# MISE EN PLACE DU SECURITY BY DESIGN DANS UNE ENTREPRISE EN MODE AGILE

Propriétaire du document : Crédit Agricole Technologies et Service

# Démarche Security by Design auprès des développeurs

- **Présentation Crédit Agricole Technologies et Services**
- **Mise en place du security by design**
- **Mise en marche des outils**
- **Difficultés**

# Crédit Agricole Technologies et Services

## Un système d'information unique et commun

**Crédit Agricole Technologies et Services** est une entreprise qui gère l'ensemble des Systèmes d'information des Caisses régionales de Crédit Agricole, de la conception technologique des offres et processus jusqu'à la gestion de leur production (en lien avec CA-GIP).

## Une ambition, 100% humain et 100% digital

Notre ambition est de faire **évoluer l'offre bancaire** des Caisses régionales de Crédit Agricole et **faciliter la relation de proximité avec leurs clients** dans un mode **100 % humain, 100 % digital.**

## Plus de 1600 collaborateurs et collaboratrices répartis sur l'ensemble du territoire

Les collaborateurs apportent leur valeur ajoutée dans un cadre où **l'innovation** dans les solutions recherchées est favorisée. Ils assurent **la maîtrise des nouvelles technologies, la qualité** et **la performance** des services délivrés à la **1ère banque de proximité en France avec ses 24 millions de clients particuliers**.

# Vision et attentes de nos clients

## 3 NIVEAUX DE CLIENTS POUR CA-TS


**Etre le moteur de la transformation digitale des Caisses régionales et contribuer à leur performance**

Les investissements IT doivent :

- Améliorer l'expérience client – utilisateur
- Contribuer au PNB
- Accélérer l'effort de productivité

