

# LA SÉCURITÉ AS A SERVICE

ou

comment industrialiser les tests de sécurité au sein du SDLC

aDvens

JFLT 2016

SECURITY FOR THE DIGITAL AGE

# AGENDA

---

- 1 Introduction
- 2 Contexte
- 3 Les risques encourus par les applications
- 4 Les démarches possibles pour sécuriser les applications
- 5 L'approche Security As A Service
- 6 Retour d'expérience

# LES SPEAKERS

JFTL 2016



## Frédéric Patouly

Responsable Programme Application  
Security Assurance - Advens



## Eric Doyen

RSSI du Groupe Humanis  
Président du Club 27001  
Trésorier du Cesin

# LA DIGITALISATION DE NOTRE QUOTIDIEN

Est aujourd'hui une réalité qui ne fait que s'accélérer



## Vie professionnelle

### Digitalisation du monde du travail

- Home Office
- BYOD
- Visio Conférence
- ...



## Vie Sociale

### Digitalisation de la vie personnelle

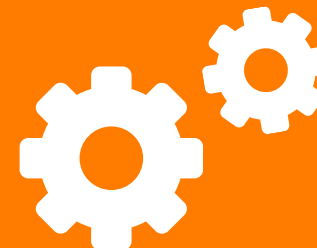
- Banques / Assurances en ligne
- Procédures administratives
- Paiement sans contact
- Réseaux sociaux
- ...



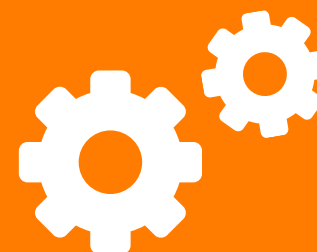
## Vie Culturelle

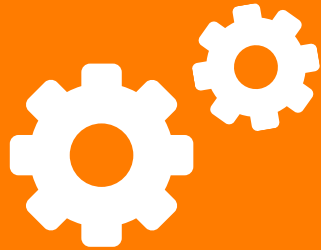
### Digitalisation de la vie culturelle

- Musiques / spectacles en ligne
- Visites virtuelles Bibliothèques / Musées
- Réalité augmentée
- Jouets connectés
- ...



## Les Applications





### Applications

#### QUALITÉ

Rendre le service attendu



#### PERFORMANCE

Etre un accélérateur de business



#### DISPONIBILITÉ

Délivrer un service en continu



#### SÉCURITÉ

Etre source de confiance pour l'utilisateur final



# QUE S'EST-IL PASSÉ CETTE ANNÉE ?

En 2015

96%

14

# CONSTRUIRE SA DÉMARCHE DE SÉCURITÉ APPLICATIVE

Deux approches possibles

## APPROCHE **RÉACTIVE**

Je dois faire face à:

- des nouvelles obligations réglementaires
- des attaques sur mon patrimoine applicatif
- la pression de mes clients pour élever le niveau de sécurité de mes applications
- etc.



## APPROCHE **PROACTIVE**

Je veux mettre en place:

- Une approche construite et phasée
- Des quick wins
- Un plan d'actions phasé
- etc.



# COMMENT SÉCURISER SES APPLICATIONS ?

---

Introduire la sécurité dans le cycle  
de développement des applications  
**Security By Design**

S'assurer régulièrement de la  
sécurité des applications  
lorsqu'elles sont en production

