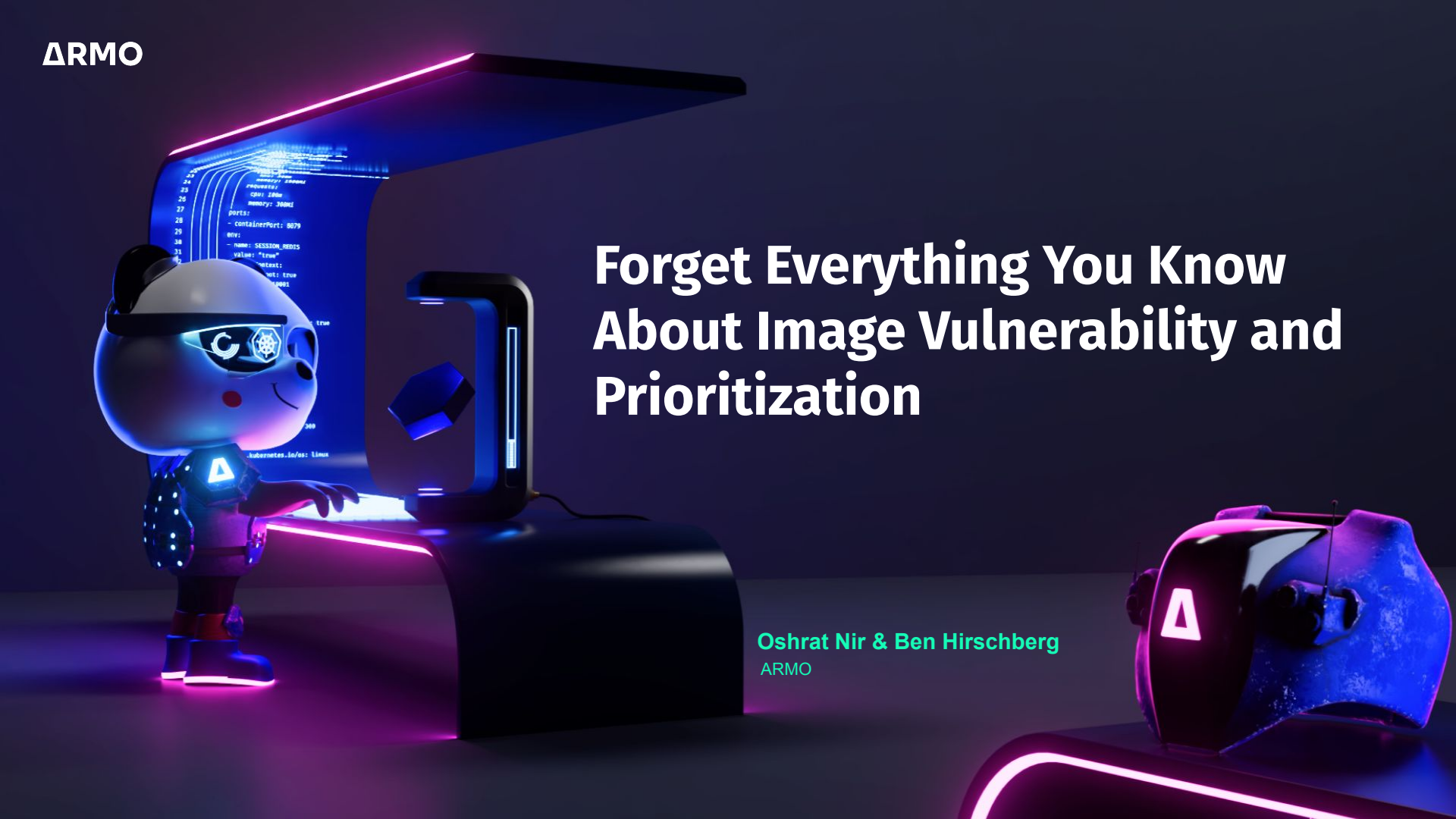
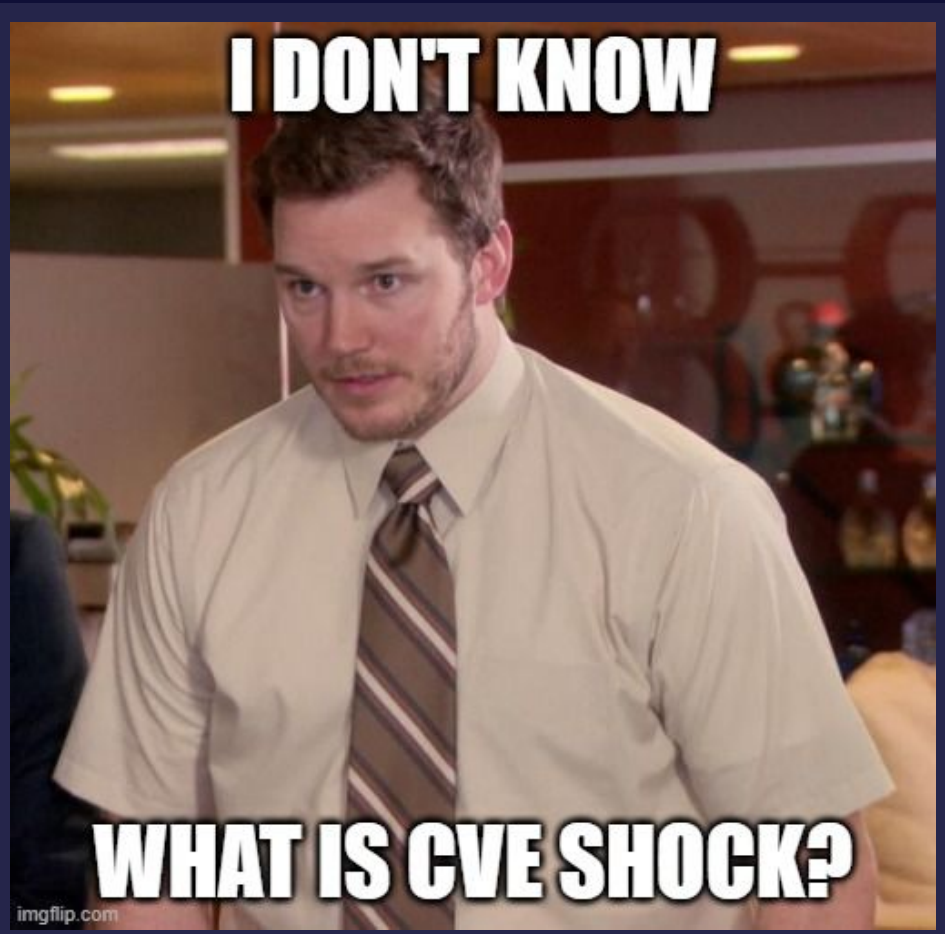
ARMO

