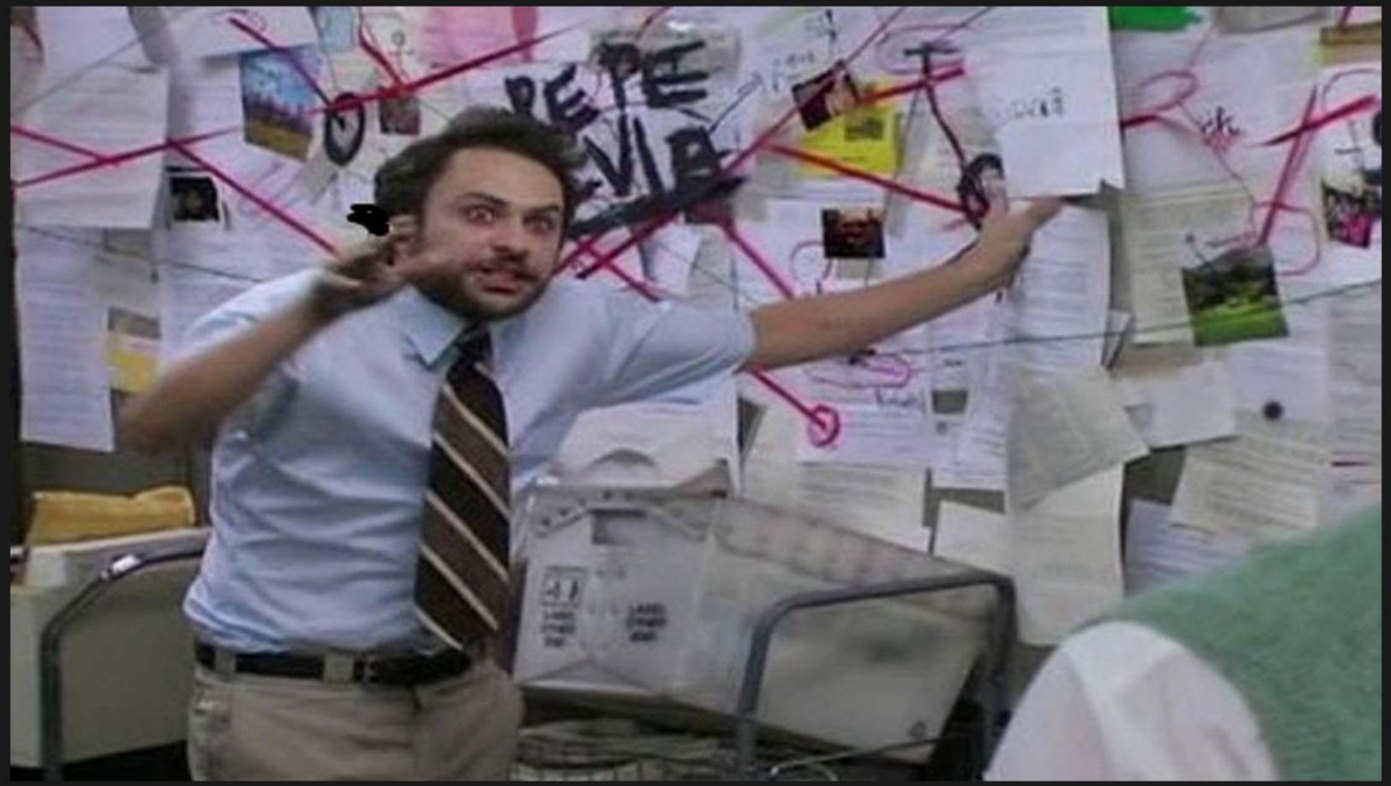
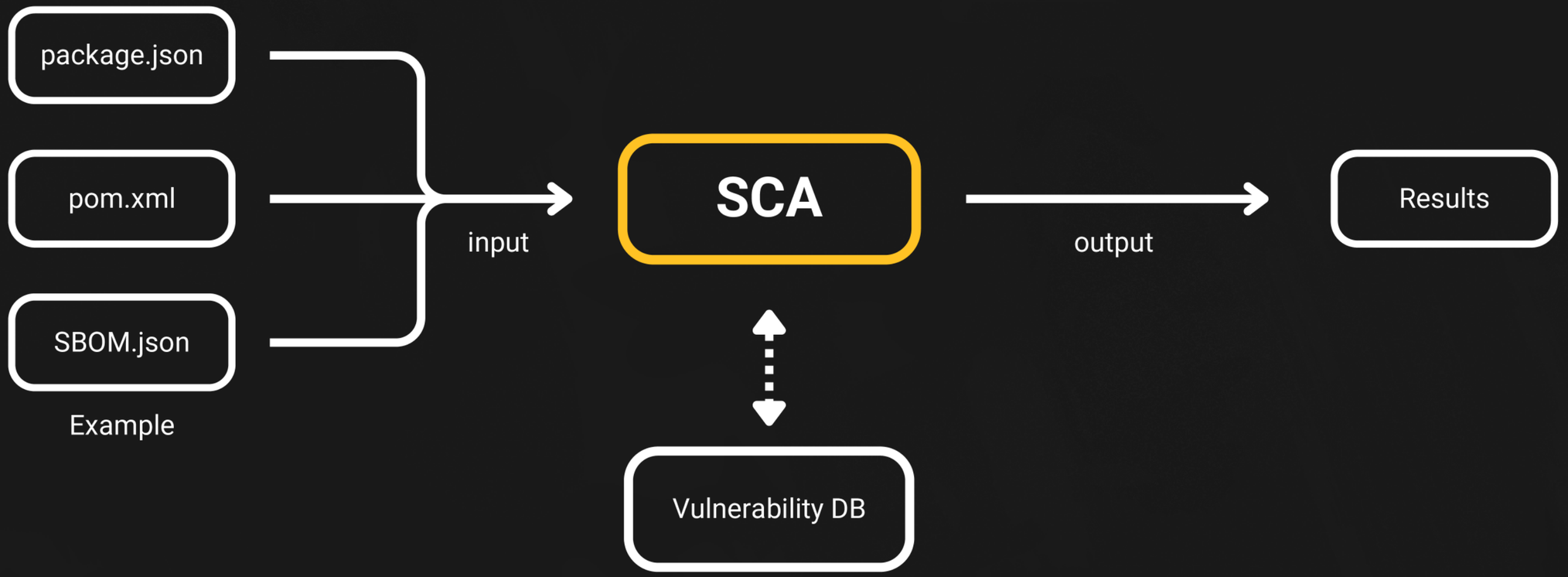
Priorisation des résultats des SCA avec EPSS