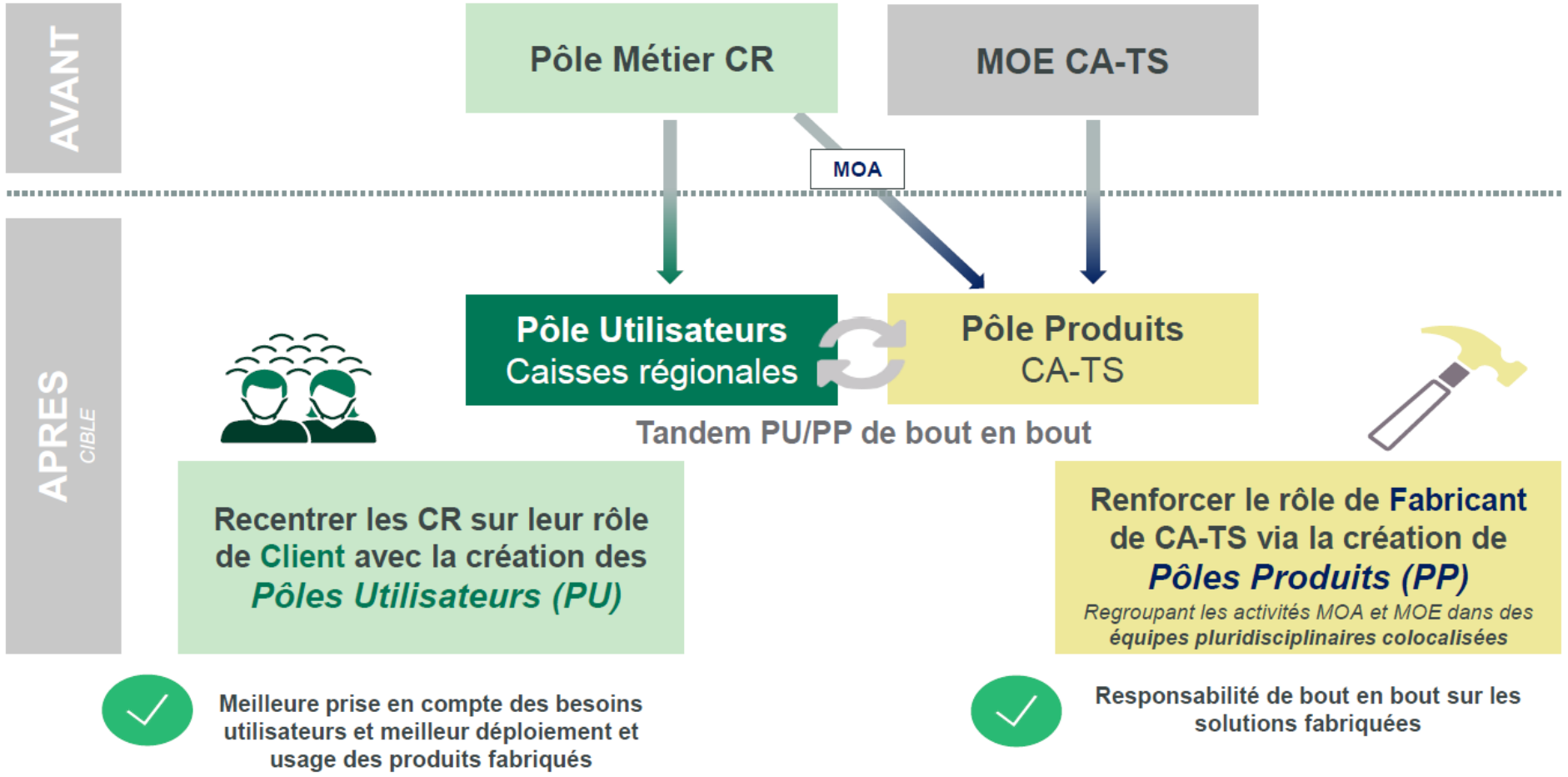

**Fournir aux utilisateurs un outil fiable et efficace au quotidien**
**Offrir une qualité de service qui s'adapte à une forte utilisation des offres**

- Faire gagner du temps administratif et conformité (productivité)
  pour + de temps de conseil avec les clients
- Renforcer l'accompagnement sur les nouveaux outils mis en place


**Simplifier la banque de tous les jours**

- Faire gagner du temps aux clients : Signature Electronique en Agence, Ma Banque, Ma Carte, Scan Chèque
- Permettre de commencer le projet bancaire sur un canal et de finaliser sur un autre

# Transformation de l'entreprise



# Une organisation Agile

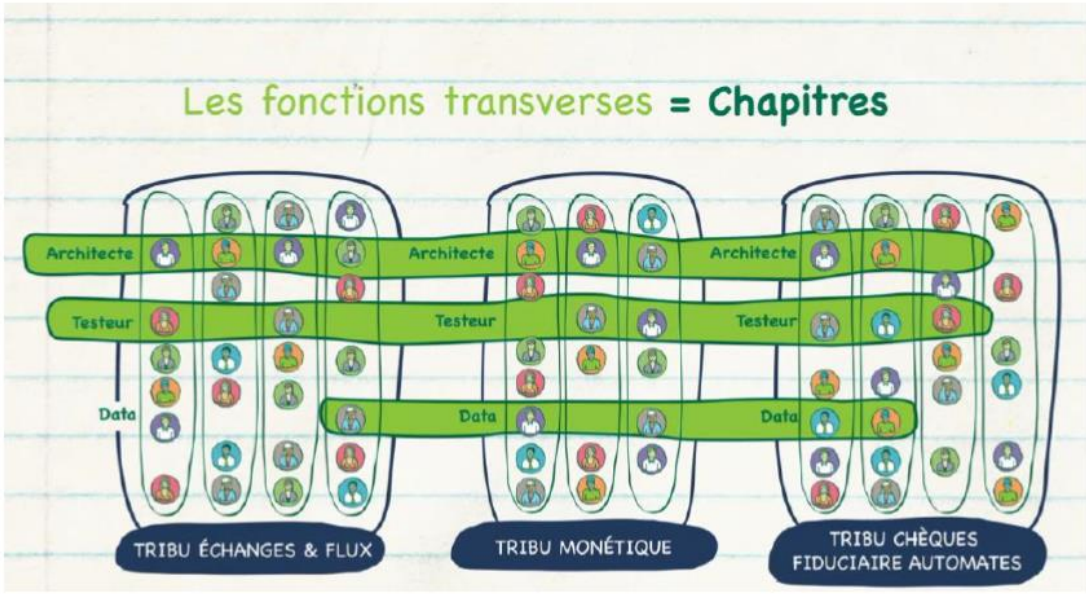
La Squad est responsable d'une famille de produits