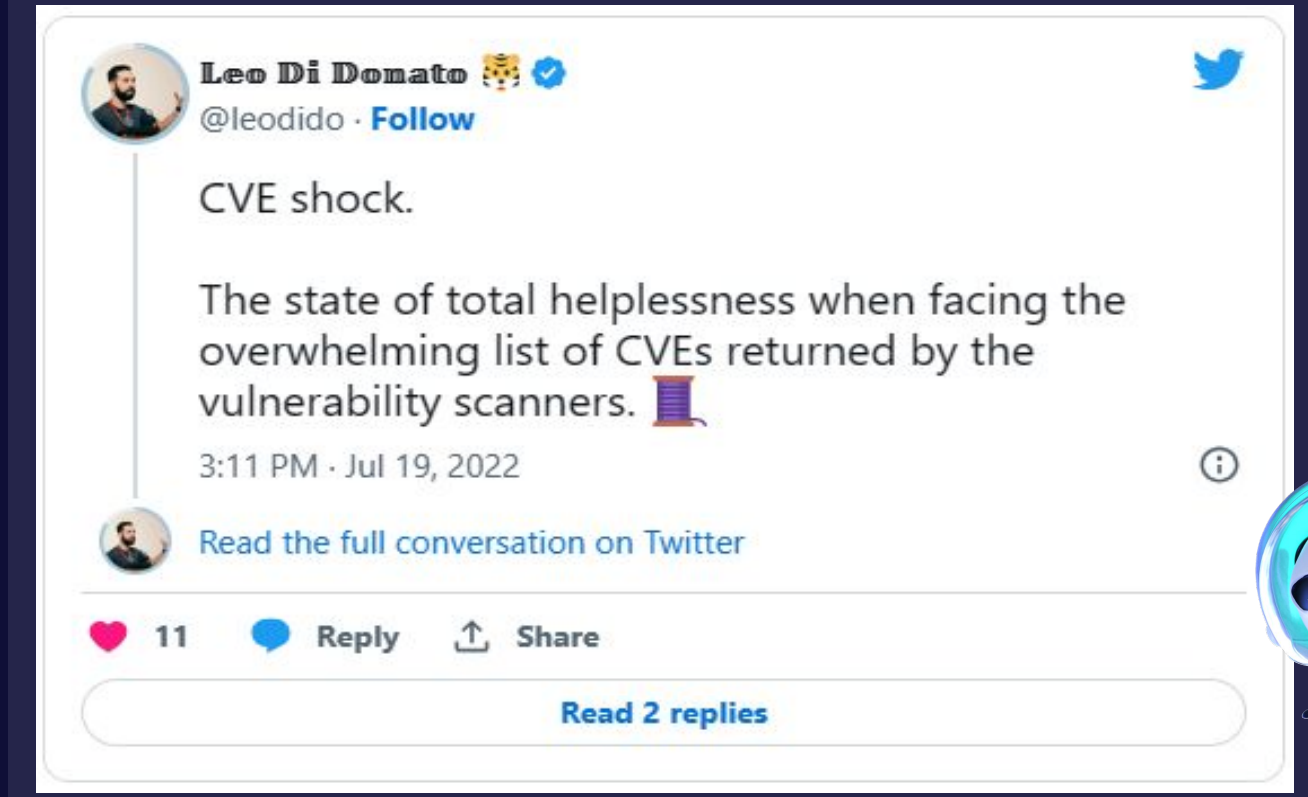


Forget Everything You Know About Image Vulnerability and Prioritization

Oshrat Nir & Ben Hirschberg
ARMO

Are you in CVE Shock?


I DON'T KNOW
WHAT IS CVE SHOCK?
imgflip.com


Leo Di Donato
@leodido · Follow
CVE shock.
The state of total helplessness when facing the overwhelming list of CVEs returned by the vulnerability scanners.
3:11 PM · Jul 19, 2022
Read the full conversation on Twitter
11
Reply
Share
Read 2 replies

/whoami

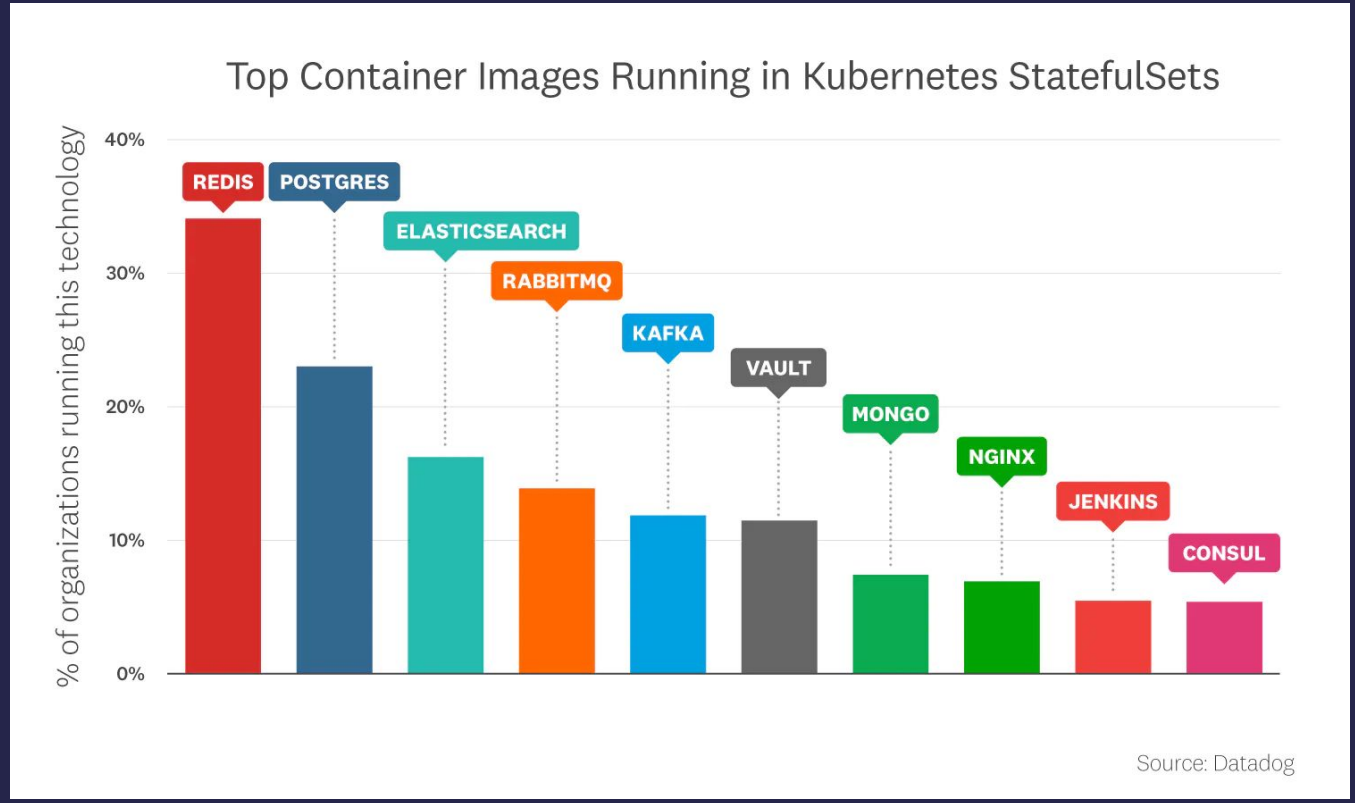
> Ben Hirschberg
> Co-founder && CTO @ARMO
> Kubescape maintainer
> Whitehat in the past (unofficially still ;-)
> Fluent in Hebrew, Hungarian, C, ASM and Go (not English)
> Contributor in CNF-WG + organizer of CNCF Jerusalem
> Father of 4 <3

