

4,2 facteurs de succès d'un déploiement DevSecOPS

OWASP France – Bordeaux

22 Février 2023

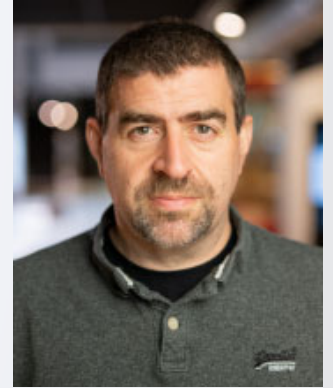
Sébastien Gioria

Agenda

- Contexte
- 4 facteurs de succès
 - Les équipes
 - Les outils
 - Les processus
 - Les indicateurs
- Et au final...

Me

- <https://www.linkedin.com/in/gioria/>
- @SPoint
- DevSecOPS Officer @Lectra;
- OWASP member (depuis 2006)



• R&D Lectra in a nutshell

12%+ Devoted to R&D investment
of revenues

LECTRA

Empowering customers through industrial intelligence

+ 330 people (Cestas,
Madrid)

RETIEWS

+ 30 people (Bruxelles,
Bucharest)

KUBiX

+ 10 people (Vicenza, Italy)

GEMINI

a LECTRA company

+ 40 people (Romania)

neteven

a LECTRA company

+ 15 people (Paris)



