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

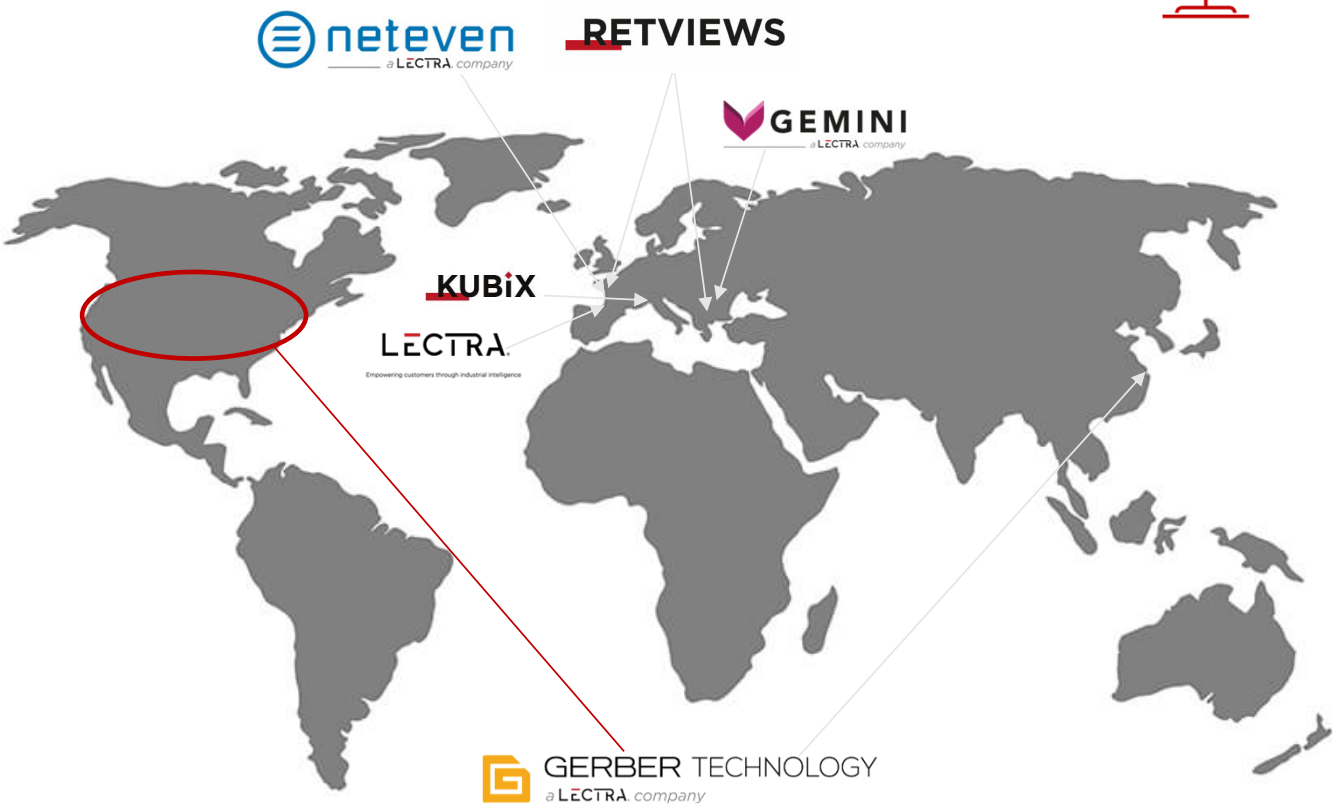
- https://www.linkedin.com/in/gioria/
- @SPoint
- DevSecOPS Officer @Lectra;
- OWASP member (depuis 2006)

R&D Lectra in a nutshell

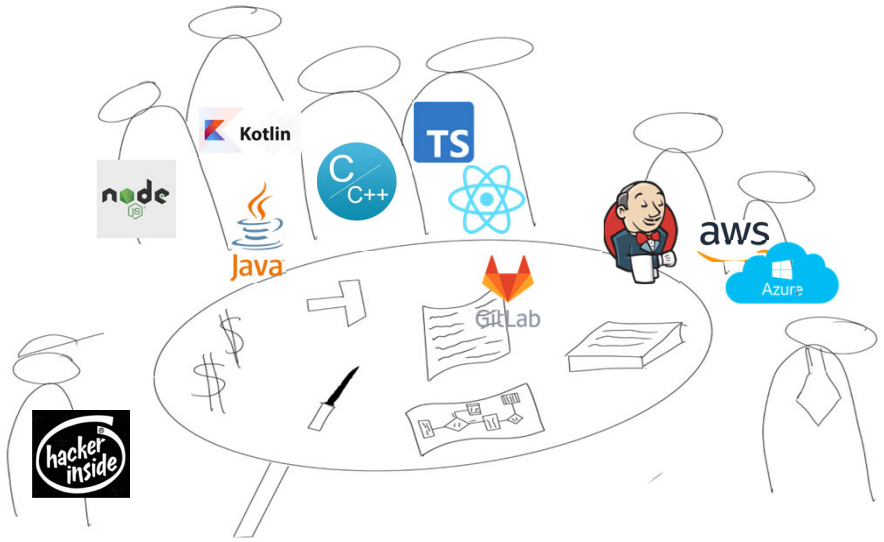
12%+ of revenues — Devoted to R&D investment

500 people

- LECTRA — Empowering customers through industrial intelligence — + 330 people (Cestas, Madrid)
