salsa") is a security framework from source to service, giving a common language
for increasing levels of software security and supply chain integrity.

https://slsa.dev/



Level	Description	Examples
1	Documentation of the build process	Unsigned provenance
2	Tamper resistance of the build service	Hosted source/build, signed provenance
3	Extra resistance to specific threats	Security controls on host, non-falsifiable provenance
4	Highest levels of confidence and trust	Two-party review + hermetic builds

Artifacts

Used Source and produced Builds

Metadata

Artifact description: Provenance, SBOMs, Vulnerability scan report

Attestation

Authenticated and signed bundle of artifact checksum and metadata

Policies

Artifact and Attestation verification enforced before deployment

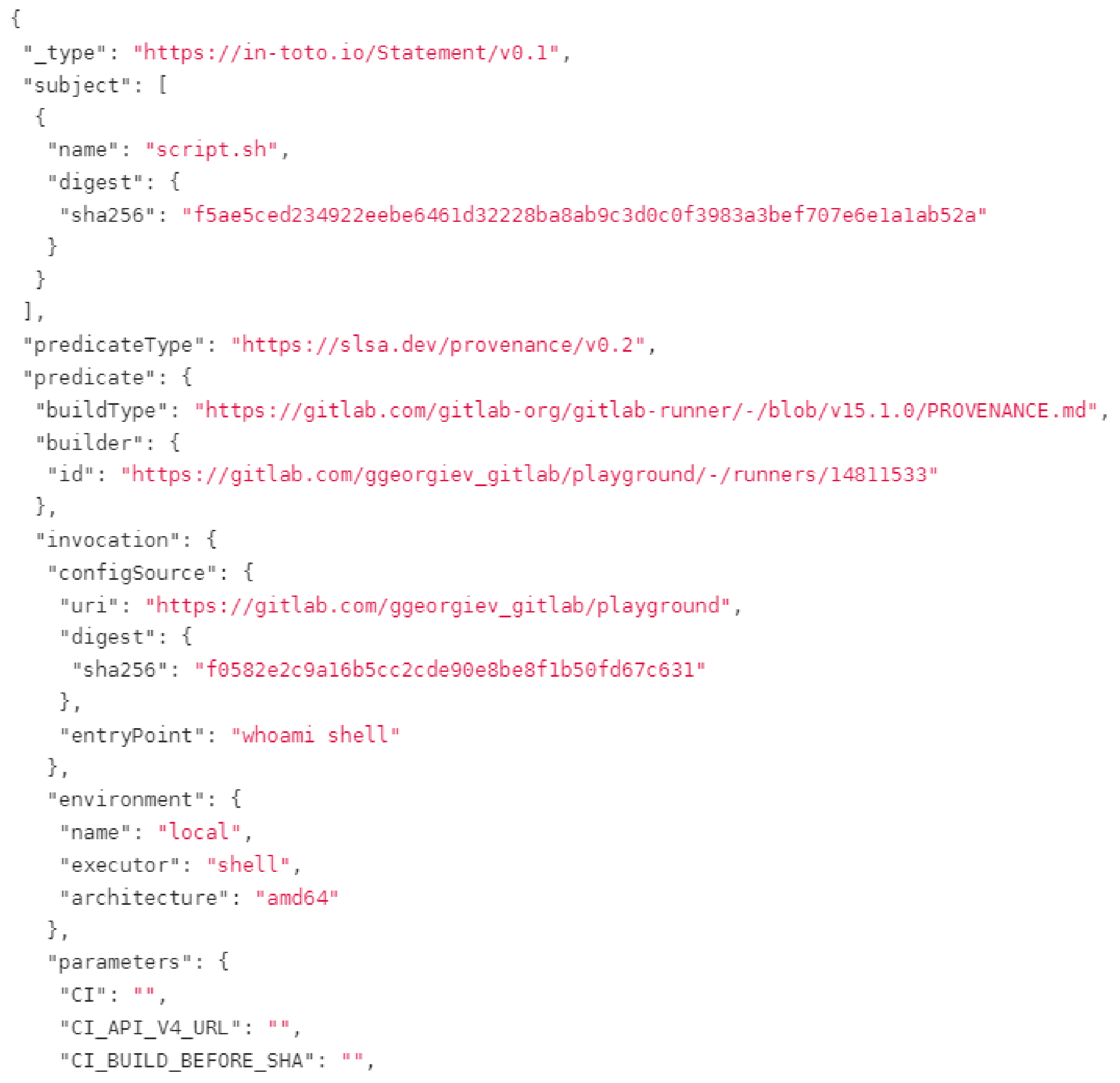
https://github.com/in-toto/attestation

Attestation SLSA Level 2 – GitLab example

.gitlab-ci.yml

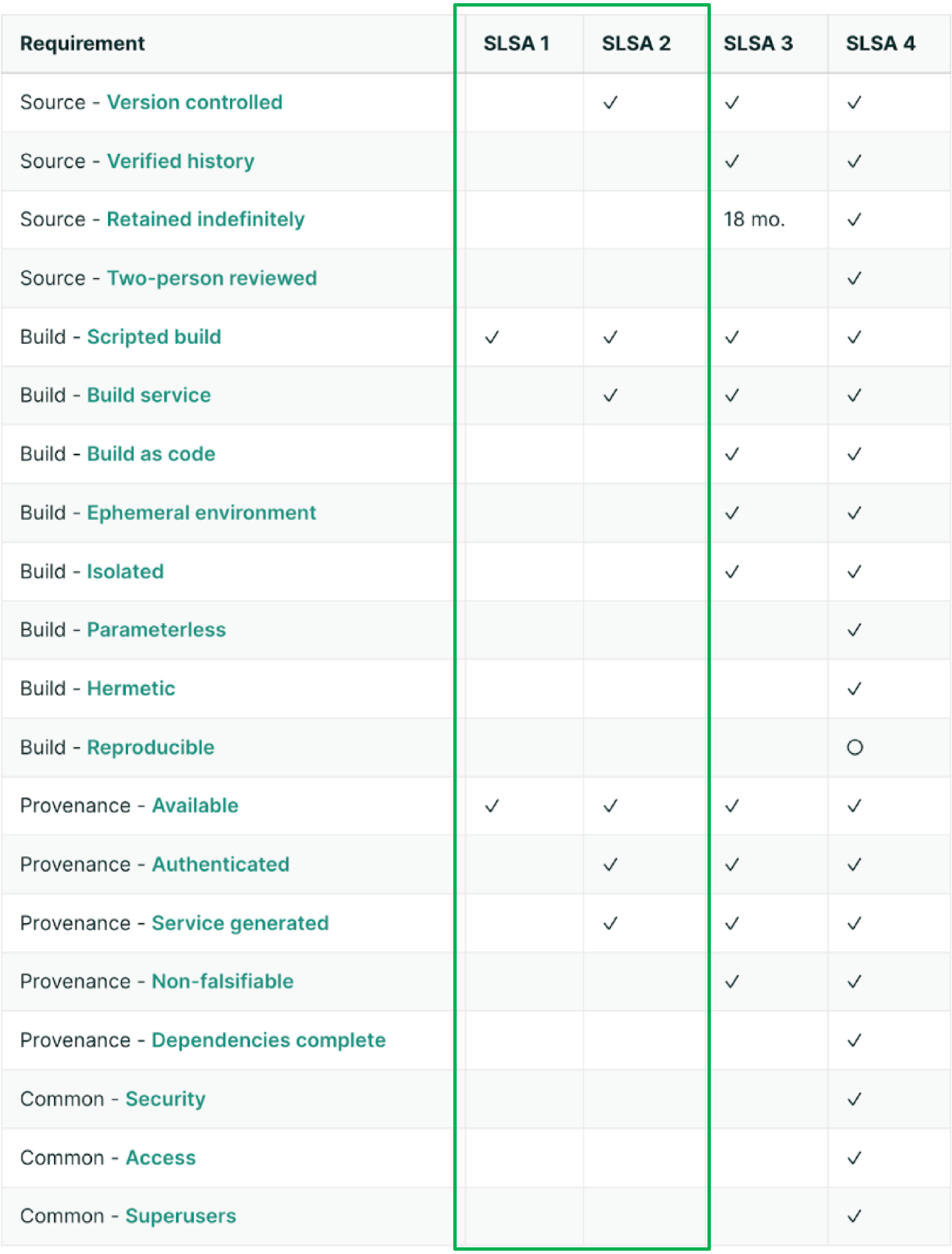
RUNNER_GENERATE_ARTIFACTS_METADATA = “true”

${BUILD-ID}-artifacts-metadata.json



```
{
 "_type": "https://in-toto.io/Statement/v0.1",
 "subject": [
  {
   "name": "script.sh",
   "digest": {
    "sha256": "f5ae5ced234922eebe6461d32228ba8ab9c3d0c0f3983a3bef707e6e1a1ab52a"
   }
  }
 ],
 "predicateType": "https://slsa.dev/provenance/v0.2",
 "predicate": {
  "buildType": "https://gitlab.com/gitlab-org/gitlab-runner/-/blob/v15.1.0/PROVENANCE.md",