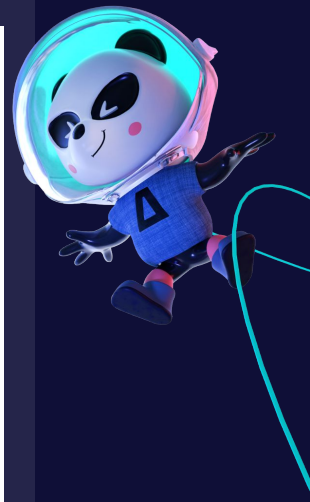
#Ben Hirschberg

linkedin.com/in/ben-hirschberg
@slashben81
github.com/slashben

Where are you looking for CVEs?

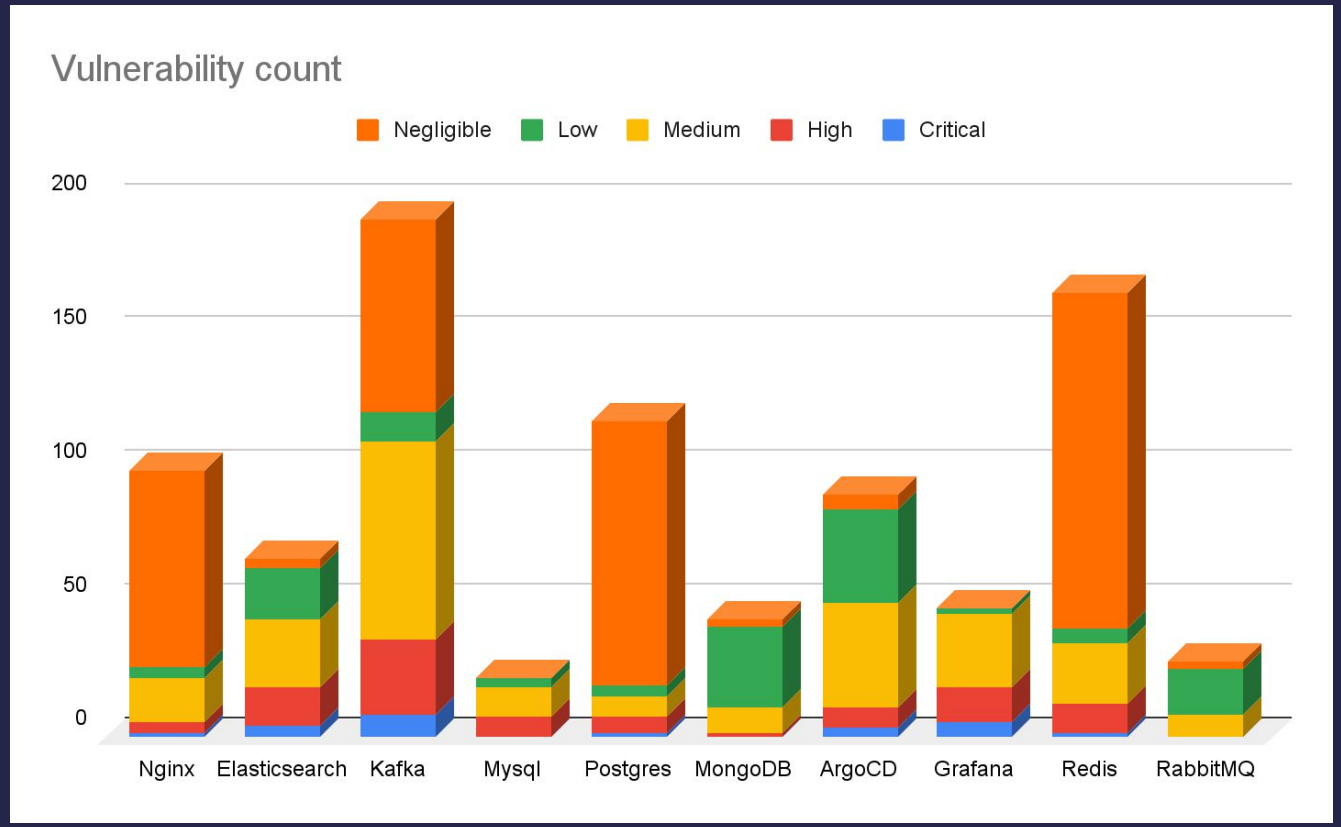
/Everybody use public images_





Unfortunately,
they come with many vulnerabilities

/Vulnerabilities in common images_



/Where are you looking for CVEs?_

Container Registry

CI/CD

Cluster

Container Images

/Reality_

Vulnerability in image

≠

Workload exploit

/Let's put things in CONTEXT_

Reachability

Asset Criticality

Provenance

Threat Intelligence

Prioritized Vulnerability

/Introducing CVSS

Common Vulnerability Scoring System - an open industry standard for assessing the severity of computer system security vulnerabilities

Used to prioritize the response to security incidents and to calculate the potential impact of incidents

Widely adopted, yet lacks context

/Introducing KEV_

KEV - A CISA maintained list of **K**nown **E**xploited **V**ulnerabilities

Vulnerabilities posing increased risk because they are being actively exploited

Required as part of a completes vulnerability management strategy

/KEV_coverage_

Total	P0 (KEV)
23,082	41
14,075	39
19,030	34
31,535	35
6,586	15

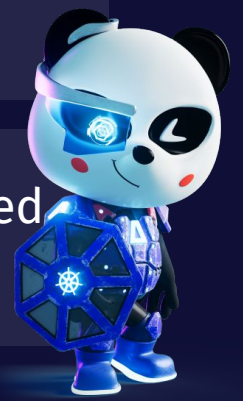
Image source: www.first.org

/Introducing EPSS_

A machine learning based model that assess the likelihood of a vulnerability being exploited in the future

Analyzes factors associated with vulnerabilities, such as its characteristics, historical exploit data, etc.

