Arch. Security Advisor

Cédric Hébert, CISSP, SAP Research Security&Trust
6 Juin 2012

PRAGMATIQUE

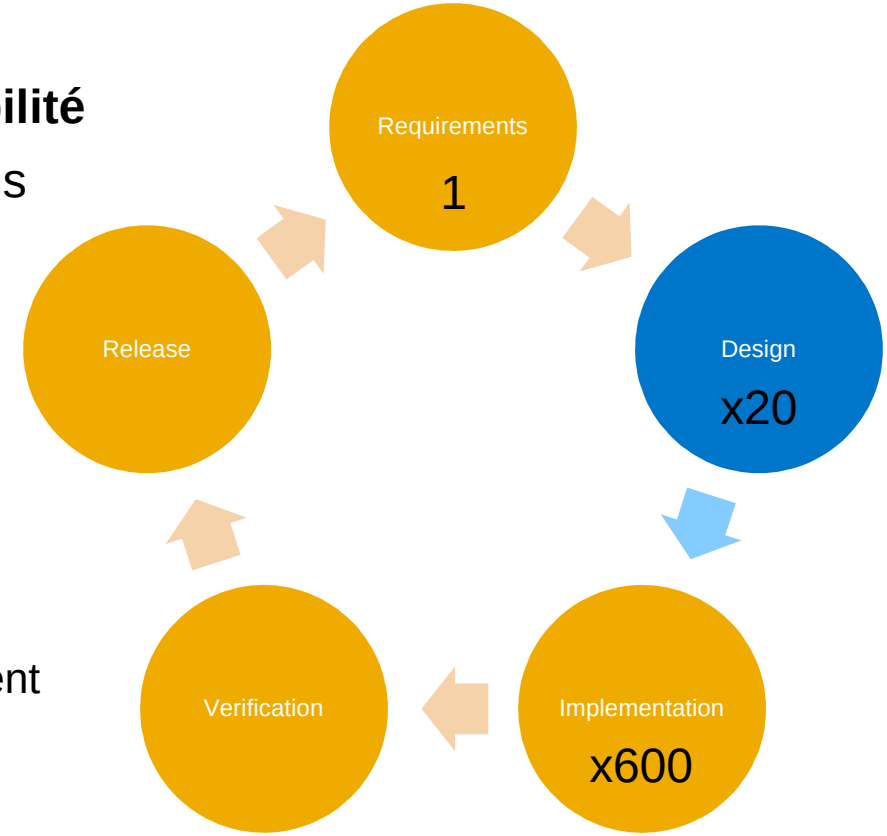
Cycle de vie d’un logiciel

Coût de réparation d’une vulnérabilité

(# personnes * # jours) / # réparations

- Prérequis: coût = 1
- Conception: coût = 20x
- Implémentation: coût = 600x

Il est crucial de prévenir les défauts
au plus tôt dans le cycle de développement



