La sécurité dans le cycle de développement d'une application web : de la théorie à la pratique

Gilbert AGOPOME, CSSI 2004, CISSP, CISA
gilbert.agopome@wanadoo.fr

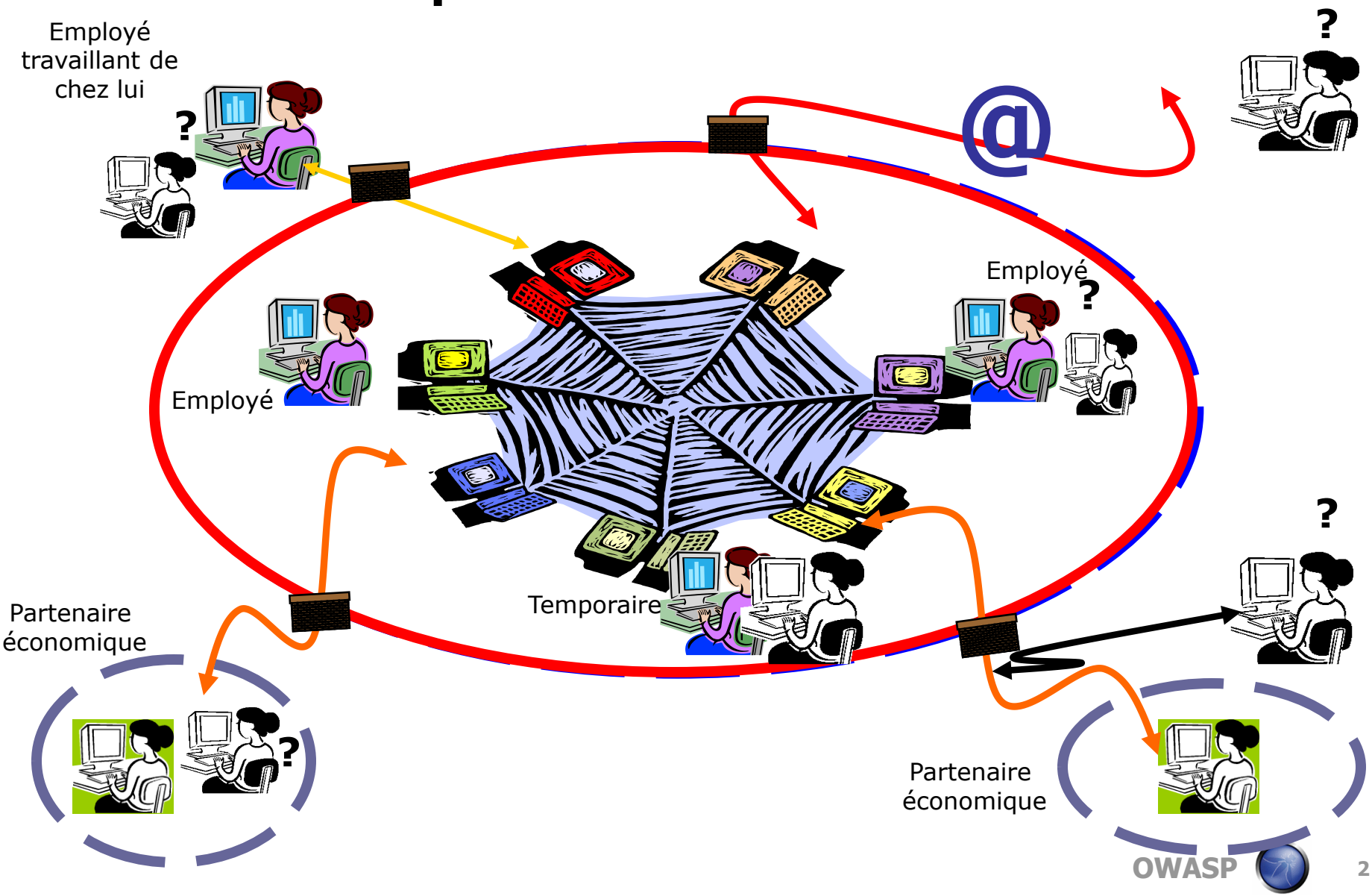
OWASP

Genève 23 Avril 2009

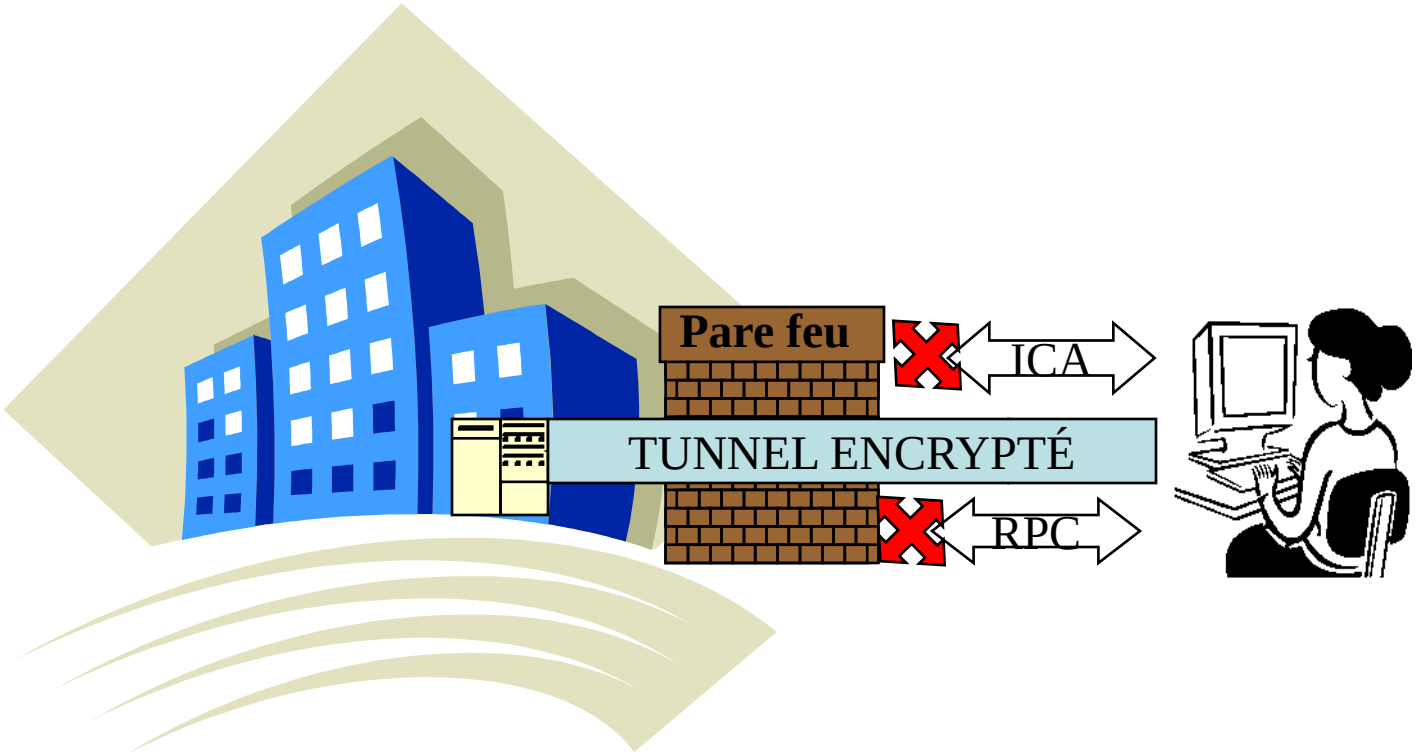
The OWASP Foundation

http://www.owasp.org