- RETVIEWS — + 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



Les équipes

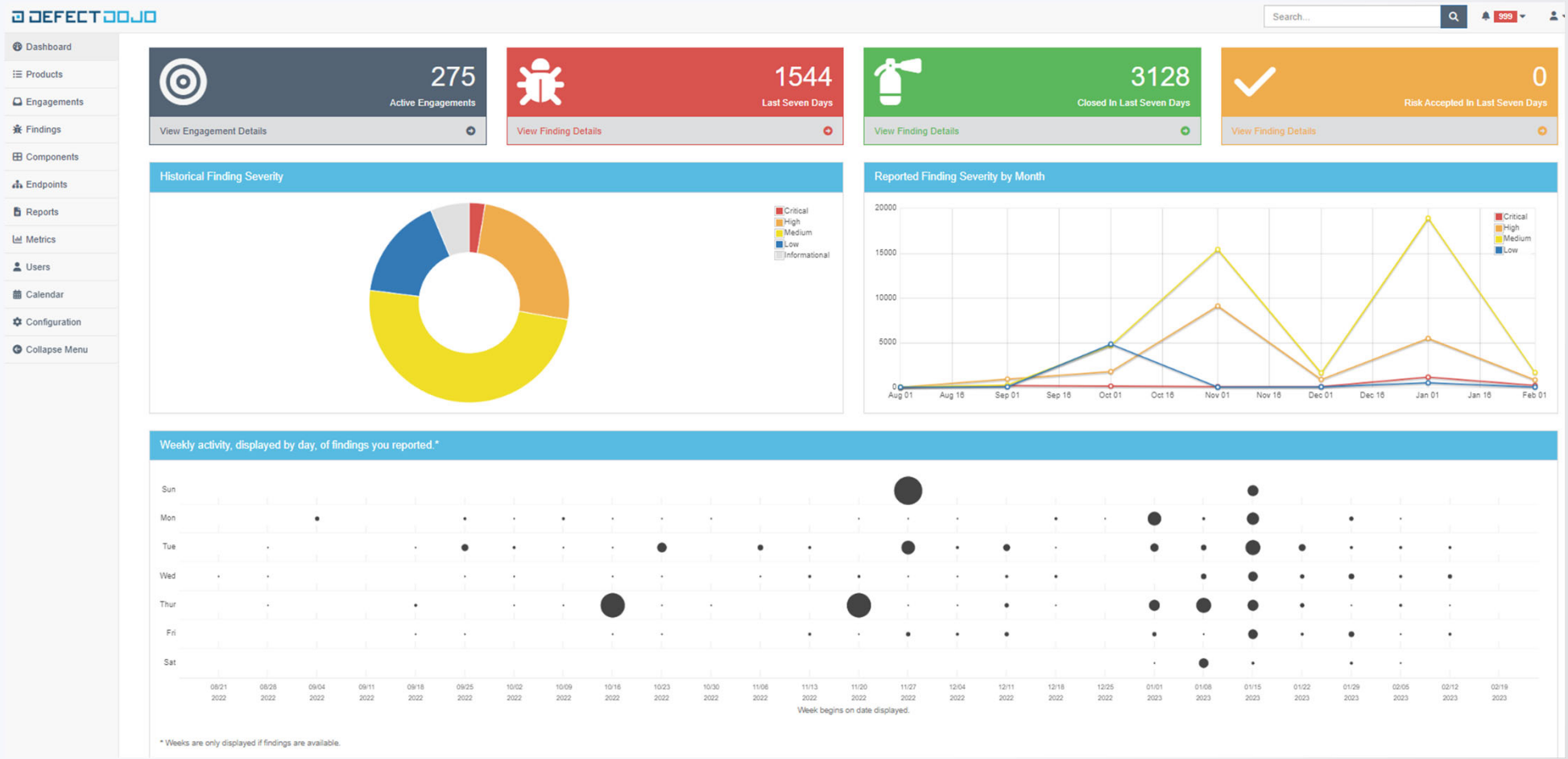


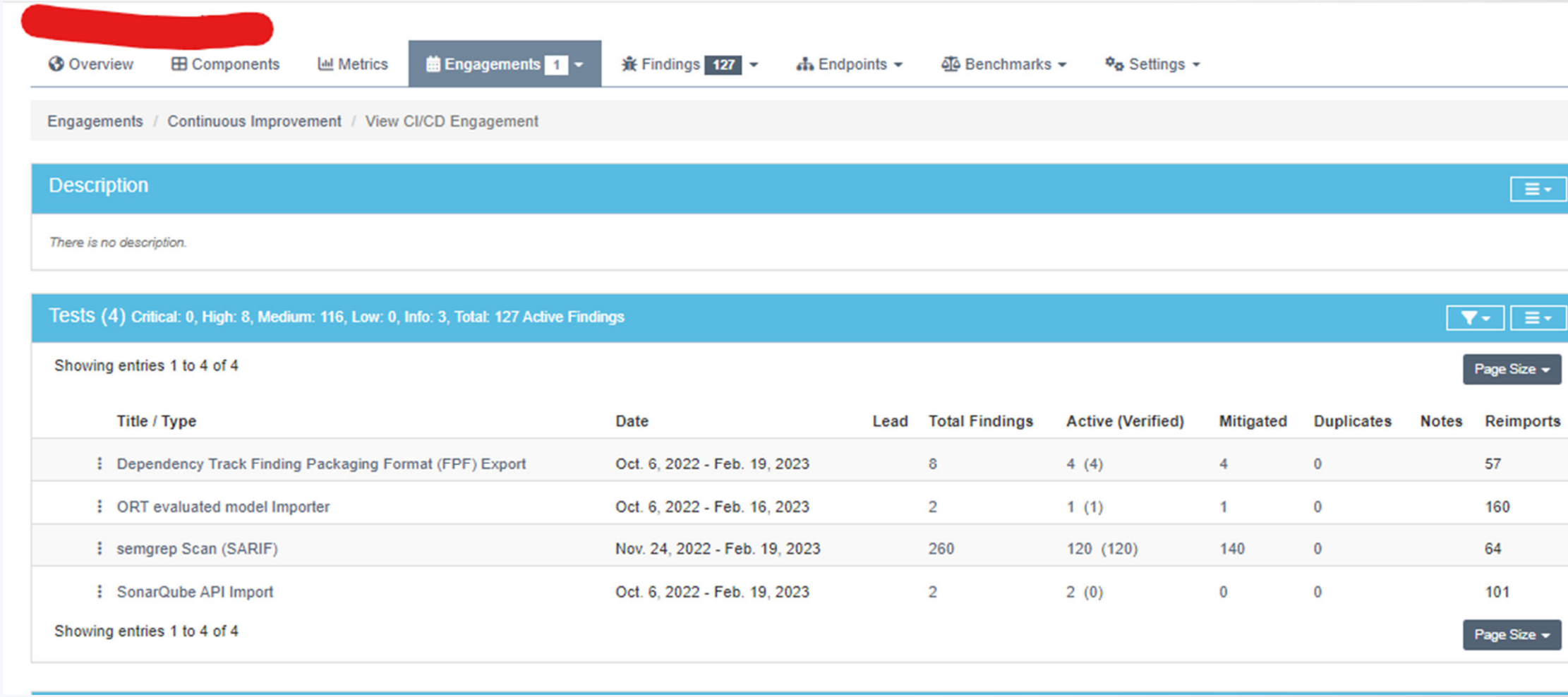
- Avant :
  - Les outils
  - Les langages
  - Les spécificités
- Pendant
  - Créer du lien
  - S’adapter

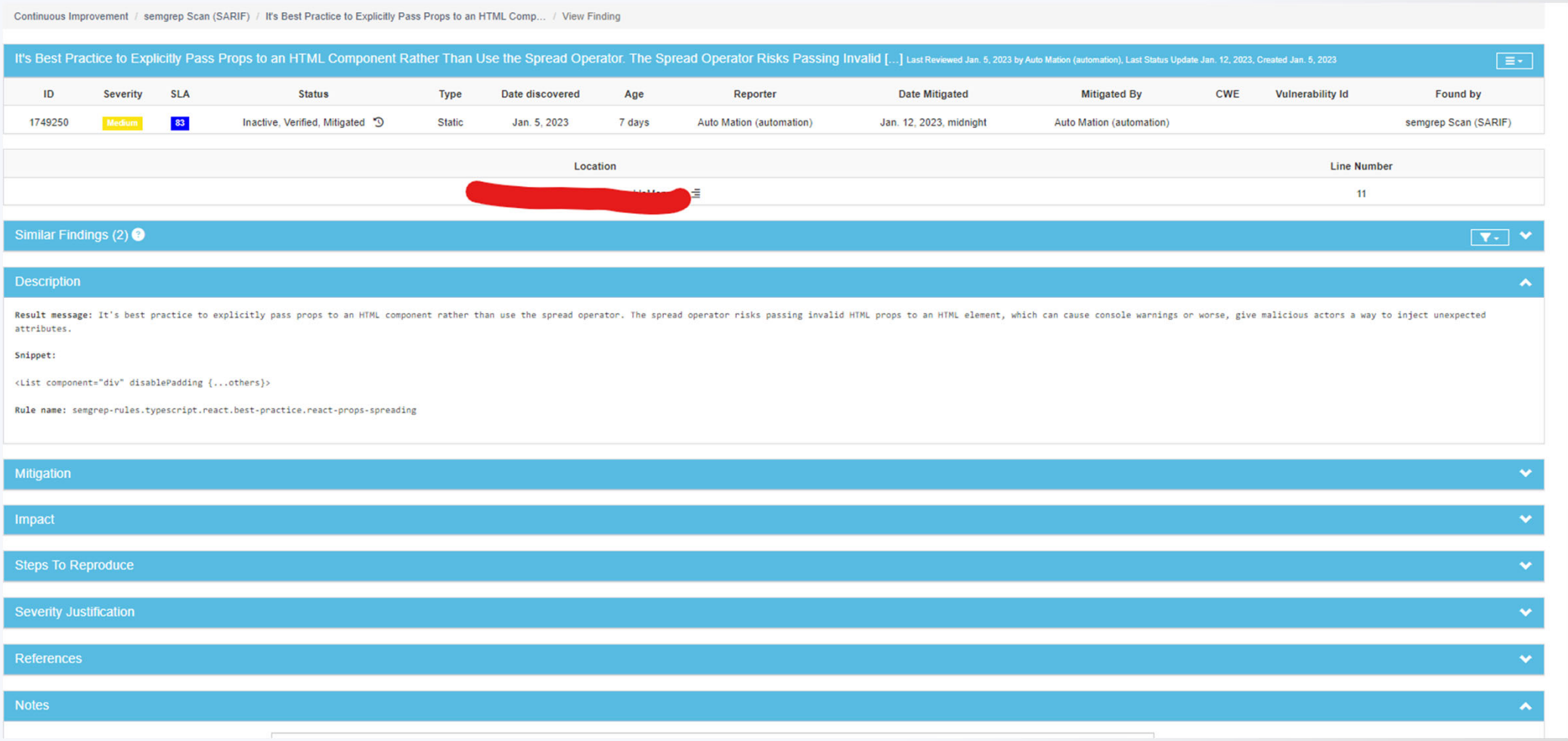
Choisir les bons outils

