Container Vulnerability Management in Kubernetes

Kevin Schu – AOE GmbH

Erinnert sich jemand an den “Equifax Hack”?

Absolut vermeidbar!

- Weit bekannte Vulnerability in Apache Struts
- Fehlende Netzwerksegmentierung
- Unverschlüsselte persönliche Passwörter auf Netzlaufwerken
- Unverschlüsselte Daten
- Eine defekte Intrusion Detection

Nicht die einzigen

IT-daily.net

Shortnews IT-Manageme

Daten-Leak bei
3 Millionen Kun

10 Terabyte sensibler Kund
wochenlang für jederman

Handelsblatt

MEINE NEWS | HOME POLITIK UNTERNEHMEN TECHNOLOGIE FINANZE

IT + Telekommunikation Gadgets Forschung

Handelsblatt > Technologie > IT + Telekommunikation > Hacker haben Zugriff auf 14 Milli

VERSANDH

Hacker haben Zugrif
Kundendatensätze vo

Süddeutsch

Ukraine | Politik | Wirtschaft | Meinung | Panorama | Sport | München | Kultur | Medien | Bayern | Report

t > Cybersicherheit > Cyberangriff > Strafe für British Airways

IT-Innovation aus Deutschland | Startklar |

ritish

DIGITAL WORLD | GERMANY

Germany: Private data from restaurant
d online

any has left vast amounts of
contact tracking form

ctures

ry

e this article

CTV NEWS
TORONTO

NEWS VIDEO SHOWS ABOUT LOCAL

TORONTO | News

ADVERTISEMENT

IKEA Canada confirms data breach involving personal information of approximately 95,000 customers

INVESTMENT BANKING | LEGAL/REGULATORY

JPMorgan Chase Hacking Affects 76 Million Households

BY JESSICA SILVER-GREENBERG, MATTHEW GOLDSTEIN AND NICOLE PERLROTH OCTOBER 2, 2014 12:50 PM

528

FORBES > INNOVATION > CYBERSECURITY

EDITORS' PICK

235 Million Instagram, TikTok And YouTube User Profiles Exposed In Massive Data Leak

Davey Winder Senior Contributor

Co-founder, Straight Talking Cyber

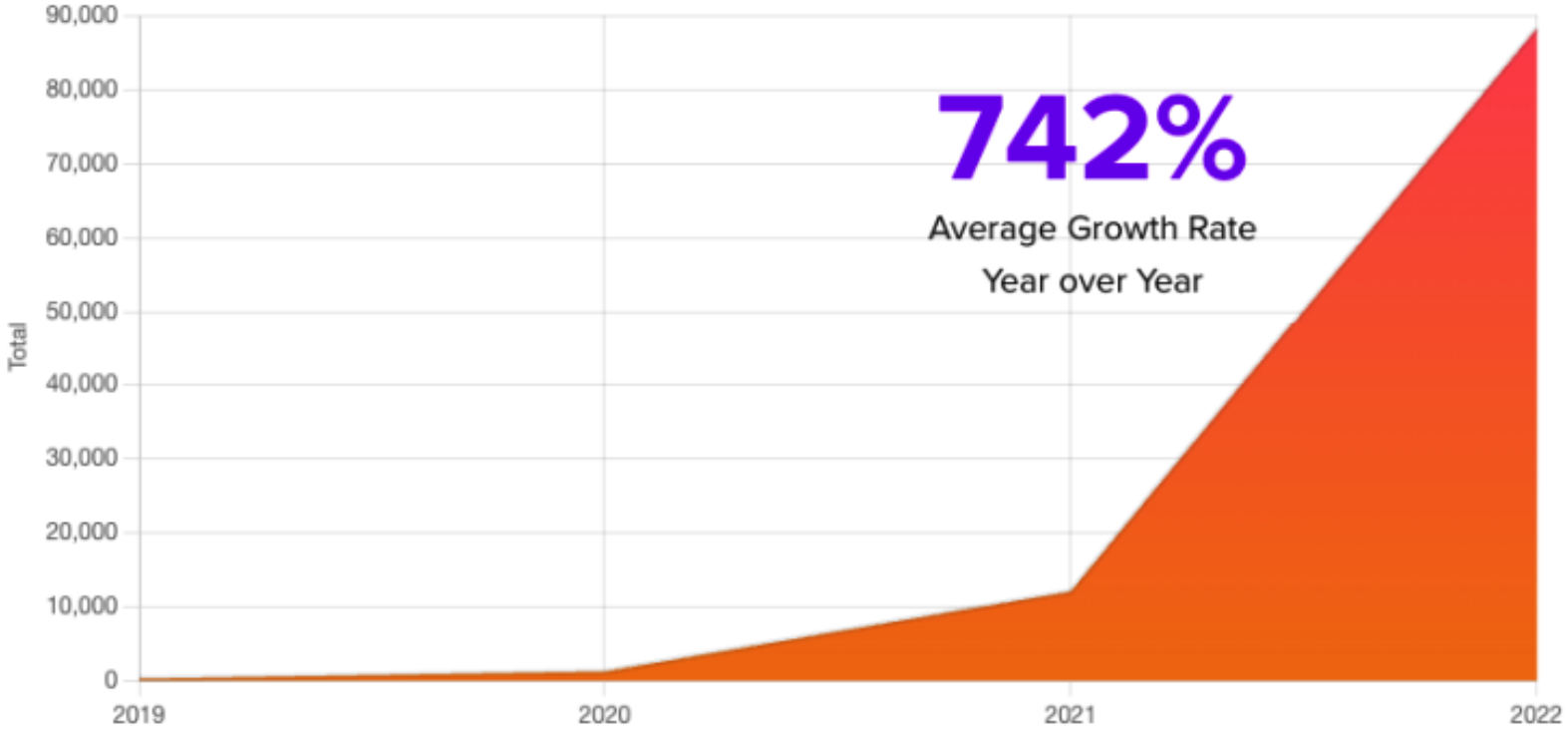
Follow

Aug 19, 2020, 09:00am EDT

AOE

Ein beunruhigender Trend
Hacking wird mehr und mehr zum Business-Modell

Anzahl der Supply-Chain Attacken (wie log4J)



https://blog.sonatype.com/2023-predictions-software-supply-chain-governance

Sicherheit basiert auf Vertrauen

A new security thinking is required
Zero Trust: Never trust, always verify!

least privilege

assume breach

strong identity verification

verify explicitly

Identities &
Identity Awareness

Device &
Device Authentication

Networking &
Firewall

Application
Security

Infrastructure
Security

Secure
Data Handling

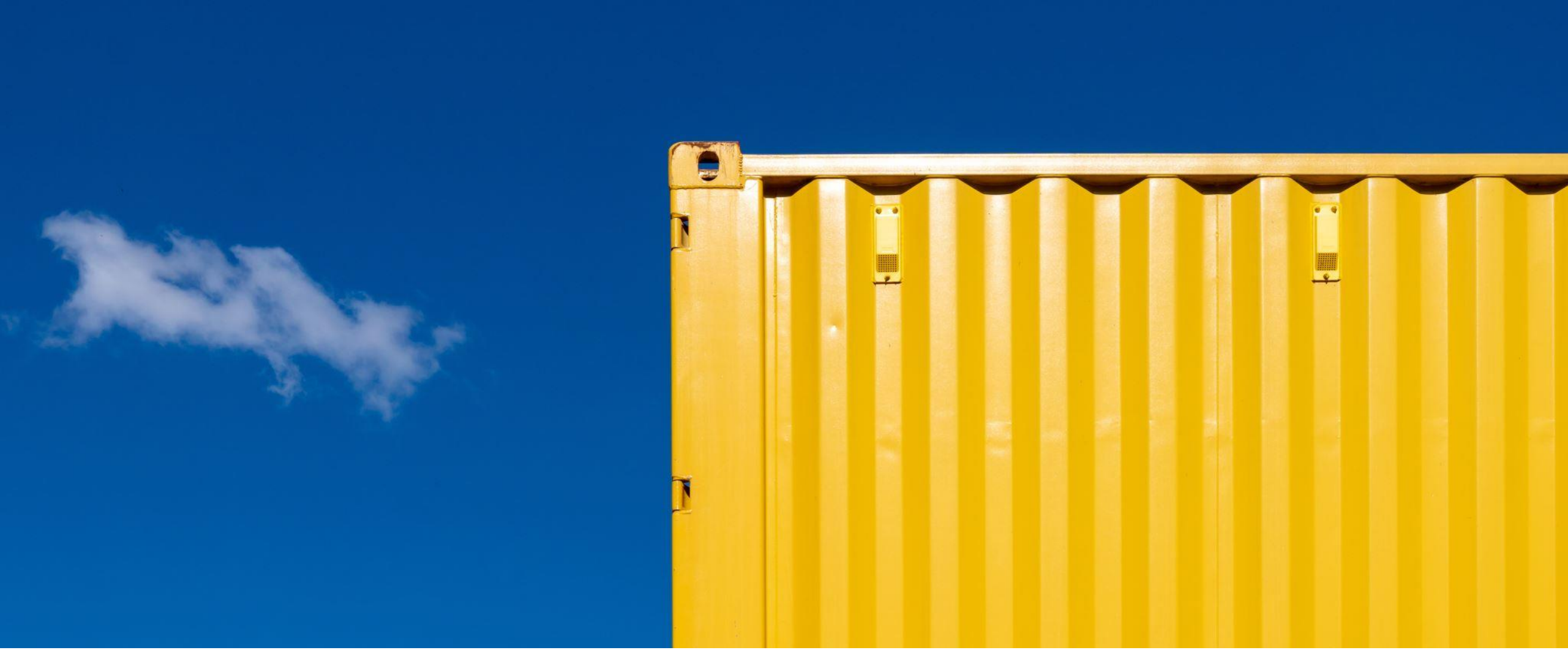
Zero Trust Aspects

Organization and
Culture

Secure
Development and
Delivery

Security
Monitoring &
Automation

Container Vulnerability Management



Container sind doch sicher…?