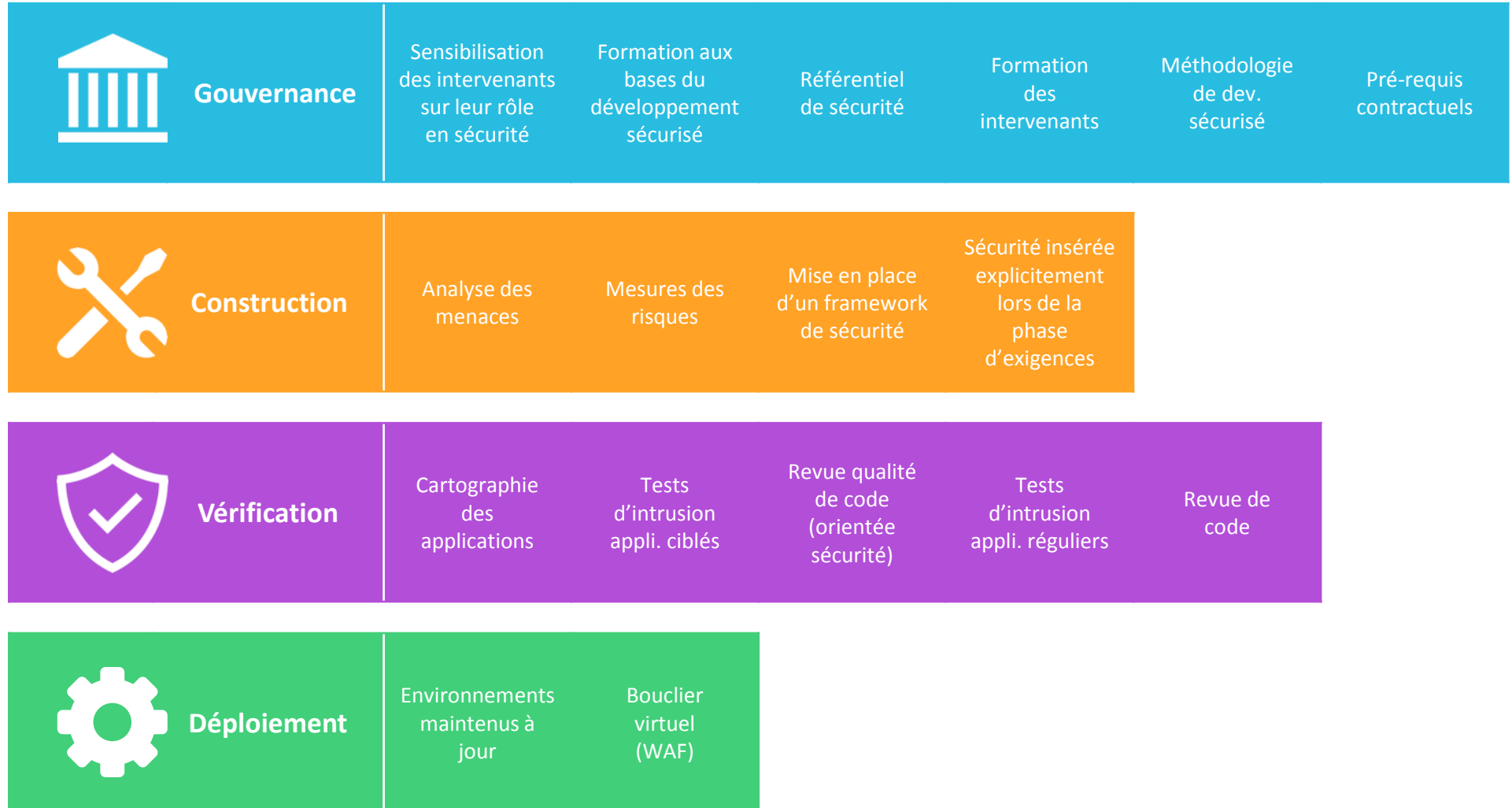
Protéger ses applications en  
production





# SECURITY BY DESIGN

## Les axes de travail



DELEGUER A UN  
TIERS DE  
CONFIANCE  
LA SECURISATION  
DE SON  
PATRIMOINE  
APPLICATIF



# L'APPROCHE SECURITY AS A SERVICE



## Apports / Gains

- Tiers de confiance avec délégation de responsabilité
- Résultats clé en main avec un choix de différents niveaux de service en fonction du besoin
- Utilisation de solutions toujours up-to-date
- Capitalisation de l'expertise multi-clients / multi-projets



## Moyens mis à disposition

- Plate-forme
- Solutions
- Expertise



## La couverture (SDLC couvert, typologie de services offerte)

- Toutes les phases depuis le développement jusqu'à la production
- Audit de code
- Audit applicatif (unitaire / périodique)
- Protection des applications

# L'APPROCHE SECURITY AS A SERVICE

1

## Audit de code As-a-Service

Réaliser régulièrement des audits de code permettant de détecter au plus tôt les vulnérabilités applicatives en tenant compte du contexte et du métier du client

2

## Détection des vulnérabilités

Valider régulièrement le niveau de sécurité de son patrimoine applicatif

3

## Protection des applications

Renforcer la protection des applications et des services en ligne

# RETOUR D'EXPÉRIENCE

Humanis



Humanis est un groupe paritaire de protection sociale français créé le 26 janvier 2012 suite au rapprochement des groupes Aprionis, Novalis Taitbout et Vauban Humanis.

Acteur de référence de la protection sociale, Humanis protège plus de 10 millions de particuliers, actifs et retraités et les salariés de 692 000 entreprises adhérentes. Outre ses activités en retraite complémentaire, Humanis est présent dans l'ensemble des domaines de la protection sociale, sous les marques Radiance Groupe Humanis et Humanis : santé, prévoyance, épargne.