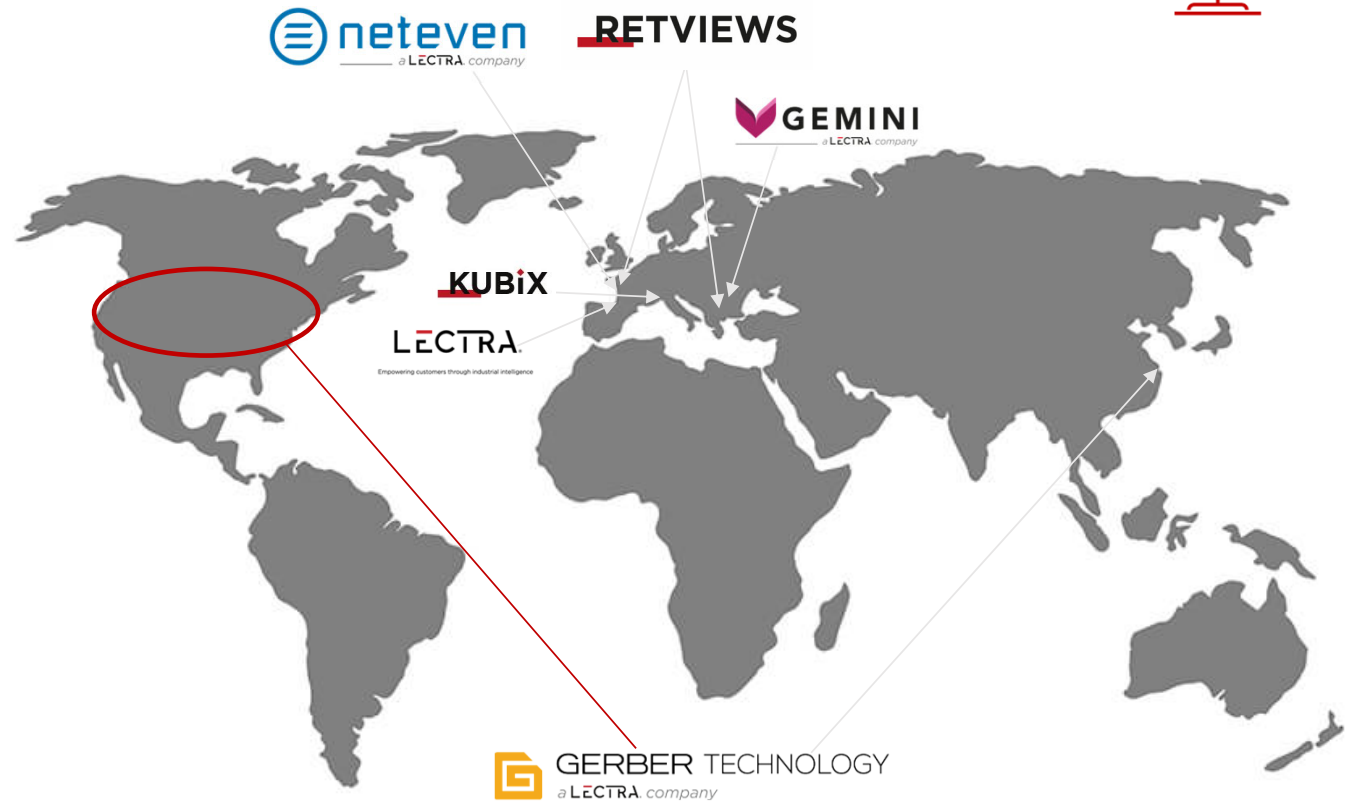
GERBER TECHNOLOGY

a LECTRA company

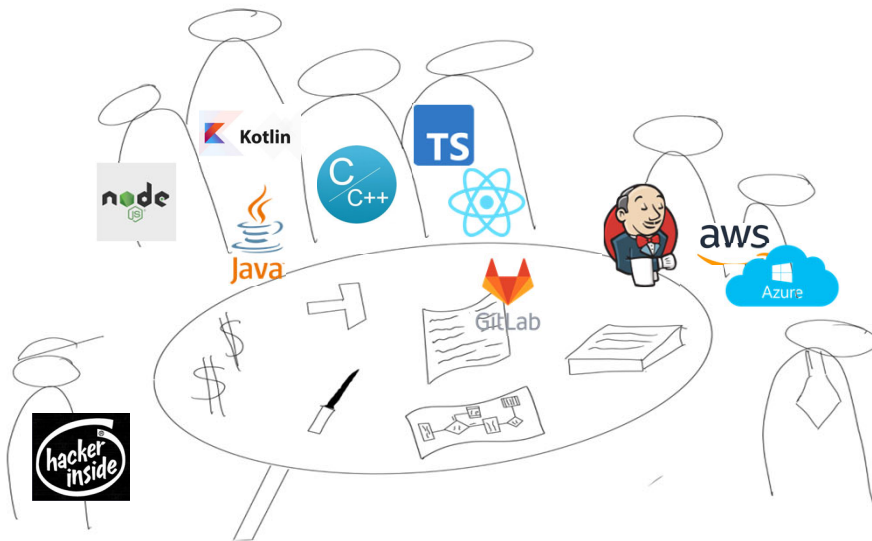
+ 75 people
(USA+China) + 65
Outsourced resources



500
people



Les équipes



- ❑ Avant :
 - Les outils
 - Les langages
 - Les spécificités
- ❑ Pendant
 - Créer du lien
 - S'adapter

Choisir les bons outils



- DAST
- SAST
- Scanner réseaux
- Analyse des licences
- Ne pas hésiter à multiplier les analyseurs....

```
post {
  always {
    archiveArtifacts allowEmptyArchive: true, artifacts: 'sources/*.sarif'
  }
}

stage("Static Security Tests Semgrep") {
  steps {
    step("sources") {
      semgrep(lang: "csharp")
    }
  }
}

stage("Dependency") {
  steps {
    dependencytrack()
  }
}

stage("SecretFinder") {
  steps {
    step("sources") {
      gitLeaks()
    }
  }
}

/*stage ("Sonar Scan") {
```

- Dashboard
- Products
- Engagements
- Findings
- Components
- Endpoints
- Reports
- Metrics
- Users
- Calendar
- Configuration
- Collapse Menu

275
Active Engagements

[View Engagement Details](#)