Faktoren, die die Container-Sicherheit beeinflussen

CVE-2020-15257

https://blog.aquasec.com/cve-2020-15257-containerd-shim-api-vulnerability

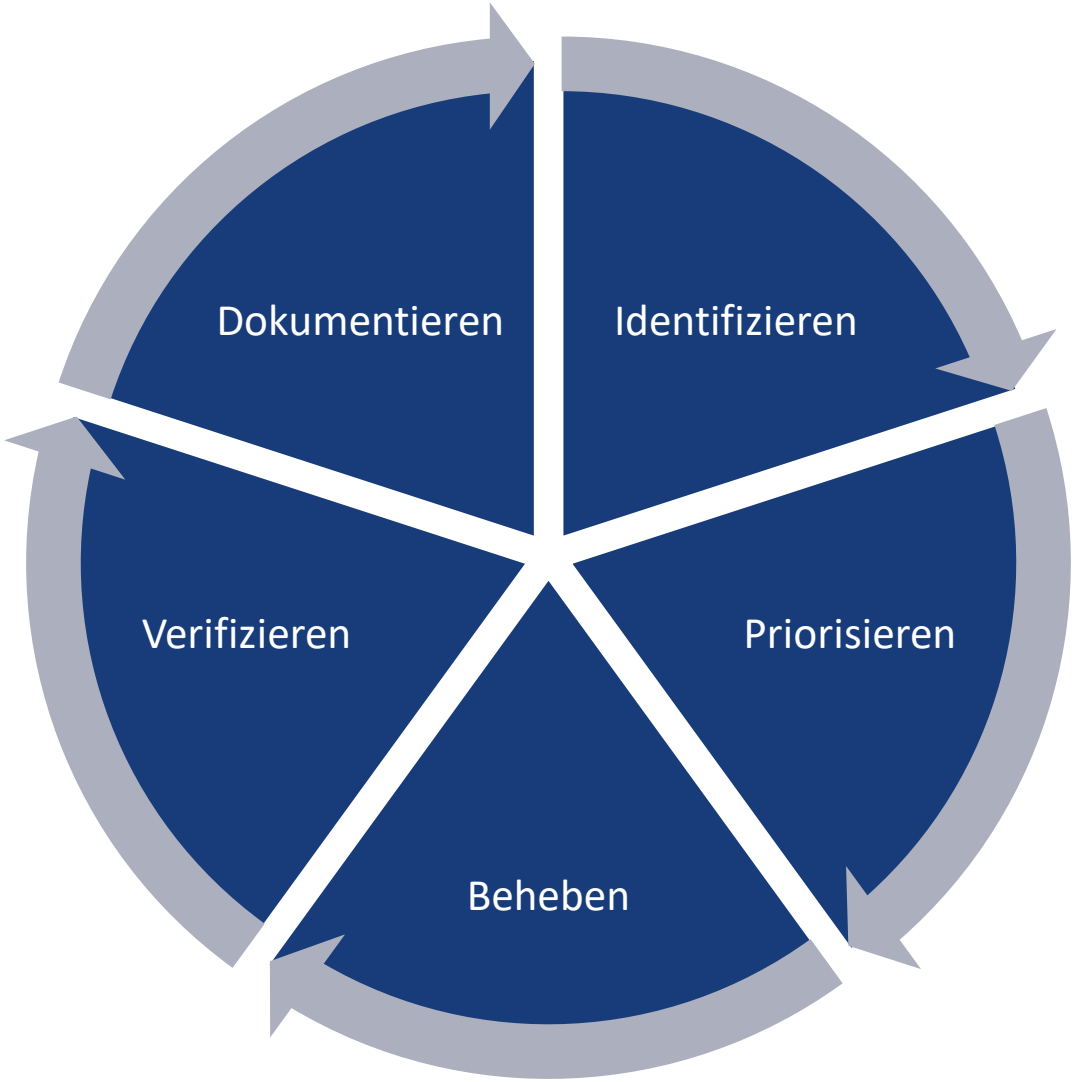
Docker: `docker run --net=host`

Kubernetes: `.spec.hostNetwork: true`

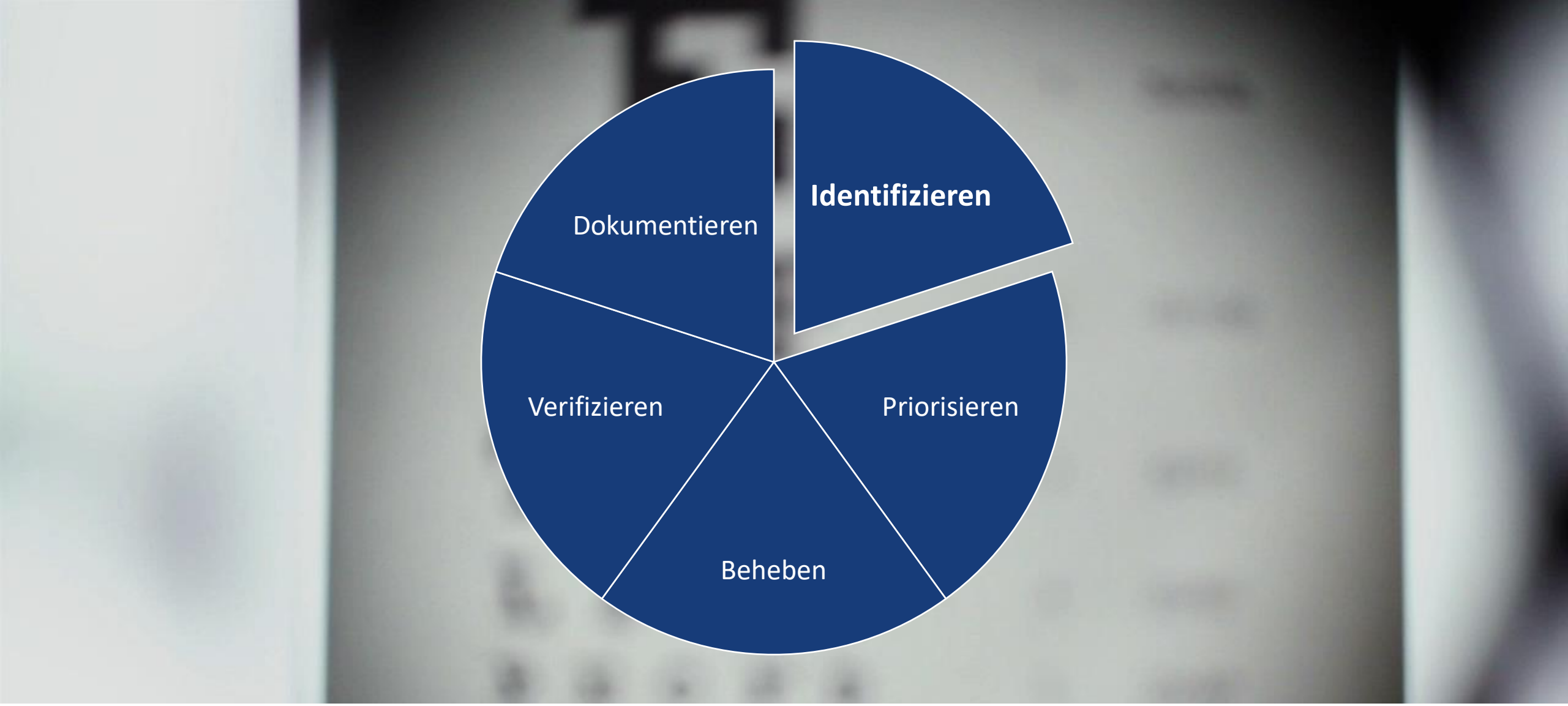
```
service Shim {
    rpc State(StateRequest) returns (StateResponse);
    rpc Create(CreateTaskRequest) returns (CreateTaskResponse);
    rpc Start(StartRequest) returns (StartResponse);
    rpc Delete(google.protobuf.Empty) returns (DeleteResponse);
    rpc DeleteProcess(DeleteProcessRequest) returns (DeleteResponse);
    rpc ListPids(ListPidsRequest) returns (ListPidsResponse);
    rpc Pause(google.protobuf.Empty) returns (google.protobuf.Empty);
    rpc Resume(google.protobuf.Empty) returns (google.protobuf.Empty);
```

https://blog.aquasec.com/cve-2020-15257-containerd-shim-api-vulnerability

Security: Takeaways

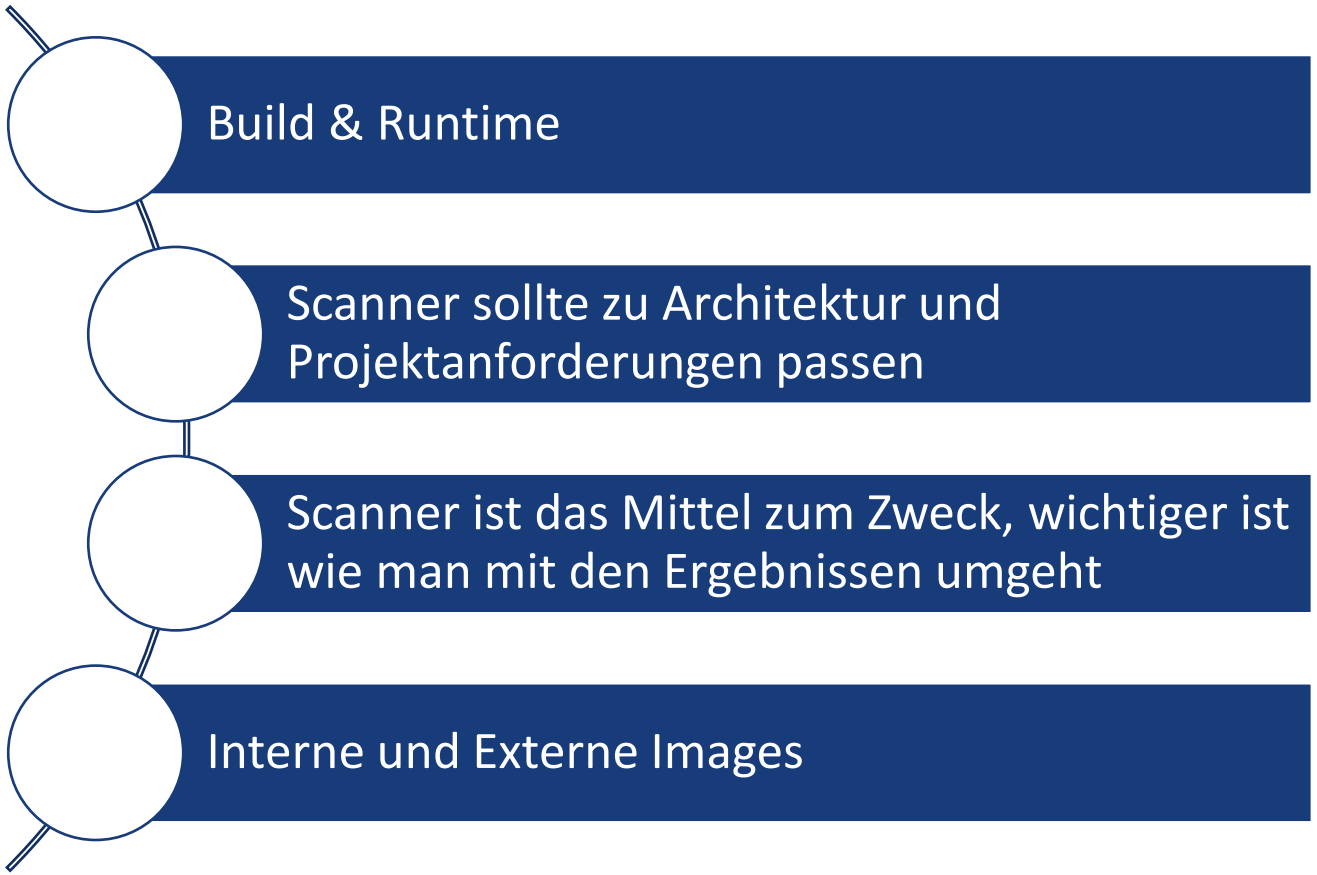


Wie also managt man Schwachstellen in Containern?