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

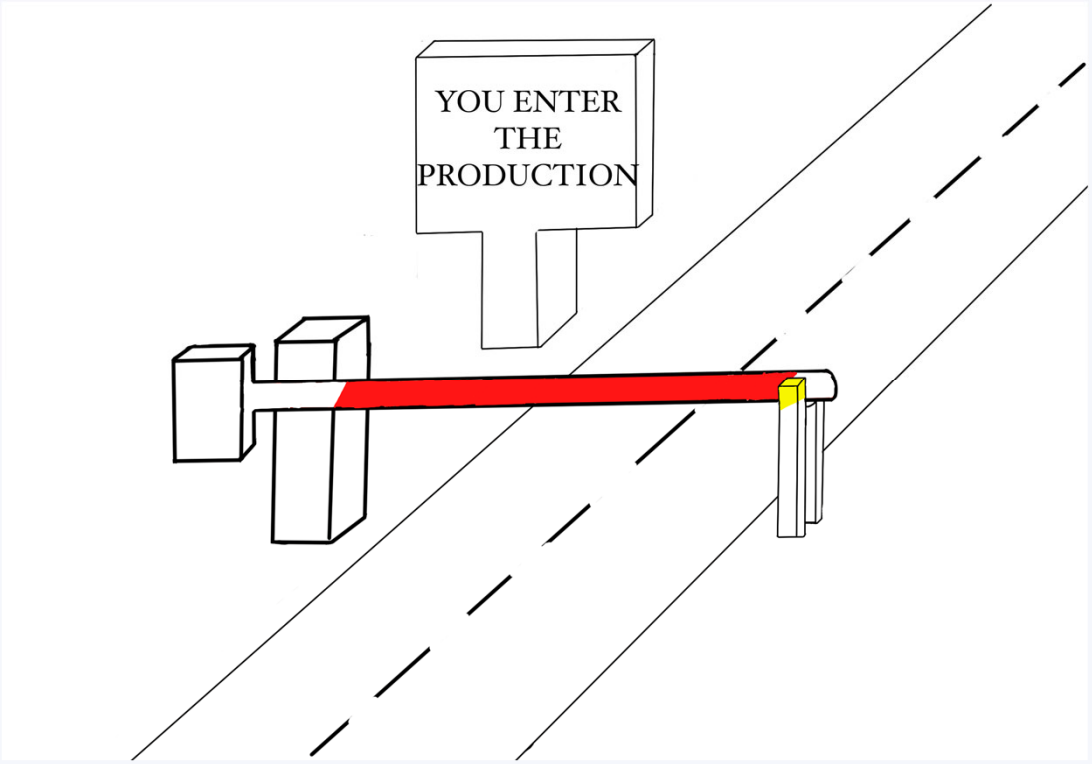
```
            post {
                always {
                    archiveArtifacts allowEmptyArchive: true, artifacts: 'sources/*.sarif'
                }
            }
        }
        stage("Static Security Tests Semgrep") {
            steps {
                dir("sources") {
                    semgrep(lang1: "csharp")
                }
            }
        }

        stage("Dependency") {
            steps {
                dependencytrack()
            }
        }
        stage("SecretFinder") {
            steps {
                dir("sources") {
                    gitleaks()
                }
            }
        }


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


DEFECTDOJO
Search...