Applications web: Gardes frontières des réseaux interne d'entreprises



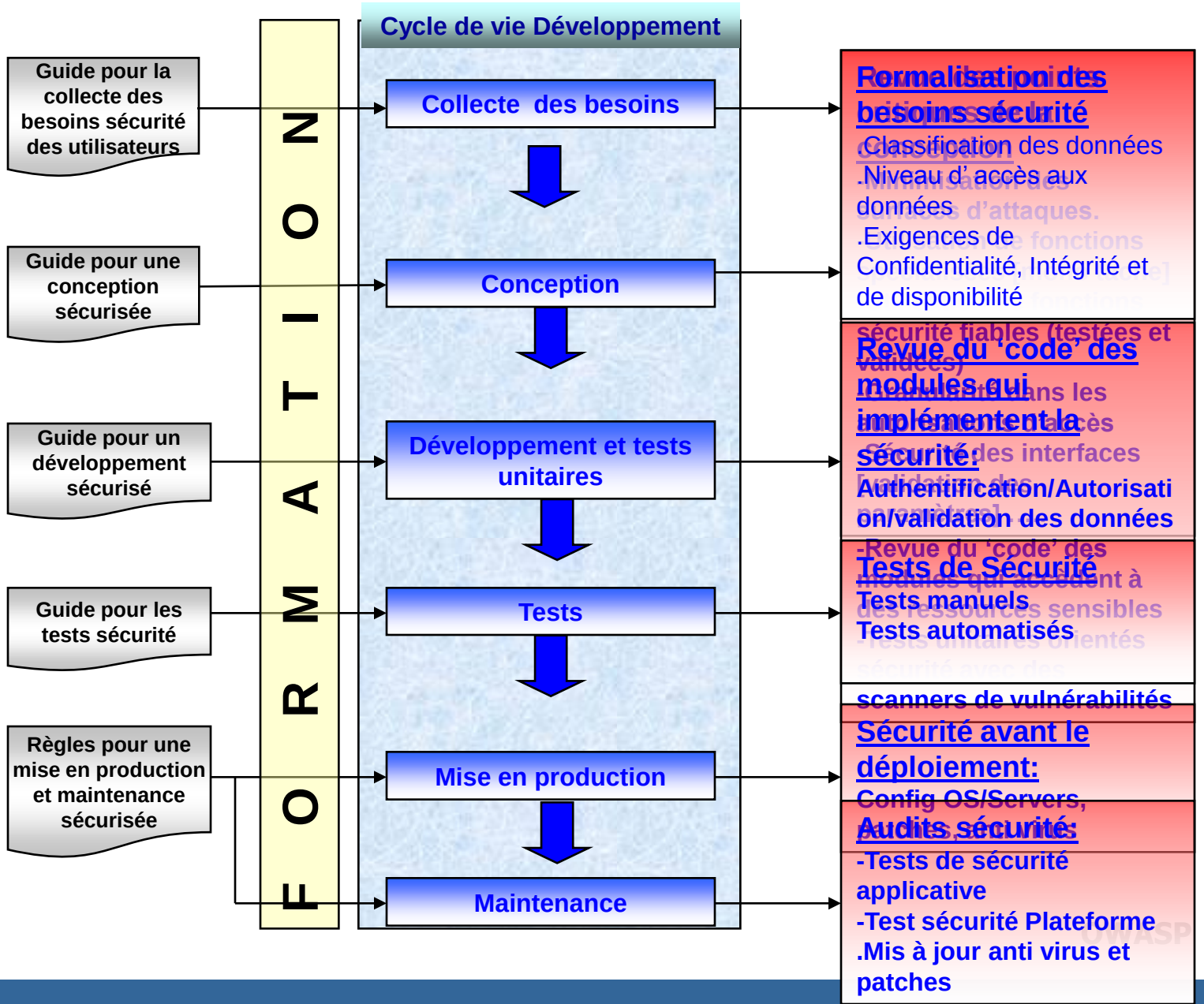
Les limites des pare-feux et autres outils de sécurité