avec 2 nouveaux rôles agiles

Product Owner

Scrum Master

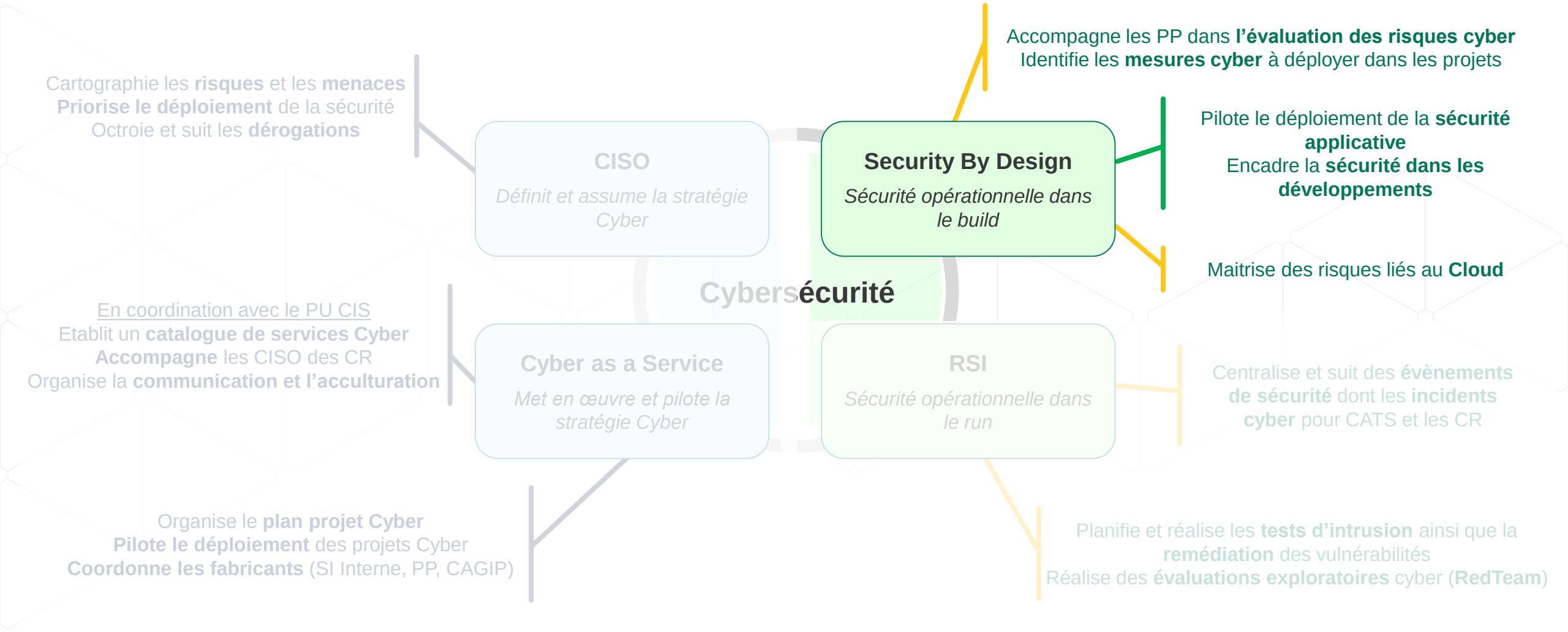
Plusieurs squads forment une Tribu
(50 à 100 personnes)
Les fonctions transverses sont animées
sous forme de chapitres




Les Tribus d'un même univers
sont regroupées au sein d'un Pôle Produits
(50 à 200 personnes)

# Organisation Cyber CATS

## Centre de compétences Security by Design



# Centre de compétences Security by Design

## Une organisation basée sur 3 profils

### Le security Champion…

**Il est l'interlocuteur privilégié pour le Leader de tribu/chapitre** pour les questions de sécurité. De préférence, il est colocalisé sur le site de rattachement du leader de tribu/chapitre.

- ✓ Il **accompagne les équipes** pour **aider à fabriquer en toute sécurité** lors des sprints notamment sur :
  - ✓ Les analyses de risques métier,
  - ✓ La démarche Cloud,
  - ✓ La sécurité des architectures et des données
  - ✓ La recette sécurité
- ✓ il **répond à ses demandes**, liées à **l'éclairage sur les risques** dans les évolutions des différents produits sous responsabilité de la tribu;
- ✓ il **propose des récits de sécurité** pour intégration aux backlogs des squads;
- ✓ il **sensibilise les squads** pour les faire gagner en autonomie;
- ✓ il **contrôle** la bonne mise en place des **récits de sécurité**.

### Le référent Cloud…

**Il est l'interlocuteur privilégié des Tribus/Squads** et des **caisses régionales** pour les questions de sécurité liés à l'utilisation de ressources **cloud** (Traitement et/ou stockage).

- ✓ Il s'assure que les risques métiers sont couverts par les mesures proposées par les tribus/squads ou le fournisseur cloud
- ✓ Il participe aux évolutions de la **politique Cloud** du Groupe
- ✓ Il organise **l'instruction des dossiers** cloud :
  - ✓ Sur le périmètre CATS
  - ✓ Sur le périmètre CR
- ✓ Il donne un **avis d'expert** sur les risques SI des usages cloud
- ✓ Il consolide les différents usages et solutions cloud utilisées via un **référentiel** et assure la **coordination avec le Groupe** CA

### Le référent SecApp…

**Il est l'interlocuteur privilégié pour les développeurs des squads** pour les questions de sécurité applicative.

- ✓ Il contribue à **l'acculturation des équipes** de fabrication
- ✓ Il formalise des **supports** d'aide aux développeurs :
  - ✓ **guides de développements**
  - ✓ **Fiches SecApp**
  - ✓ **Fiches d'analyse des vulnérabilités**
- ✓ Il participe à la mise en place **des outils de détection de vulnérabilités** dans la chaine CI/CD
- ✓ il **assiste la squad MSQC** dans l'analyse des vulnérabilités détectées dans le codes sources ou les composants des différentes solutions;
- ✓ il participe aux travaux nationaux sur le **standard SECAPI**;