  "builder": {
   "id": "https://gitlab.com/ggeorgiev_gitlab/playground/-/runners/14811533"
  },
  "invocation": {
   "configSource": {
    "uri": "https://gitlab.com/ggeorgiev_gitlab/playground",
    "digest": {
     "sha256": "f0582e2c9a16b5cc2cde90e8be8f1b50fd67c631"
    },
    "entryPoint": "whoami shell"
   },
   "environment": {
    "name": "local",
    "executor": "shell",
    "architecture": "amd64"
   },
   "parameters": {
    "CI": "",
    "CI_API_V4_URL": "",
    "CI_BUILD_BEFORE_SHA": "",
```

https://github.com/in-toto/attestation



Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source - Version controlled		✓	✓	✓
Source - Verified history			✓	✓
Source - Retained indefinitely			18 mo.	✓
Source - Two-person reviewed				✓
Build - Scripted build	✓	✓	✓	✓
Build - Build service		✓	✓	✓
Build - Build as code			✓	✓
Build - Ephemeral environment			✓	✓
Build - Isolated			✓	✓
Build - Parameterless				✓
Build - Hermetic				✓
Build - Reproducible				○
Provenance - Available	✓	✓	✓	✓
Provenance - Authenticated		✓	✓	✓
Provenance - Service generated		✓	✓	✓
Provenance - Non-falsifiable			✓	✓
Provenance - Dependencies complete				✓
Common - Security				✓
Common - Access				✓
Common - Superusers				✓

COMMUNITY ATTESTATION SERVICE

immudb

High performance and easy to integrate open source immutable database with cryptographical verification of no tampering. Supports both Key-Value & SQL