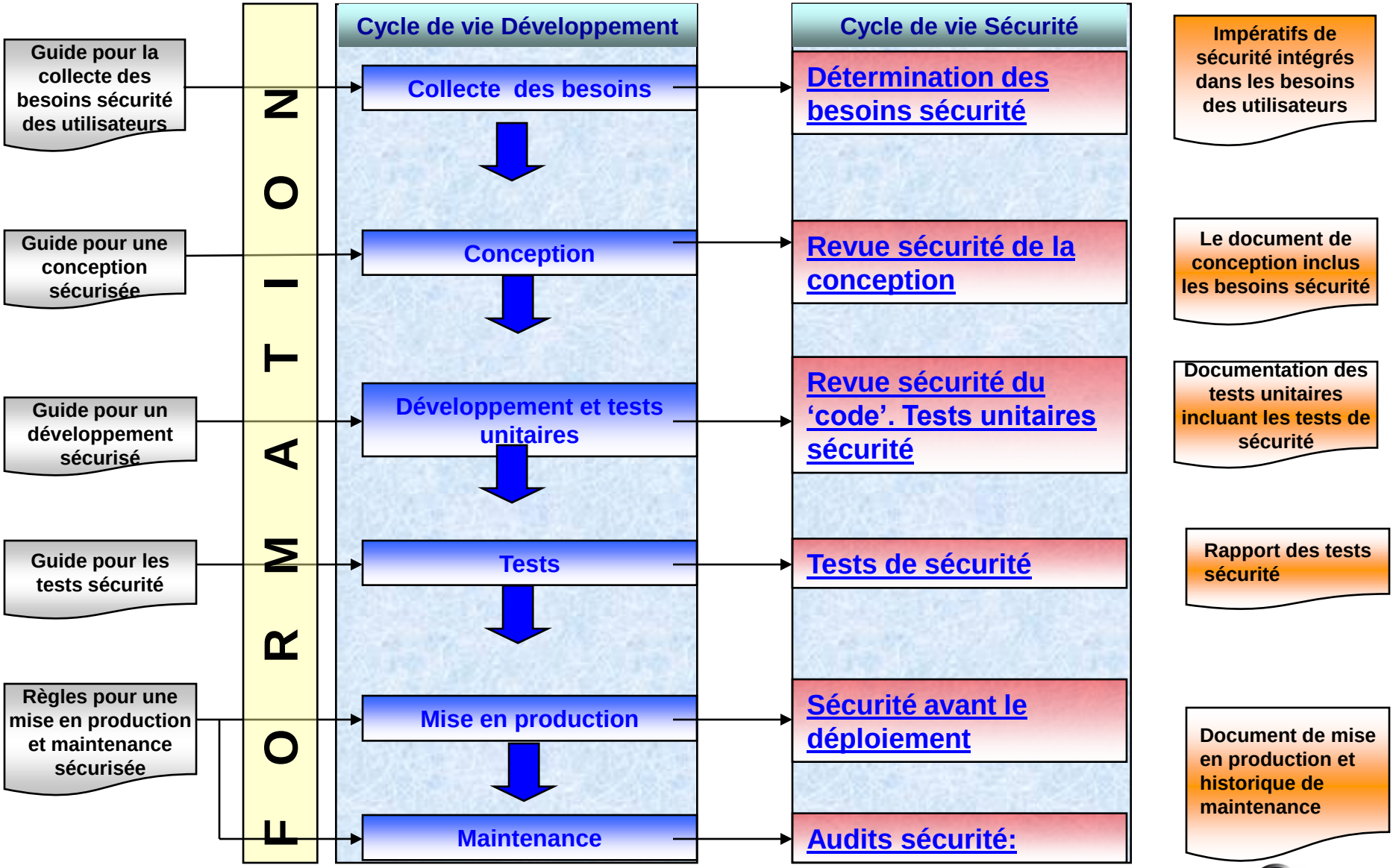
Conclusion: L'application web doit pouvoir se défendre par elle même

Sécurité Intégrée

Sécurité Intégrée



Sécurité Intégrée



Sécurité Intégrée

- Comment aborder la mise en œuvre de la sécurité applicative ?

- Les contraintes
  - Jeune discipline (très peu de référence)
  - Le cycle de vie traditionnel de développement des applications existe et fonctionne
  - Les équipes de développement sont formatées pour opérer dans le cadre du cycle de vie traditionnel
  - Les contraintes de 'temps de développement' sont toujours aussi fortes
  - L'existant : y a t-il des applications en production, vulnérables ?

Expériences d’une mise en œuvre de la sécurité applicative

Démarrer la sécurité applicative 1/2

- Inventaire de l'existant (pas facile dans une organisation décentralisée)
- Identification des applications critiques dans l'existant
  - Exercice qui est fait avec les représentants du business
- Sous-traitance de l'évaluation de la sécurité des applications critiques existantes
- Partager le résultat de l'audit sécurité de l'existant avec le management

Démarrer la sécurité applicative 2/2

- Laisser le soin à la direction de demander à l'équipe de développement de corriger les failles sécurités révélées par l'audit sécurité

Soyez prêt à prendre des coups!