# Accompagnement des développeurs

## Les référents SecApp

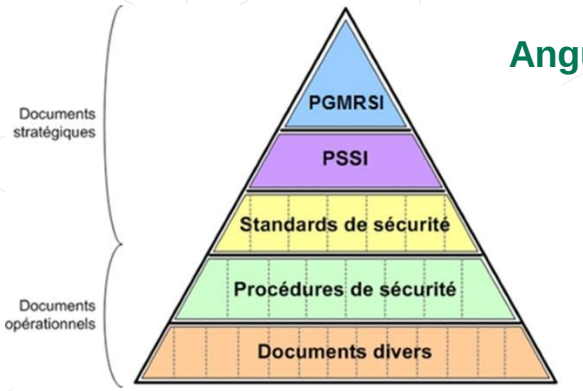
- Objectif : Accompagner les développeurs pour une prise en compte des développements sécurisés au plus tôt dans la chaine de fabrication en coordination avec :
  - La Tribu DevOps : Mise en place des différents outils et assistance à la fabrication
  - Les équipes socles de l'opérateur de production
  - Les équipes support IT

- Pour parvenir à mettre en place la fabrication sécurisée, les référents SecApp travaillent sur plusieurs axes :
  - Rédaction des standards, documentations et bonnes pratiques,
  - Création de contenus de formation
  - Utilisation d'outils d'analyse
  - Accompagnement et expertise sur les résultats

# Documentation

## Standard et guides de développement

- Un standard sécurité dans les applications (SECAPI) basé sur OWASP SAMM et OWASP Top Ten
- Les exigences décrites dans le standard SECAPI sont déclinées dans les guides en mesures concrètes et implémentables
- Documents centrés sur une technologie ou un langage spécifique
- Référentiels complets pour développer de manière sécurisée sur une technologie ou dans un langage spécifique




NodeJS

Angular

PHP

Cobol ?


iOS

Android

JAVA

# Documentation

## Des fiches SecApp : Objectifs et contenus

Être un **support de référence** attractif et simple pour les développeurs

Proposer des **solutions de remédiation aux vulnérabilités courantes**

**Contenir l'essentiel des règles** de sécurité applicative

**Décliner** clairement les règles de sécurité applicative

**Sensibiliser** les développeurs aux bonnes pratiques

Permettre aux développeurs de **contribuer à ces fiches**

Intégrées au Portail développeur et au chatbot d'entreprise

Description (comprendre l'importance du point traité)

Décrit les contrôles pour savoir comment vérifier si ce point est conforme

Bonnes pratiques (indiquer comment intervenir pour limiter/éviter les vulnérabilités associées)

Correspondance **OWASP**

Implémentations (donner une solution concrète en fonction des technologies / langages)

Liaison du contenu de la fiche avec application **SECAPI** pour lire les règles correspondantes des standards

# Formation dédiée et ciblée

## Une formation SecApp à CATS

- Objectif : Mettre le développeur dans la peau de l'attaquant pour exploiter des vulnérabilités et ensuite essayer de les corriger

### Ambition

Une **formation sur-mesure** basée sur le référentiel SECAPI, le top Ten de l'OWASP et contextualisée à CA-TS

### Engagement

Une formation **obligatoire**

### Notre cible

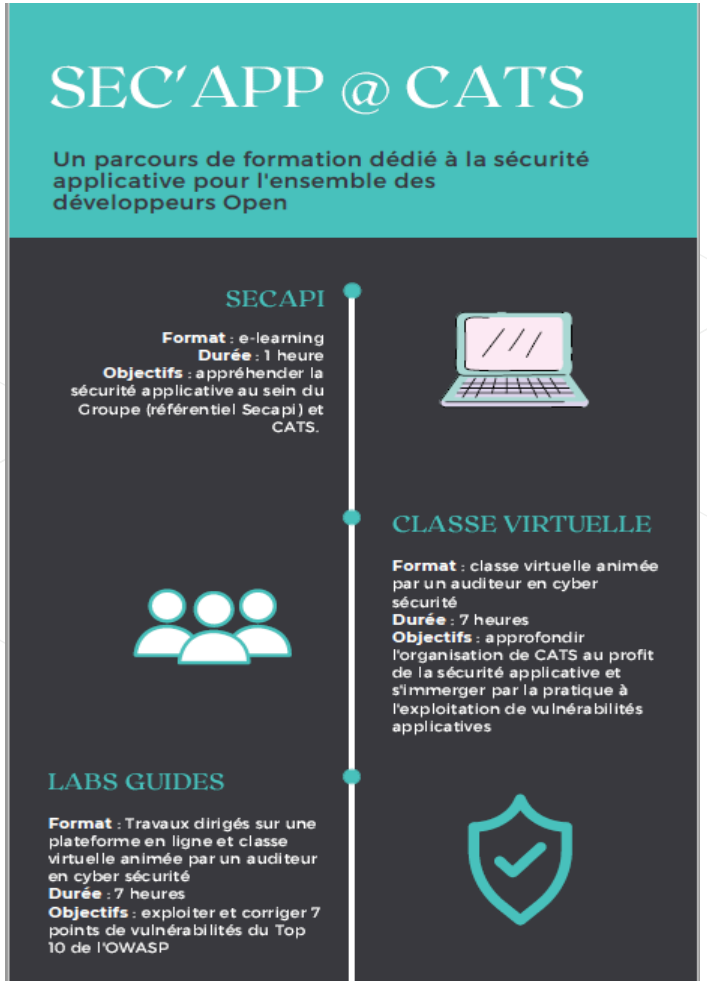
Les **développeurs OPEN** en particulier WEB, Mobile (350 à 400 pers.)