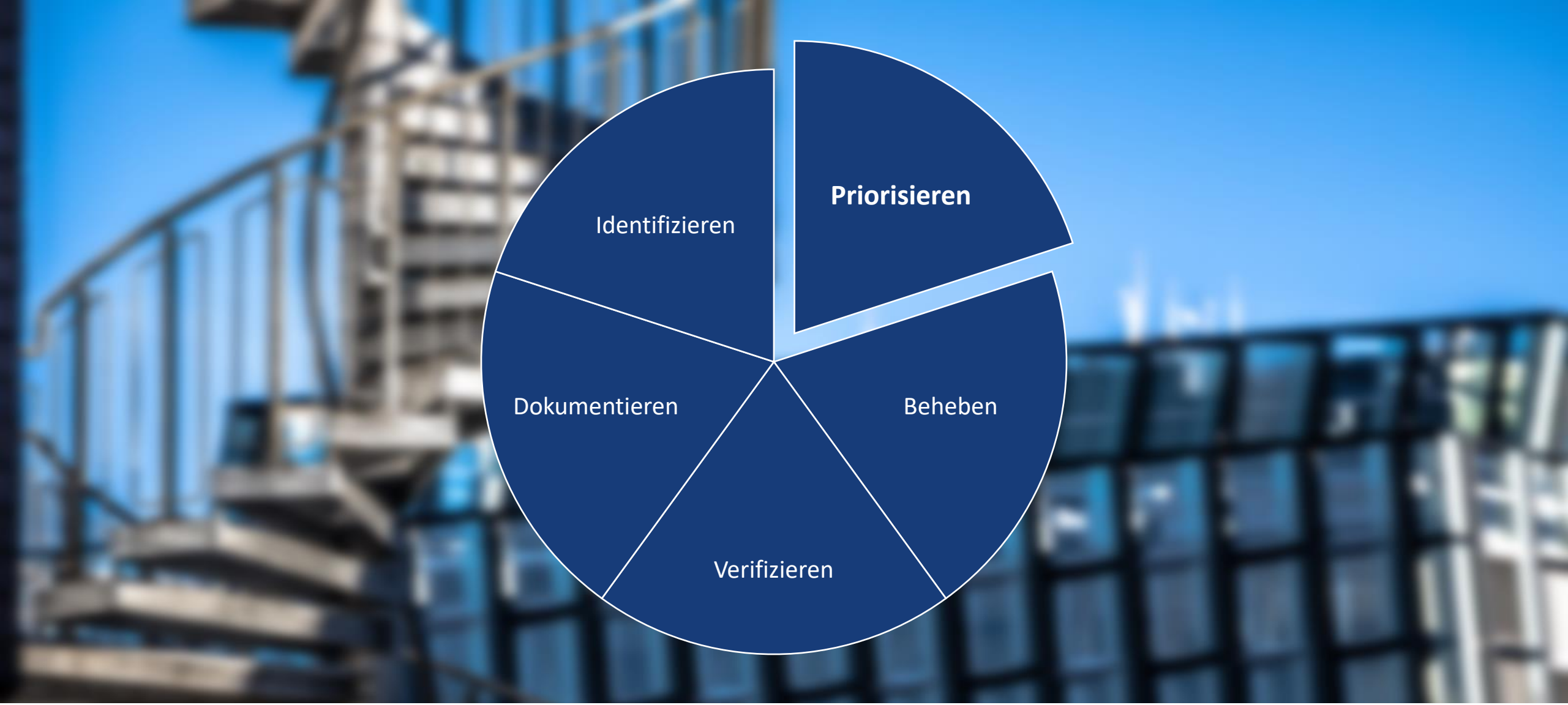


Identifizieren

Build- und Runtime-Scans



Identifizierung: Takeaways



Auf die Priorisierung kommt es an

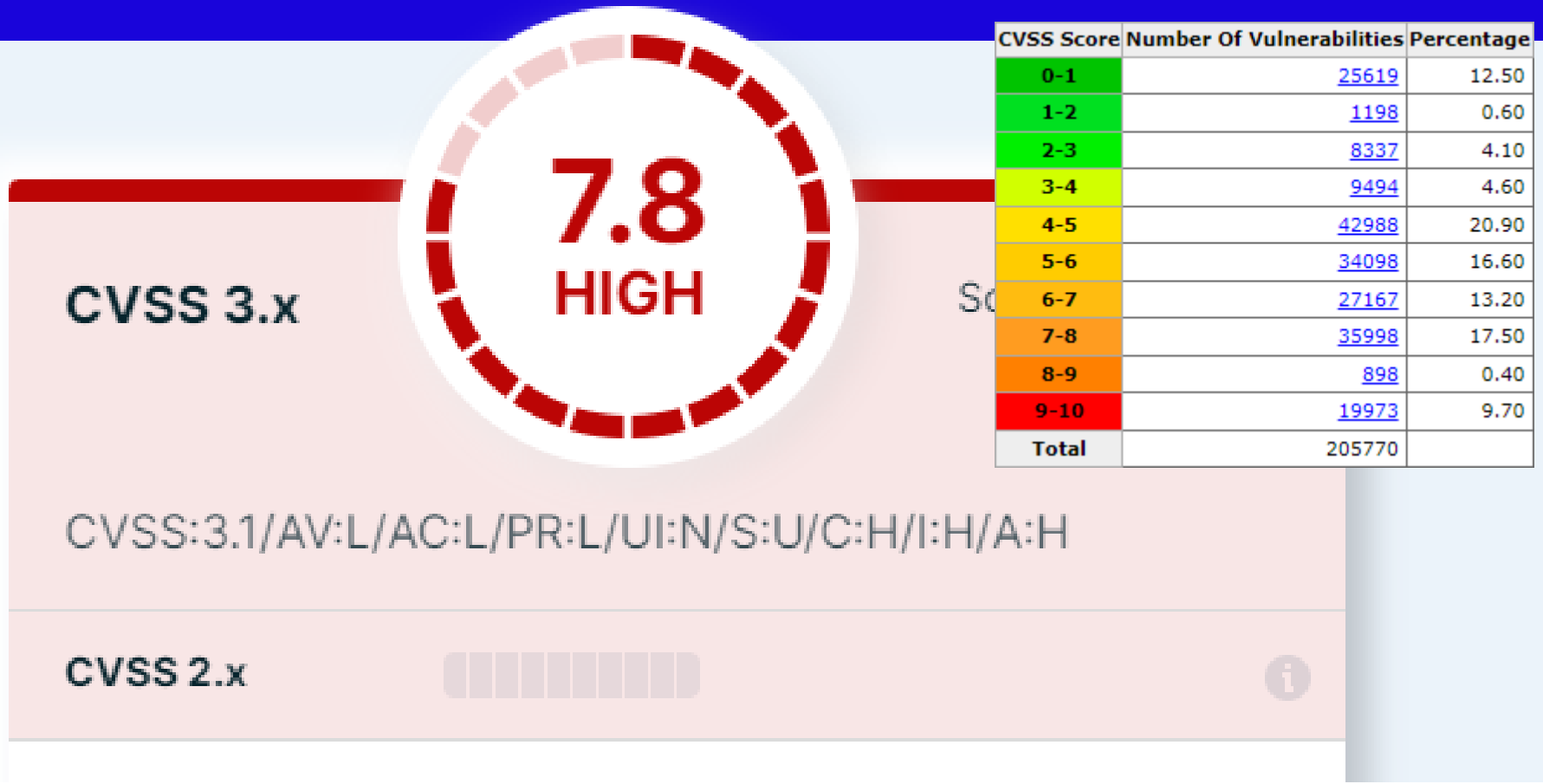
```
kevin@AIR-K-SCHU:~$ trivy image nginx:1.25.0-alpine3.17
2023-06-20T09:33:55.769+0200    INFO    Vulnerability scanning is enabled
2023-06-20T09:33:55.769+0200    INFO    Secret scanning is enabled
2023-06-20T09:33:55.769+0200    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2023-06-20T09:33:55.769+0200    INFO    Please see also https://aquasecurity.github.io/trivy/v0.42/docs/secret/scanning/#recommendation for faster secret d
2023-06-20T09:34:00.879+0200    INFO    Detected OS: alpine
2023-06-20T09:34:00.879+0200    INFO    Detecting Alpine vulnerabilities...
2023-06-20T09:34:00.888+0200    INFO    Number of language-specific files: 0

nginx:1.25.0-alpine3.17 (alpine 3.17.3)

Total: 7 (UNKNOWN: 0, LOW: 0, MEDIUM: 3, HIGH: 4, CRITICAL: 0)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
libcrypto3	CVE-2023-2650	HIGH	3.0.8-r3	3.0.9-r0	Possible DoS translating ASN.1 object identifiers https://avd.aquasec.com/nvd/cve-2023-2650
	CVE-2023-1255	MEDIUM		3.0.8-r4	Input buffer over-read in AES-XTS implementation on 64 bit ARM https://avd.aquasec.com/nvd/cve-2023-1255
libssl3	CVE-2023-2650	HIGH		3.0.9-r0	Possible DoS translating ASN.1 object identifiers https://avd.aquasec.com/nvd/cve-2023-2650
	CVE-2023-1255	MEDIUM		3.0.8-r4	Input buffer over-read in AES-XTS implementation on 64 bit ARM https://avd.aquasec.com/nvd/cve-2023-1255
libx11	CVE-2023-3138		1.8.4-r0	1.8.4-r1	InitExt.c can overwrite unintended portions of the Display structure if the extension...