Indicates the probability of a vulnerability being targeted by attackers within the next 30 days



/Proving the point with EPSS_

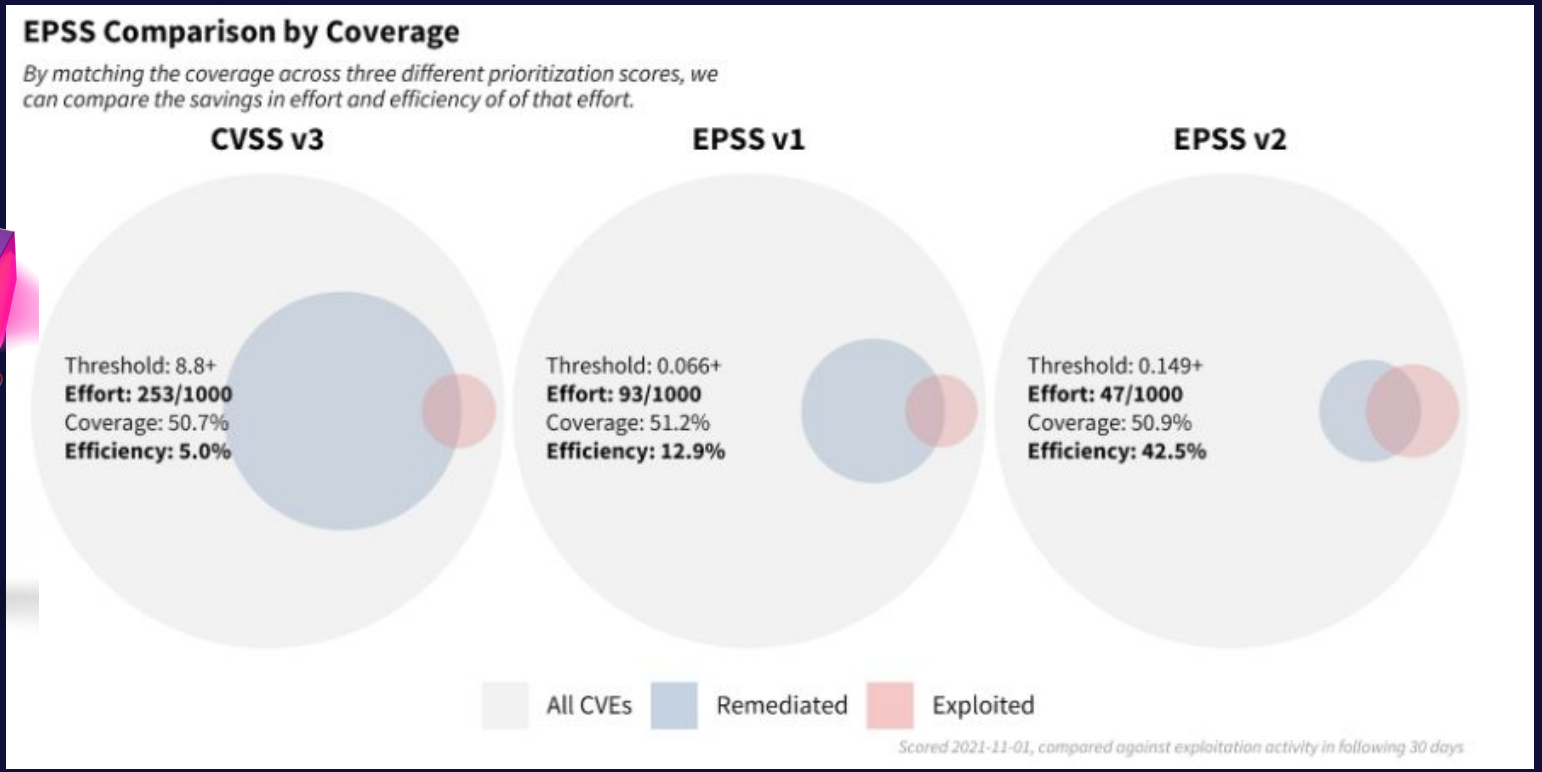


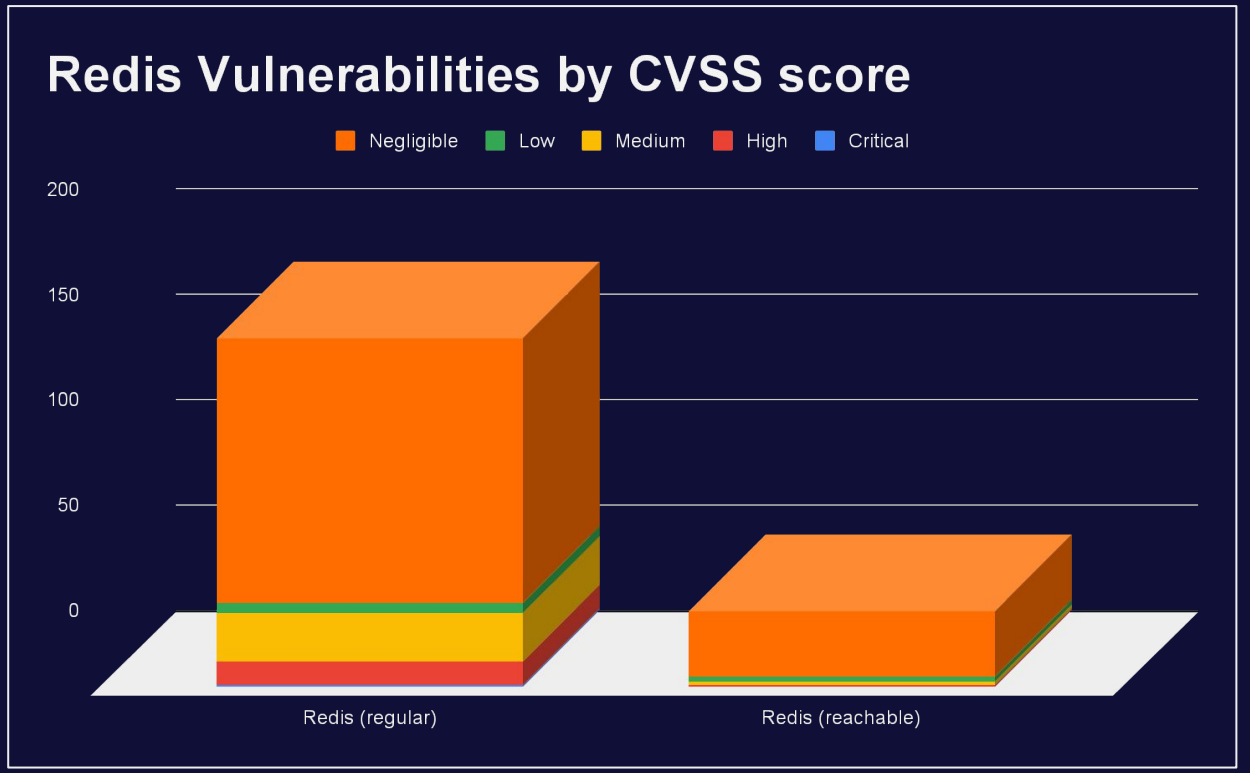
Image source: www.first.org

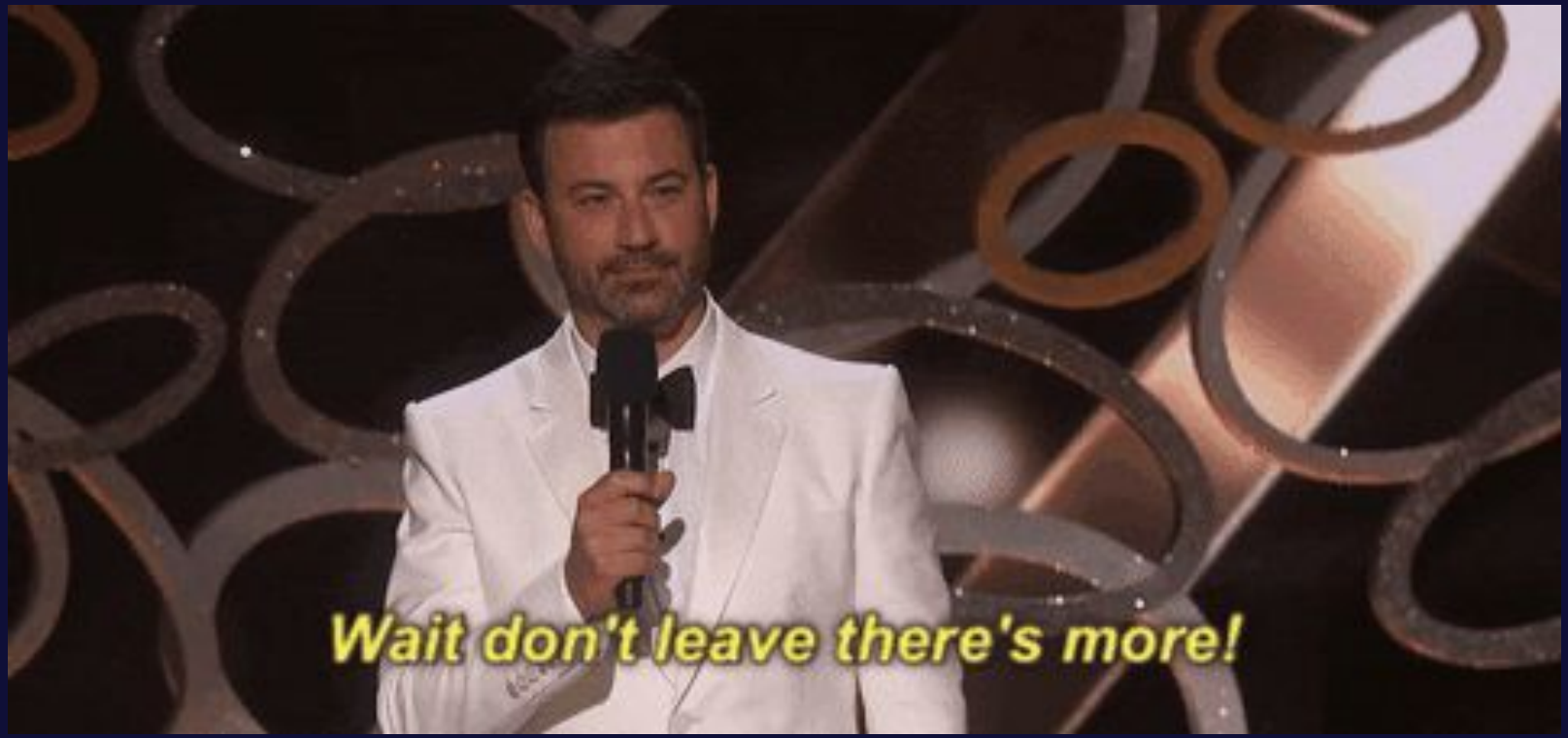