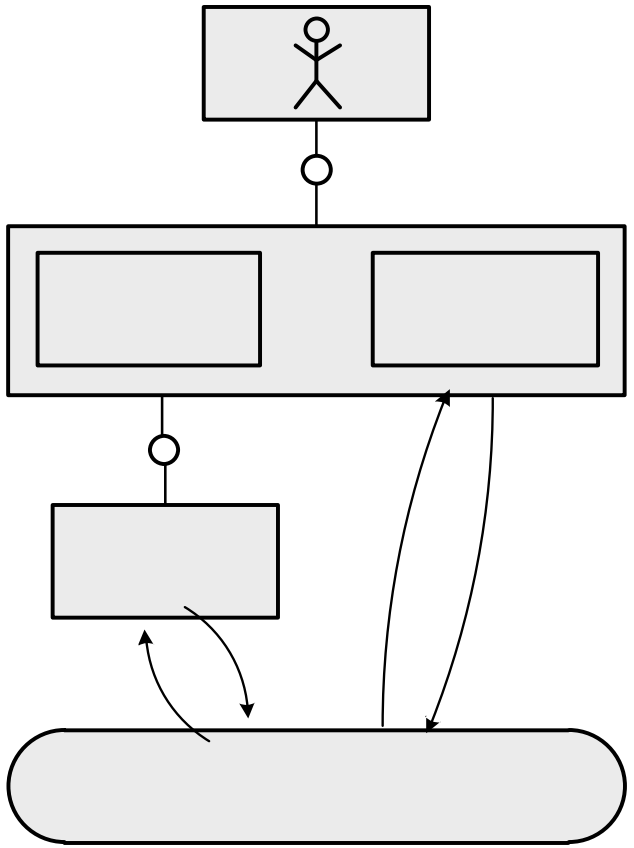
Phase de Design

Document d'Architecture

Détaille les nouvelles fonctionnalités

- Diagramme "TAM"
- Description détaillée
- Impact sur les applications existantes

Capture les déviations par rapport aux standards



Standards de sécurité…

OWASP: Top 10

SANS: Top 20

STRIDE: 74 tests de couverture

CAPEC: plus de 400 attaques répertoriées

… sans compter les législations en vigueur (SOX, BASEL II, HIPAA)

… ni les ‘best practices’ internes

Un outil de support…

… Pour l’architecte

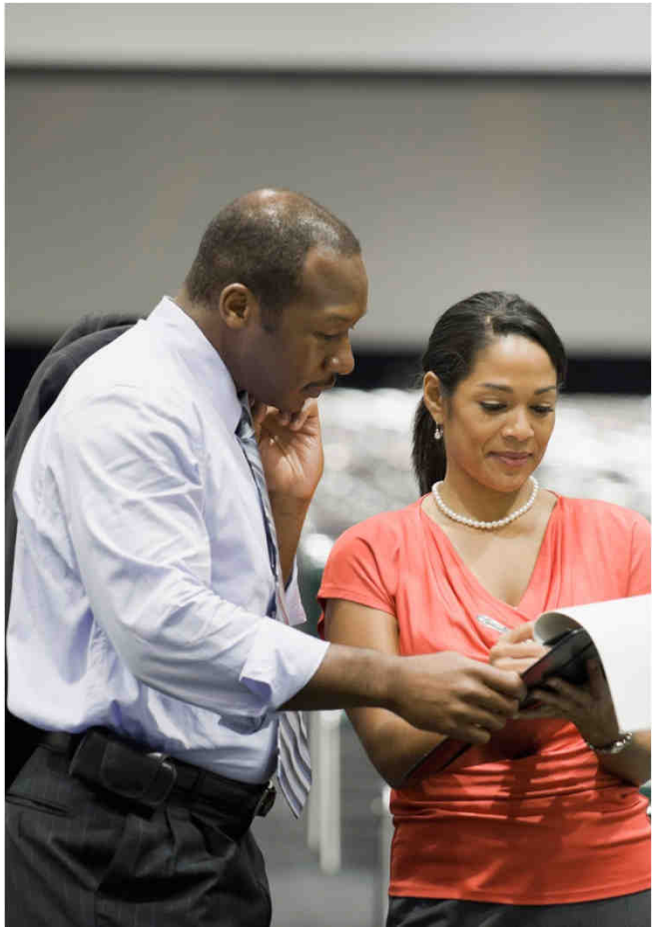
“Que dois je considérer pour sécuriser mon application ? ”

… Pour l’expert en sécurité

“Quelles sont les spécificités de l’application que je dois auditer? ”

… Pour les développeurs

“Comment implémenter correctement mon application sécurisée? ”