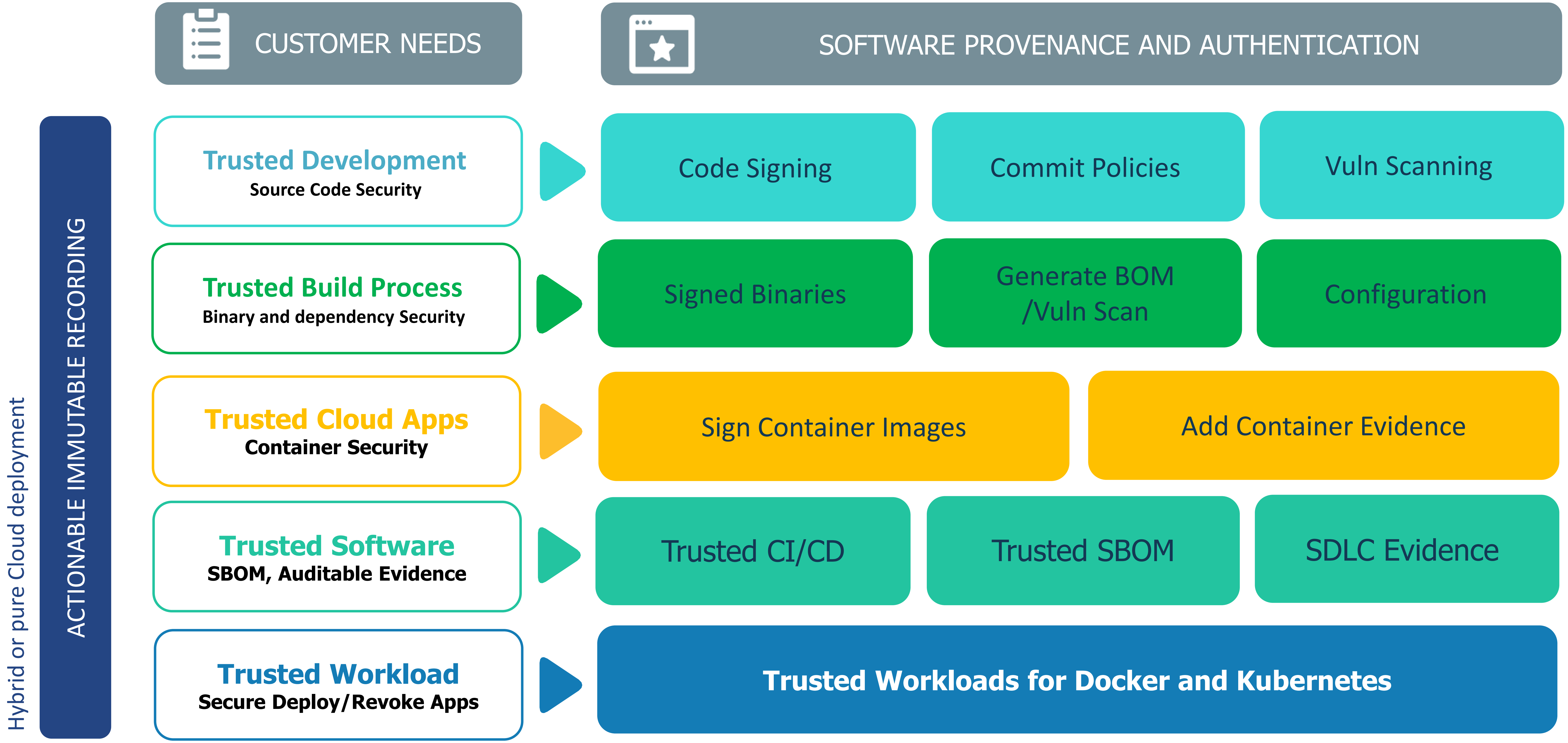
OPEN-SOURCE FOUNDATION

https://cas.codenotary.com

	FREE COMMUNITY OFFERING cas Community Attestation Service	COMMERCIAL OFFERING Codenotary Trustcenter
Attestation	File & Git Repo	File, Folder & Git Repo
SBOM	Docker binary	Docker binary & base layer Source (Python, .NET, Java, Nodejs, Go) Binary (Java, Go) & Custom (C/C++)
User & Key Management, Evidence	✗	✓

Codenotary Trustcenter

As a customer I want to run only approved software and be able to detect and revoke unwanted components at any time and within minutes



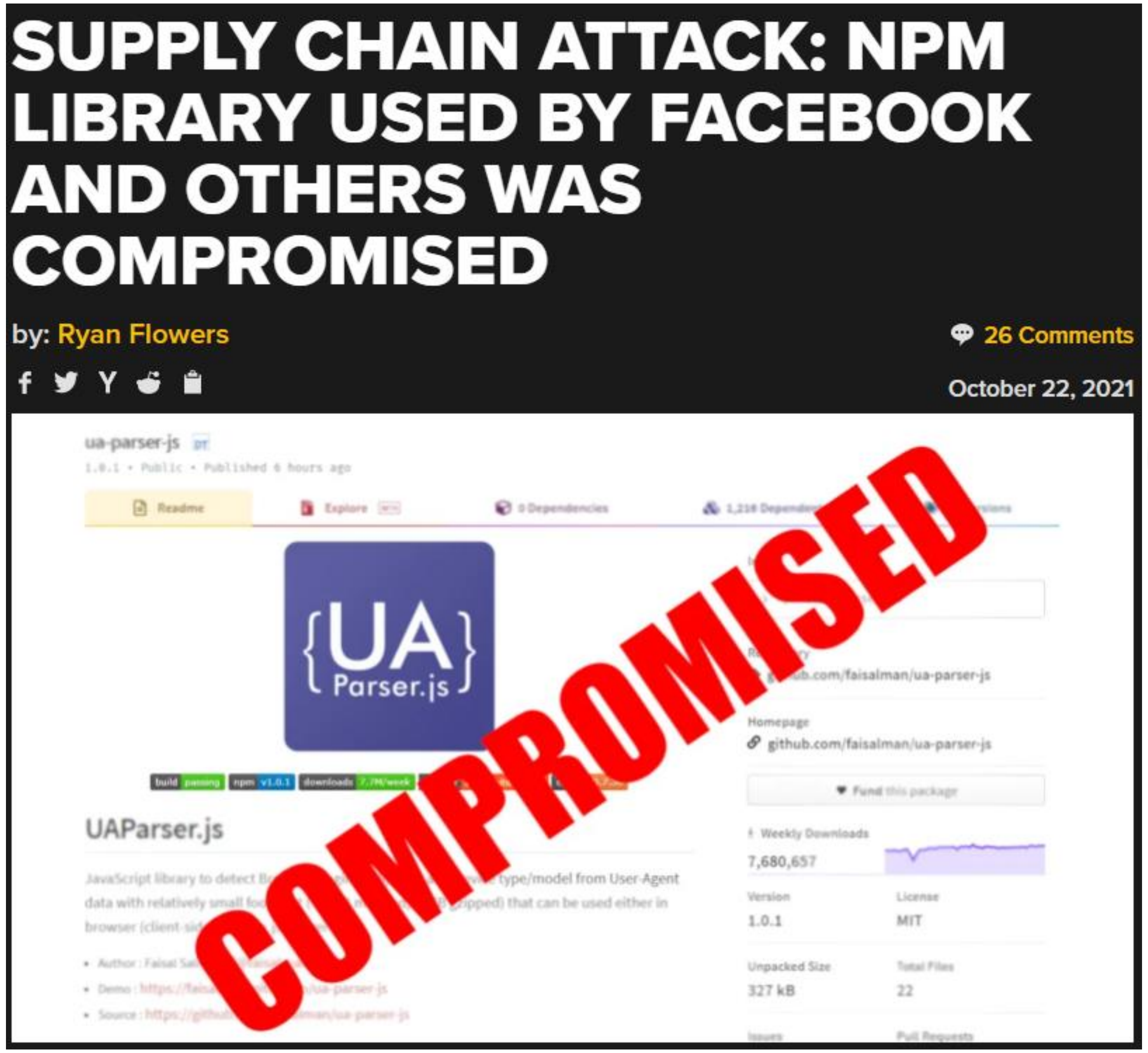
CUSTOMER NEEDS	SOFTWARE PROVENANCE AND AUTHENTICATION		
Trusted Development Source Code Security	Code Signing	Commit Policies	Vuln Scanning
Trusted Build Process Binary and dependency Security	Signed Binaries	Generate BOM /Vuln Scan	Configuration
Trusted Cloud Apps Container Security	Sign Container Images	Add Container Evidence	
Trusted Software SBOM, Auditable Evidence	Trusted CI/CD	Trusted SBOM	SDLC Evidence
Trusted Workload Secure Deploy/Revoke Apps	**Trusted Workloads for Docker and Kubernetes**		