### Modalités

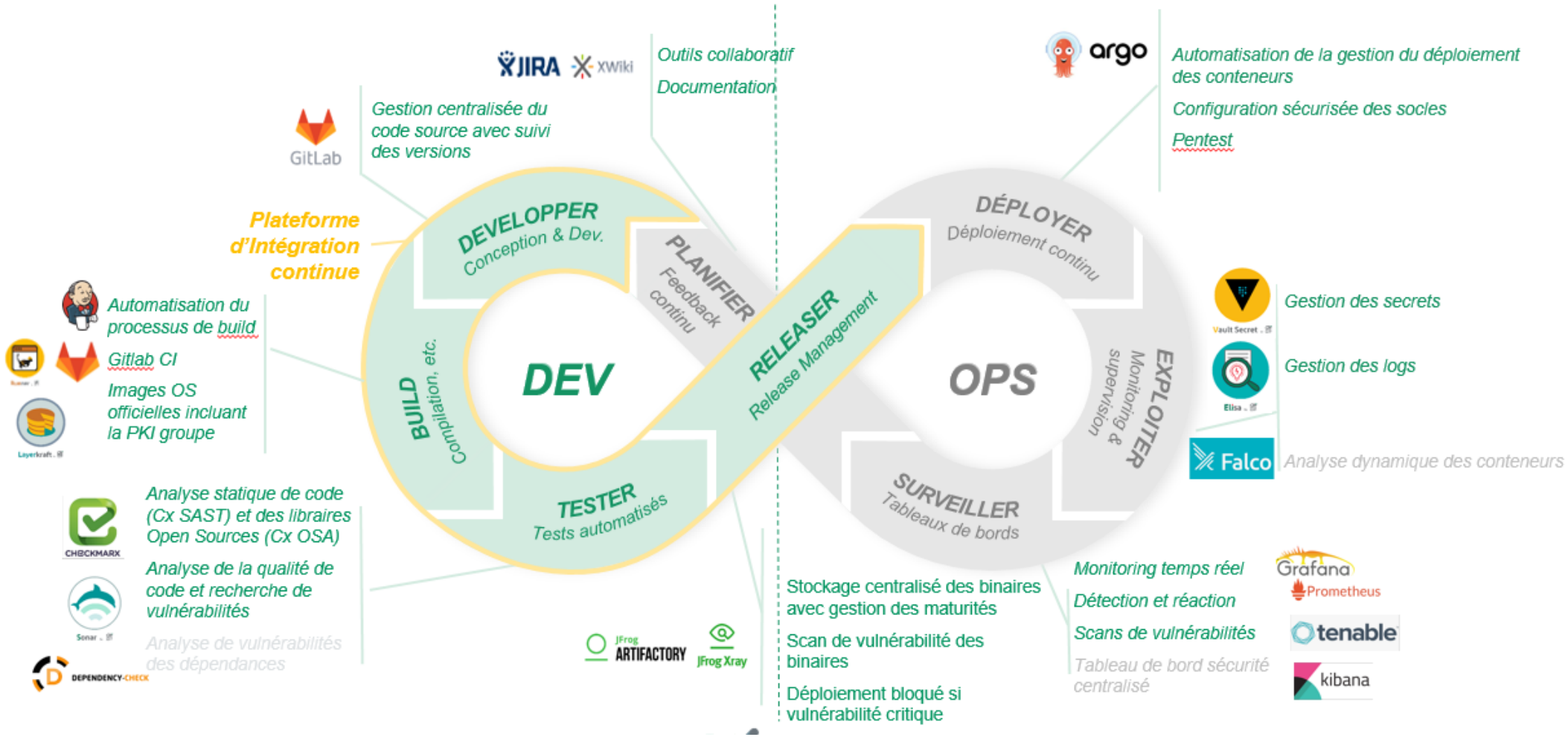
Une formation **100% distancielle**

**Multi formats** : e-learning, classe virtuelle, entraînements, ancrage

Du **contenu théorique** et des **ateliers pratiques** (labs – entraînement en situation réelle)