Architecture Security Advisor

DEMO

ASA et le cycle de vie

Une base de connaissances

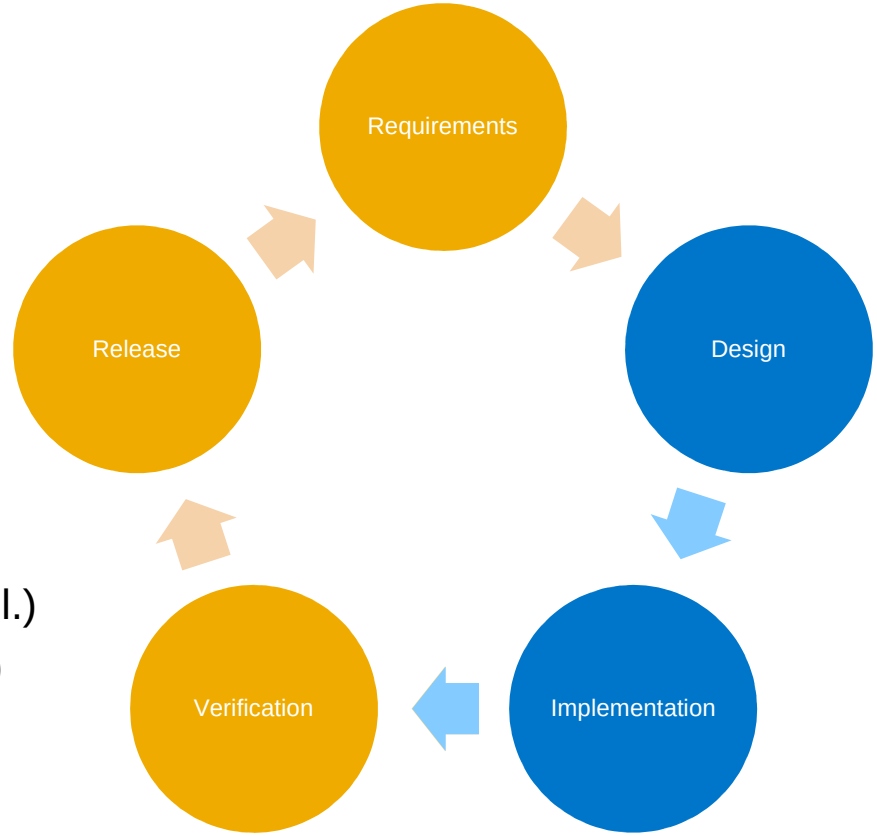
Les informations sont utilisables:

- Pour la sécurité
- Pour d'autres standards

Une construction par couches

Les briques existantes:

- Étendent la portée des évaluations (impl.)
- Réduisent la fenêtre d'évaluation (delta)



Travaux en cours

Exploiter davantage le diagramme

Parcours du diagramme

- Détection des flux de données

Annotations des agents

- Détection des ‘backend’, ‘frontend’, etc.

Automatiser l’évaluation

Simulation de scénarios d’attaque sur le TAM

- Travaux en cours sur des arbres d’attaque

Généraliser l’approche

Rendre le prototype disponible pour d’autres tests

- Une dizaine de listes de directives à suivre
- Amélioration de la qualité des diagrammes
  - Et des analyses