ACTIONABLE IMMUTABLE RECORDING
Hybrid or pure Cloud deployment

Topics

- Software Supply Chain Attacks
- Executive Order
- Vulnerability Scanner
- SBOMs (Software Bill of Materials)
- SLSA and Attestation
- The Runtime problem
- Ways to protect CI/CD pipelines/applications

EXAMPLE: UI-PARSER ATTACK OCTOBER 2021

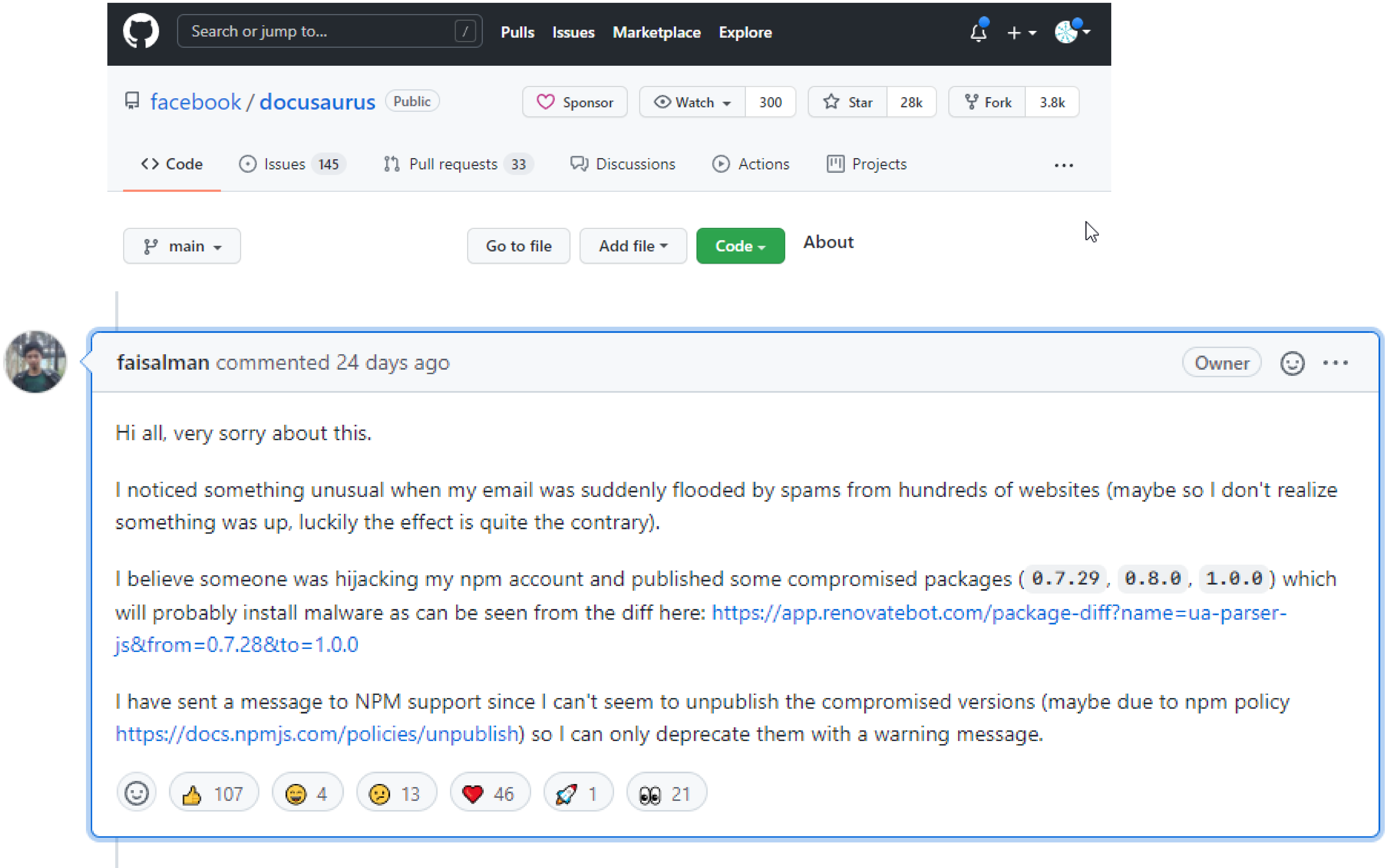


SUPPLY CHAIN ATTACK: NPM LIBRARY USED BY FACEBOOK AND OTHERS WAS COMPROMISED

by: Ryan Flowers

26 Comments

October 22, 2021



faisalman commented 24 days ago

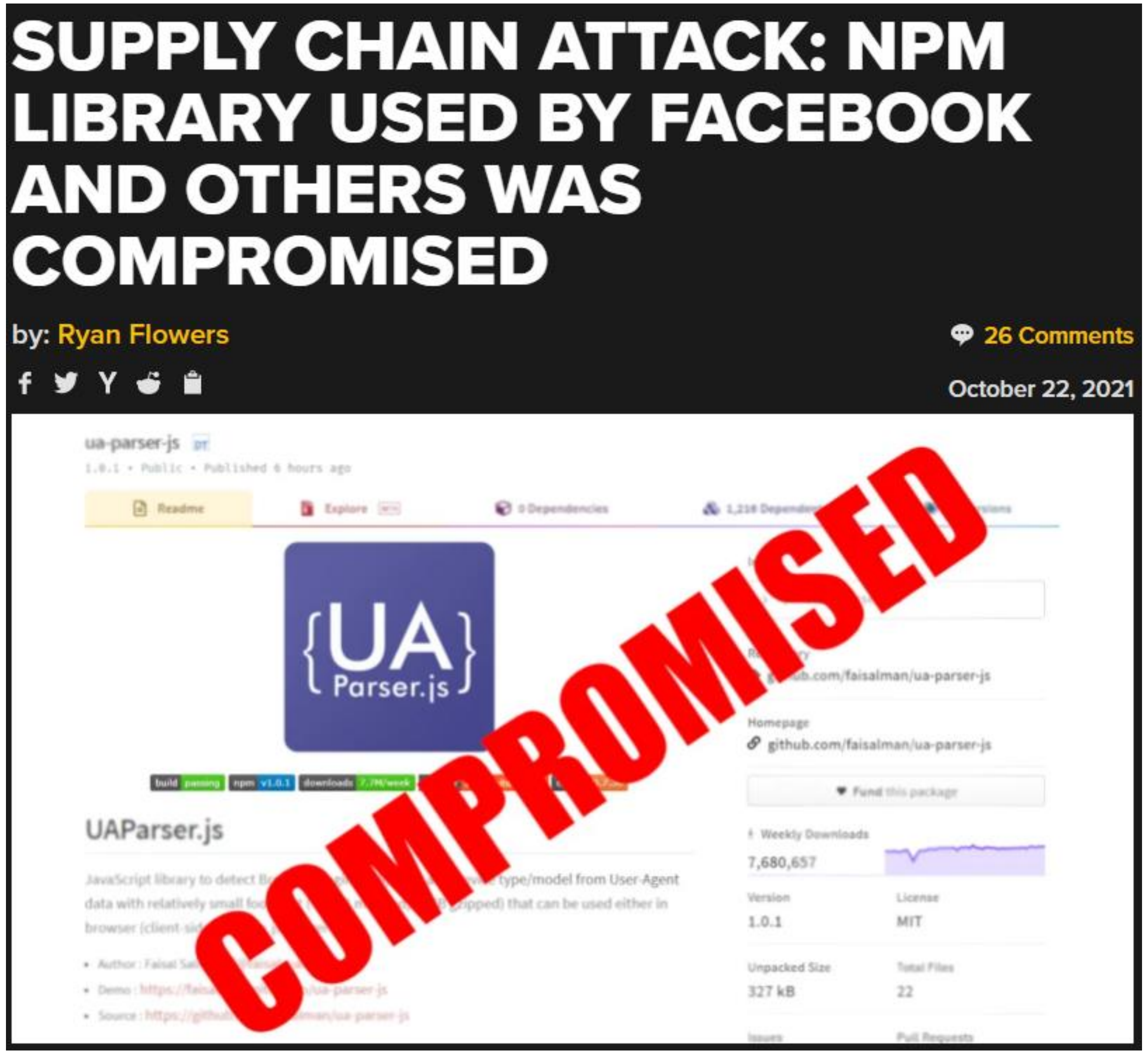
Hi all, very sorry about this.

I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don't realize something was up, luckily the effect is quite the contrary).

I believe someone was hijacking my npm account and published some compromised packages (`0.7.29`, `0.8.0`, `1.0.0`) which will probably install malware as can be seen from the diff here: https://app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0

I have sent a message to NPM support since I can't seem to unpublish the compromised versions (maybe due to npm policy https://docs.npmjs.com/policies/unpublish) so I can only deprecate them with a warning message.