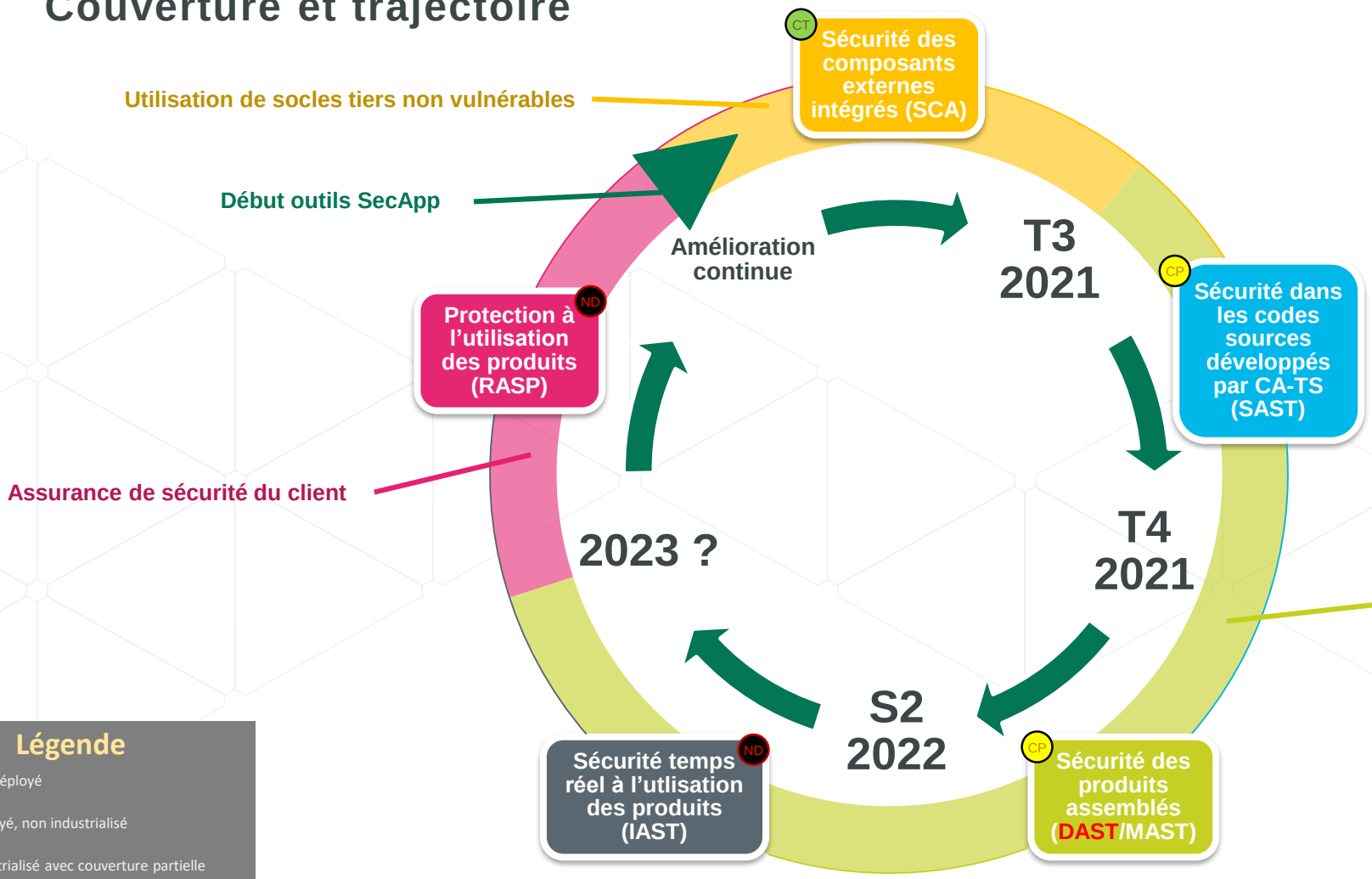


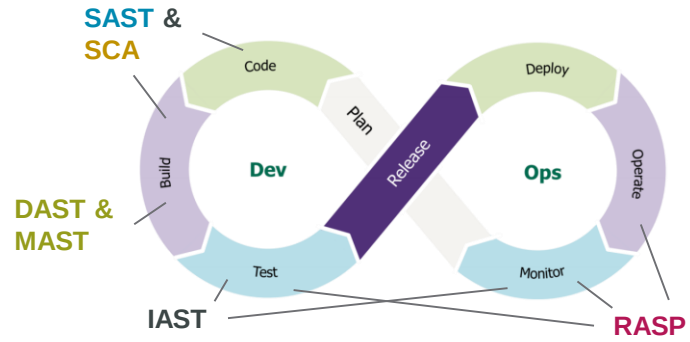
# Une chaine CI/CD outillée



# Ambitions : Outils d'analyse de sécurité applicative

## Couverture et trajectoire




**Analyse au plus tôt dans la fabrication**

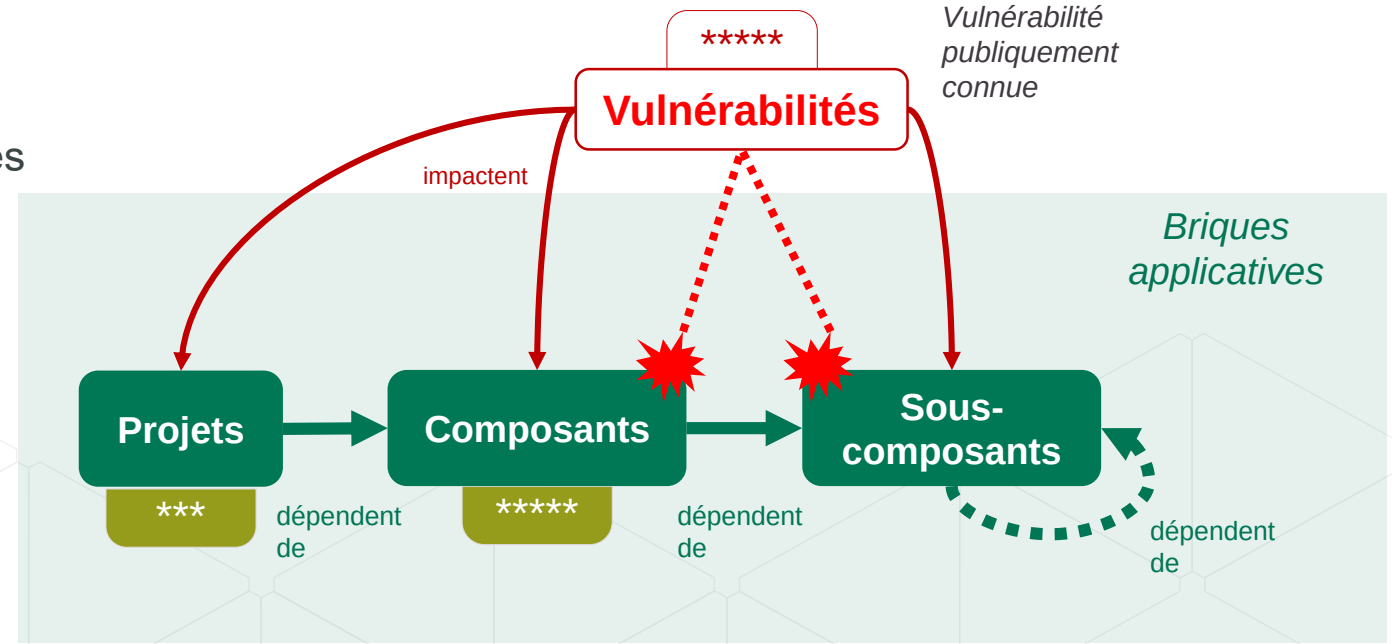
**Légende**

- ND — Outil non déployé
- NI — Outil déployé, non industrialisé
- CP — Outil industrialisé avec couverture partielle