ncurses-libs	CVE-2023-29491	HIGH	6.3_p20221119-r0	6.3_p20221119-r1	Local users can trigger security-relevant memory corruption via malformed data https://avd.aquasec.com/nvd/cve-2023-29491
ncurses-terminfo-base					

elevant memory
a the TERMINFO or



CVSS Score	Number Of Vulnerabilities	Percentage
0-1	25619	12.50
1-2	1198	0.60
2-3	8337	4.10
3-4	9494	4.60
4-5	42988	20.90
5-6	34098	16.60
6-7	27167	13.20
7-8	35998	17.50
8-9	898	0.40
9-10	19973	9.70
Total	205770	

CVSS - Common Vulnerability Scoring System

https://avd.aquasec.com/nvd/2023/cve-2023-29491/

CVE Vulnerabilities

CVE-2023-29491

Out-of-bounds Write

Published: Apr 14, 2023 | **Modified:** May 17, 2023

ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO TERM environment variable.

Weakness

The product writes data past the end, or before the beginning, of the intended buffer.

Affected Software

Name	Ven
Ncurses	Gnu
Ncurses	Ubu
Ncurses	Ubu

Ncurses	Ubuntu	trusty/esm	*
Ncurses	Ubuntu	upstream	*
Ncurses	Ubuntu	xenial	*

Potential Mitigations

- Use a language that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
- For example, many languages that perform their own memory management, such as Java and Perl, are not subject to buffer overflows. Other languages, such as Ada and C#, typically provide overflow protection, but the protection can be disabled by the programmer.
- Be wary that a language's interface to native code may still be subject to overflows, even if the language itself is theoretically safe.
- Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