UI-PARSER ATTACK OCTOBER 2021



SUPPLY CHAIN ATTACK: NPM LIBRARY USED BY FACEBOOK AND OTHERS WAS COMPROMISED

by: Ryan Flowers

26 Comments

October 22, 2021

ua-parser-js

1.0.1 • Public • Published 6 hours ago

UAParser.js

JavaScript library to detect B… type/model from User-Agent data with relatively small fo… gipped) that can be used either in browser (client-sid…

- Author : Faisal Sa…
- Demo : https://faisa…/ua-parser-js
- Source : https://github…aman/ua-parser-js

Repository: …ub.com/faisalman/ua-parser-js

Homepage: github.com/faisalman/ua-parser-js

Weekly Downloads: 7,680,657

Version: 1.0.1

License: MIT

Unpacked Size: 327 kB

Total Files: 22

Issues

Pull Requests

TAKE IMMEDIATE ACTION!

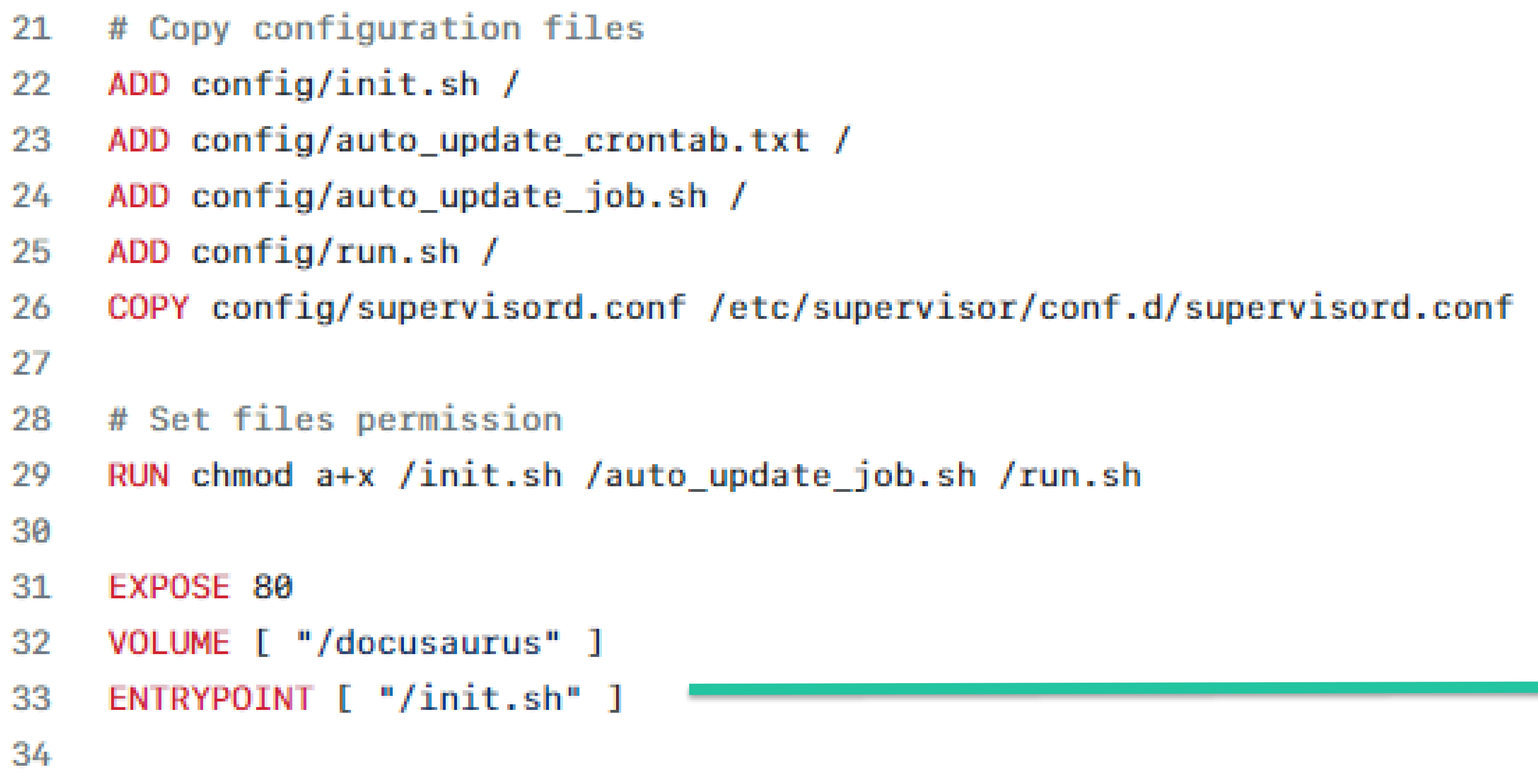
1. Use SBOM to find projects using that dependency
2. Better to have SBOM generation as part of the build
3. Better to have SBOM generation as part of the runtime
4. Be able to Untrust the affected dependency
5. Be able to Unsupport or Untrust all affected projects
6. Workload integrations can act on unsupport/untrust action
7. Ship updated and trusted application
8. Make sure everything is stored tamperproof!