- CT — Outil industrialisé avec couverture totale

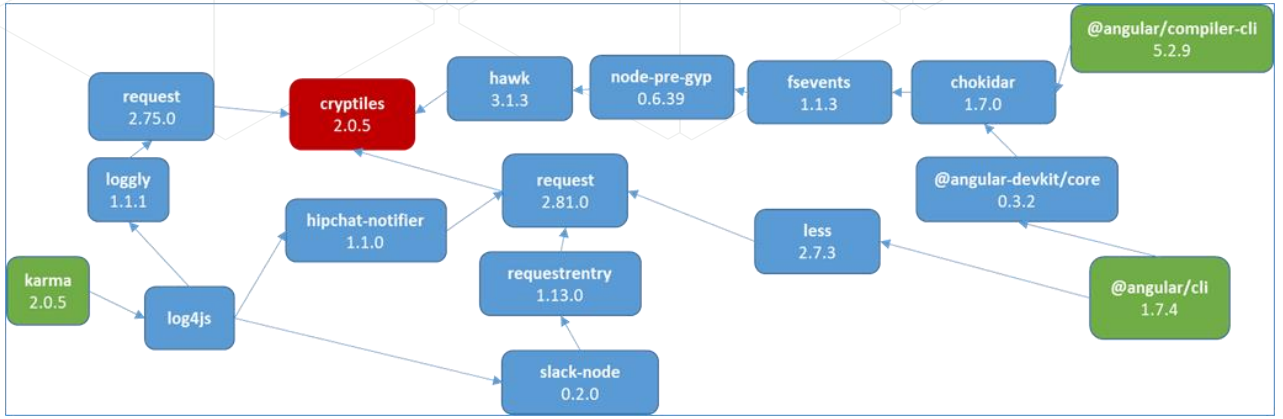
SCA Xray mis en place
Sur Kubernetes

# Initialisation du stock et chaîne de liaison (SCA)

- Utilisation de l'OWASP DC sur l'ensemble des projets legacy stockés dans les différents repositories
  - 10095 projets analysés




- Difficulté à corriger le composant vulnérable, le composant vulnérable étant un sous composant de plusieurs librairies choisies par le développeur