/Introducing Reachability_

- AKA “Relevancy”
- Vulnerable software component is loaded into the memory
- Not loaded, cannot be exploited

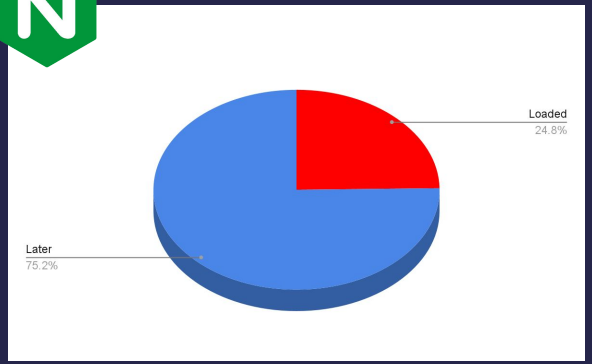
/Research subjects_

/Consider Redis_

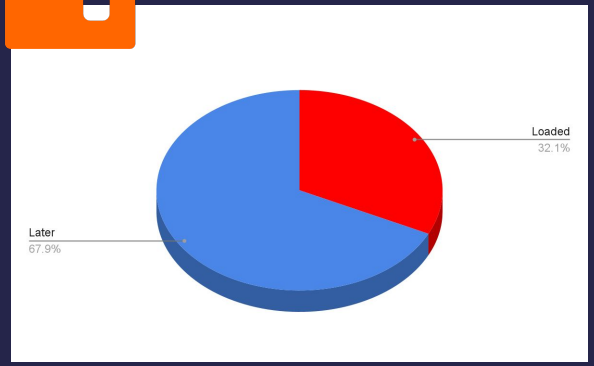



Wait don't leave there's more!