999
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
Historical Finding Severity
Critical
High
Medium
Low
Informational
Reported Finding Severity by Month
20000
15000
10000
5000
0
Aug 01
Aug 16
Sep 01
Sep 16
Oct 01
Oct 16
Nov 01
Nov 16
Dec 01
Dec 16
Jan 01
Jan 16
Feb 01
Critical
High
Medium
Low
Weekly activity, displayed by day, of findings you reported.*
Sun
Mon
Tue
Wed
Thur
Fri
Sat
08/21 2022
08/28 2022
09/04 2022
09/11 2022
09/18 2022
09/25 2022
10/02 2022
10/09 2022
10/16 2022
10/23 2022
10/30 2022
11/06 2022
11/13 2022
11/20 2022
11/27 2022
12/04 2022
12/11 2022
12/18 2022
12/25 2022
01/01 2023
01/08 2023
01/15 2023
01/22 2023
01/29 2023
02/05 2023
02/12 2023
02/19 2023
Week begins on date displayed.
* Weeks are only displayed if findings are available.

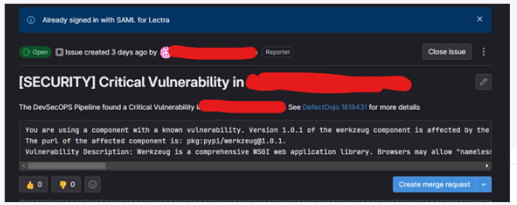

Overview
Components
Metrics
Engagements 1
Findings 127
Endpoints
Benchmarks
Settings
Engagements / Continuous Improvement / View CI/CD Engagement
Description
There is no description.