UI-PARSER ATTACK OCTOBER 2021

WHY IS IT BETTER TO HAVE SBOM GENERATION AS PART OF THE RUNTIME?

Dockerfile (Build File)

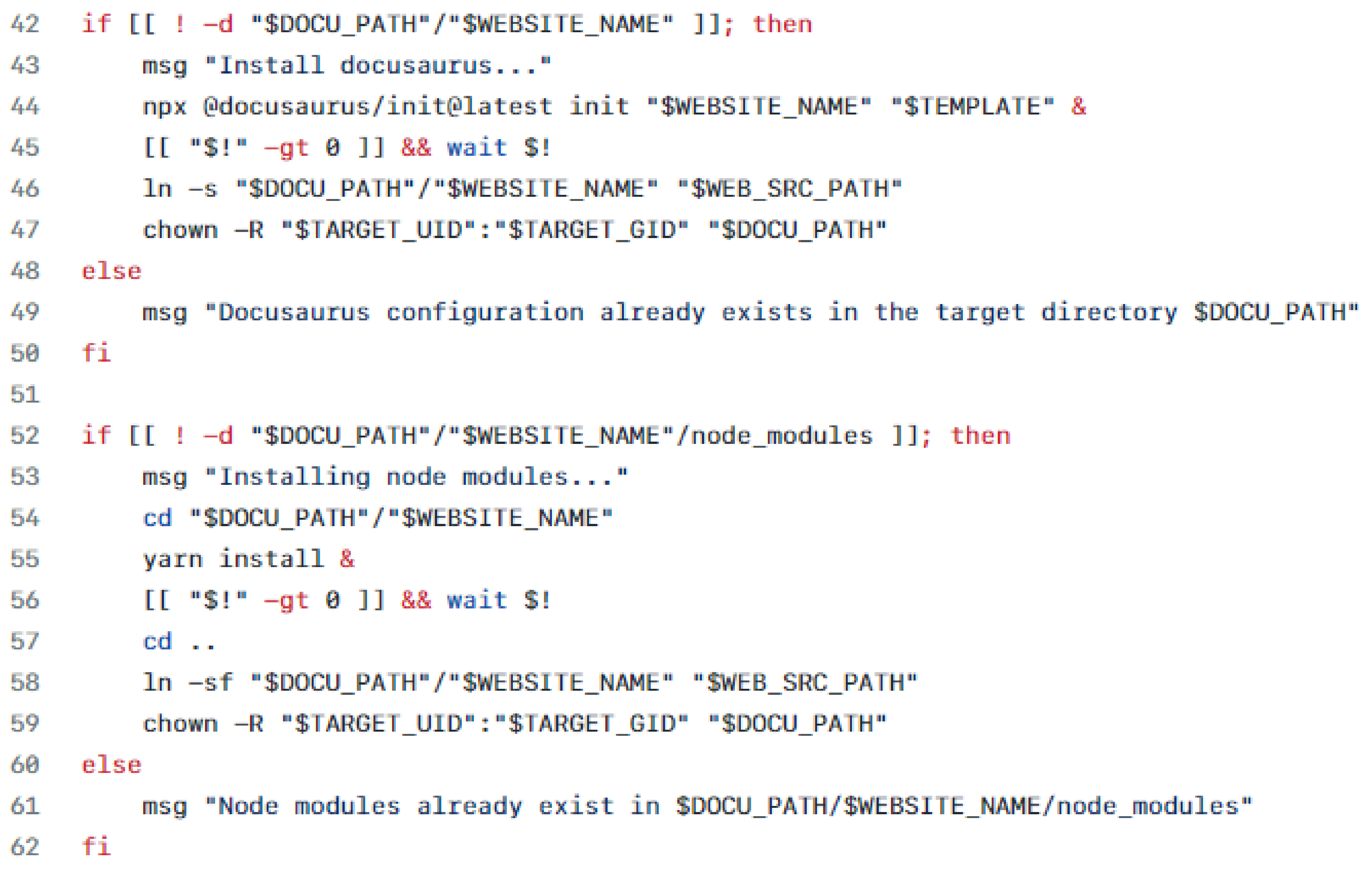
284 Dependencies



```
# Copy configuration files
ADD config/init.sh /
ADD config/auto_update_crontab.txt /
ADD config/auto_update_job.sh /
ADD config/run.sh /
COPY config/supervisord.conf /etc/supervisor/conf.d/supervisord.conf

# Set files permission
RUN chmod a+x /init.sh /auto_update_job.sh /run.sh

EXPOSE 80
VOLUME [ "/docusaurus" ]
ENTRYPOINT [ "/init.sh" ]