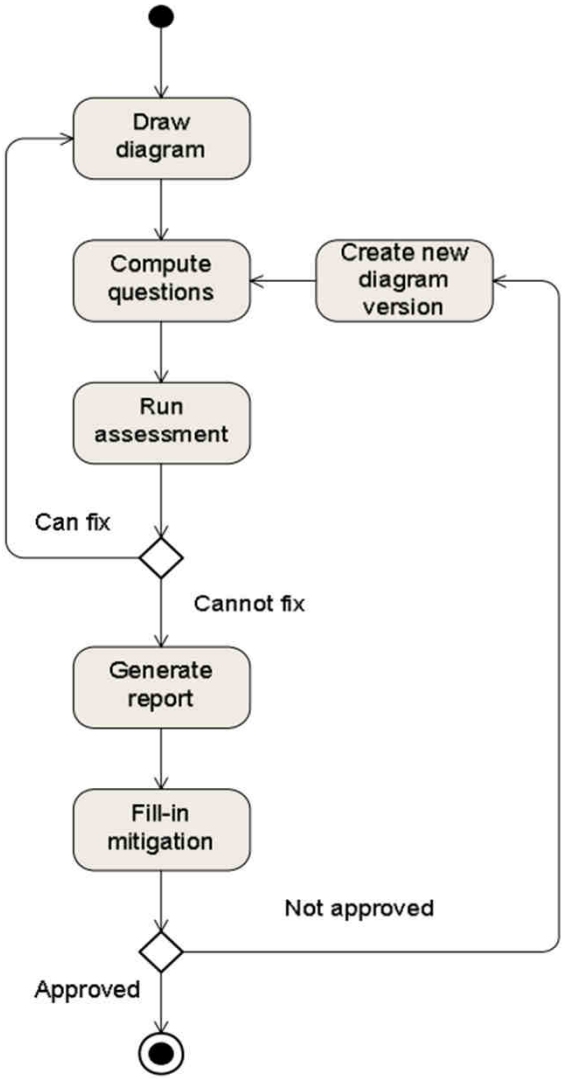
Merci !

Me contacter:

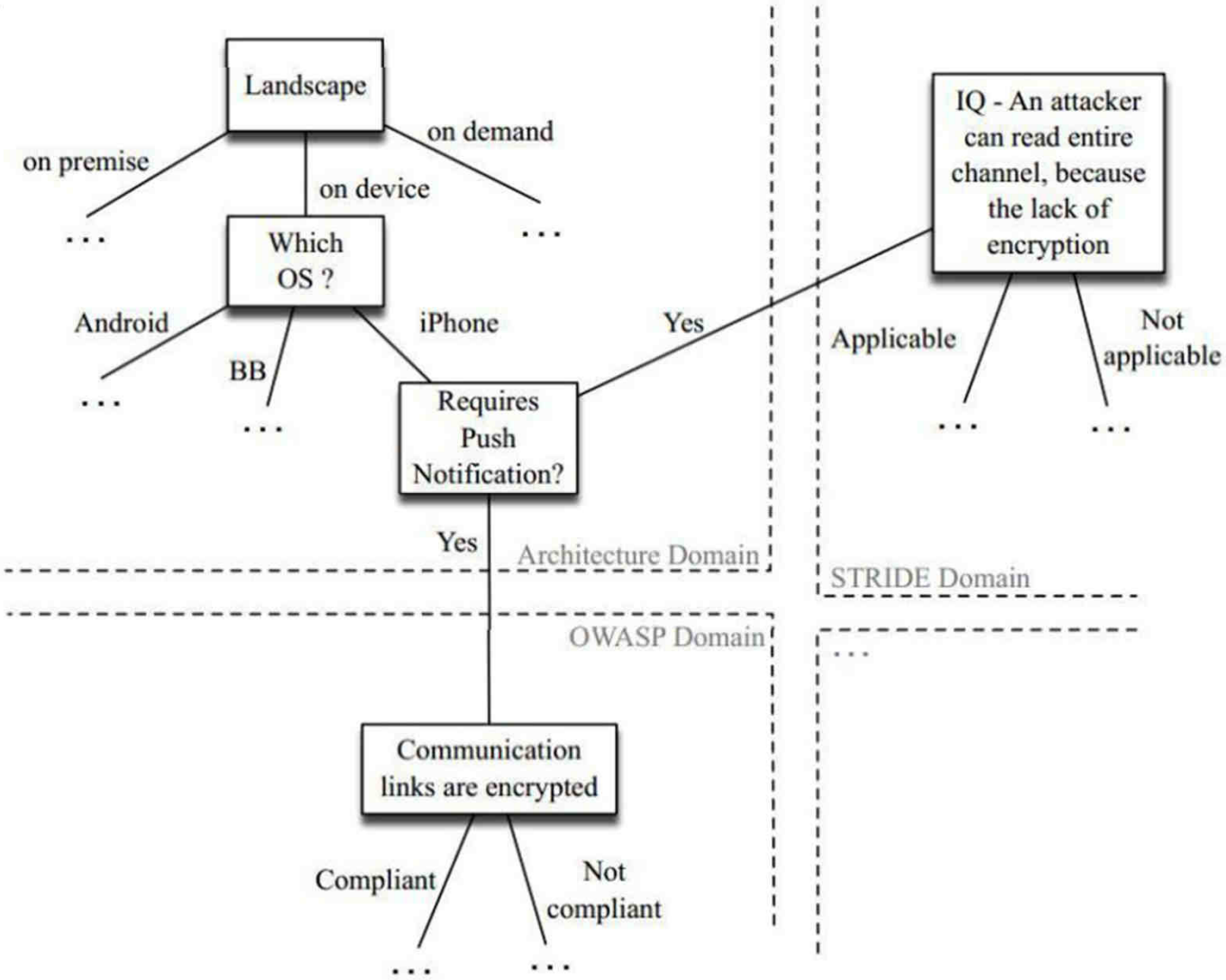
Cédric Hébert
SAP Labs France
1, rue du Docteur Maurice Donat – 06250 Mougins
cedric.hebert@sap.com

