

Arch. Security Advisor

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



PRAGMATIQUE

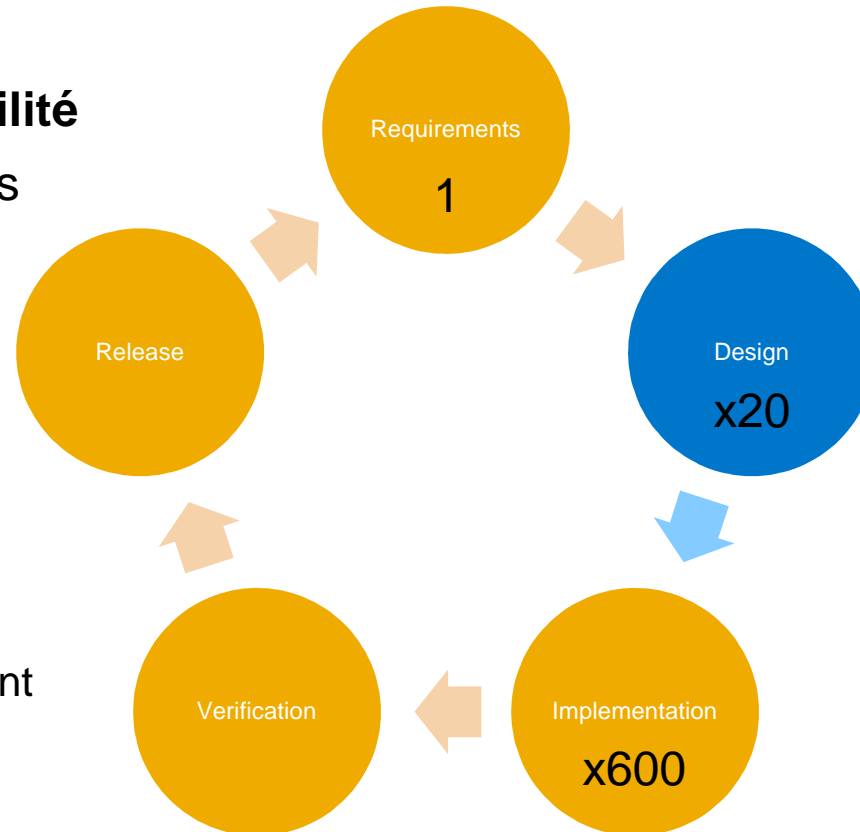
Cycle de vie d'un logiciel

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



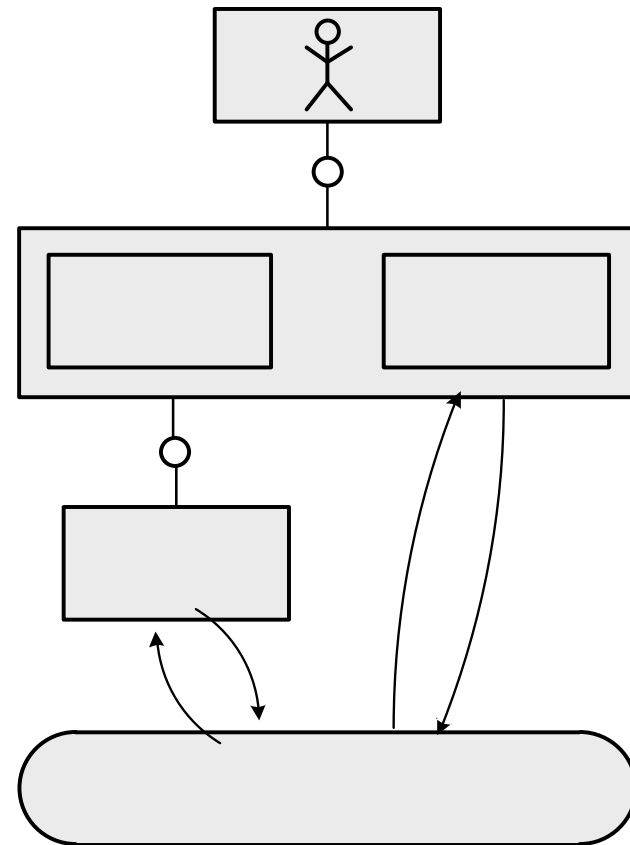