/Additional results_

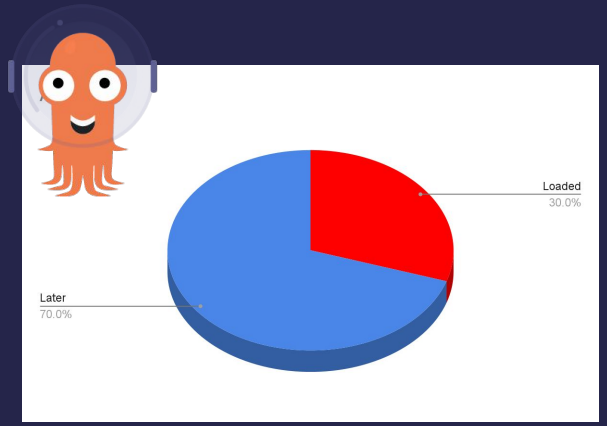


Only 25%
reachable CVEs

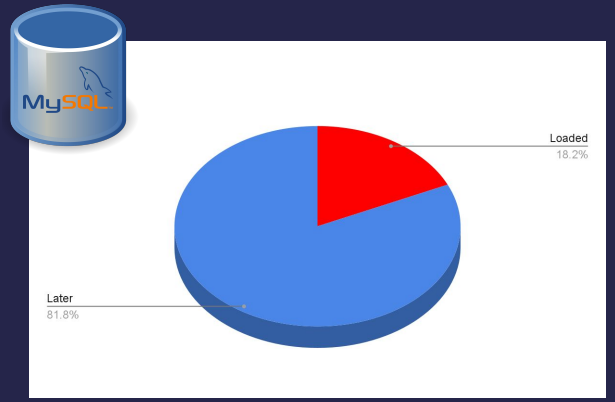


Less than a third
reachable CVEs

/Additional results_



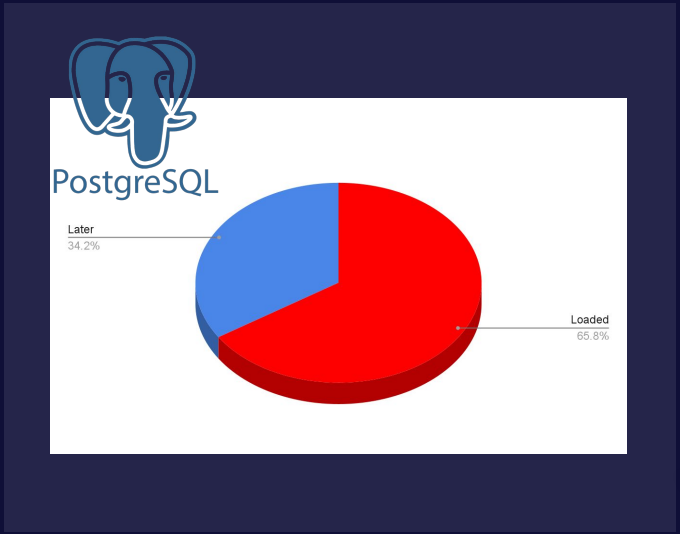
Less than half
reachable CVEs

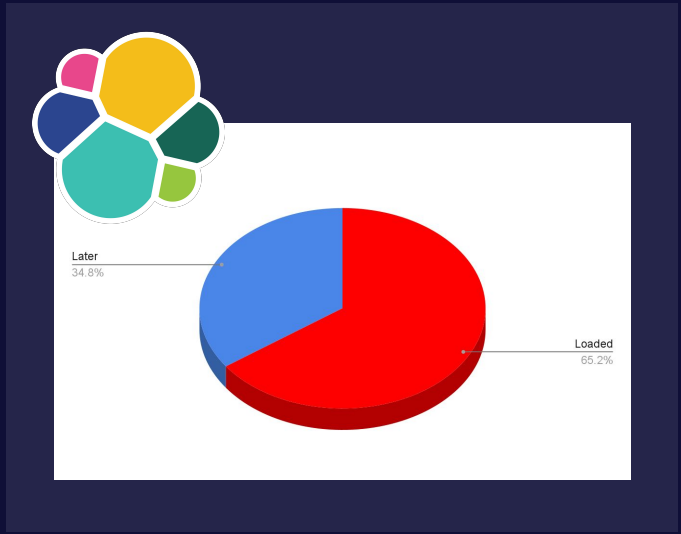


Less than 20%
reachable CVEs


CAUTION
QUARANTINE
AREA
I THINK IT'S TIME
FOR REALITY CHECK

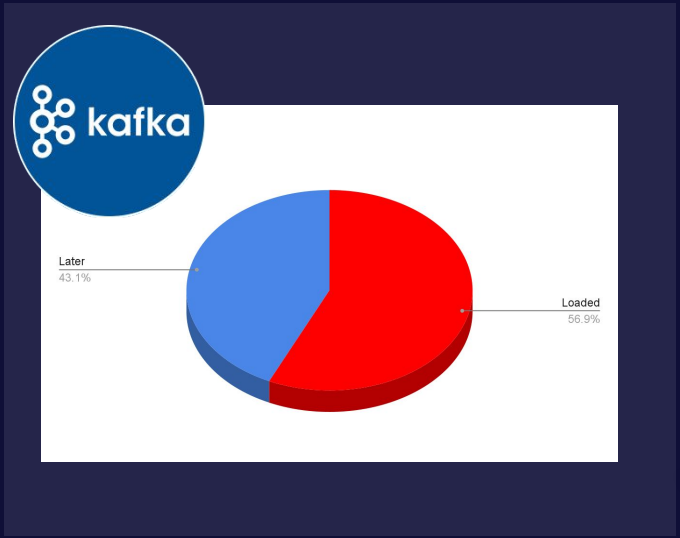
/Additional results_

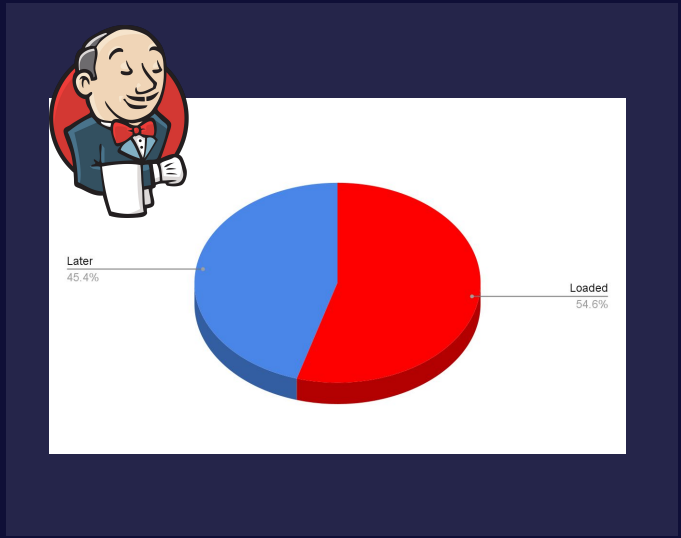