Le point d'entrée dans le cycle de développement : Tests de sécurité

- Facile à faire tant qu'il existe un environnement de test séparé de l'environnement de développement
  - Utilisation de scanner de failles de sécurité
- Sert à démontrer un retour sur investissement immédiat
- Sert à démontrer rapidement que les équipes de développement ont besoin d'un accompagnement pour livrer des applications sécurisées
- Attention, il ne s'agit pas de réduire la sécurité applicative à des tests d'intrusions. Dans la phase de l'implémentation, ils servent à 'vendre' la sécurité applicative aux différents acteurs de sa mise en œuvre

Rechercher des sponsors et les sensibiliser…

- Qui a le plus à perdre quand une faille applicative conduit
  - à la divulgation des secrets compagnie [propriété intellectuelle, données classées]
  - à l'altération des données
  - à la non disponibilité de la plateforme, des applications ou données
  - au non respect des lois en vigueurs [protection des données personnel, SOX, ..]
- Qui a le plus à gagner dans la promotion des outils de collaboration en ligne
  - Faire comprendre aux responsables du Personnel/marketing/ achats/ventes que la sécurité applicative permet de gagner des parts de marché en facilitant la collaboration en ligne [mise a disposition des processus business automatisés et sécurisés] avec les employés, les clients, fournisseurs et partenaires

Rechercher des sponsors et les sensibiliser…

- Organiser des séances de 'sensibilisation' à la sécurité applicative pour les responsables business
- Se positionner auprès du business comme le défenseur de leurs intérêts auprès des équipes de développement
- Expliquer aux responsables business que leurs applications et leurs données sont en danger d'une part et peuvent être utilisées comme vecteur d'attaque du réseau de la compagnie d'autre part.
- L'équipe sécurité applicative est là pour les aider à se protéger

Guides de sécurité applicative

- Développer des guides sécurité applicative à l'intention des équipes de développement
  - Guide pour collecter des besoins sécurité des utilisateurs
  - Guide pour une conception sécurisée
  - Guide pour un codage sécurisée
  - Guide pour les tests de sécurité applicative
- Attention aux 'copy/paste'. Les guides doivent être adaptés aux méthodes et outils utilisés par les équipes de développement
- Il est important que les contrôles recommandés dans les guides soient validés par les équipes de développement

Sensibiliser les équipes de développement à la sécurité applicative (exercice difficile)

- Formation des concepteurs et des développeurs sur la prévention des failles les plus fréquentes 'Top 10 OWASP'
  - Comment tenir compte des 'TOP 10' pendant les phases de conception et de codage
- Faire développer et mettre à disposition des développeurs des 'modules sécurité' centraux
  - Module de validation des paramètres
  - Module de gestion des autorisations
  - Module de gestion des erreurs
  - .....
- Avoir beaucoup de tact car les développeurs n'aiment pas trop que quelqu'un leur 'apprenne' comment coder...

Les revues sécurité dans le cycle de vie

- Adopter 2 ou 3 architectures de référence
  - Faire auditer les architectures par des experts en sécurité
- Pendant les revues, s'assurer que la conception intègre une des architectures de référence
- Une bonne compréhension des protocoles de communication est vitale
  - Se méfier des protocoles propriétaires
- S'assurer que les règles définies dans les Guides sont appliquées

Les revues sécurité dans le cycle de vie

- Alors que la revue sécurité dans la phase de conception est relativement facile, la revue sécurité du code est souvent la plus difficile à mettre en œuvre
- Une approche possible est de faire faire la revue sécurité du code par les développeurs eux mêmes
- Dans ce cas, l'équipe sécurité applicative assiste les développeurs pendant la revue en leur indiquant les modules les plus importants à revoir

Les tests sécurité dans le cycle de vie

- Tests unitaires de sécurité pendant le développement
  - Difficile à mettre en œuvre à moins de le faire faire par les développeurs eux-mêmes (tests manuels seulement)

- Tests sécurité intégrés
  - Tests manuels
    - Authentification
    - Autorisation
    - ….
  - Tests automatisés
    - Se méfier des faux positifs

Les tests sécurité dans le cycle de vie

- Les failles révélées par les tests sécurité sont classées comme: Élevée, Moyenne et Faible

- La classification prend en compte plusieurs paramètres
  - La nature de l'application
  - L'importance de la faille
  - L'environnement de l'application (internet, extranet, intranet)
  - Les caractéristiques des groupes d'utilisateurs

Les tests sécurité dans le cycle de vie

- Les failles sécurité classées Élevées, sont corrigées avant la mise en production
- Les failles sécurité classées Moyennes, sont corrigées avant la mise en production [sauf situation exceptionnelle]. Dans ce cas, un délai est accordé pour la correction
- Si les failles classées faibles ne peuvent être corrigées dans l'immédiat, elles seront corrigées dans la release suivante de l'application