- Examples include the Safe C String Library (SafeStr) by Messier and Viega [REF-57], and the Strsafe.h library from Microsoft [REF-56]. These libraries provide safer versions of overflow-prone string-handling functions.
- Use automatic buffer overflow detection mechanisms that are offered by certain compilers or compiler extensions.

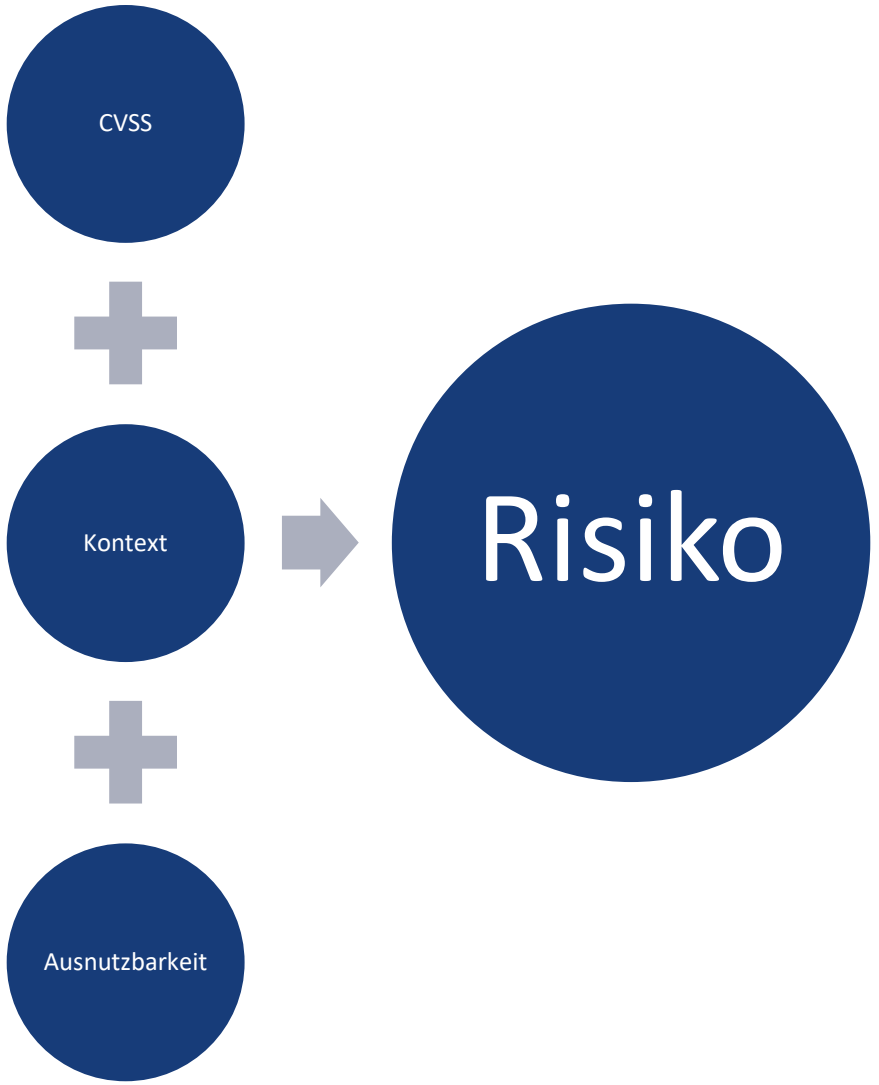
instruction executed is exclusively at a mem

- For more information on these techniques s
1336].

References

- https://www.openwall.com/lists/oss-security
- https://www.openwall.com/lists/oss-security
- http://ncurses.scripts.mit.edu/?p=ncurses.git;a=commit;h=eb51b1ea1f75a0ec17c9c5937cb28df1e8eeec56
- http://www.openwall.com/lists/oss-security/2023/04/19/10
- http://www.openwall.com/lists/oss-security/2023/04/19/11
- https://security.netapp.com/advisory/ntap-20230517-0009/

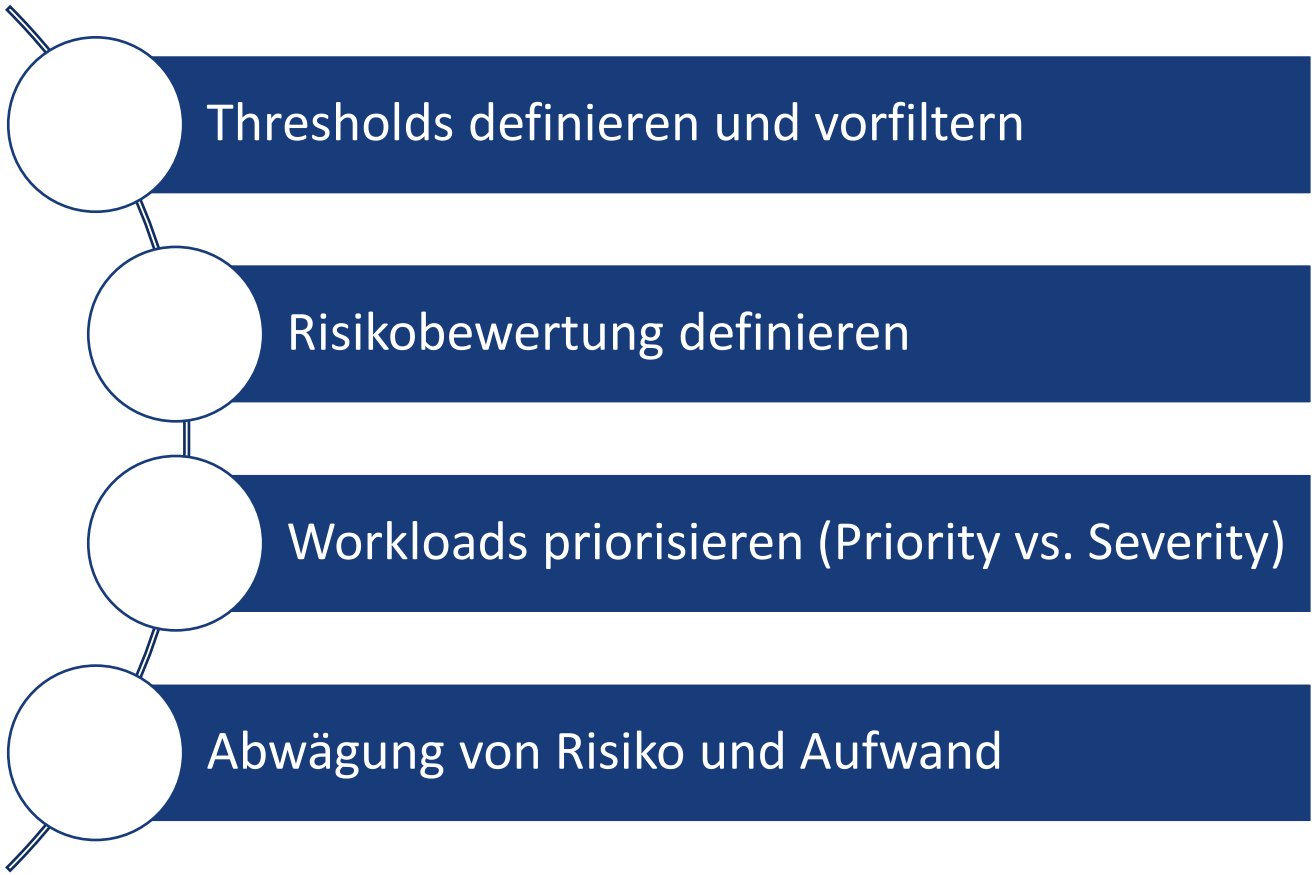
https://avd.aquasec.com/nvd/2023/cve-2023-29491/



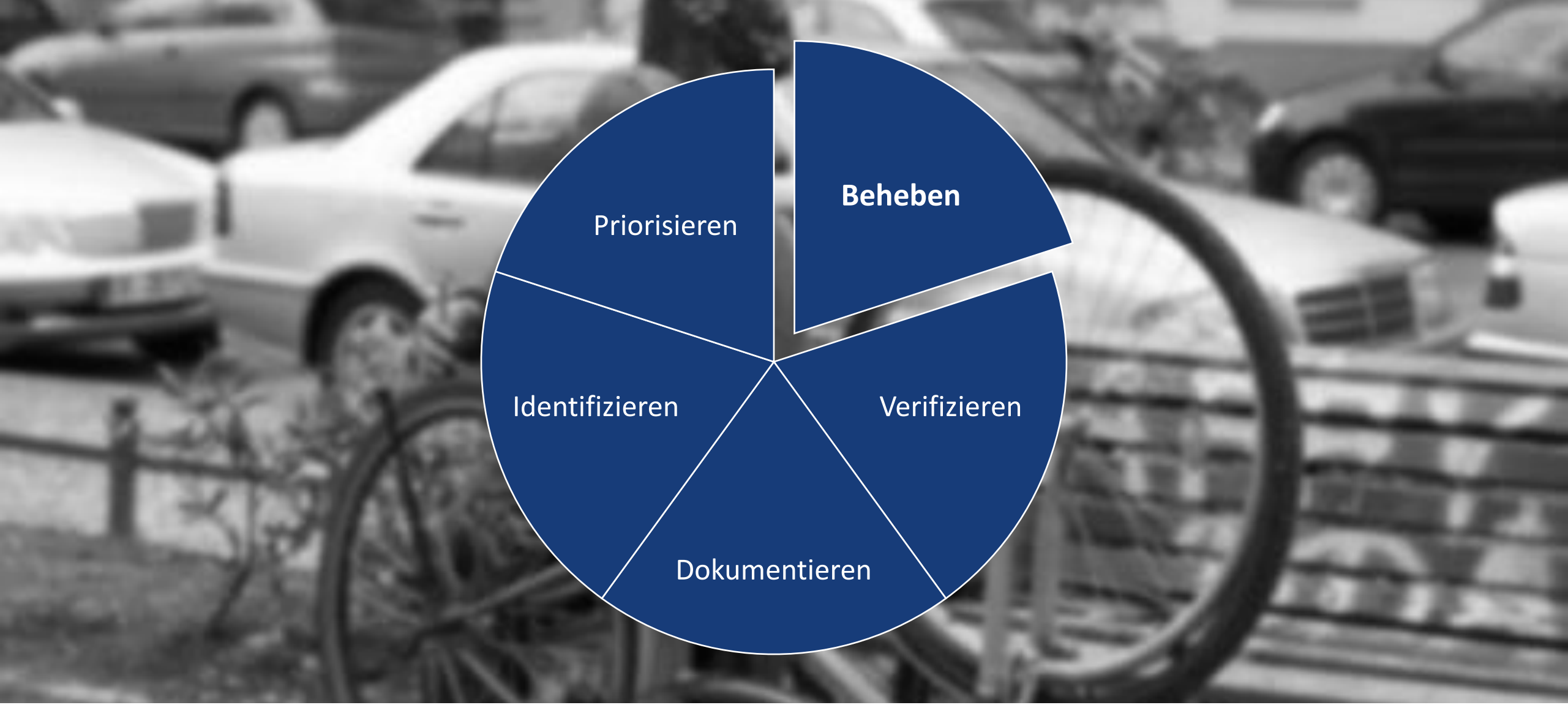
Wie definiere ich das Risiko?

	low	normal	high	top
	1	3	5	
13	13	39	65	
8	8	24	40	
5	5	15	25	
3	3	9	15	
1	1	3	5	

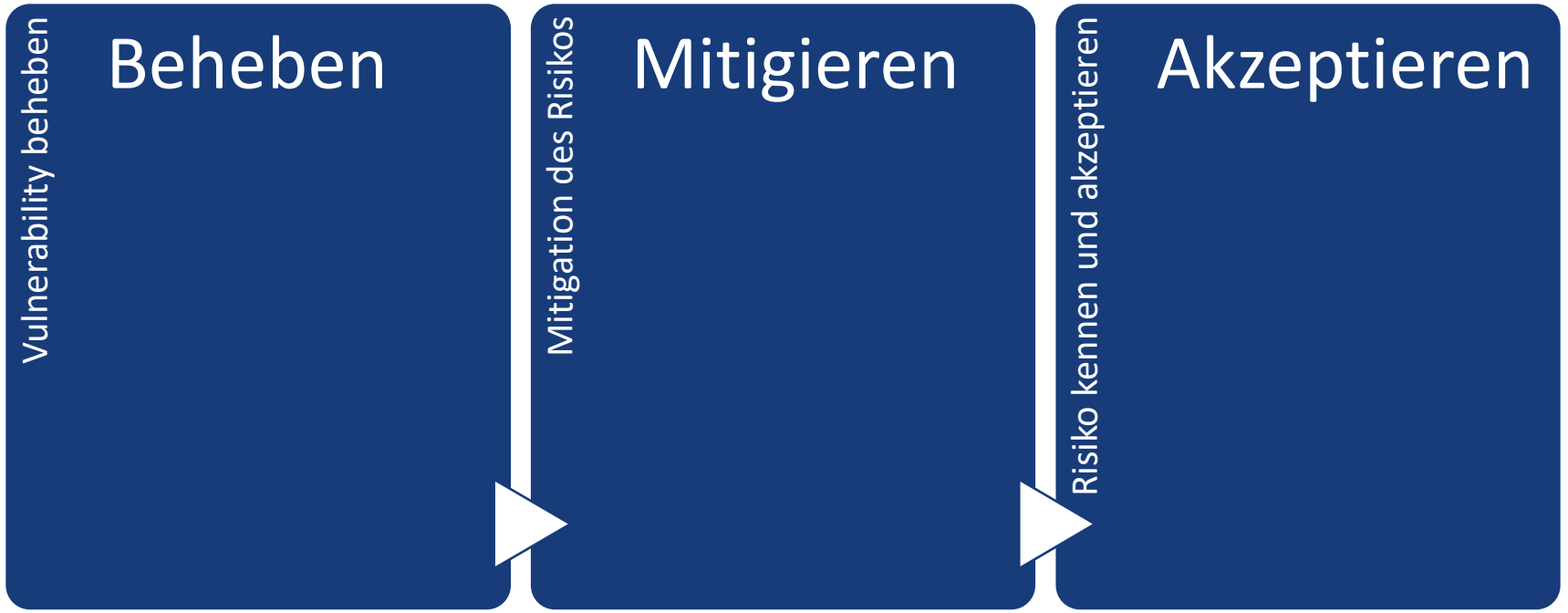
Kontext: Priority vs. Severity



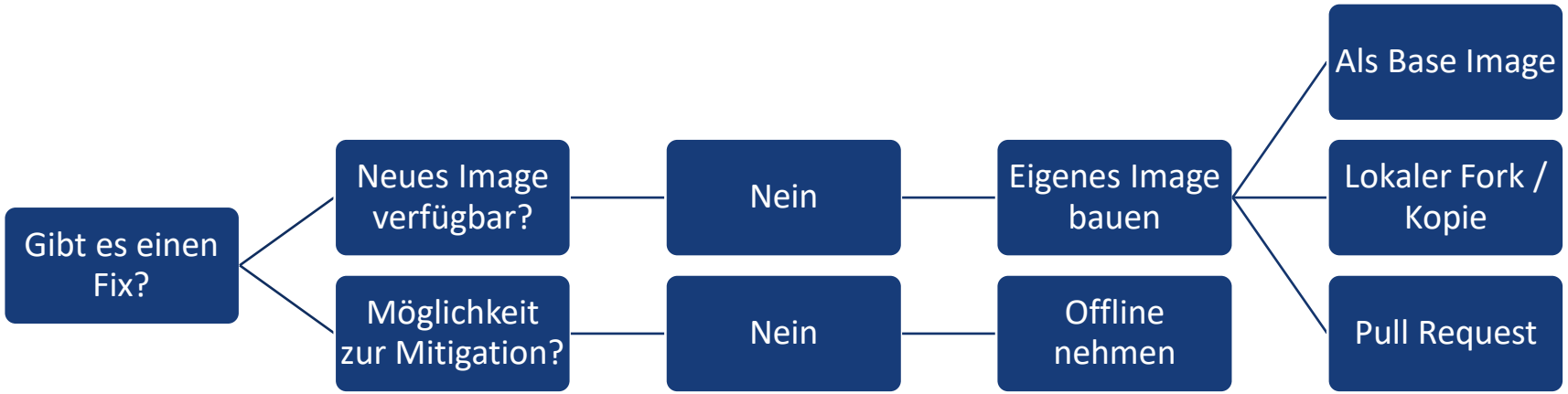
Priorisierung: Takeaways


Beheben
Verifizieren
Dokumentieren
Identifizieren
Priorisieren

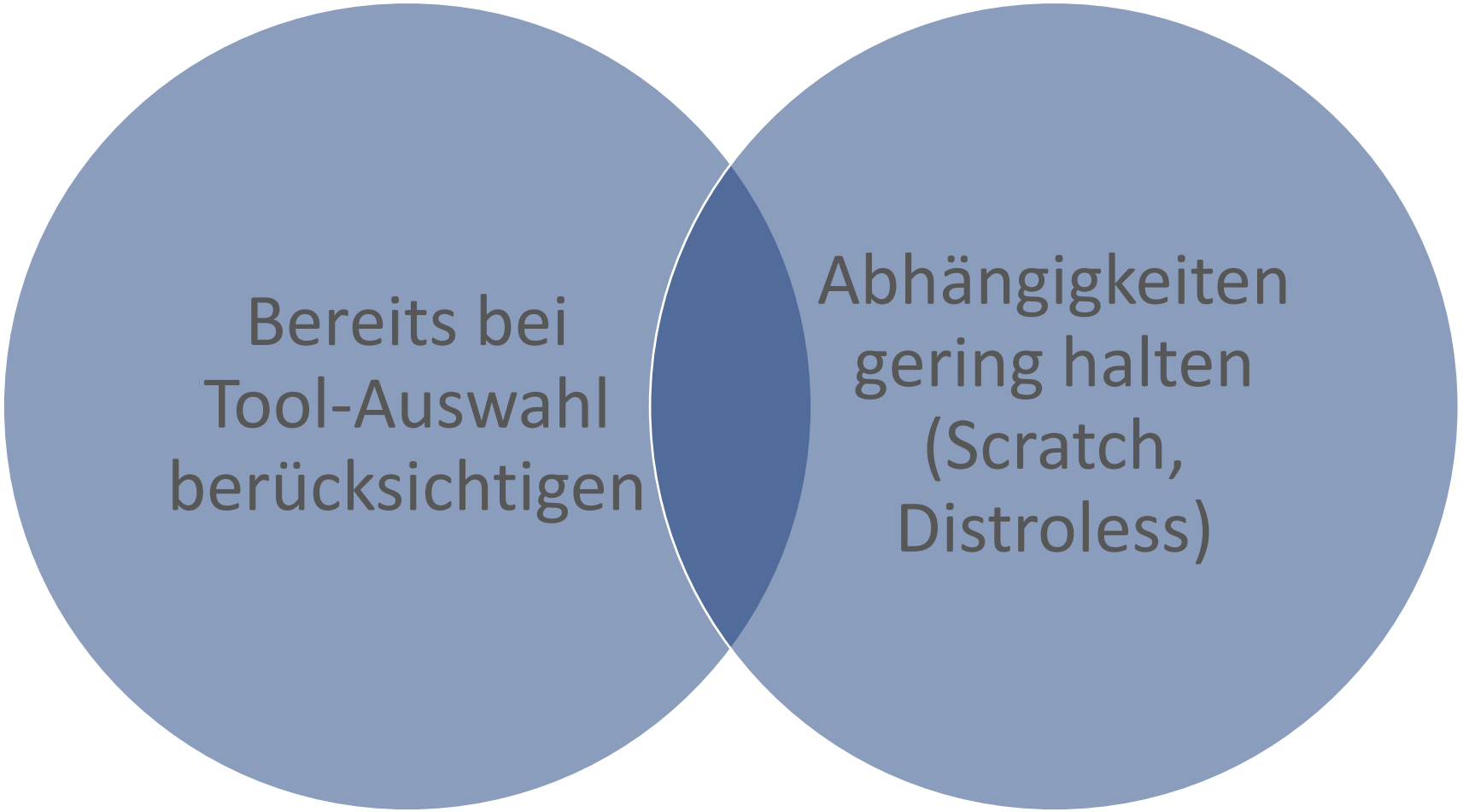
Beheben



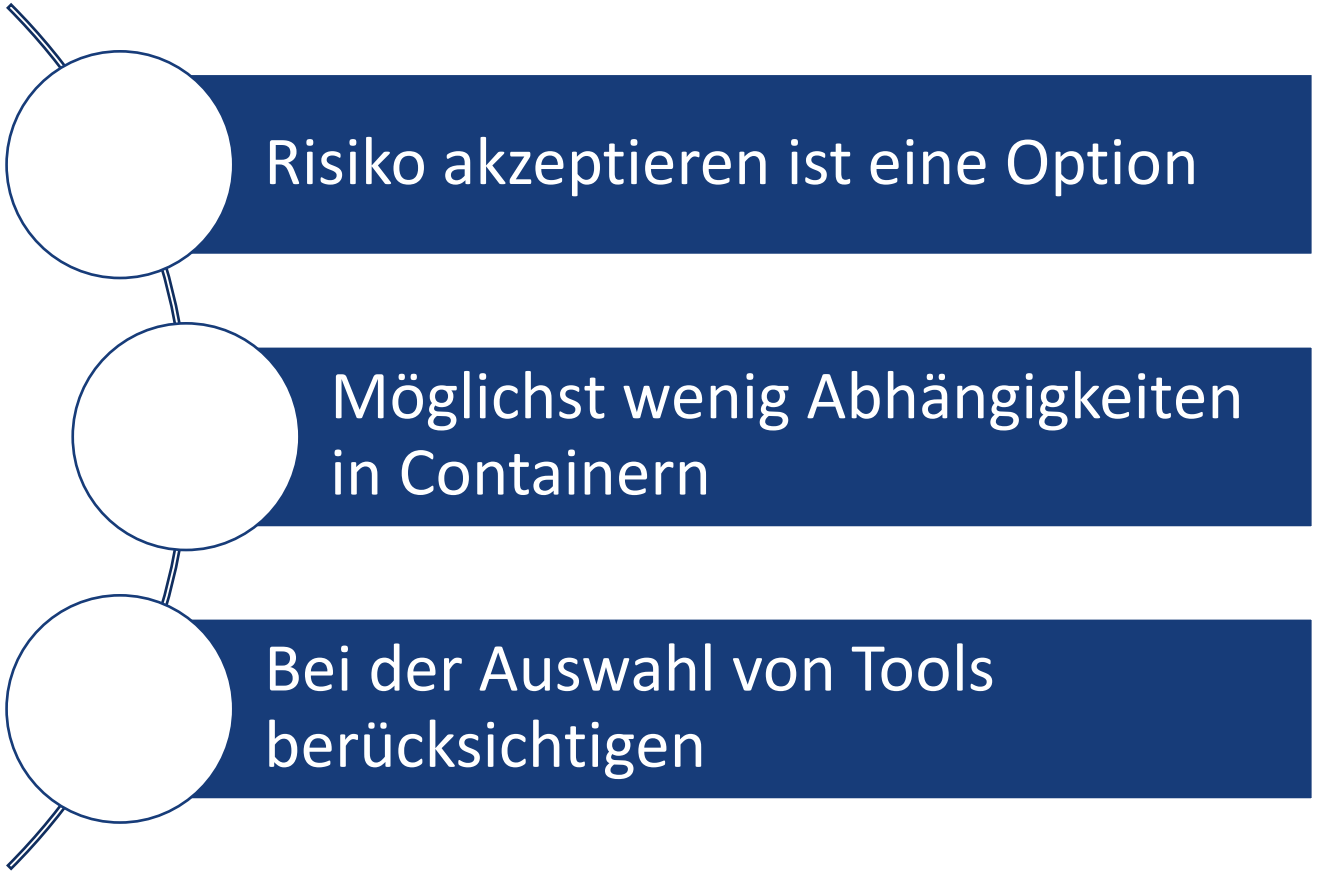
Welche Optionen habe ich?



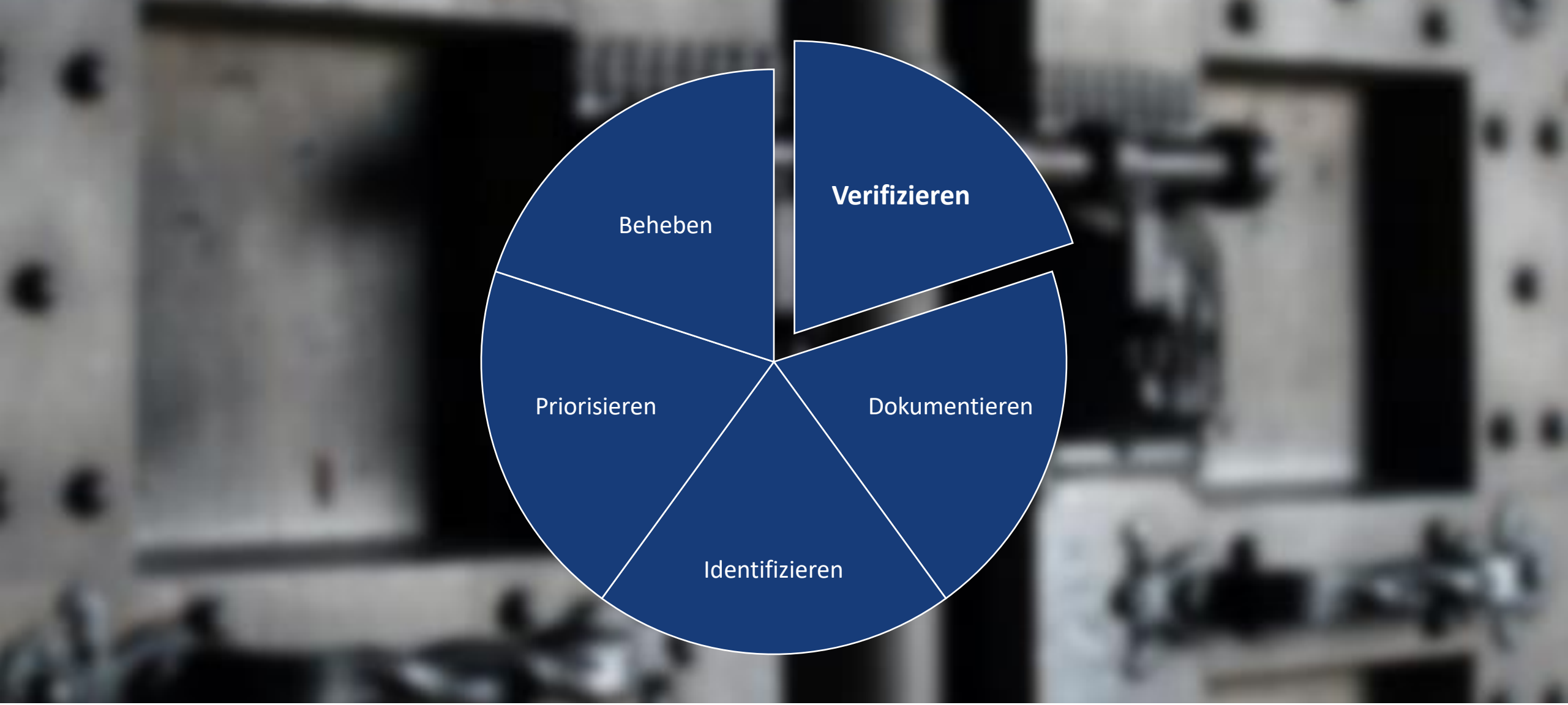
Eine Behebung kann schnell kompliziert und aufwendig werden



Aufwand kann vorher schon minimiert werden



Beheben: Takeaways



Vertrauenswürdige Quelle?

Container-Signierung