1544
Last Seven Days

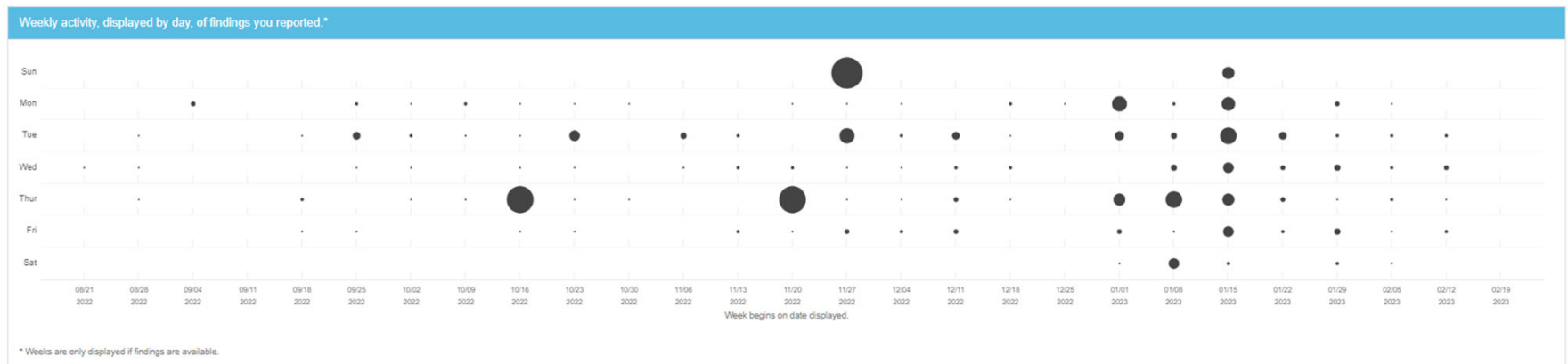
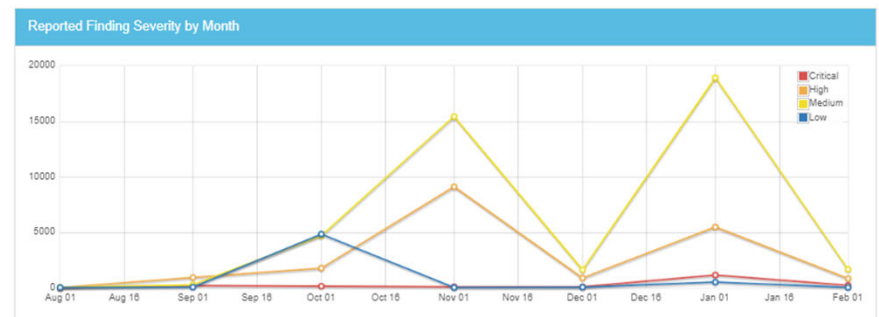
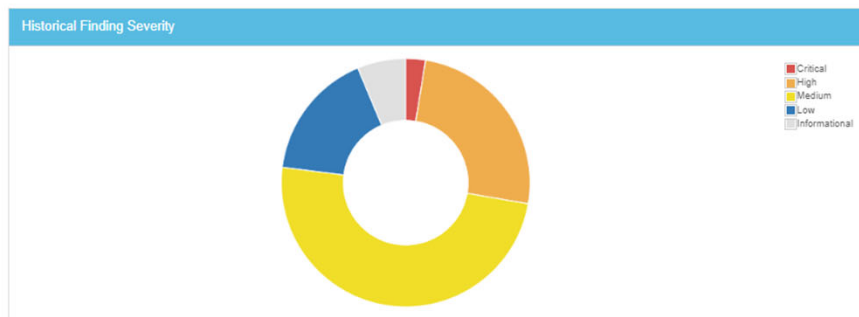
[View Finding Details](#)

3128
Closed In Last Seven Days

[View Finding Details](#)

0
Risk Accepted In Last Seven Days

[View Finding Details](#)



Description

There is no description.

Tests (4) Critical: 0, High: 8, Medium: 116, Low: 0, Info: 3, Total: 127 Active Findings

Showing entries 1 to 4 of 4

Page Size

Title / Type	Date	Lead	Total Findings	Active (Verified)	Mitigated	Duplicates	Notes	Reimports
Dependency Track Finding Packaging Format (FPF) Export	Oct. 6, 2022 - Feb. 19, 2023		8	4 (4)	4	0		57
ORT evaluated model Importer	Oct. 6, 2022 - Feb. 16, 2023		2	1 (1)	1	0		160
semgrep Scan (SARIF)	Nov. 24, 2022 - Feb. 19, 2023		260	120 (120)	140	0		64
SonarQube API Import	Oct. 6, 2022 - Feb. 19, 2023		2	2 (0)	0	0		101