Les tests sécurité dans le cycle de vie

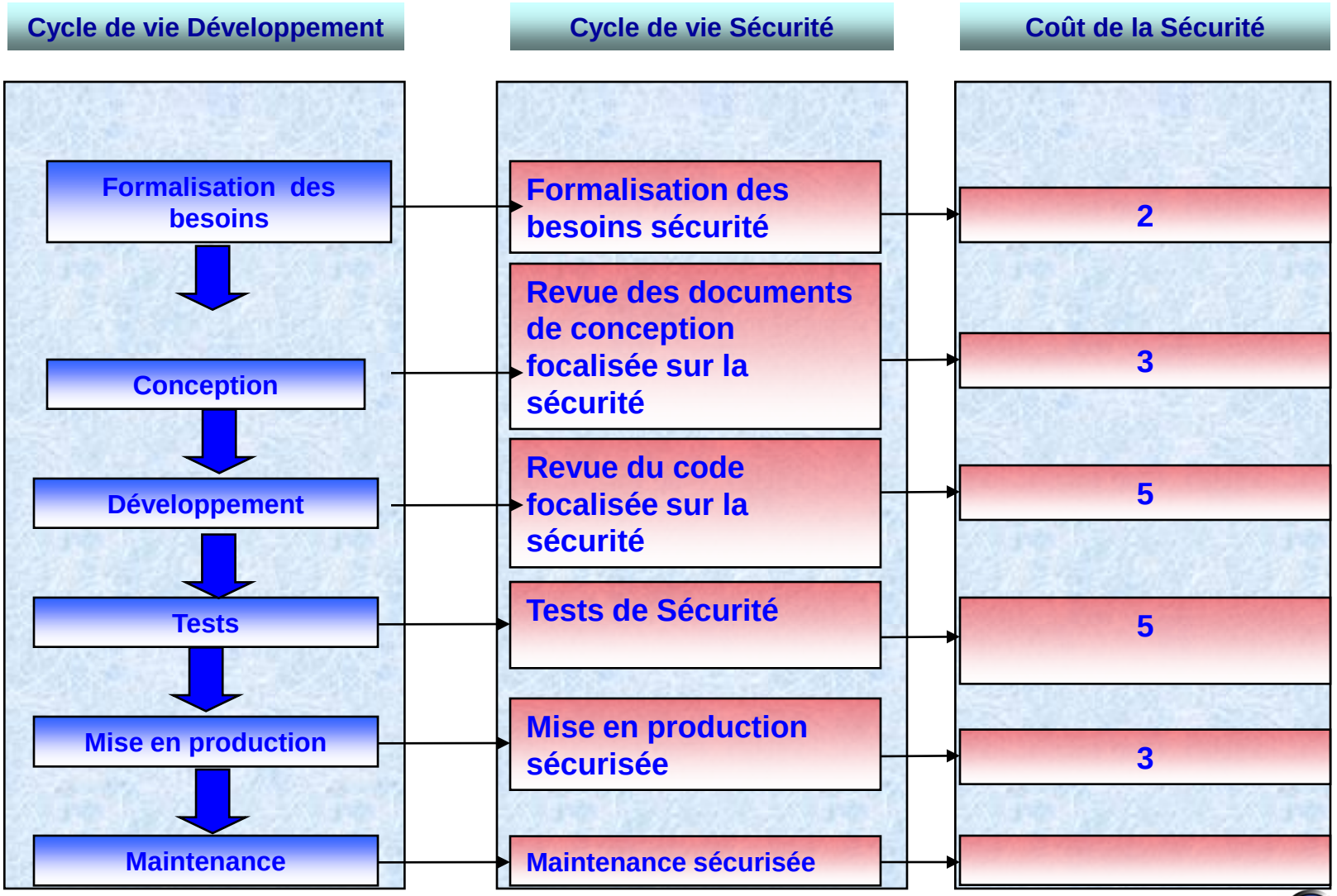
- Les tests de sécurité sont un bon baromètre de la sécurité intégrée.

- Plus il y a de failles sécurité identifiées lors des tests, moins la sécurité est intégrée dans le cycle de vie, et plus d'efforts (temps+argent) sont requis pour corriger les failles de sécurité.