```
trivy image --format cosign-vuln --output vuln.json <IMAGE>
cosign attest --key /path/to/cosign.key --type vuln --predicate vuln.json <IMAGE>
```

Vulnerability Attestation

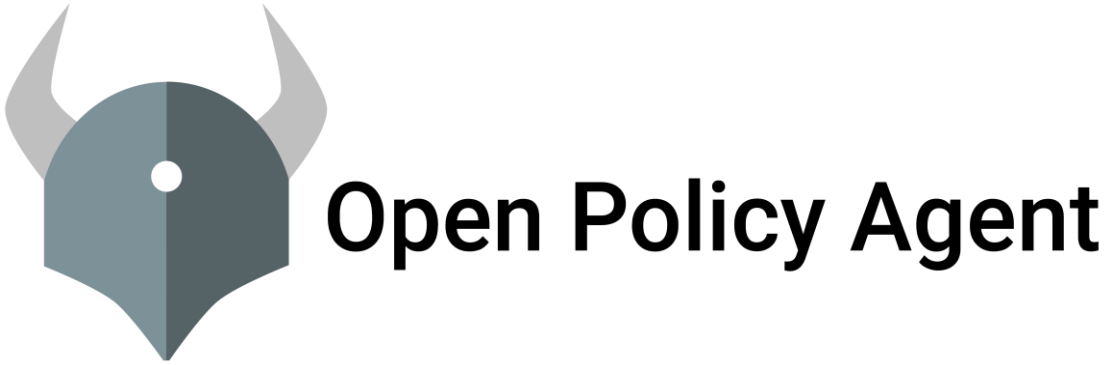
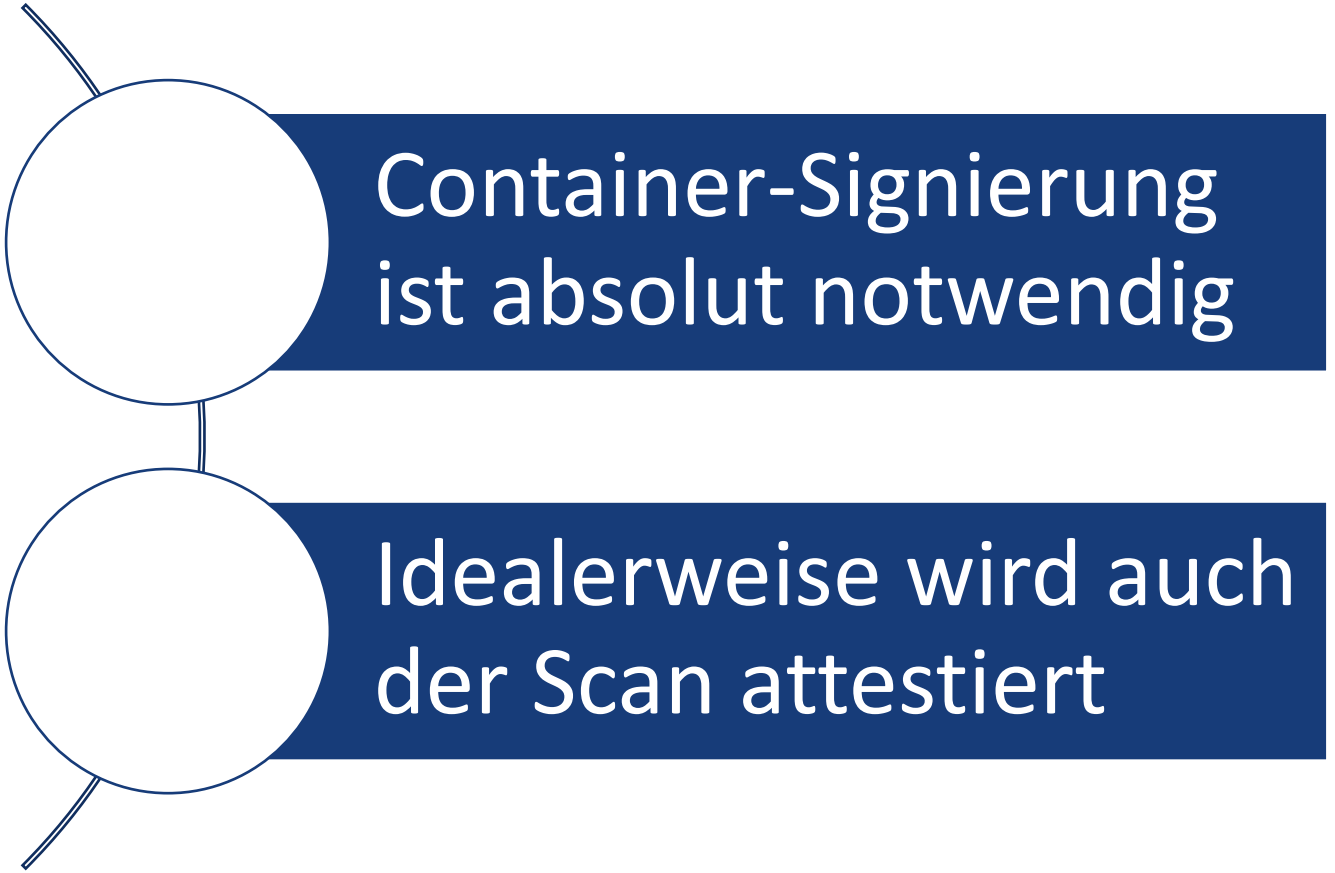
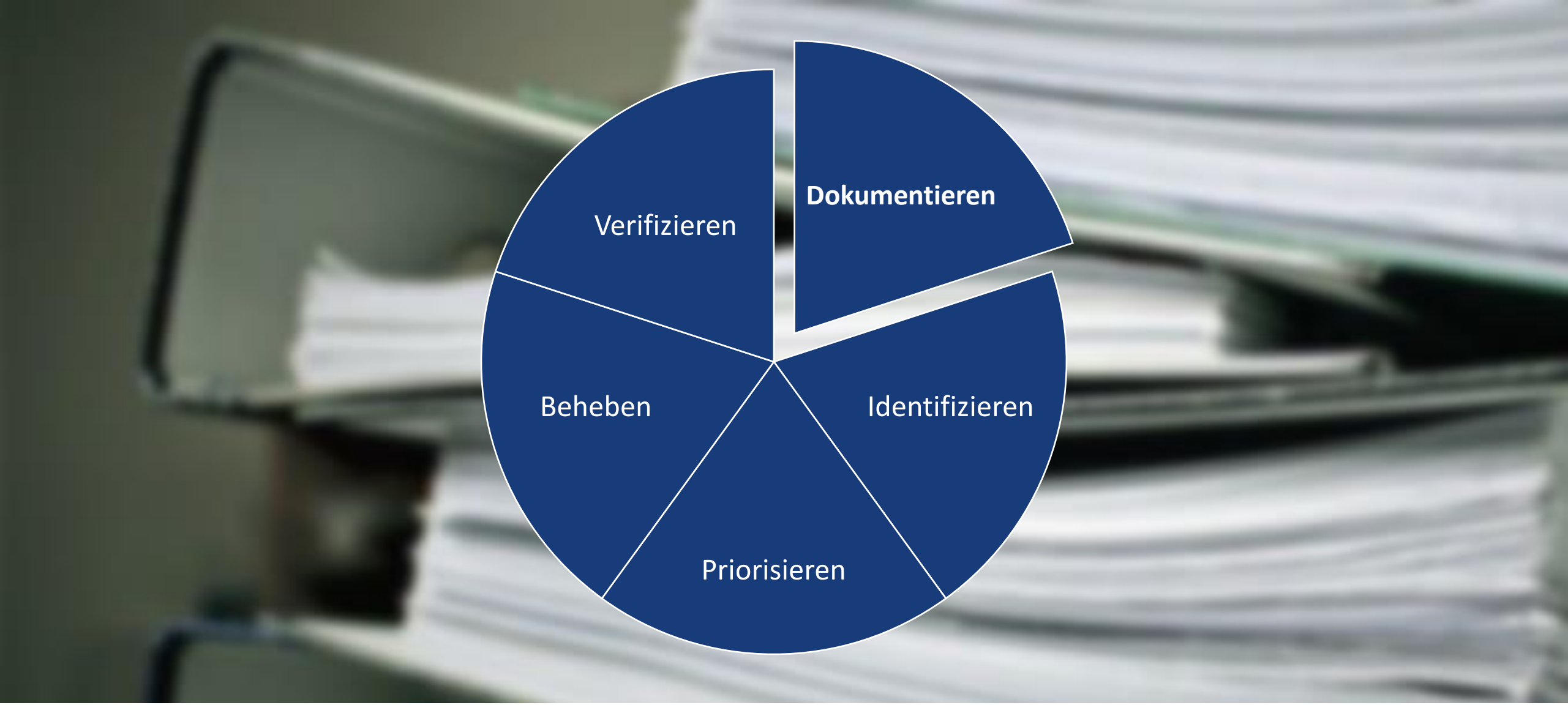


Image Verification in Kubernetes



Verifizieren: Takeaways



Dokumentieren

Seiten / ... / CVE Management

Bearbeiten Favorit Beobachten Teilen ...

CVE-2022-41721 & CVE-2022-41723 golang.org/x/net

Erstellt von [redacted] zuletzt geändert von [redacted] am 17 Mai 2023

Status	IRRELEVANT
Betroffene Componenten	buildkit Helm terragrunt

relevante Links

> A request smuggling attack is possible when using MaxBytesHandler. When using MaxBytesHandler, the body of an HTTP request is not fully consumed. When the server attempts to read HTTP2 frames from the connection, it will instead be reading the body of the HTTP request, which could be attacker-manipulated to represent arbitrary HTTP2 requests.
>