BACKUP

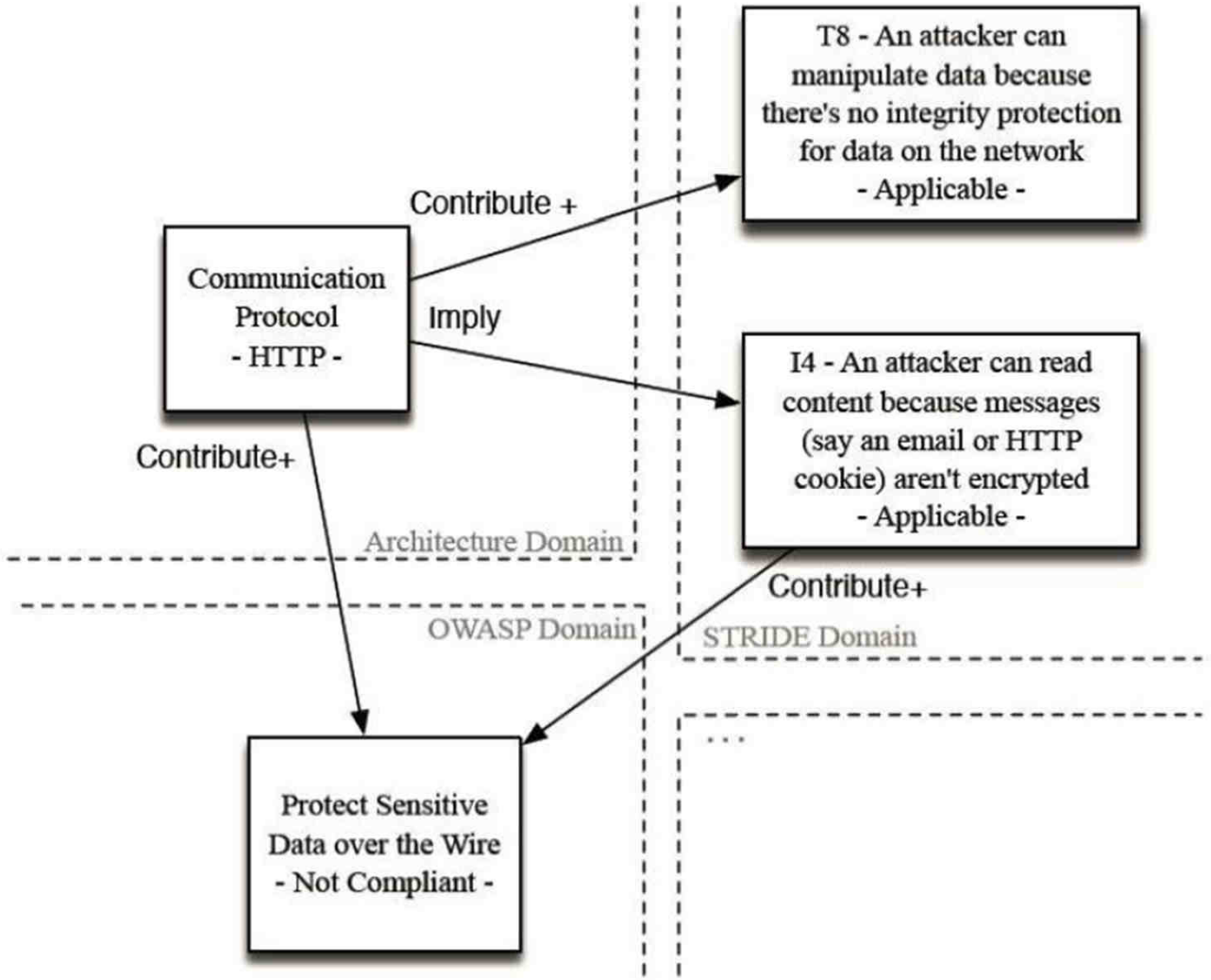
Processus principal



Projections de dépendances