Tests (4) Critical: 0, High: 8, Medium: 116, Low: 0, Info: 3, Total: 127 Active Findings
Showing entries 1 to 4 of 4
Page 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

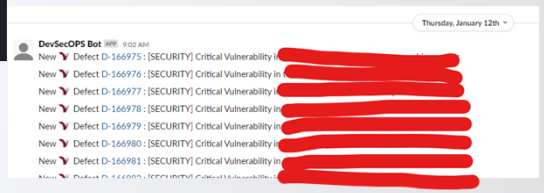

Continuous Improvement / semgrep Scan (SARIF) / It's Best Practice to Explicitly Pass Props to an HTML Comp... / View Finding
It's Best Practice to Explicitly Pass Props to an HTML Component Rather Than Use the Spread Operator. The Spread Operator Risks Passing Invalid [...] Last Reviewed Jan. 5, 2023 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

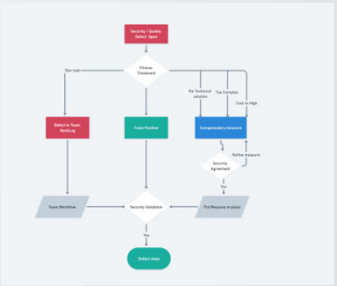


- Ne pas ajouter d’outils sécurité inutiles



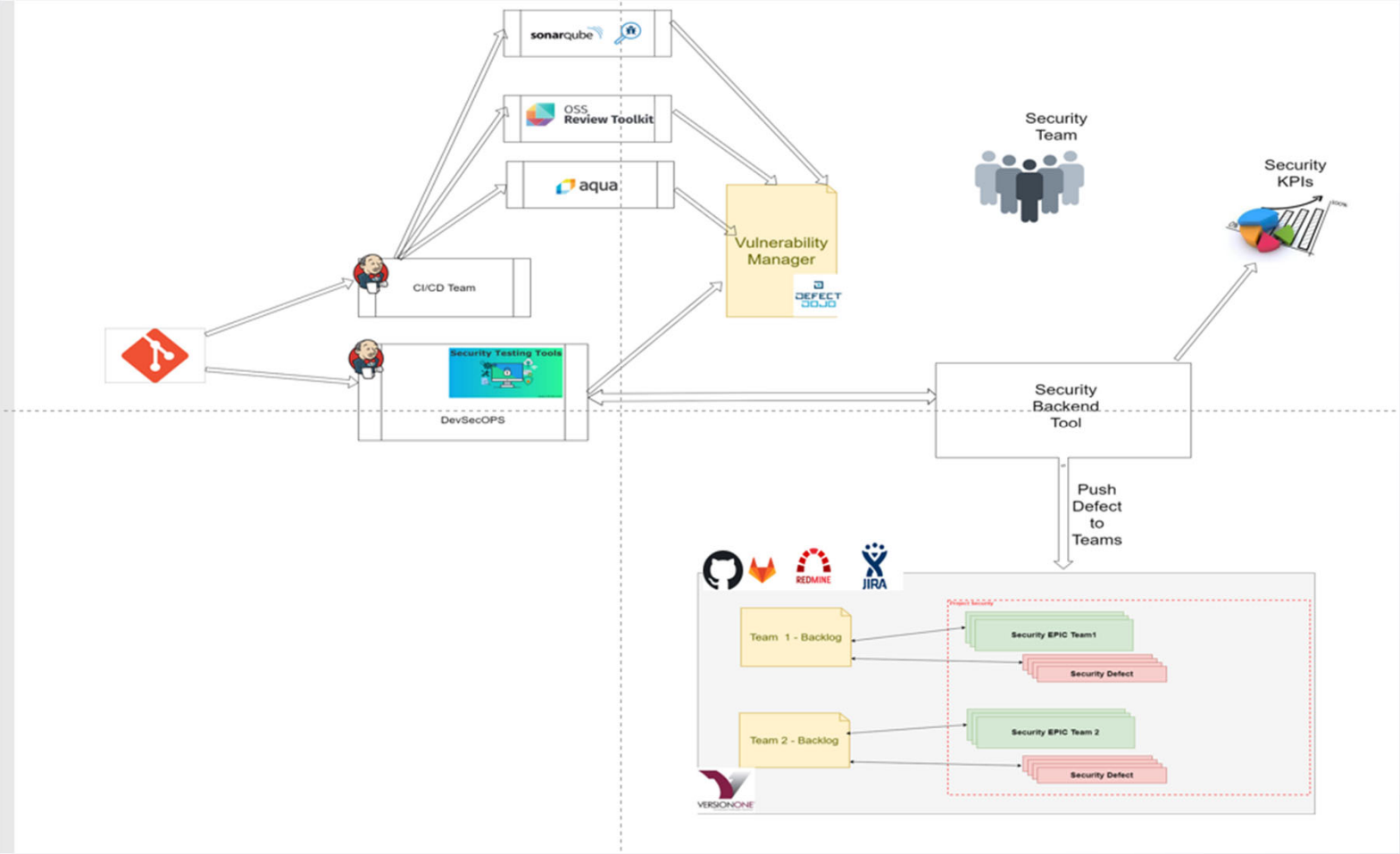


- Définir le processus de correction



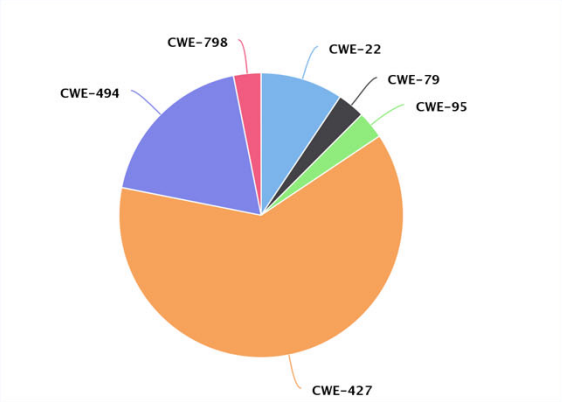
- **Le Mythe de la gate**

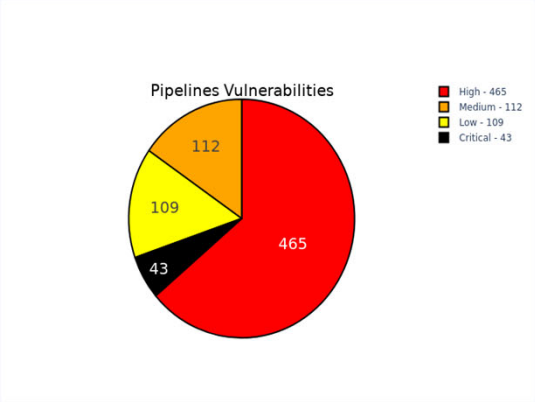
S’insérer dans les processus de développement

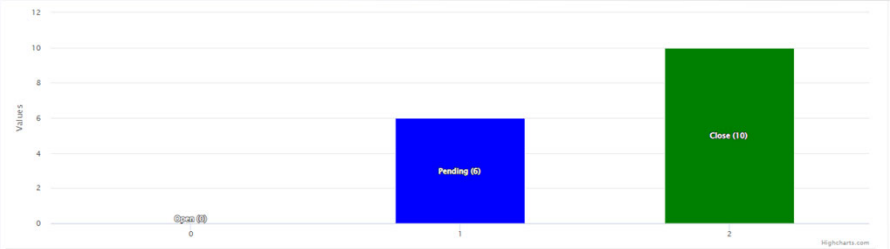


Produire les bons indicateurs (pour les équipes)

Project ID	Project	Vulnerabilities
244	[redacted]	15 42 64 0 26
248		2 7 24 0 6