> https://avd.aquasec.com/nvd/2022/cve-2022-41721/

> A maliciously crafted HTTP/2 stream could cause excessive CPU consumption in the HPACK decoder, sufficient to cause a denial of service from a small number of small requests.
>
> https://avd.aquasec.com/nvd/2022/cve-2022-41723/

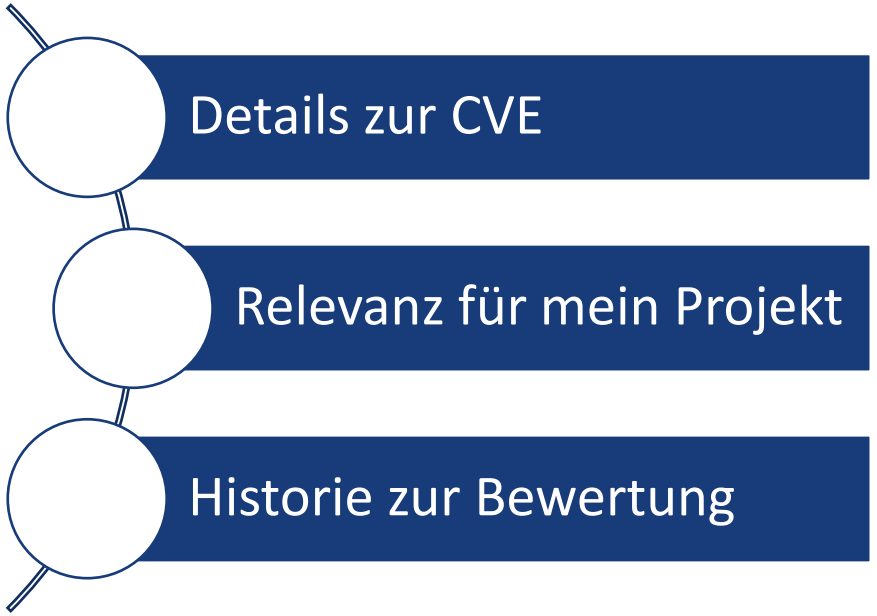
Bewertung

06.02.2023 Interne Komponente und Library in einem Tool, das wir nicht selbst aktualisieren.

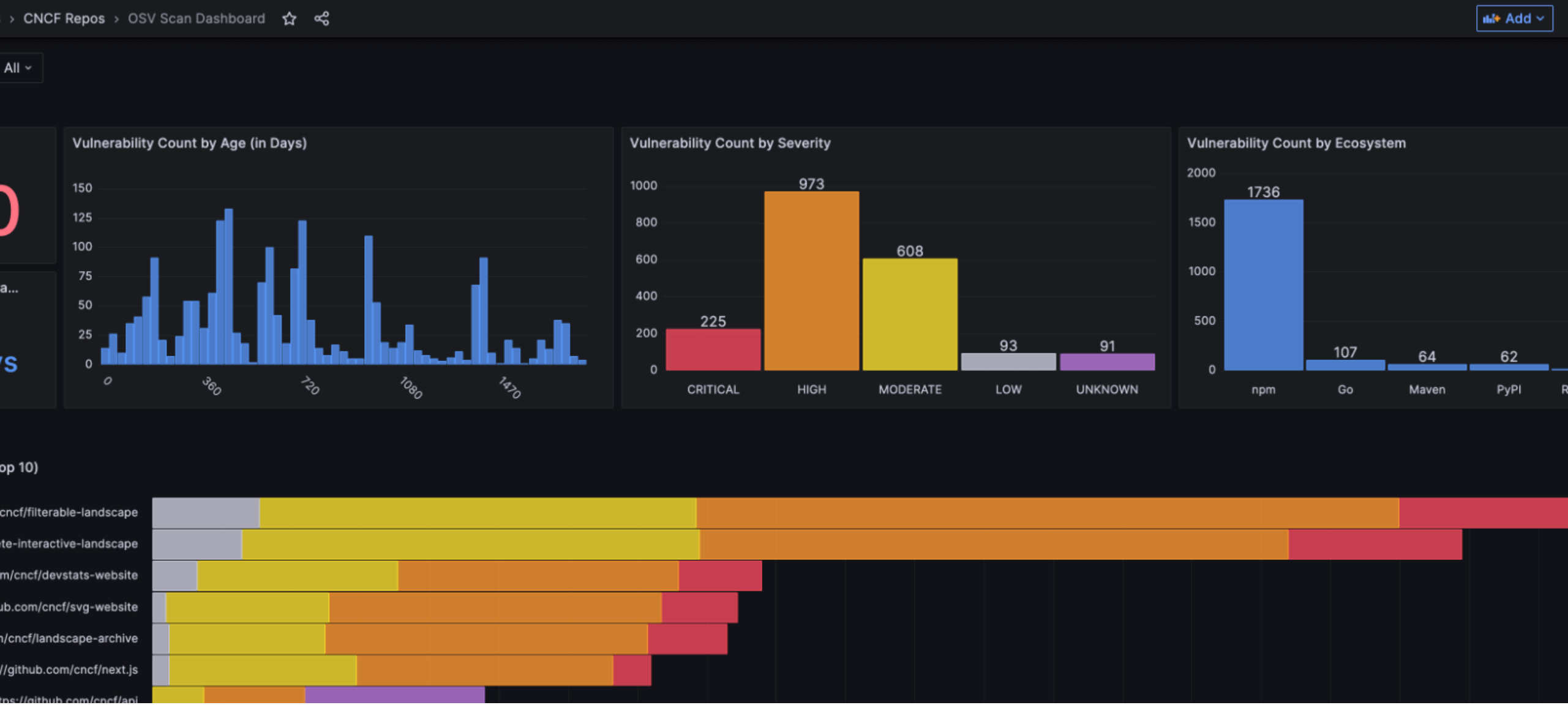
17.05.2023 CVE-2022-41721 durch Update gefixt.

Gefällt mir Sei der Erste, dem dies gefällt.

cve



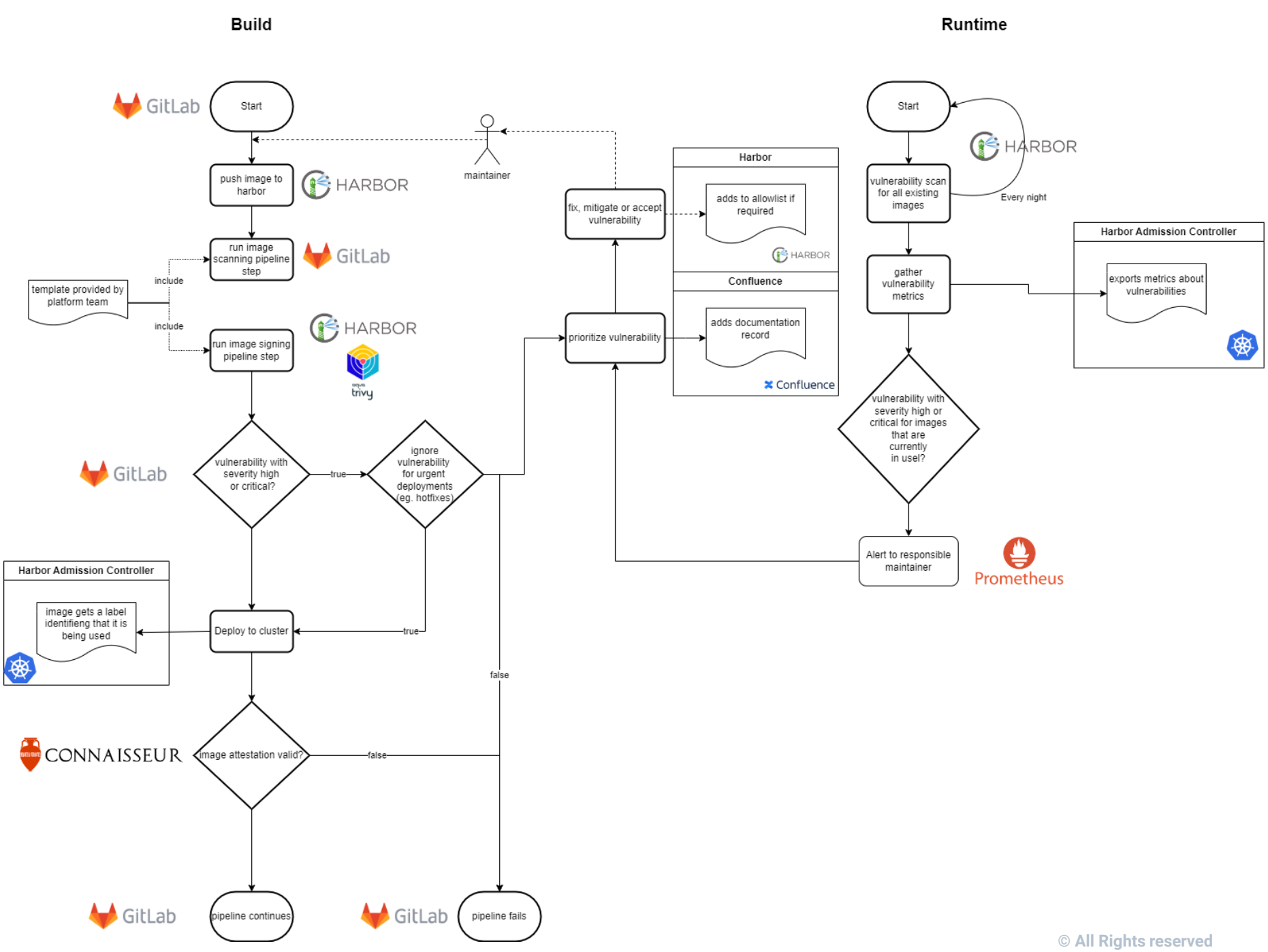
Wichtigste Informationen dokumentieren

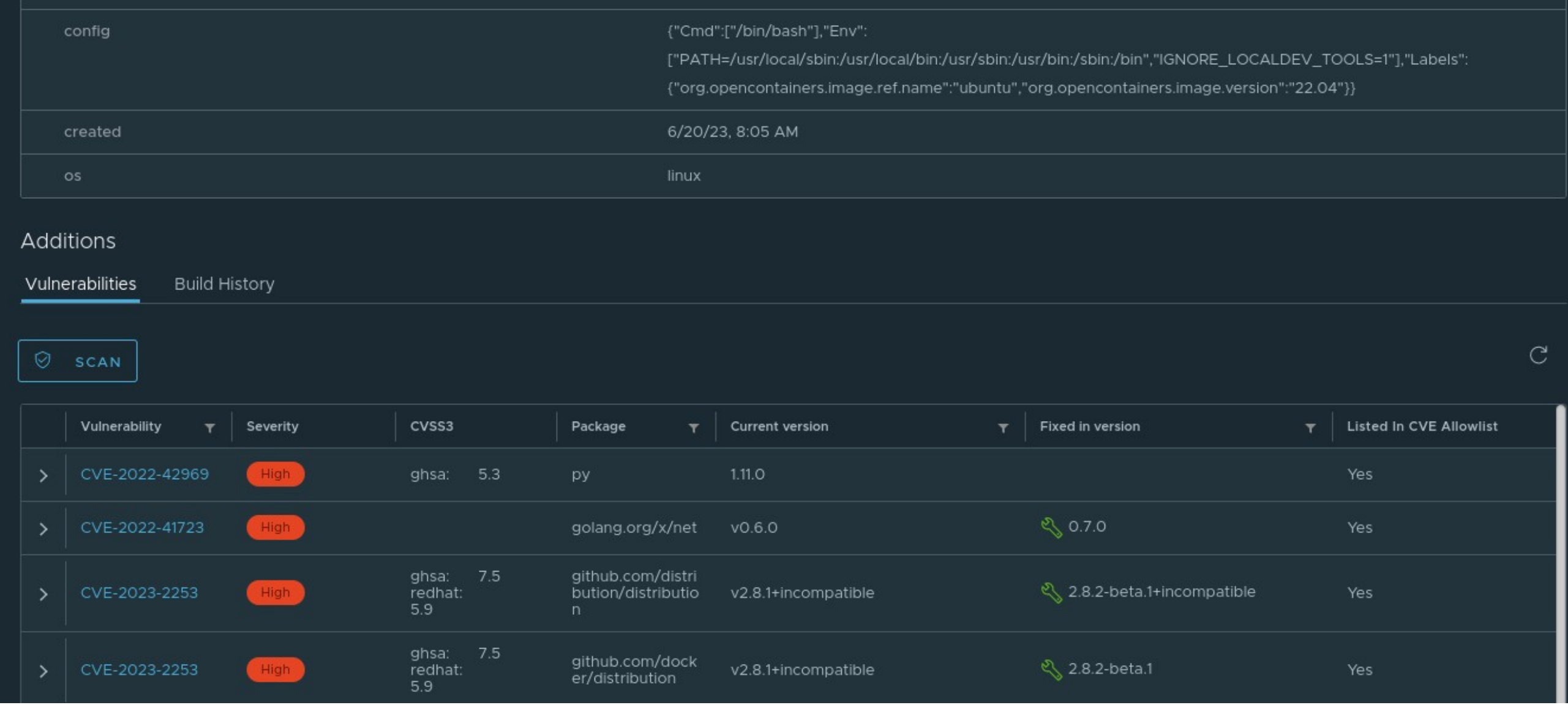


Monitoring

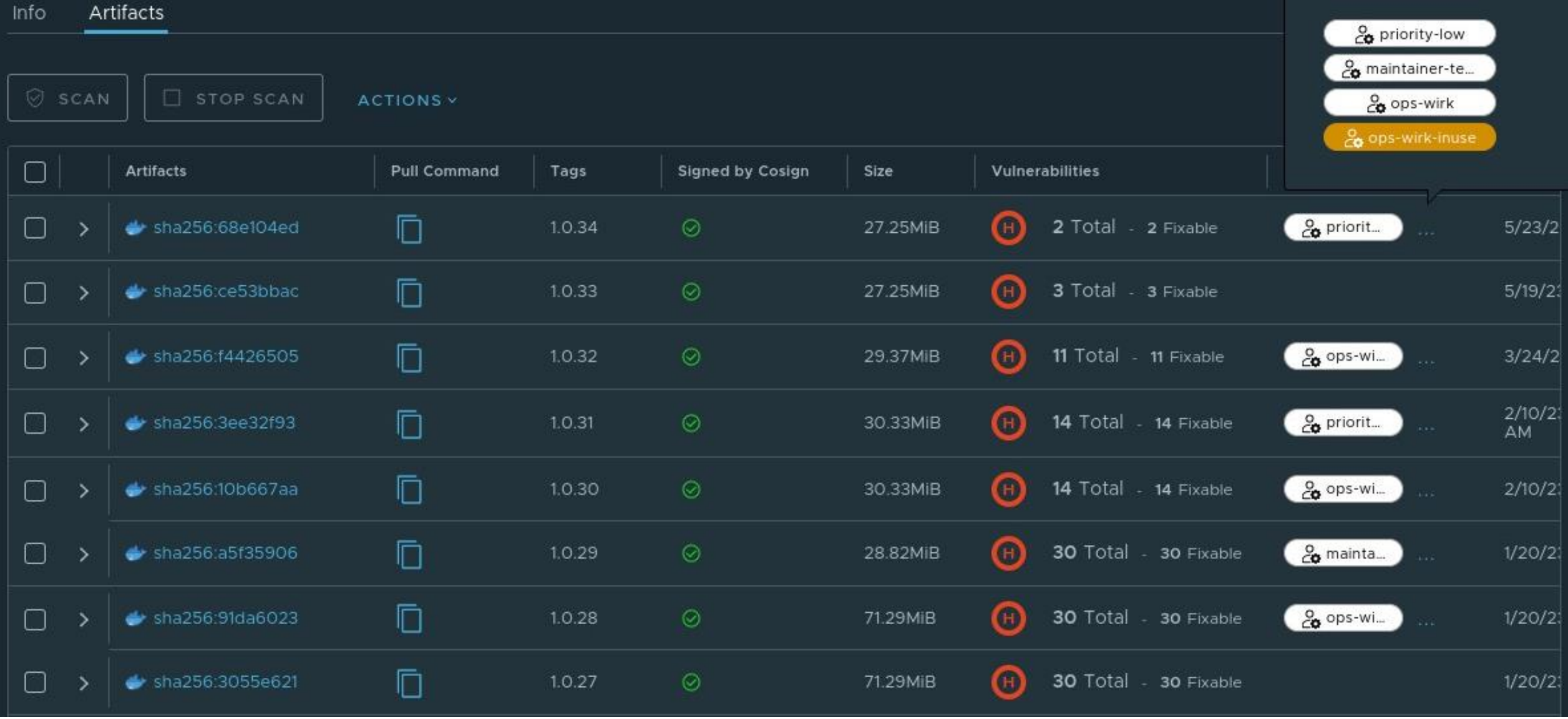
https://grafana.com/blog/2023/05/25/how-to-manage-cve-security-vulnerabilities-with-grafana-mergestat-and-osv-scanner/

Fallbeispiel: Harbor, Trivy, Cosign, Connaisseur, Grafana, Prometheus





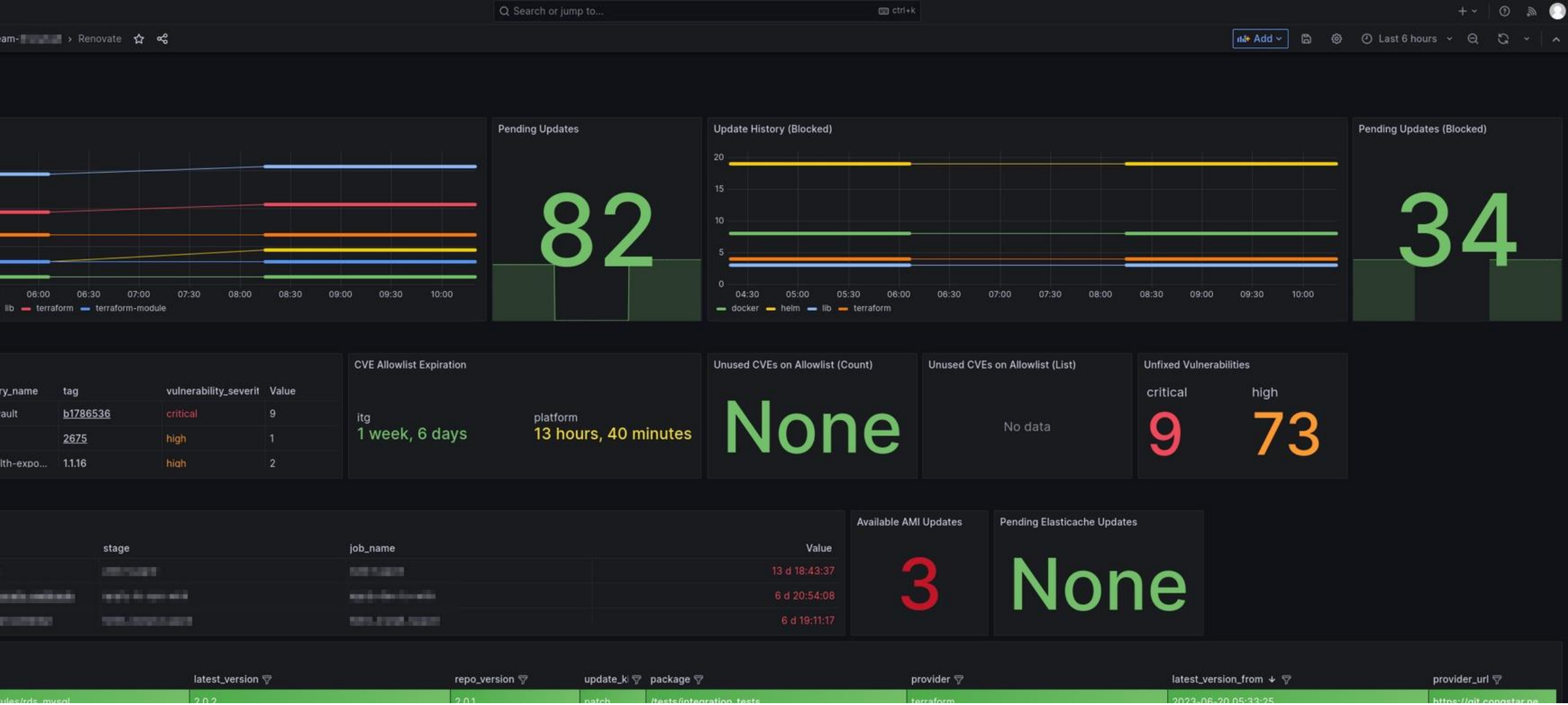
Vulnerabilities in Harbor



Admission Controller Labels