Introduction aux SCA



Introduction aux SCA



Introduction aux SCA

SCA

aqua
trivy

SCA

- Identification des dépendances vulnérables (CVE, GHSA, ...)
- Vérification de la conformité des licences des composants tiers

- Tous les outils peuvent détecter des vulnérabilités qui ne sont pas nécessairement exploitables dans le contexte spécifique de l'application
- La plupart des outils SCA se basent sur des bases de données publiques comme la NVD
- Peut générer une grande quantité de résultats

SCA

```
$ trivy fs --severity HIGH,CRITICAL --dependency-tree /path/to/your_node_project

package-lock.json (npm)
=======================
Total: 162 (HIGH: 112, CRITICAL: 50)
```

Introduction aux SCA

Ok, mais comment prioriser la remédiation ?

Introduction à l'EPSS

Introduction à l’EPSS

CVSS

CVSS évalue la gravité d'une vulnérabilité en se basant sur son impact potentiel et la complexité d'une attaque.

EPSS

L'EPSS est conçu pour combler les lacunes du CVSS en tenant compte de la probabilité qu'une vulnérabilité soit exploitée dans un futur proche. Il fournit une approche plus pragmatique, orientée vers l'action, en évaluant le risque réel d'exploitation.

Cas d’utilisation de l’EPSS

- Priorisation des correctifs
- Réduction du temps de réponse
- Équilibrage des ressources

Limitation de l’EPSS

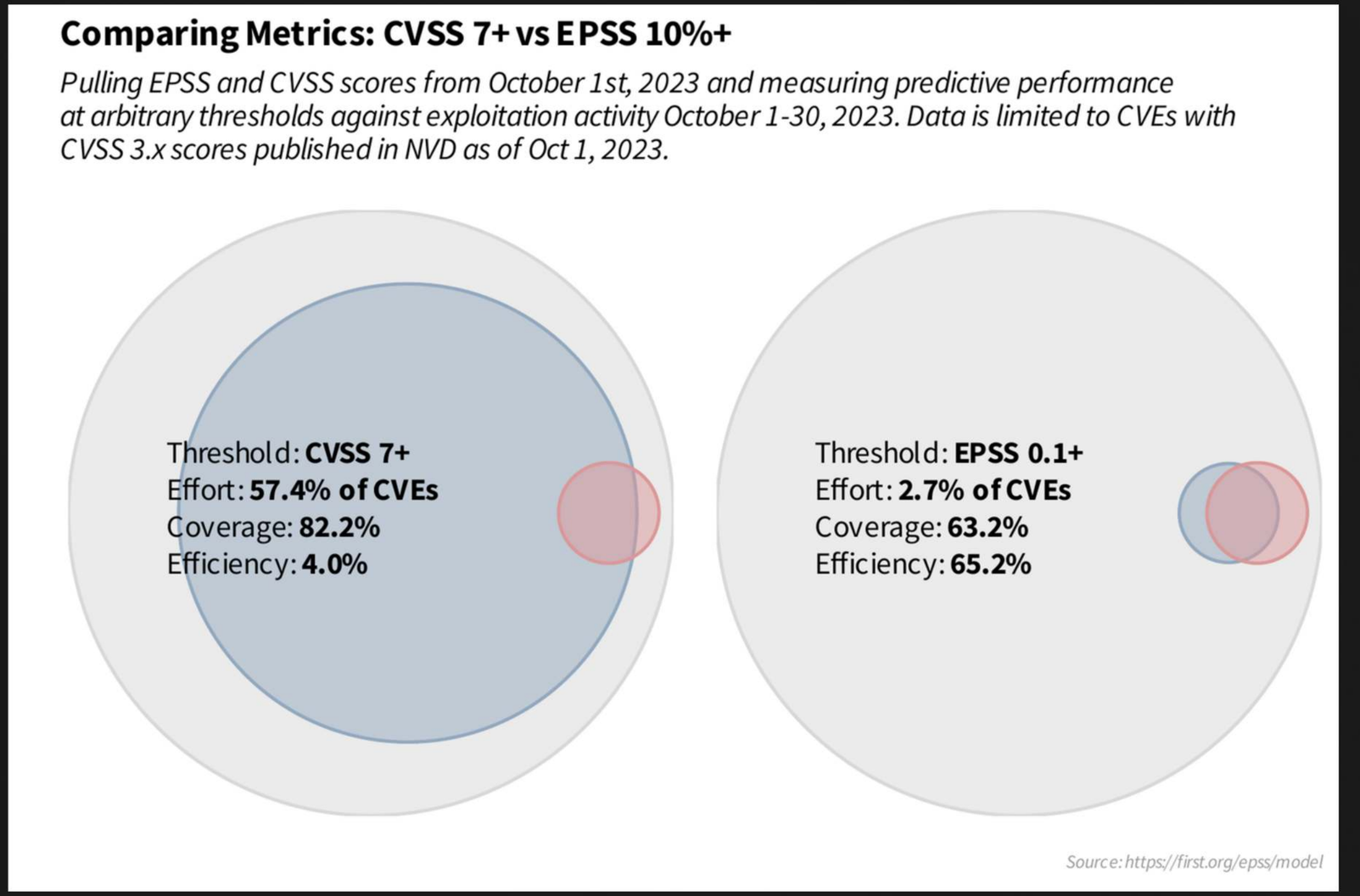
- Absence de certitude absolue
- Dépendance aux données publiques
- Variation du score dans le temps
- Dépend de disponibilité de l’API