Phase de Design

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

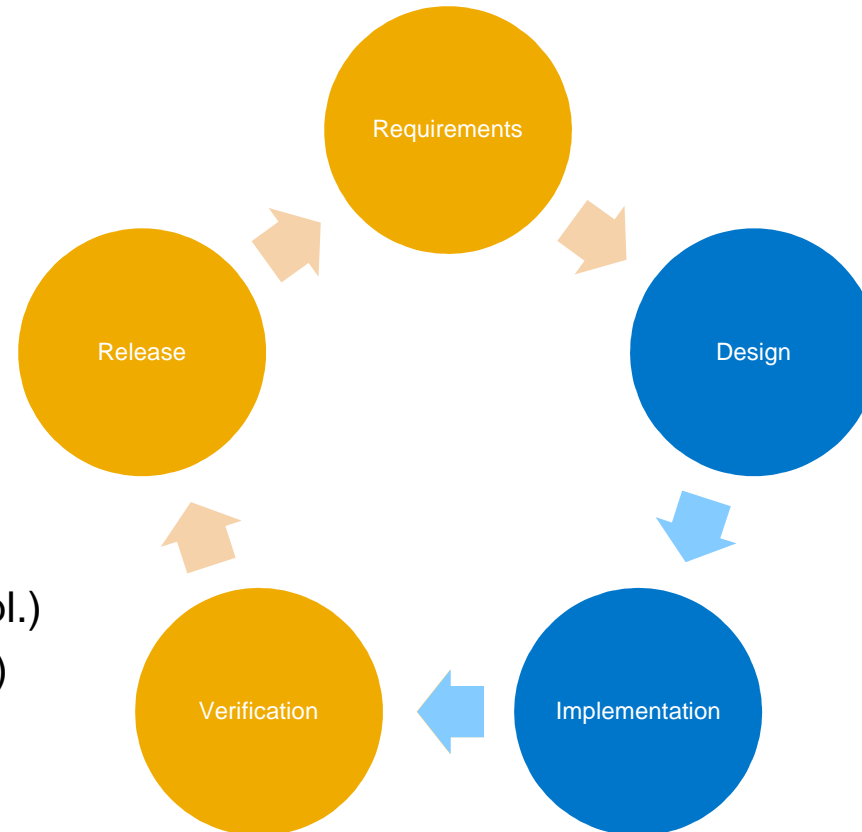
Les informations sont utilisables:

- 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





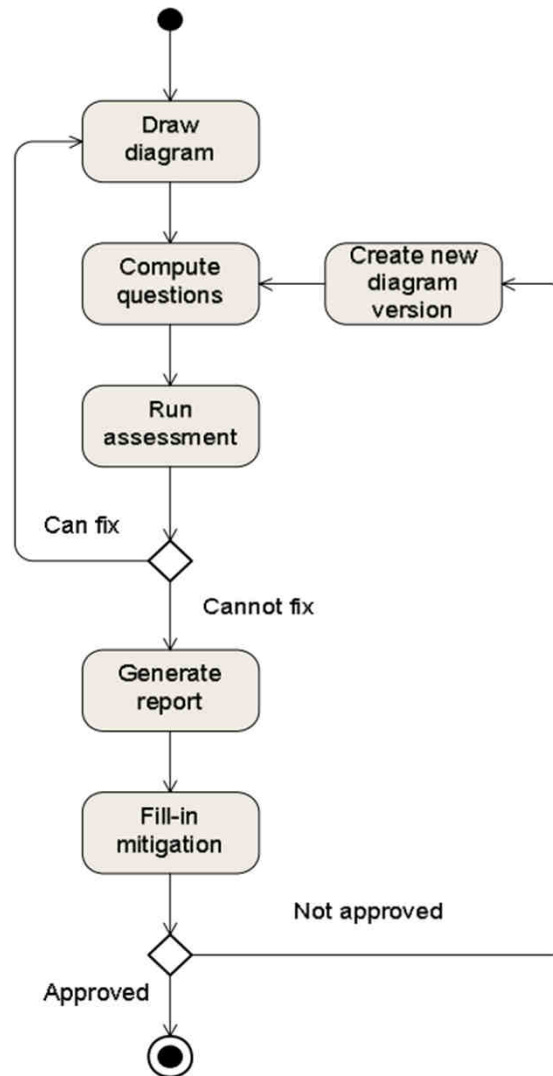
Merci !