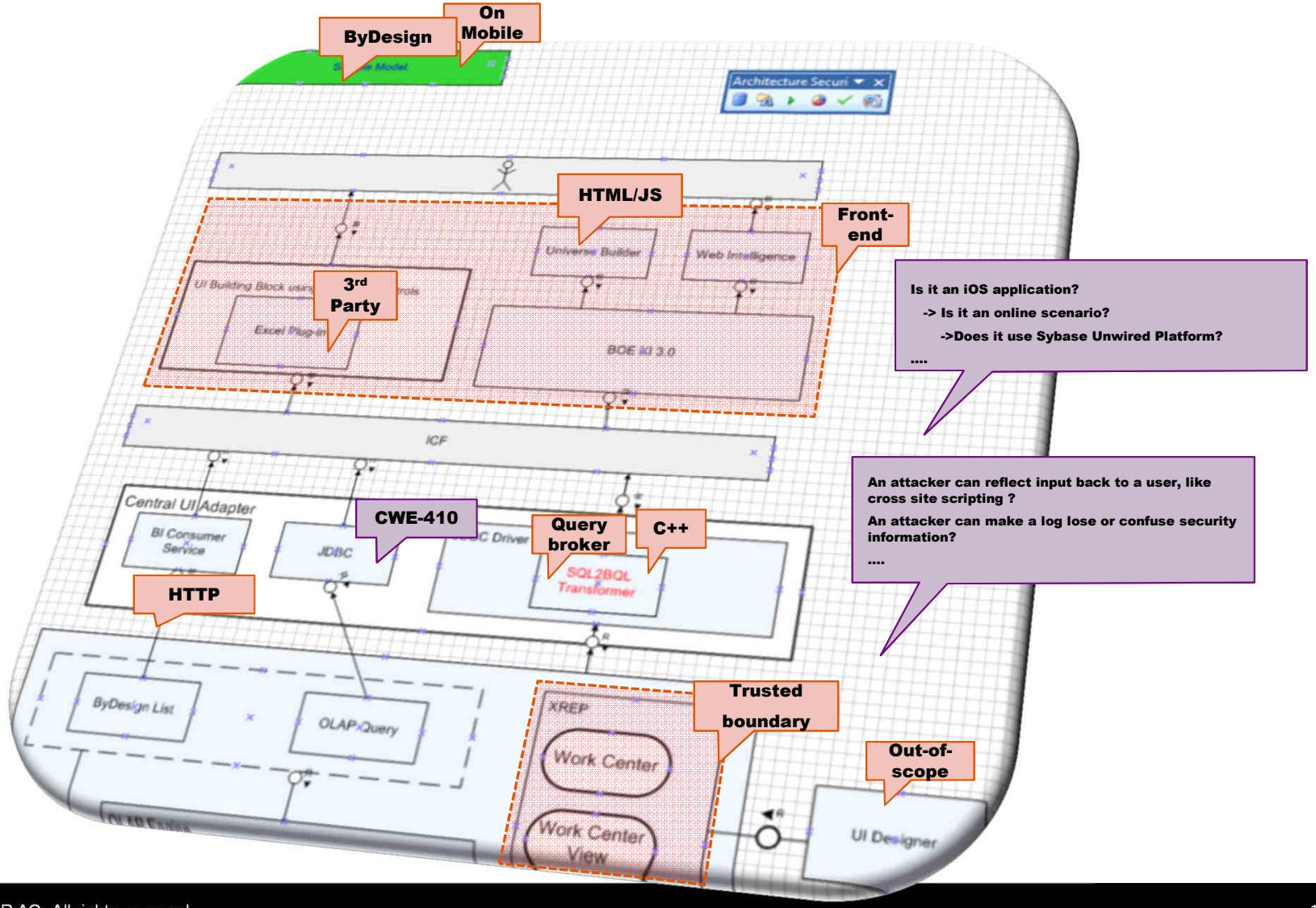


Projections d’impact



Architecture driven security assessment