Les audits de sécurité en production

- Tests sécurité automatisés sur la production 2 fois par an
- Tous les 2 ans des tests sont conduits par des compagnies d'audits externes
- Pas de défi particulier à part la maÎtrise des outils d'audit utilisés

Risques d'implémentation d'un cycle de vie de la sécurité applicative en parallèle



Les obstacles à l'implémentation de la sécurité applicative

- Lorsque le management IT/Business n'est pas sensibilisé à la sécurité applicative
- Lorsque le cycle de développement des applications est inexistant ou pas assez structuré
- Lorsqu'il y a résistance au changement et des luttes de pouvoir
- Lorsque l'équipe de sécurité applicative est en dehors de l'équipe de développement

Les obstacles a l'implémentation de la sécurité applicative

- Lorsque l'équipe de sécurité applicative ne peut parler la même langue que les développeurs
- Lorsque les projets de développement d'applications sont cachés à l'équipe de sécurité applicative
- Lorsque le chef de projet ne se sent pas responsable de la sécurité de son application
- Lorsque la sécurité n'est pas intégrée, mais est parallèle au cycle de vie (coût apparent en temps et en argent)

Sécurité intégrée

Notification pendant la phase d'initiation du projet. Rendez vous est pris avec le chef de projet pour la phase de collecte des besoins

Collecte des besoins fonctionnels incluant les besoins sécurité

Conception

Validation du plan de déroulement du projet qui doit inclure les étapes sécurité

Revue 'sécurité' de la conception

.Revue sécurité assurée par l'expert sécurité applicative

Développement et tests unitaires incluant la sécurité

.Test unitaires sécurité assurés par les développeurs
.Revue sécurité assurée par les développeurs avec l'aide de l'expert sécurité applicative

Tests

Tests de Sécurité

.Tests de sécurité assurés par l'expert sécurité applicative

Mise en production sécurisée

.Par l'équipe 'mise en production' sur base de checklist sécurité.

Audit sécurité

.Audit sécurité assuré/coordonné par l'expert sécurité applicative

Conclusion

- Les contraintes de la mise en œuvre de la sécurité intégrée sont les mêmes pour les organisations ayant adopté le cycle de vie de développement d'application traditionnel
- Les voies et les moyens de la mise en œuvre de la sécurité intégrée sont forcément liés au type d'organisation en place dans les entreprises
- Une sécurité intégrée effective passe par la formation et l'intégration d'experts sécurité applicative dans les équipes de développement
- Il faut compter 2 à 3 ans pour que la machine soit rodée

QUESTIONS?

Backup : introduction

- Je suis donc Gilbert Agopome un ancien du CSSI

- Pendant un peu plus d'une demi heure, je vais vous présenter en quelques diapos :
  - Rappeler le contexte : pourquoi les applications business sont davantage à risque aujourd'hui qu'elles ne l'étaient hier?
  - Je vous présenterai ensuite l'approche théorique de l'intégration de la sécurité applicative dans le cycle de vie de développement des applications
  - Et enfin je partagerai avec vous une expérience personnelle de la mise en œuvre de cette théorie dans l'entreprise pour laquelle je travaille

Backup : introduction à diapo 2

- On pourrait se demander pourquoi tout ce tintamarre autour des applications web ?
- Dans le temps [il y a 15, 20 ans], je suis sûr que les applications avaient déjà des failles de sécurité.
- Qu'est ce qui a changé ?

Backup : Introduction diapo 7 Sécurité Intégrée

- Le cadre proposé par la théorie pour intégrer la sécurité dans le cycle de vie du développement est tout à fait cohérent

- Ce que la théorie ne dit pas, c'est le comment
  - Comment arriver à sauter dans le train du cycle de vie traditionnel de développement des applications, le rattraper et l'intégrer en marche et sans le ralentir

Backup : introduction diapo 9

- Mon expérience de la mise œuvre de la sécurité applicative est intimement liée, j'en suis sûr, à la configuration de l'organisation de l'entreprise pour laquelle je travaille
- D'autres type d'organisations induiraient, j'en suis convaincu, des expériences différentes
- Dans mon cas, les donneurs d'ordres sont dans l'entreprise et je les côtoie tous les jours
- Dans mon cas, je connais l'équipe sécurité de nos partenaires stratégiques [cela a son importance…]