249		3 7 23 0 9
250		0 0 0 0 0

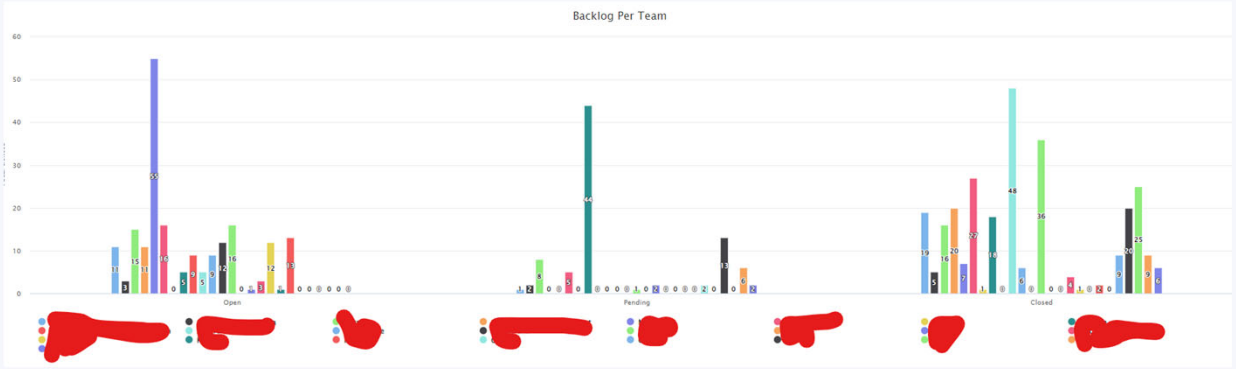


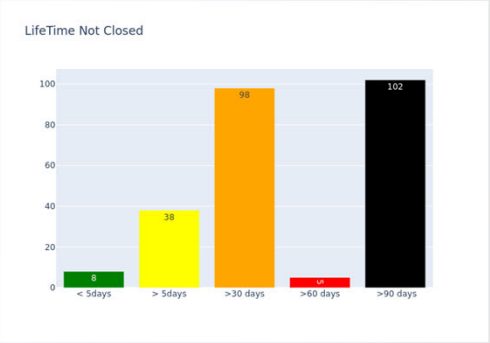


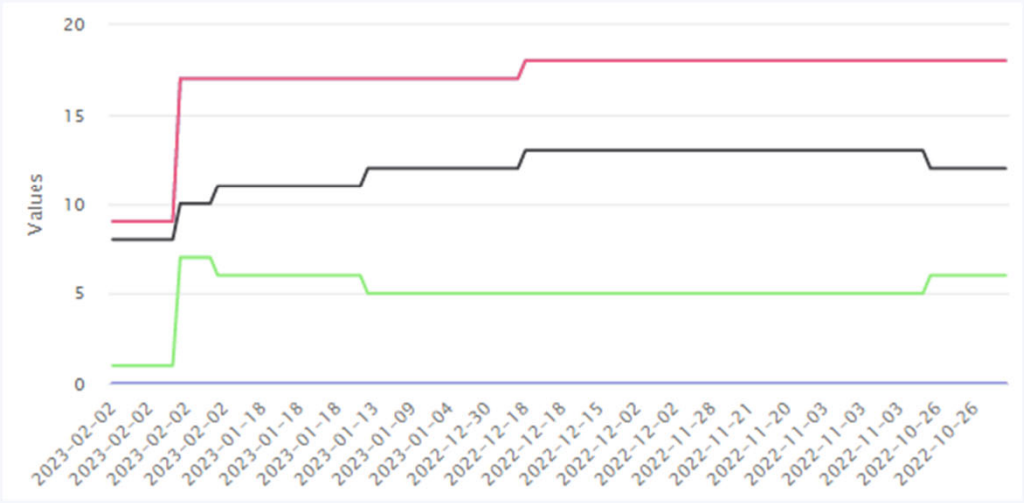


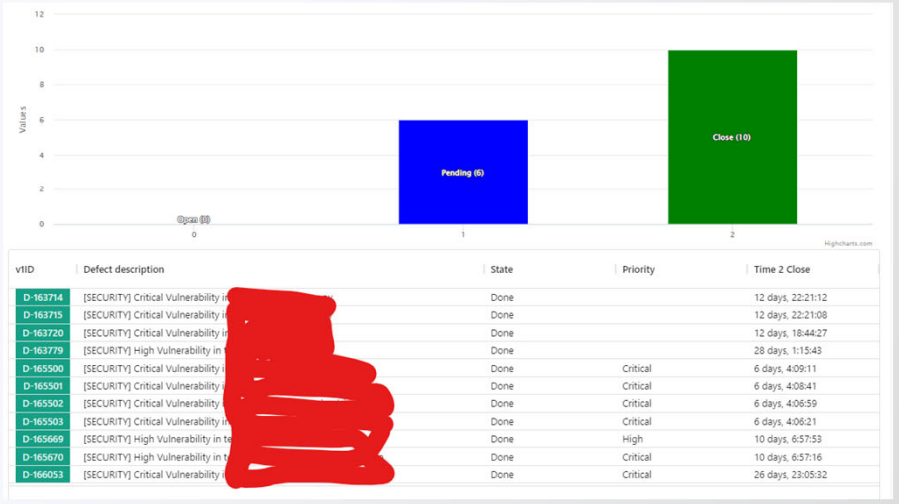
vIID	Defect description	State	Priority	Time 2 Close
D-163714	[SECURITY] Critical Vulnerability	Done		12 days, 22:21:12
D-163715	[SECURITY] Critical Vulnerability	Done		12 days, 22:21:08
D-163720	[SECURITY] Critical Vulnerability	Done		12 days, 18:44:27
D-163779	[SECURITY] High Vulnerability	Done		28 days, 1:15:43
D-165500	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:09:11
D-165501	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:08:41
D-165502	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:06:59
D-165503	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:06:21
D-165669	[SECURITY] High Vulnerability	Done	High	10 days, 6:57:53
D-165670	[SECURITY] High Vulnerability	Done	Critical	10 days, 6:57:16
D-166053	[SECURITY] Critical Vulnerability	Done	Critical	26 days, 23:05:32

Produire les bons indicateurs (pour le suivi exec)