```

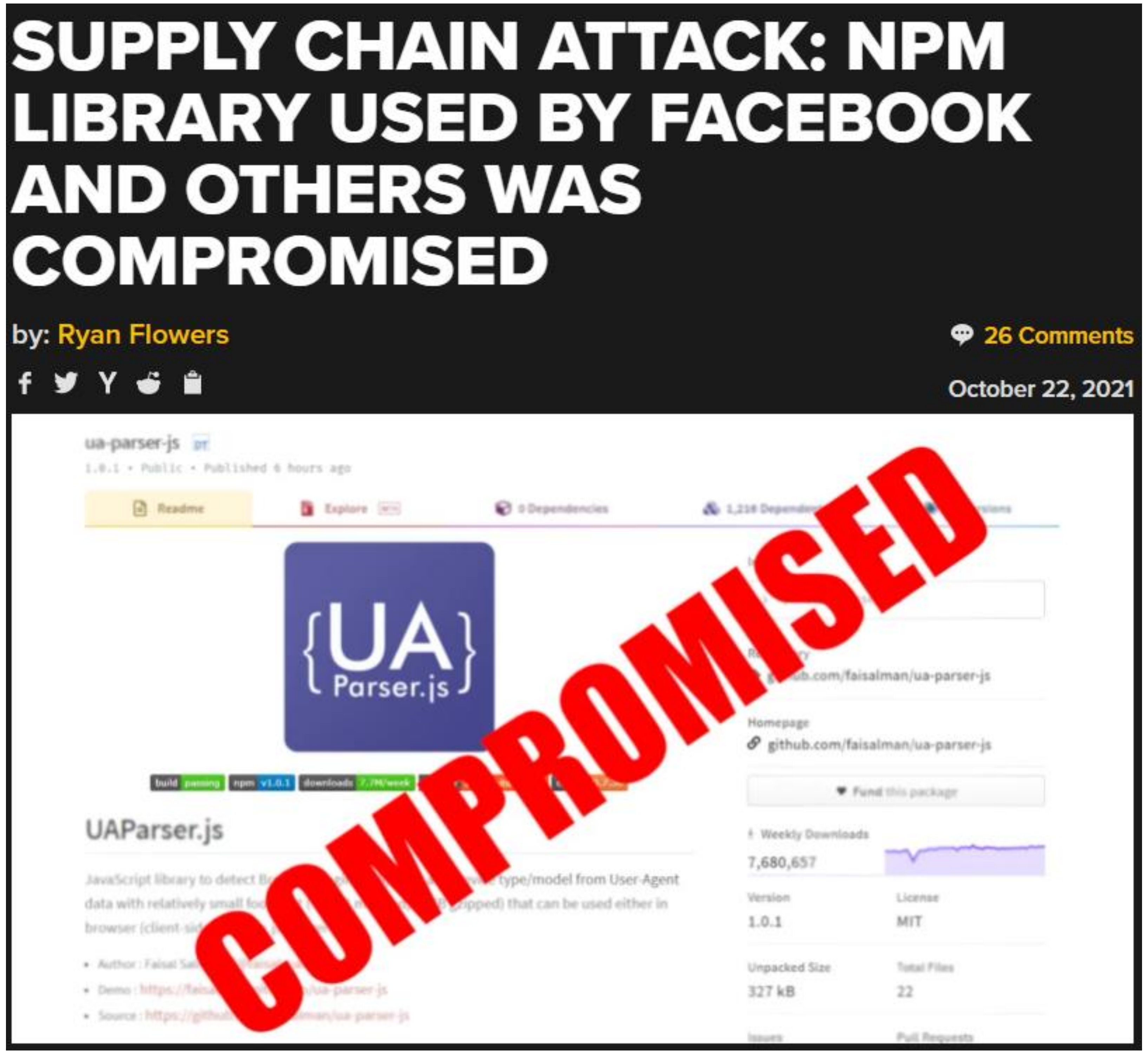
Init.sh (Container Start)

1416 Dependencies



```
if [[ ! -d "$DOCU_PATH"/"$WEBSITE_NAME" ]]; then
    msg "Install docusaurus..."
    npx @docusaurus/init@latest init "$WEBSITE_NAME" "$TEMPLATE" &
    [[ "$!" -gt 0 ]] && wait $!
    ln -s "$DOCU_PATH"/"$WEBSITE_NAME" "$WEB_SRC_PATH"
    chown -R "$TARGET_UID":"$TARGET_GID" "$DOCU_PATH"
else
    msg "Docusaurus configuration already exists in the target directory $DOCU_PATH"
fi

if [[ ! -d "$DOCU_PATH"/"$WEBSITE_NAME"/node_modules ]]; then
    msg "Installing node modules..."
    cd "$DOCU_PATH"/"$WEBSITE_NAME"
    yarn install &
    [[ "$!" -gt 0 ]] && wait $!
    cd ..
    ln -sf "$DOCU_PATH"/"$WEBSITE_NAME" "$WEB_SRC_PATH"
    chown -R "$TARGET_UID":"$TARGET_GID" "$DOCU_PATH"
else
    msg "Node modules already exist in $DOCU_PATH/$WEBSITE_NAME/node_modules"
fi
```