Me contacter:

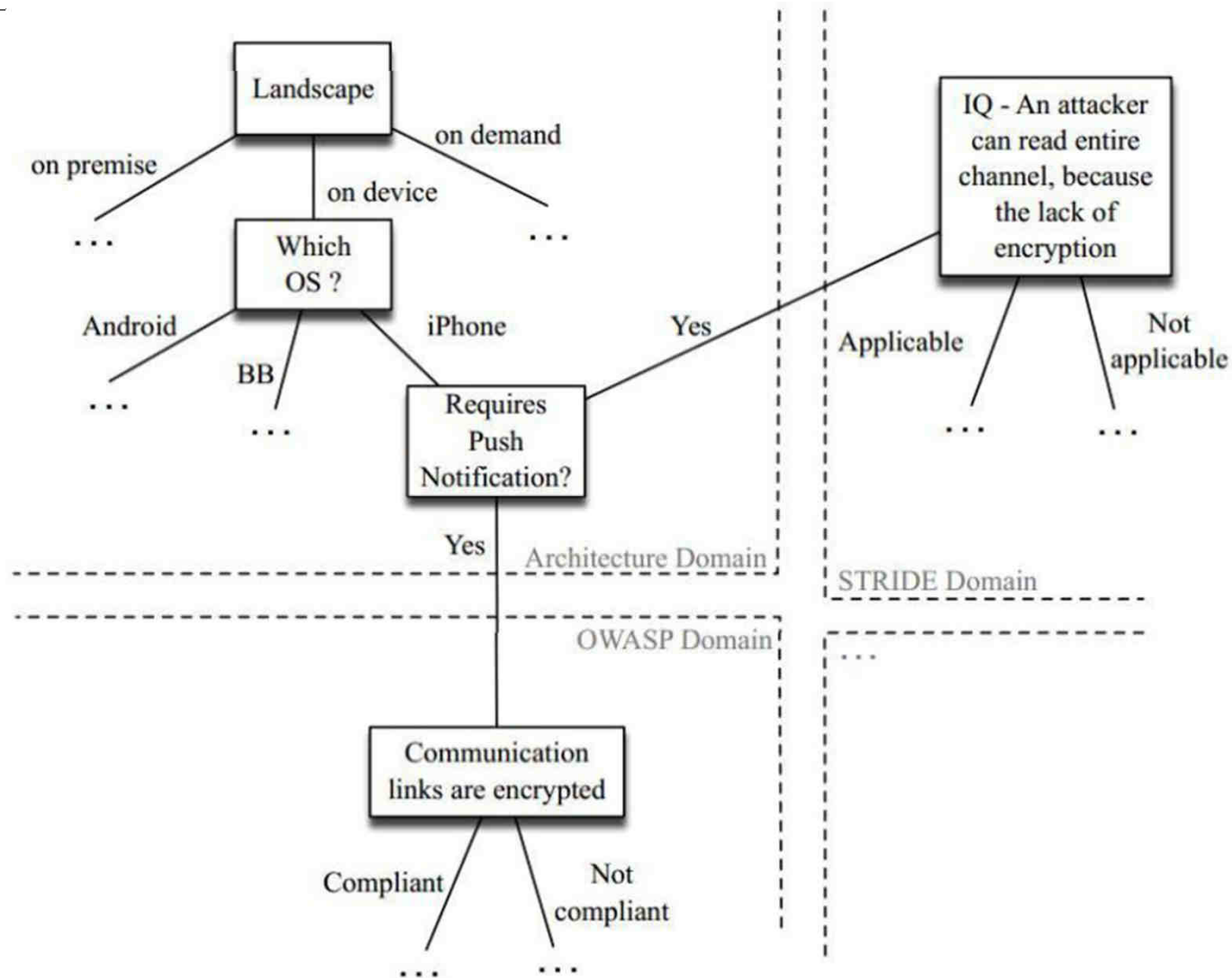
Cédric Hébert
SAP Labs France
1, rue du Docteur Maurice Donat – 06250 Mougins
cedric.hebert@sap.com