Less than 2/3 reachable CVEs

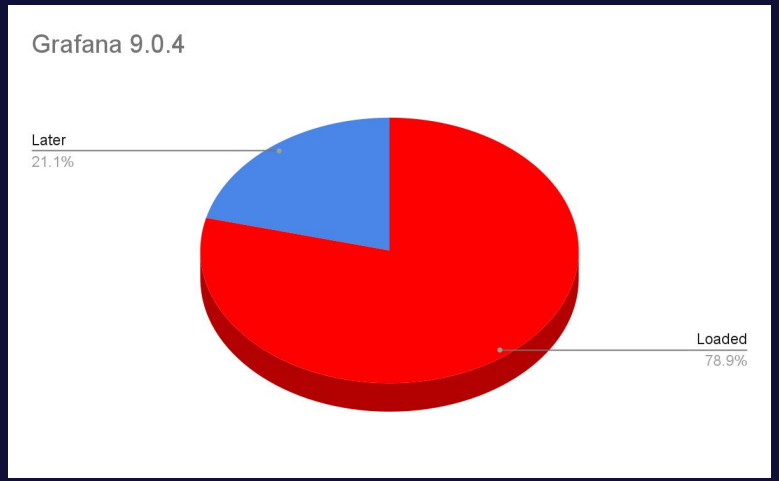
/Additional results_



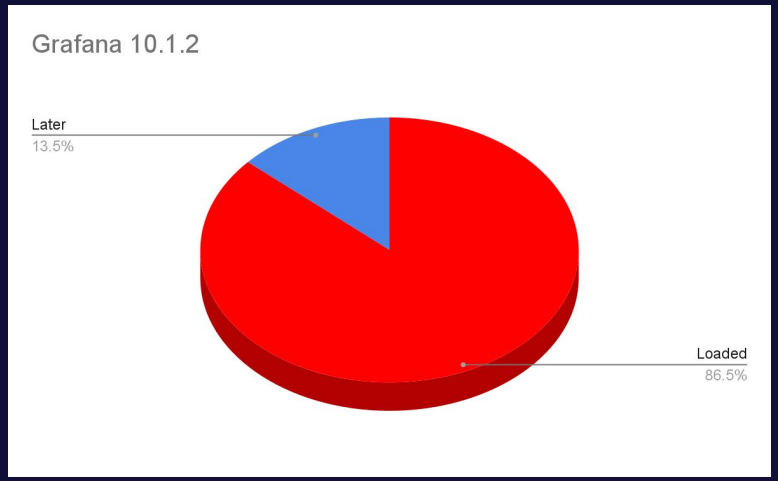


Less than 60% reachable CVEs

/The case of Grafana_

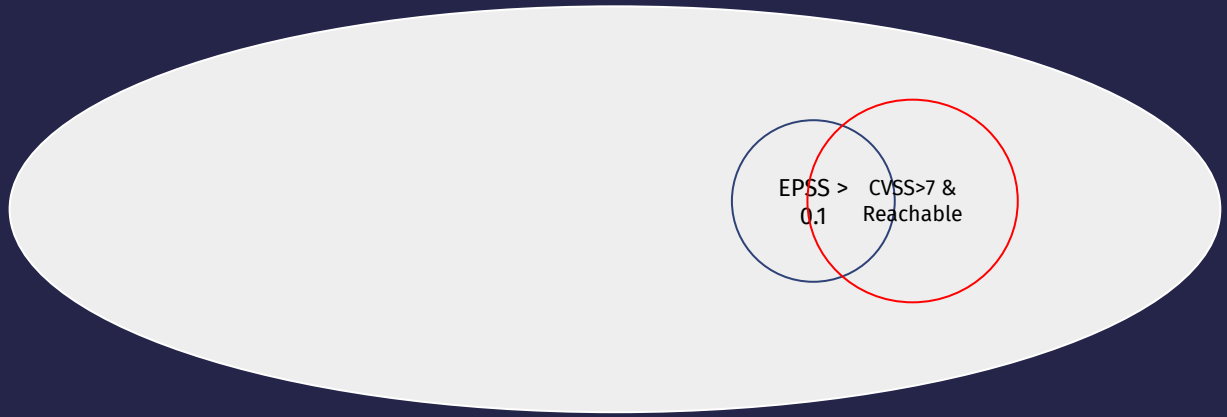


May



October

/Reachability_n_EPSS_

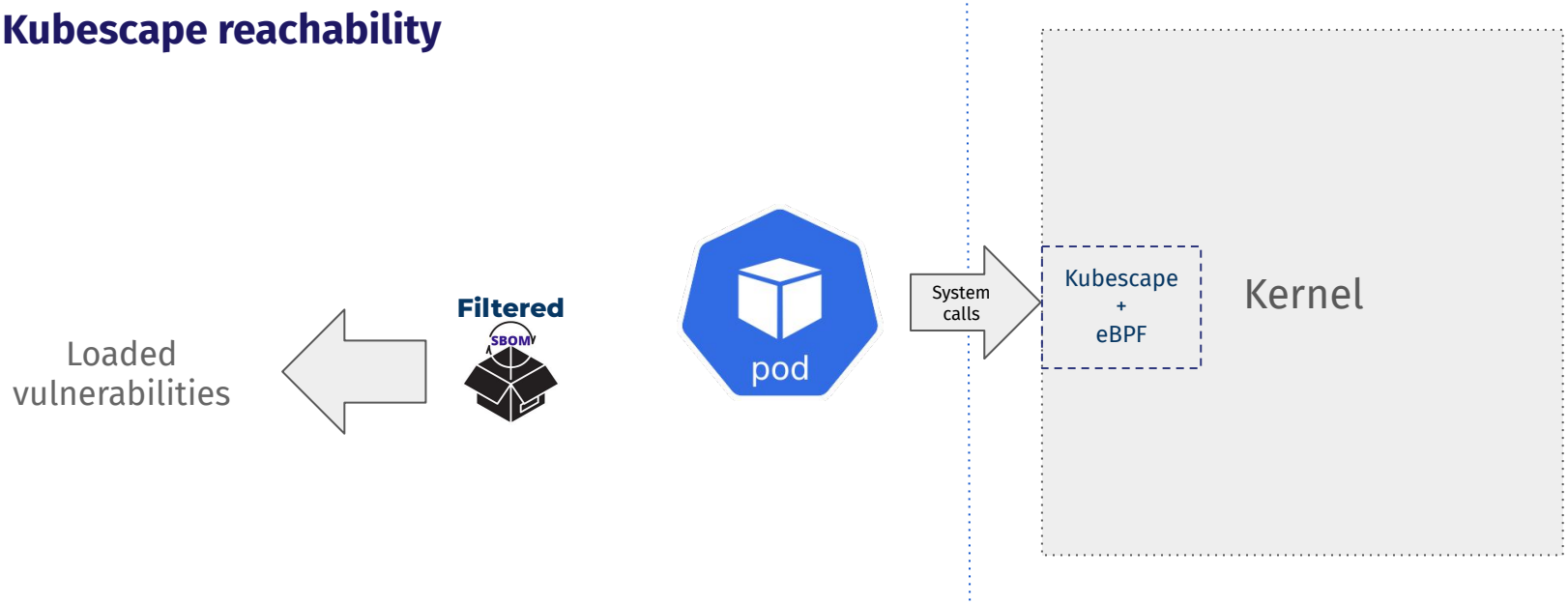


48% of EPSS>0.1 not reachable

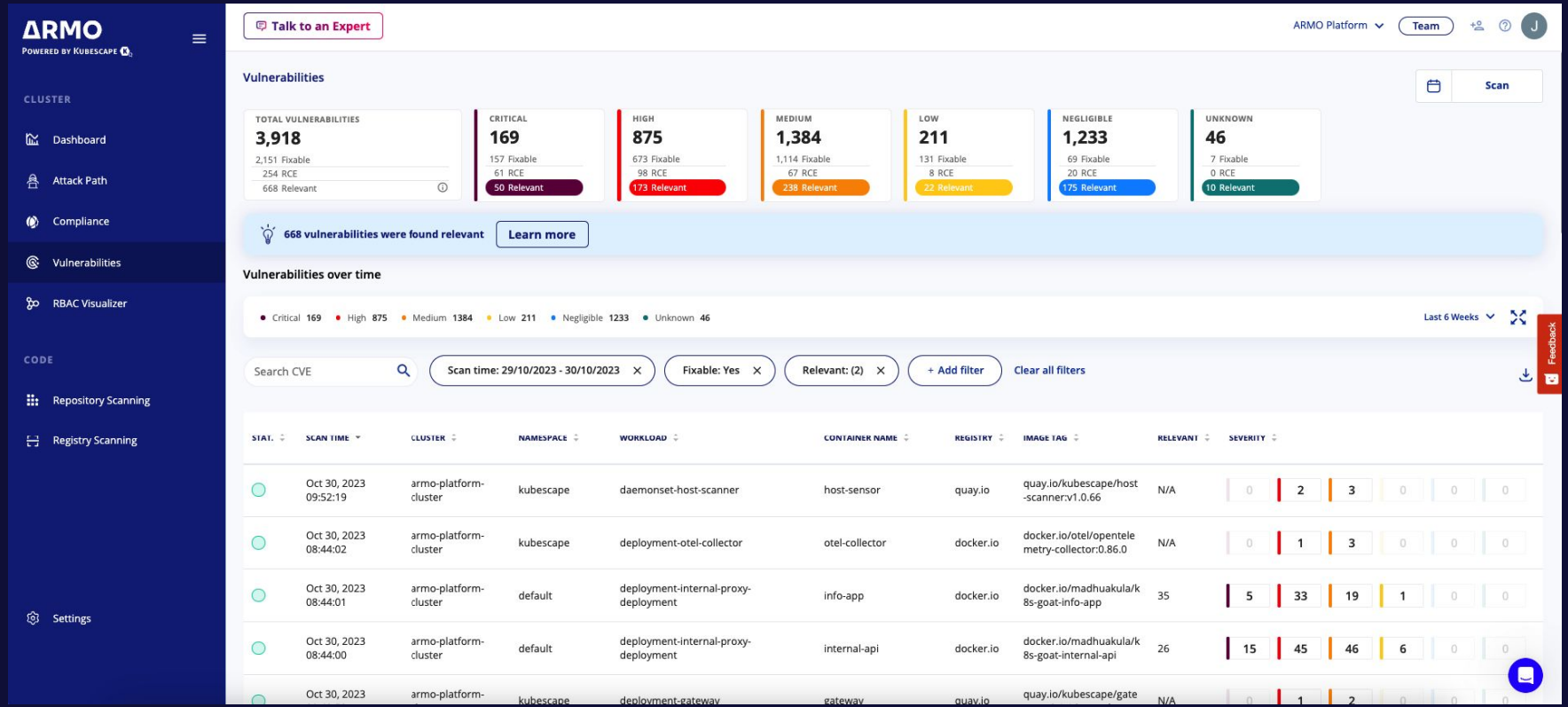
/kubescape-vuln-filter_

Kubescape

Kubescape reachability



/ARMO platform (powered by Kubescape) > Relevant CVEs