UI-PARSER ATTACK OCTOBER 2021



SUPPLY CHAIN ATTACK: NPM LIBRARY USED BY FACEBOOK AND OTHERS WAS COMPROMISED

by: Ryan Flowers

26 Comments

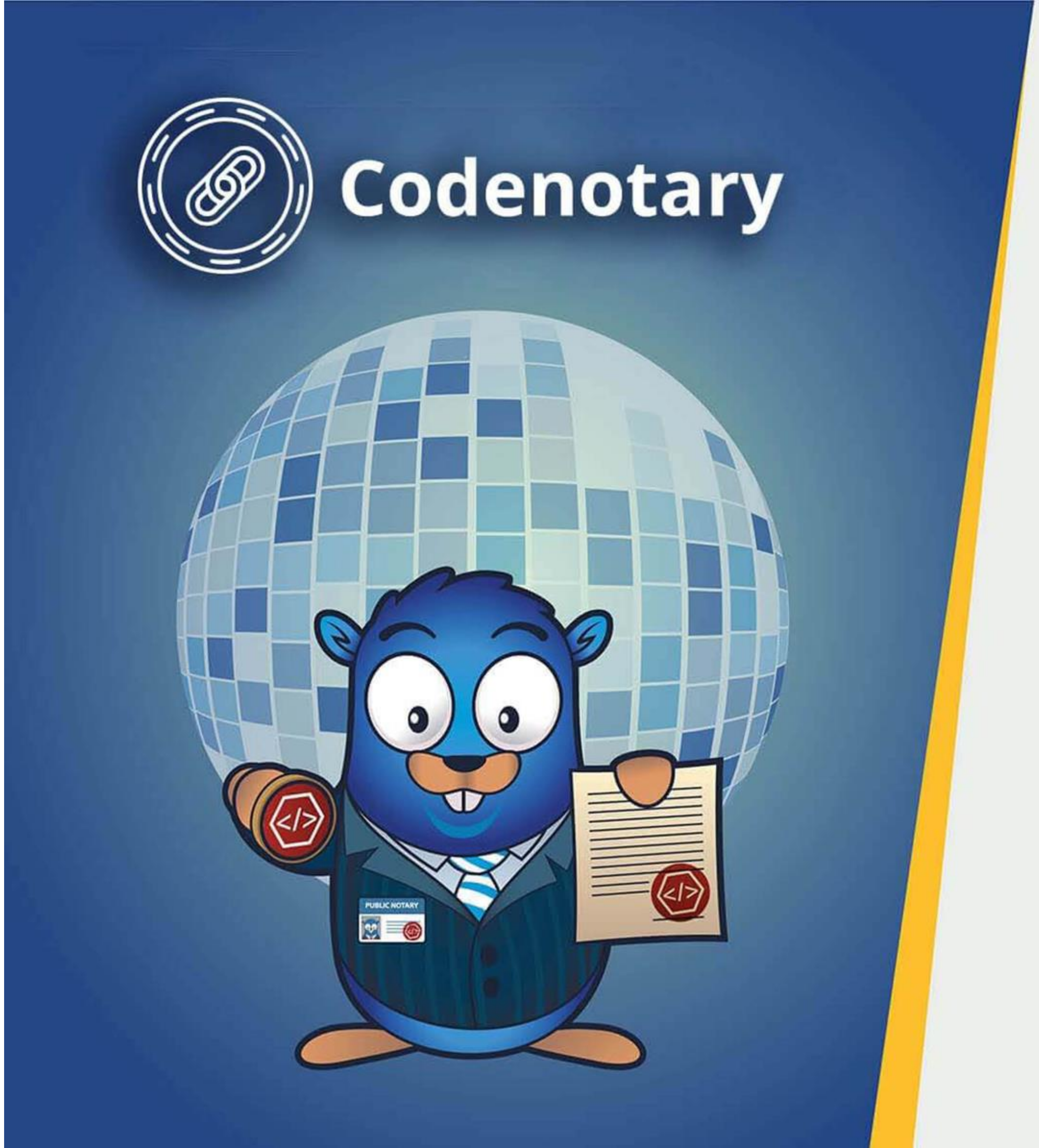
October 22, 2021

ALTERNATIVE DIGITAL CERTIFICATES

1. Use SBOM to find projects using that dependency
2. Revoke the certificate your dependencies have been signed with
3. Revoke all project certificates
4. Revoke all container image certificates
5. Rebuild and sign new application container images
6. Redistribute and redeploy

DISADVANTAGES

1. Hard to manage
2. Lack of provenance
3. Not precise
4. Mass revocation instead of individual search and rreplace



Topics

- Software Supply Chain Attacks
- Executive Order
- Vulnerability Scanner
- SBOMs (Software Bill of Materials)
- SLSA and Attestation
- The Runtime problem
- Protect CI/CD pipelines/applications

BENEFITS FROM ADOPTING SBOMs IN YOUR CI/CD

Know what is running and where!

IDENTIIFCATION OF THE APPLICATION OR CONTAINER CONTENT

- Identifying and avoiding known vulnerabilities
- Quantifying and managing licenses
- Identifying both security and license compliance requirements
- Enabling quantification of the risks inherent in a software package
- Managing mitigations for vulnerabilities (including patching and compensating controls for new vulnerabilities)
- Lower operating costs due to improved efficiencies and reduced unplanned and unscheduled work

These **benefits** can be seen by those who **develop software**, those who **select or purchase software**, and those who **operate software**, across every sector

NTIA

National Telecommunications and Information Administration

United States Department of Commerce

Source: https://www.ntia.gov/SBOM

CI/CD PIPELINE SECURITY

Protect the CI/CD Pipeline!

PROTECTION OF THE CI/CD PIPELINES

- Restrict permissions to add or change CI/CD pipelines, Recipes and Secrets
- Secure PR code commits; Multi-user approval, protect recipe from override
- Tamperproof track and audit changes, addition or removal of recipes
- Use policies inside the CI/CD pipelines
- Use strong authentication and authorization to limit user and administrator access, as well as to limit the attack surface.
- Use log auditing so that administrators can monitor activity and be alerted to potential malicious activity.
- Periodically review pipeline settings and use policies to help ensure risks are appropriately accounted.

Make sure all software used including the CI/CD software is tracked (ideally including attestation), patched regularly and checked for vulnerabilities as well.

CI/CD APPLICATION SECURITY

Protect the CI/CD runner and the deployment environment!

PROTECTION OF THE APPLICATION OR CONTAINER CONTENT

- Use Attestation to store important metadata with the artifacts
- Use Policies to secure workflows, restrict deployments and continuously check runtime
- Scan containers and Pods for vulnerabilities or misconfigurations.
- Run containers and Pods with the least privileges possible.
- Use network separation to control the amount of damage a compromise can cause.
- Use tools to limit container access after deployment
- Use log auditing so that administrators can monitor activity and be alerted to potential malicious activity.

Action Plan

SOFTWARE COMPLEXITY AND VELOCITY IS GROWING EXPONENTIAL

AUTOMATION IS IMPORTANT

- Pick the SBOM standard that fits you best and ask your Closed Vendors to provide it; Open Source <- automate it
- SBOMs and SDLC evidence need to be implemented at scale
- Vulnerability and compliance scanner results needs to be actionable and stored with the software (timestamped)
- Storing data immutable is crucial to not open the next attack surface
- Make sure you can find bad software, unwanted software, non-compliant or risky components real-time or at near-time

How do you escalate when there is a finding?

- Escalation, GDPR, internal, public
- How to remove affected software from test, stage, production

Open Questions

- Cloud SaaS – how to handle SBOMs or Security Leaks unknown to you
- Enterprise Software – what if SAP or VMware is affected

THANK YOU

CONTACT US

Codenotary Inc.
6750 West Loop South, Suite 845
Bellaire, TX 77401
contact@codenotary.com
www.codenotary.com