BACKUP

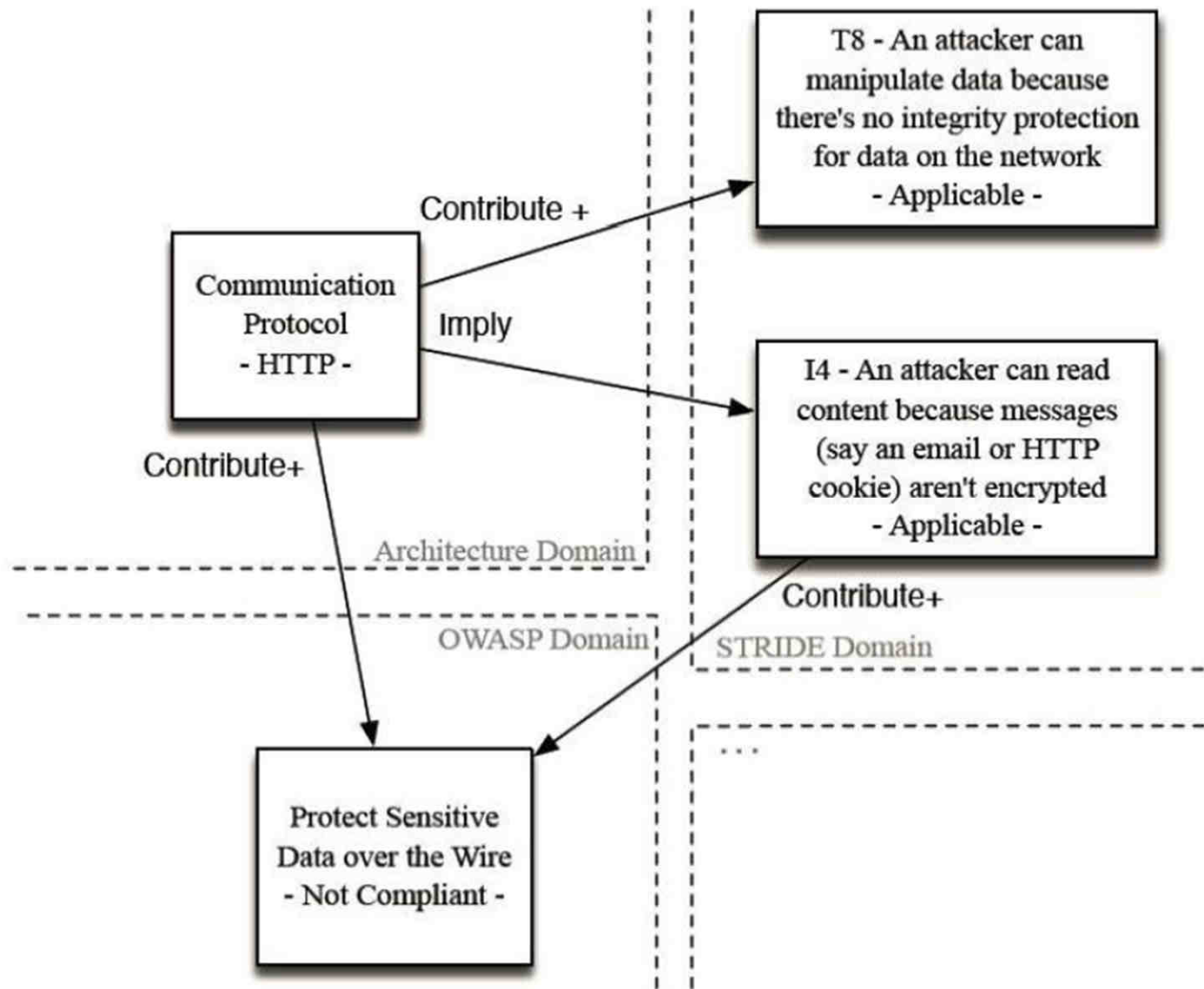
Processus principal



Projections de dépendances

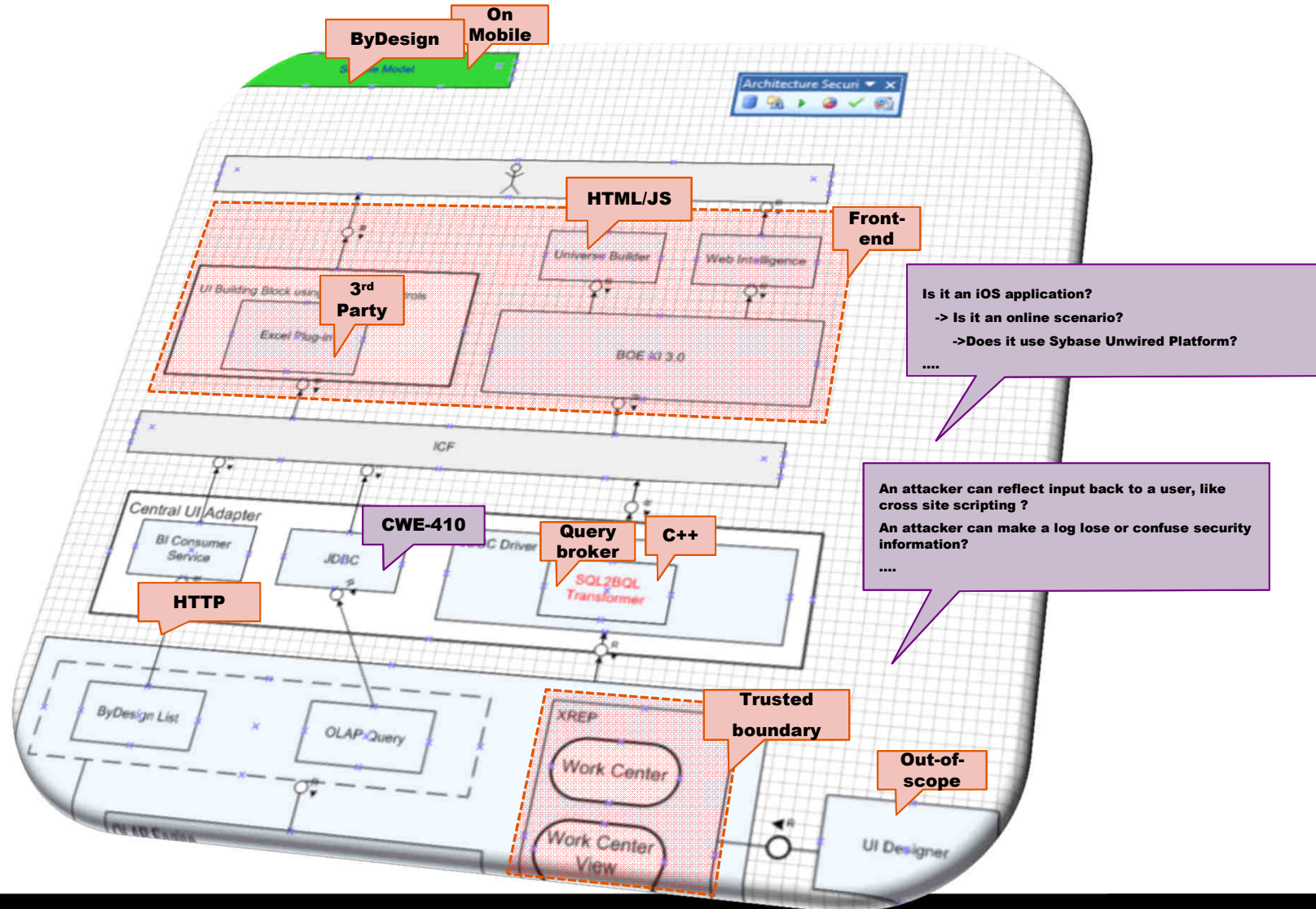


Projections d'impact



Architecture driven security assessment

Collect architecture information and focus on security related inputs



Security expert system

Contextual and guided assessment

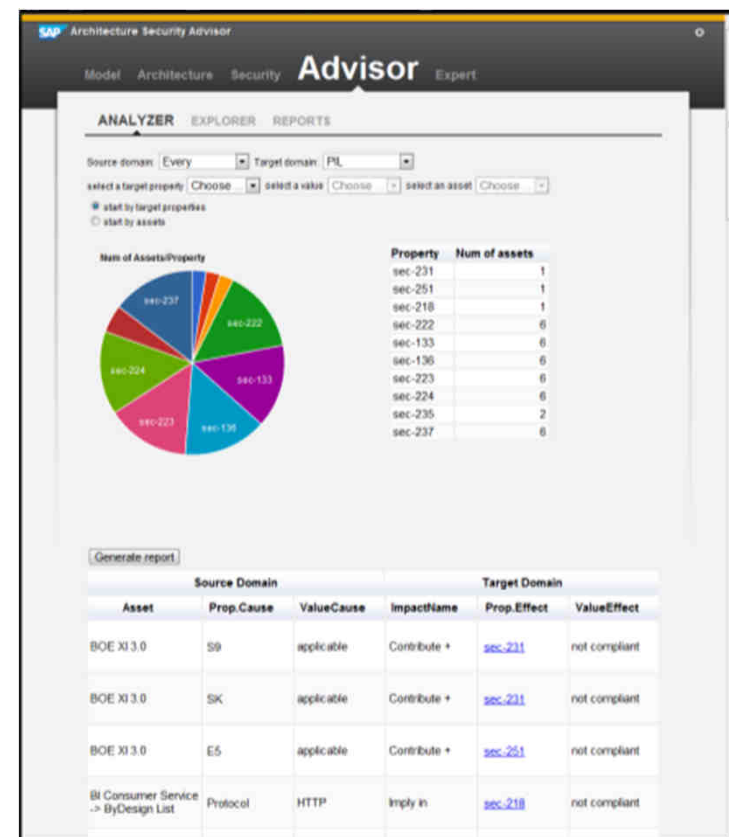
Expert system with Security inside

The screenshot displays the SAP Architecture Security Advisor interface. The top navigation bar includes 'Model', 'Architecture', 'Security', 'Advisor', and 'Expert'. The main content area is titled 'Architecture' and shows a tree view for 'SQL2BQL Transformer' under 'Component Design'. A 'Security' view is overlaid, showing a table of security questions (DQ, D1, D2, etc.) with columns for 'Pro...', 'Question', 'Value', and 'Proposals'. The 'Proposals' column contains dropdown menus with options like 'True', 'False', 'Silverlight Java applets', and 'WebDynpro ABAP/UIVA'. A 'Work Center View' is visible at the bottom right.

Pro...	Question	Value	Proposals
D2	An attacker can make your authentication system unusable or unavailable		Proposals
D3	An attacker can make a client unavailable or unusable but the problem goes away when the attacker stops		Proposals
D4	An attacker can make a server unavailable or unusable but the problem goes away when the attacker stops		Proposals
D5	An attacker can make a client unavailable or unusable without ever authenticating but the problem goes away when the attacker stops		Proposals
D6	An attacker can make a server unavailable or unusable without ever authenticating but the problem goes away when the attacker stops		Proposals