Eric Doyen  
Resp. pôle SSI du Groupe Humanis  
Vice-Président du Club 27001  
Trésorier du CESIN

# ENJEUX DE LA SÉCURITÉ NUMÉRIQUE

c'est s'engager à protéger...

**Humanis 2018** : 100% de l'activité et des informations sont traitées par le numérique (de nombreuses réformes ANI, DSN, nouveaux parcours de soin, en santé et en prévoyance, ...)

**La sécurité des systèmes d'information répond à 4 principaux enjeux :**

Protéger  
l'information  
sensible de nos  
affiliés, de nos  
allocataires

Garantir le respect  
des obligations  
légales,  
réglementaires et  
contractuelles

Assurer la  
continuité des  
processus Métiers

Adapter la  
protection du SI à la  
transformation  
rapide d'une activité  
BtoB à BtoC

# NOTRE CONTEXTE

en Quelques chiffres ...

- De nombreuses réformes du monde de la protection sociale, de la Retraite Complémentaire.
- Portfolio applications Web (30 intranets / extranets métiers et partenaires, 5 portails Web)
- 50% sont jugées critiques, exposant des données sensibles
- Développement assuré pour la majeure partie en interne mais plusieurs CMS
- Environ 10/15 développeurs répartis en 2 équipes

# UNE REPONSE SSI ARTICULÉE

autour de nos trois valeurs



## Ambition

- Intégrer la sécurité dans nos développements
- Contrôler et protéger les accès à l'information
- Surveiller en continu les vulnérabilités
- Etre exemplaire et responsable

## Partage

- Accompagner les projets
- Impliquer les responsables opérationnels dans le dispositif de défense et d'amélioration continue

## Engagement

- Disponibilité de notre SI
- Garantir la sécurité des données à caractère personnel
- Contrôler la bonne orientation des mesures à l'aide d'un tableau de bord et d'indicateurs dédiés



# UN CYCLE DE VIE « AGILE »

intégrant une automatisation des tests de SECURITE

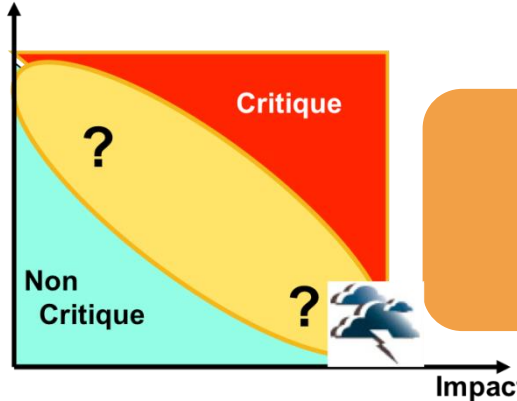
**ROI = Réduire les risques** = Une faille applicative a un coût de correction ...

Probabilité

Développement  
Intégration

Outiller et accompagner les développeurs

Spécifications



Recette

Analyse de code on demand



Maintenir le niveau de risque résiduel

Pré-production  
Production

Assurer une meilleure couverture de détection des vulnérabilités



Pentest

# NOS CRITERES DE CHOIX

face à ses exigences

## **Priorité 2016/2017 : CONFORMITE, mieux contrôler son exposition aux nouveaux risques, nouvelles vulnérabilités, nouveaux partenaires et exigences réglementaires**

- Savoir être agile, et valoriser l'expérience utilisateur
- Temps d'appropriation court favorisant l'accompagnement
- Diminuer le nombre de Pentest, au profit d'une plus forte responsabilisation et d'un meilleur code.
- S'assurer de la meilleure expertise sans contrainte sur la production (service en mode SaaS)
- Améliorer nos engagements de service vis-à-vis de nos partenaires
- Améliorer notre résilience et notre robustesse

# LES ÉCUEILS QUE NOUS SOUHAITIIONS ÉVITER ...

- Se détacher de la réalité du fonctionnement
- Ne pas voir, les failles liées aux transactions
- Ne rien faire en cas d'applications sous-traitées
- Utilisation uniquement par des spécialistes de la sécurité
- Trop verbeux et inexploitable en mode agile
- Ne pas pouvoir maintenir en condition opérationnelle

# LES FACTEURS CLÉS DE SUCCÈS...

- **Responsabiliser**
  - › Avoir un sponsor et des parties prenantes impliquées (MOA Métier, MOE, SSI, développeurs, etc.)
- **S'engager**
  - › à conduire et à accompagner le changement
- **Sensibiliser**
  - › les développeurs et les métiers
- **Adopter**
  - › une approche holistique
- **Automatiser et faciliter**
  - › l'analyse des vulnérabilités et la remédiation

Q&A