Showing entries 1 to 4 of 4

Page Size

It's Best Practice to Explicitly Pass Props to an HTML Component Rather Than Use the Spread Operator. The Spread Operator Risks Passing Invalid [...] Last Reviewed Jan. 5, 2023 by Auto Mation (automation), Last Status Update Jan. 12, 2023, Created Jan. 5, 2023



ID	Severity	SLA	Status	Type	Date discovered	Age	Reporter	Date Mitigated	Mitigated By	CWE	Vulnerability Id	Found by
1749250	Medium	83	Inactive, Verified, Mitigated	Static	Jan. 5, 2023	7 days	Auto Mation (automation)	Jan. 12, 2023, midnight	Auto Mation (automation)			semgrep Scan (SARIF)

Location

Line Number

11

Similar Findings (2)



Description



Result message: It's best practice to explicitly pass props to an HTML component rather than use the spread operator. The spread operator risks passing invalid HTML props to an HTML element, which can cause console warnings or worse, give malicious actors a way to inject unexpected attributes.

Snippet:

```
<List component="div" disablePadding {...others}>
```

Rule name: semgrep-rules.typescript.react.best-practice.react-props-spreading

Mitigation



Impact



Steps To Reproduce



Severity Justification



References

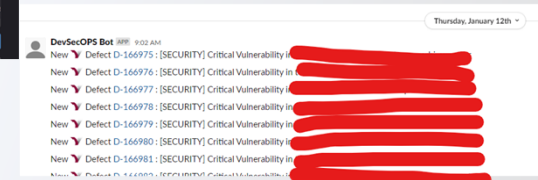
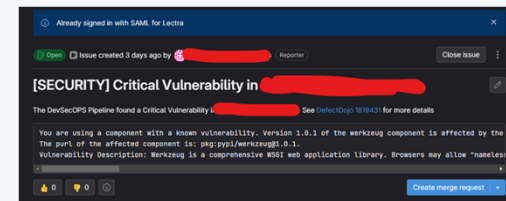
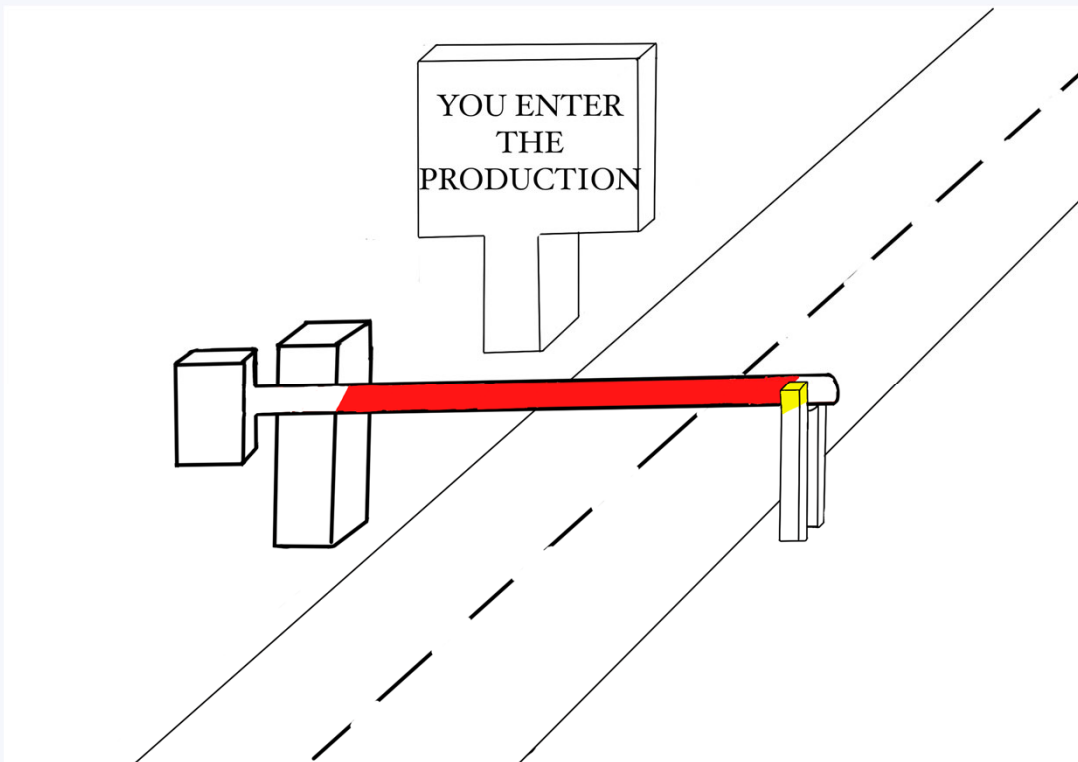