```
e: harbor-repository-vulnerabilities
es:
 alert: HarborInUseRepositoryHasVulnerabilities
 expr: sum(harbor_vulnerabilities{harbor_labels=~".*inuse.*",vulnerability_severity=~"high|critical",maintainer="[redacted]"}) by (namespace,maintainer,priority,repository,vulnerability_severity,t
 labels:
   runbook: RB-0051
   severity: warning
   priority: high
 annotations:
   description: 'In use repository {{ $labels.repository }} with tag {{ $labels.tag }} has {{ $value }} {{ $labels.vulnerability_severity }} vulnerabilities'
   summary: 'In use repository {{ $labels.repository }} has vulnerabilities'
 alert: HarborVulnerabilitiesUnknown
 expr: absent_over_time(harbor_vulnerabilities[75m])
 for: 5m
 labels:
   runbook: RB-0080
   maintainer: [redacted]
   severity: warning
   priority: high
   namespace: ops
 annotations:
   description: 'There is no data on harbor vulnerability scans in prometheus. Alerts on vulnerabilities can not be created.'
   summary: 'Harbor Vulnerability information unknown'
 alert: HarborVulnerabilitiesError
 expr: harbor_scans_error > 0
 labels:
   runbook: RB-0070
   maintainer: [redacted]
   severity: warning
   priority: low
 annotations:
   description: "Vulnerability Scan of {{ $labels.repository }}:{{ $labels.tag }} did not run properly. We can't say whether it has vulnerabilities or not."
   summary: 'Harbor Vulnerability Scan did not run properly on {{ $labels.repository }}:{{ $labels.tag }}'
```

Alerting auf Vulnerability Metriken


Search or jump to...
ctrl+k
Renovate
Add
Last 6 hours
06:00 06:30 07:00 07:30 08:00 08:30 09:00 09:30 10:00
lib terraform terraform-module
Pending Updates
82
Update History (Blocked)
20 15 10 5 0
04:30 05:00 05:30 06:00 06:30 07:00 07:30 08:00 08:30 09:00 09:30 10:00
docker helm lib terraform
Pending Updates (Blocked)
34
ry_name tag vulnerability_severit Value
ault b1786536 critical 9
2675 high 1
lth-expo... 1.1.16 high 2
CVE Allowlist Expiration
itg
1 week, 6 days
platform
13 hours, 40 minutes
Unused CVEs on Allowlist (Count)
None
Unused CVEs on Allowlist (List)
No data
Unfixed Vulnerabilities
critical
9
high
73
stage
job_name
Value
13 d 18:43:37
6 d 20:54:08
6 d 19:11:17
Available AMI Updates
3
Pending Elasticache Updates
None
latest_version
repo_version
update_ki
package
provider
latest_version_from
provider_url

Monitoring

Vielen Dank!

aoe.com/devops