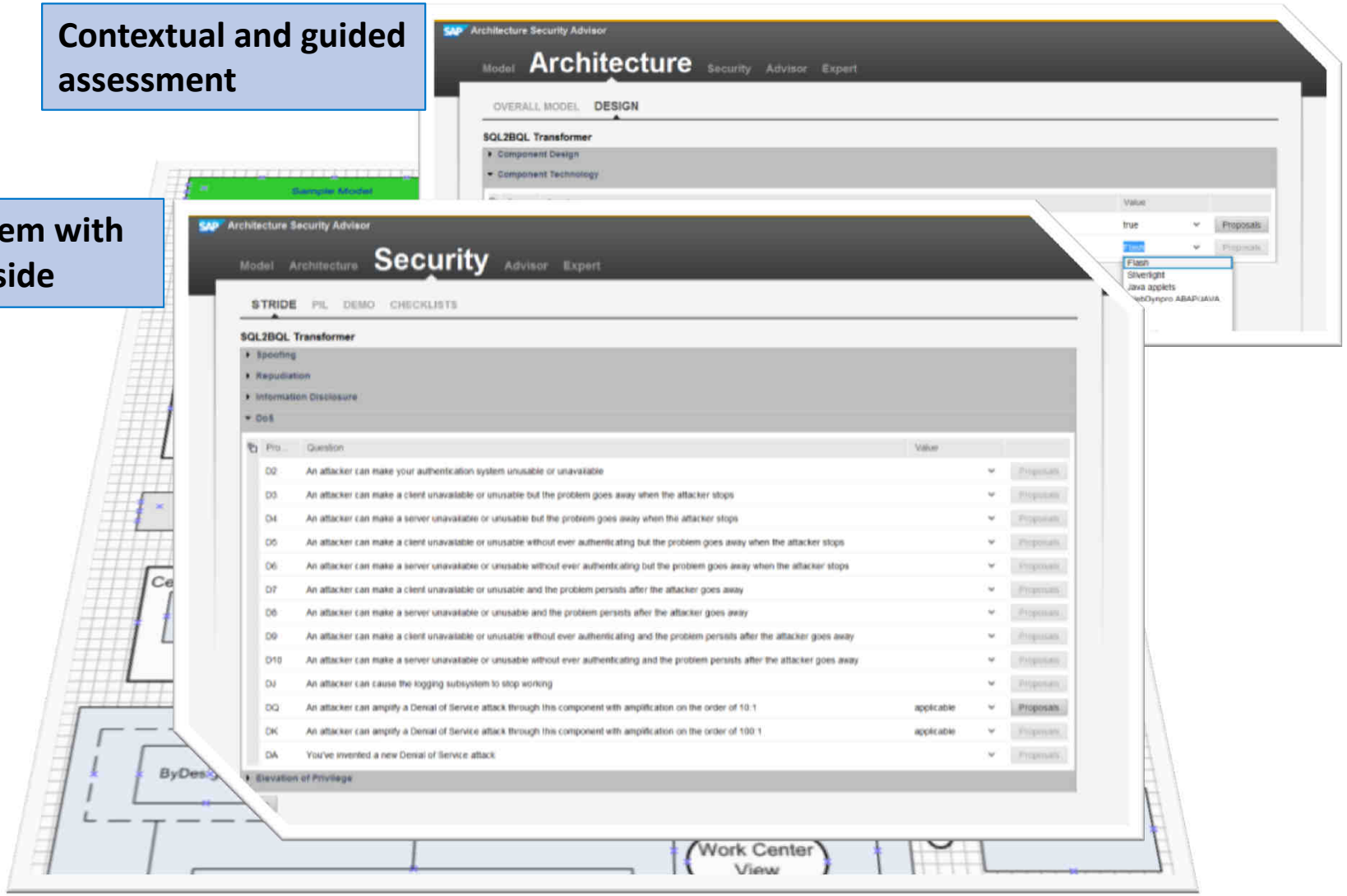
Collect architecture information and focus on security related inputs