/Conclusion_

Using public images exposes you to vulnerabilities

The results of vulnerability scans may cause CVE Shock

Reachable vulnerabilities point to the small subset that should be addressed first

ARMO

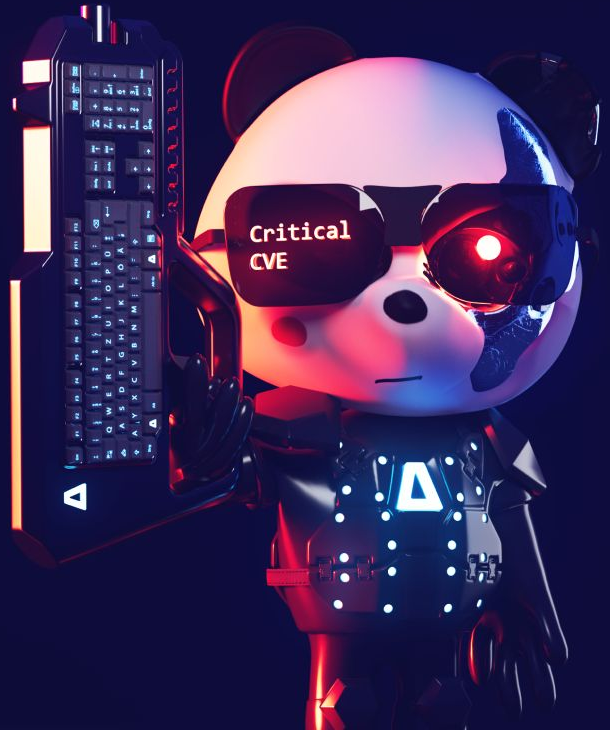
The Makers of Kubescape

Hasta la vista, CVE

Interested in becoming a K8s CVE terminator?

Come and meet us at ARMO booth F12

There's cool swag waiting for you...



_Terminate your most relevant CVEs, now />

Thank you_

ARMO

Kubescape