Notes

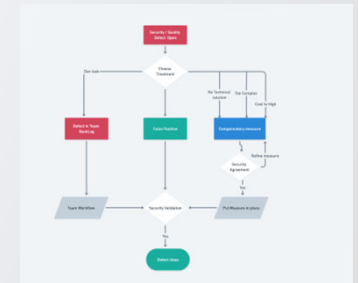


S'insérer dans les processus de développement

- Ne pas ajouter d'outils sécurité inutiles

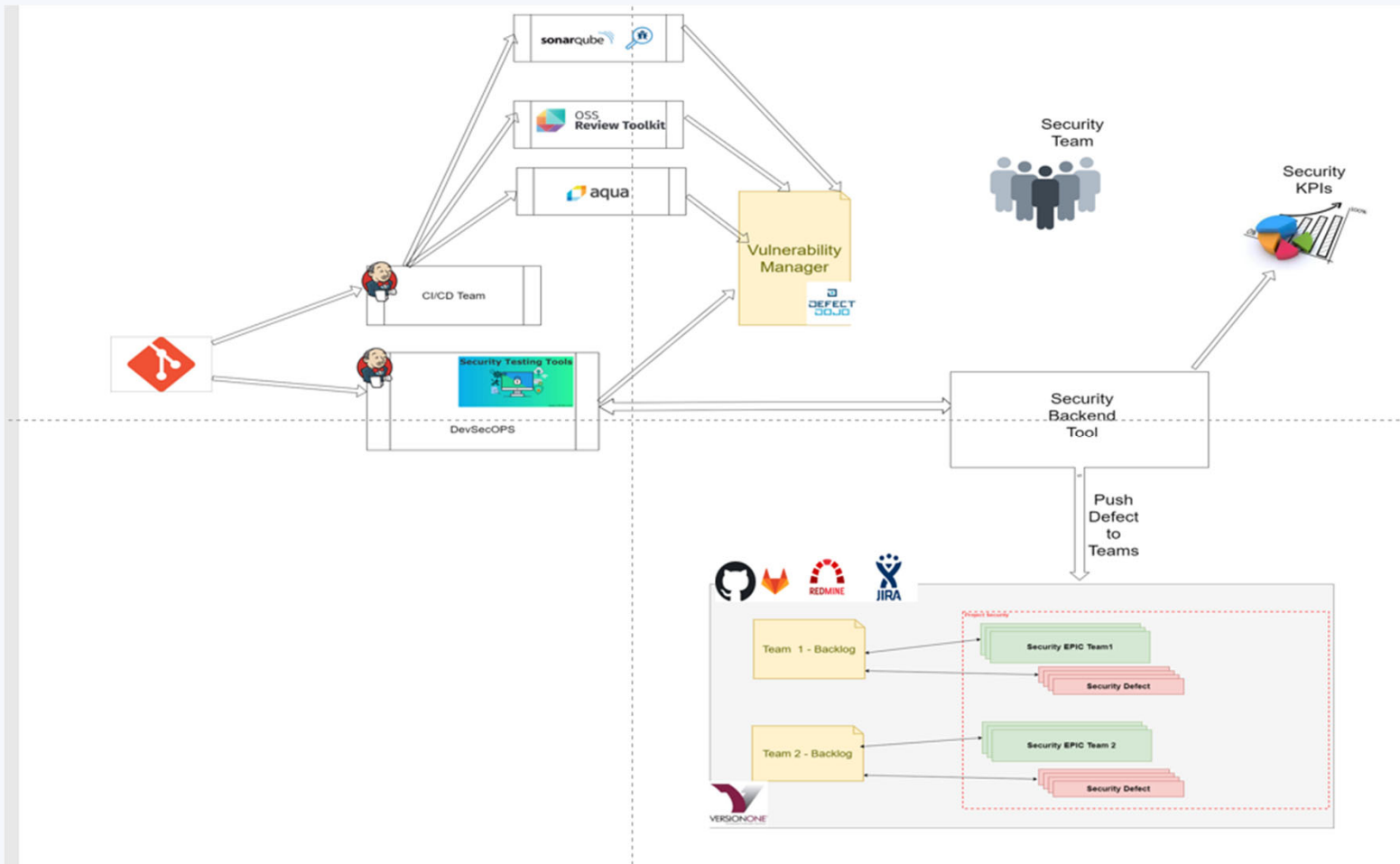


- Définir le processus de correction



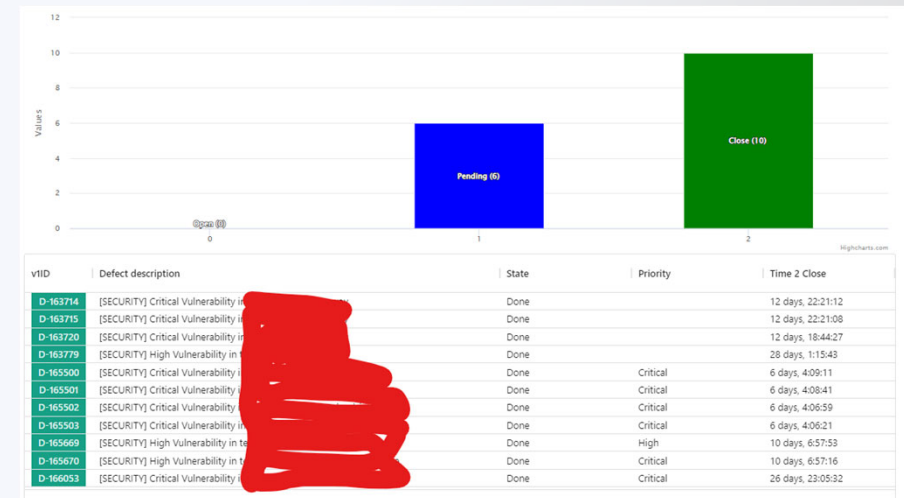
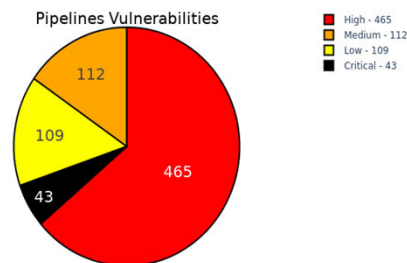
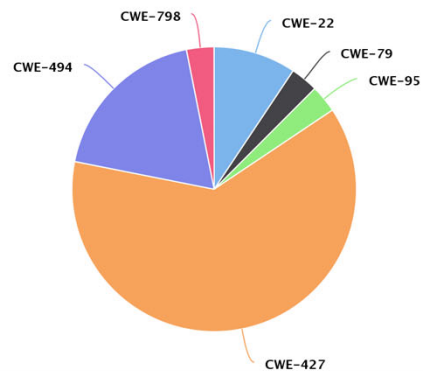
- **Le Mythe de la gate**

S'insérer dans les processus de développement



Produire les bons indicateurs (pour les équipes)

Project ID	Project	Vulnerabilities
244	[REDACTED]	<div> <div>🔔 15</div> <div>❌ 42</div> <div>⚠️ 64</div> <div>😊 0</div> <div>🔍 26</div> </div>
248	[REDACTED]	<div> <div>🔔 2</div> <div>❌ 7</div> <div>⚠️ 24</div> <div>😊 0</div> <div>🔍 6</div> </div>
249	[REDACTED]	<div> <div>🔔 3</div> <div>❌ 7</div> <div>⚠️ 23</div> <div>😊 0</div> <div>🔍 9</div> </div>
250	[REDACTED]	<div> <div>🔔 0</div> <div>❌ 0</div> <div>⚠️ 0</div> <div>😊 0</div> <div>🔍 0</div> </div>



Produire les bons indicateurs (pour le suivi exec)