D7	An attacker can make a client unavailable or unusable and the problem persists after the attacker goes away		Proposals
D8	An attacker can make a server unavailable or unusable and the problem persists after the attacker goes away		Proposals
D9	An attacker can make a client unavailable or unusable without ever authenticating and the problem persists after the attacker goes away		Proposals
D10	An attacker can make a server unavailable or unusable without ever authenticating and the problem persists after the attacker goes away		Proposals
D1	An attacker can cause the logging subsystem to stop working		Proposals
DQ	An attacker can amplify a Denial of Service attack through this component with amplification on the order of 10:1	applicable	Proposals
DK	An attacker can amplify a Denial of Service attack through this component with amplification on the order of 100:1	applicable	Proposals
DA	You've invented a new Denial of Service attack		Proposals

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.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, PowerPoint, Silverlight, and Visual Studio are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, z10, z/VM, z/OS, OS/390, zEnterprise, PowerVM, Power Architecture, Power Systems, POWER7, POWER6+, POWER6, POWER, PowerHA, pureScale, PowerPC, BladeCenter, System Storage, Storwize, XIV, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, AIX, Intelligent Miner, WebSphere, Tivoli, Informix, and Smarter Planet are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the United States and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and its affiliates.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems Inc.

HTML, XML, XHTML, and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Apple, App Store, iBooks, iPad, iPhone, iPhoto, iPod, iTunes, Multi-Touch, Objective-C, Retina, Safari, Siri, and Xcode are trademarks or registered trademarks of Apple Inc.

IOS is a registered trademark of Cisco Systems Inc.

RIM, BlackBerry, BBM, BlackBerry Curve, BlackBerry Bold, BlackBerry Pearl, BlackBerry Torch, BlackBerry Storm, BlackBerry Storm2, BlackBerry PlayBook, and BlackBerry App World are trademarks or registered trademarks of Research in Motion Limited.

Google App Engine, Google Apps, Google Checkout, Google Data API, Google Maps, Google Mobile Ads, Google Mobile Updater, Google Mobile, Google Store, Google Sync, Google Updater, Google Voice, Google Mail, Gmail, YouTube, Dalvik and Android are trademarks or registered trademarks of Google Inc.

INTERMEC is a registered trademark of Intermec Technologies Corporation.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

Bluetooth is a registered trademark of Bluetooth SIG Inc.

Motorola is a registered trademark of Motorola Trademark Holdings LLC.

Computop is a registered trademark of Computop Wirtschaftsinformatik GmbH.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, SAP HANA, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase Inc. Sybase is an SAP company.

Crossgate, m@gic EDDY, B2B 360° , and B2B 360° Services are registered trademarks of Crossgate AG in Germany and other countries. Crossgate is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.