*Exemple d'analyse de chaine de dépendance d'un composant vulnérable*

# Une priorisation obligatoire

- Obligation de trouver des critères de priorisation, les composants les plus vulnérables portant les plus forts risques pour l'entreprise

| Composants tiers vulnérables | Nombre de projets | IRS | Vulnérabilités du stock | dont CRITIQUES |
|---|---|---|---|---|
| x**********.jar | 66 | 6864 | 1188 | 1122 |
| j**********.jar | 12 | 2639 | 425 | 389 |
| b**********.js | 159 | 2382 | 798 | 0 |
| **********.jar | 41 | 2252 | 653 | 287 |
| **********.jar | 69 | 2139 | 1035 | 276 |
| **********.js | 135 | 2031 | 681 | 0 |
| **********.js | 103 | 1956 | 672 | 0 |
| **********.jar | 62 | 1922 | 806 | 248 |
| **********.jar | 16 | 1740 | 526 | 256 |
| **********.jar | 12 | 1728 | 394 | 258 |
| **********.jar | 14 | 1722 | 508 | 256 |
| **********.jar | 14 | 1722 | 510 | 256 |
| **********.jar | 14 | 1716 | 456 | 256 |
| **********.jar | 12 | 1592 | 364 | 238 |
| **********.jar | 12 | 1426 | 315 | 213 |
| **********.jar | 11 | 1276 | 198 | 187 |
| **********.js | 86 | 1140 | 385 | 0 |
| **********.jar | 34 | 1089 | 247 | 127 |
| **********.jar | 8 | 952 | 288 | 168 |

# IRS : score de risque

- Inherited Risk Score
  - un score de risque considérant le nombre des vulnérabilités pondéré à leur sévérité
  - aidant à la priorisation : plus il est élevé, plus il est essentiel de corriger
  - applicable à une tribu, un produit, une solution, un projet, un composant vulnérable

**Précisions sur le calcul**

- *Si la vulnérabilité est une CVE* : la sévérité d'une vulnérabilité est déterminée à l'aide du score de sévérité CVSS associé quand il s'agit d'une CVE

10.0 < Bloquante <= 9.0
9.0 < Critique <= 7.0
7.0 < Majeure <= 4.0
4.0 < Mineure < 0.0

Le CVSSv3 est appliqué en priorité s'il existe, sinon CVSSv2

- *Si la vulnérabilité n'est pas une CVE* : elle n'a pas de sévérité

Ce qui explique qu'on peut avoir des vulnérabilités et un score de risque IRS nul

**IRS**
=
Bloquantes *** 7** + Critiques *** 5** + **Majeures * 3** + **Mineures * 1**

*Source : https://github.com/dependency-check/dependency-check-sonar-plugin*

# Difficultés rencontrées

- Le volume des vulnérabilités découverte à la mise en route des outils sur les applications historiques doit être expliqué aux squads en charge des différents produits impactés
- Si la mise en place d'outils de détection est relativement rapide, l'analyse de la pertinence des résultats est beaucoup plus chronophage
- L'objectif de mettre en place des security gates bloquantes n'est pas atteignable à court terme
- Un processus de validation / dérogation doit être mis en place pour ne pas mettre en péril le Time To Market
- Les impacts de la mise en place du SCA retarde l'exploitation des résultats des modules SAST et l'intégration des modules DAST, IAST, RASP et peu remettre en cause l'ordre de mise en place des outils.
- Priorisation dans les sprints planning basés sur la valeur métier apportée mais très rarement sur la réduction du risque
    - Sensibilisation des product owners et leader de tribu
    - Contribuer au calcul du score risque sécurité produit
        - Objectif : déterminer un score à partir duquel une squad « devra » consacrer une partie de sa CAF pour le réduire
        - Idée : (ind1 + ind 2 + …. + indN) x Exposition x dICp
            - Ind1 : Analyse des risques existante
            - Ind2 : Code source passé dans les outils

# Annexes : CVE – Définitions

- *Common Vulnerabilities and Exposures*
  - Une vulnérabilité « CVE »
    - c'est une faiblesse dans une application ou son environnement
    - qui peut être exploitée pour atteindre à la disponibilité, l'intégrité ou la confidentialité de l'application
    - générant un impact métier

- Les CVE sont publiques, nombreuses et partout
  - Produits du domaine libre autant que chez les éditeurs (Adobe, Microsoft, etc.)

- Référentiels de CVE
  - MITRE : https://cve.mitre.org/
  - *National Vulnerability Database* (NVD) du NIST : https://nvd.nist.gov/

# Annexes : CVE – CVSS

- *Common Vulnerability Scoring System*
  - Une méthode de calcul
    - pour donner un **score numérique** de 0 à 10 reflétant la **sévérité** d'une vulnérabilité
    - appliquée à chaque CVE selon des critères généraux
    - proposée et maintenue par les experts en sécurité du FIRST : https://www.first.org/cvss/

- Score de base et scores pondérés
  - **Score de base**
    - Déterminé par l'auditeur à la découverte de la vulnérabilité
    - Selon des critères généraux (vecteur d'attaque, complexité d'attaque, privilèges requis, interaction utilisateur, périmètre, impact confidentialité, intégrité, disponibilité)
  - Score temporel
    - Réévalue selon l'existence d'exploits, l'applicabilité de solutions et la confiance en le rapport.
  - Score d'environnement
    - Réévalue le score de base d'après l'environnement
    - Sur des critères propres « ops » et « métier » (redéfinition des critères généraux, et selon nos objectifs de sécurité en disponibilité, intégrité et confidentialité)