Accès aux données EPSS

- Scores pour les CVE les plus récents :
  - `api.first.org/data/v1/epss`
- Score pour un seul CVE :
  - `api.first.org/data/v1/epss?cve=CVE-2022-27225`
- Scores pour plusieurs CVE (Batch) :
  - `api.first.org/data/v1/epss?cve=CVE-2022-27225,CVE-2022-27223,CVE-2022-27218`
- Documentation :
  - `https://www.first.org/epss/api`

Démonstration

Démonstration

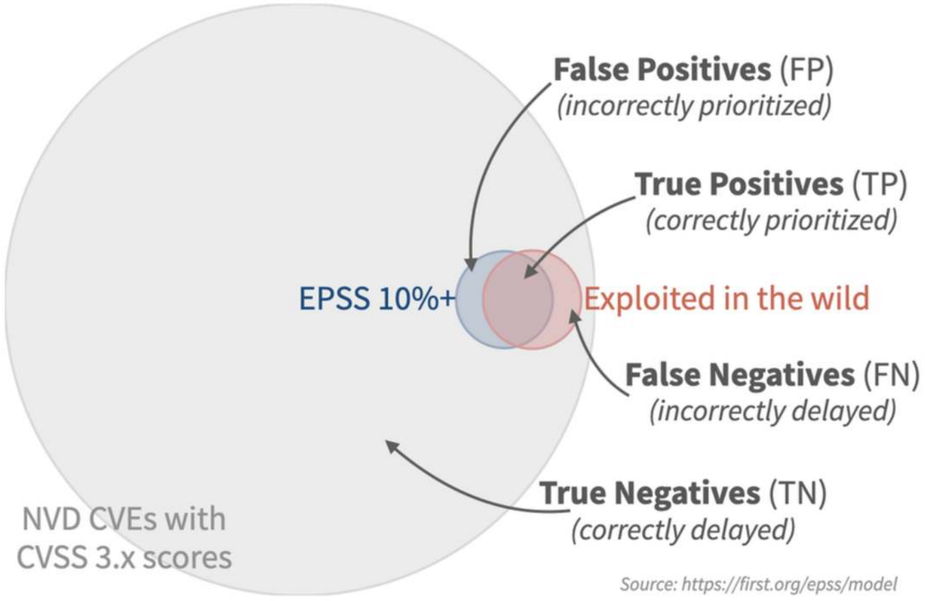


Démonstration

Performance: Remediating EPSS 10% and above

Looking at the performance of EPSS scores produced October 1st, 2023, comparing against the observed exploitation activity recorded from Oct 1st to Oct 30th, 2023. EPSS threshold is (arbitrarily) set at 10%.

Our Decision…	Exploitation Activity… Observed	Exploitation Activity… Not Observed
Remediate (EPSS 10%+)	2,435 (1.8%) *True Positives (TP)*	1,300 (0.9%) *False Positives (FP)*
Delay (< EPSS 10%)	1,417 (1%) *False Negatives (FN)*	134,321 (96.3%) *True Negatives (TN)*



Allez plus loin

- Excellent blog parlant de l’EPSS :
  - riskbasedprioritization.github.io/epss/Introduction_to_EPSS/
- Projet open source pour l’analyse de résultat :
  - TrivySummary de EdgewareRoad