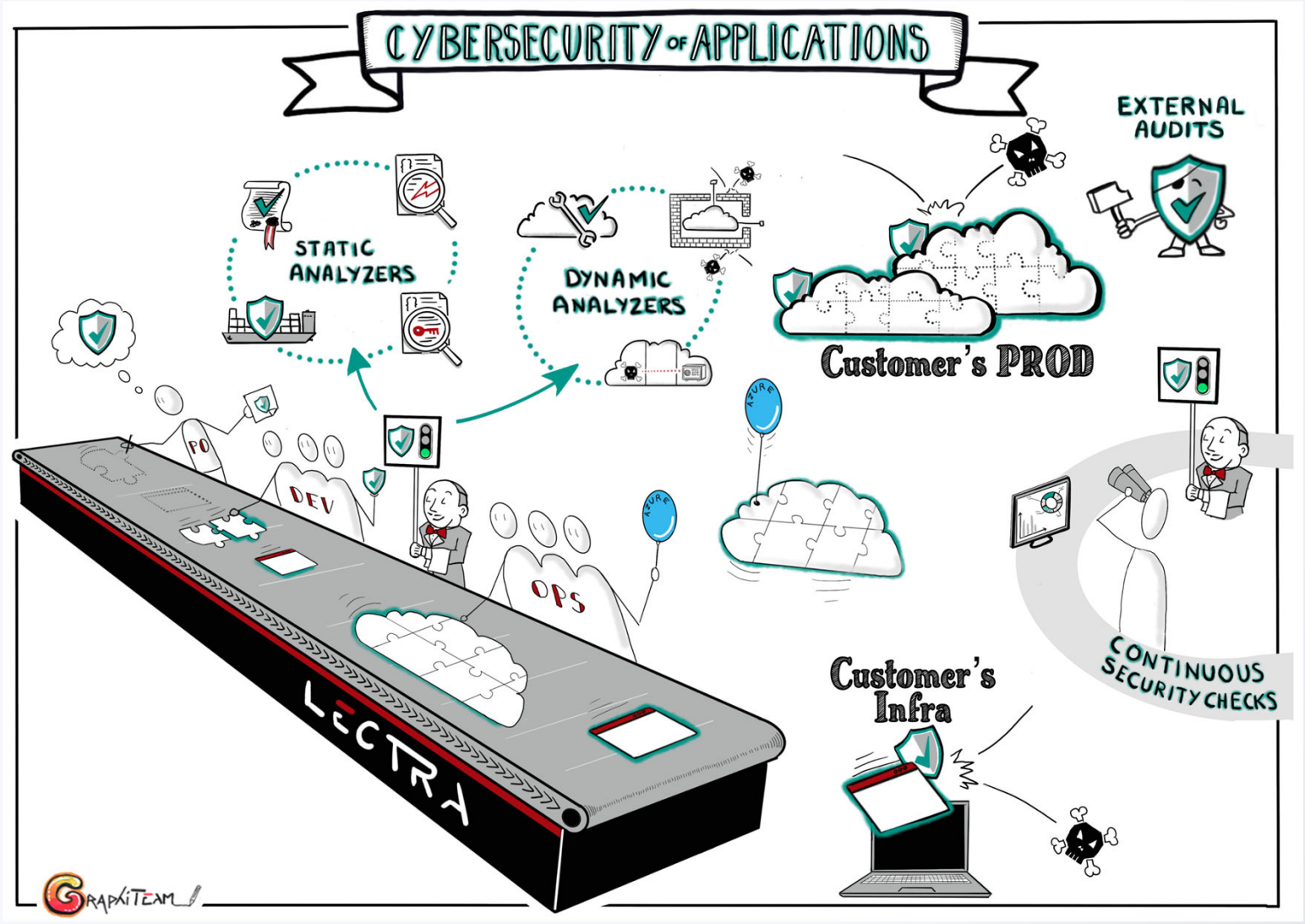








vIID	Defect description	State	Priority	Time 2 Close
D-163714	[SECURITY] Critical Vulnerability	Done		12 days, 22:21:12
D-163715	[SECURITY] Critical Vulnerability	Done		12 days, 22:21:08
D-163720	[SECURITY] Critical Vulnerability	Done		12 days, 18:44:27
D-163779	[SECURITY] High Vulnerability	Done		28 days, 1:15:43
D-165500	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:09:11
D-165501	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:08:41
D-165502	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:06:59
D-165503	[SECURITY] Critical Vulnerability	Done	Critical	6 days, 4:06:21
D-165669	[SECURITY] High Vulnerability	Done	High	10 days, 6:57:53
D-165670	[SECURITY] High Vulnerability	Done	Critical	10 days, 6:57:16
D-166053	[SECURITY] Critical Vulnerability	Done	Critical	26 days, 23:05:32


CYBERSECURITY OF APPLICATIONS
EXTERNAL AUDITS
STATIC ANALYZERS
DYNAMIC ANALYZERS
Customer's PROD
PO
DEV
OPS
LECTRA
Customer's Infra
CONTINUOUS SECURITY CHECKS
GRAPHITEAM