Security expert system

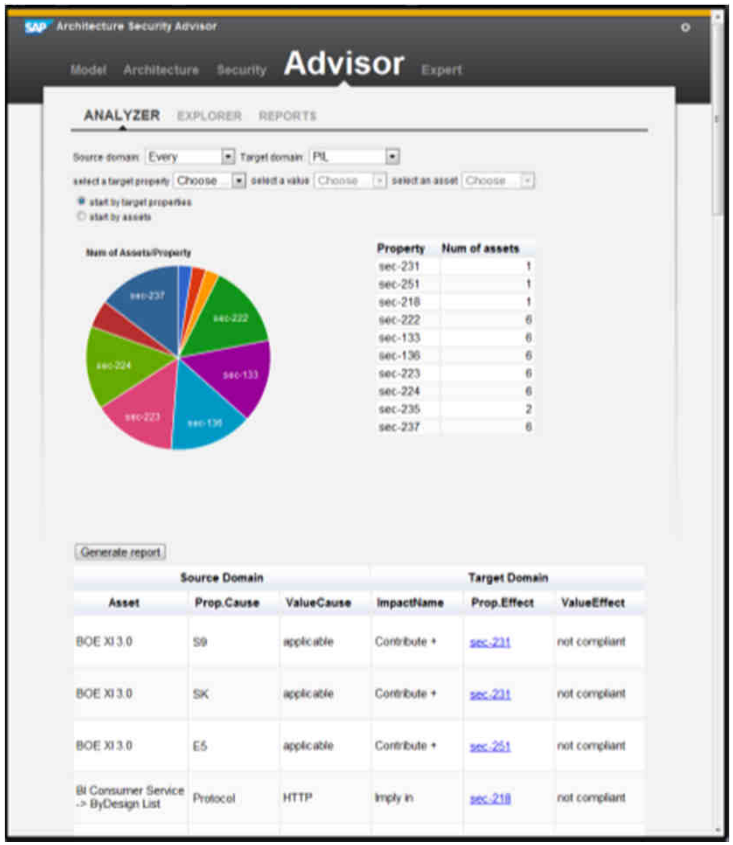
Contextual and guided assessment

Expert system with Security inside



Security Advisor

Detect and understand the cause of potential security issues in order to mitigate and comply with Product Standard Security Requirements



© 2012 SAP AG. All rights reserved.