IBM Security

Sécurité des applications: développements internes & Open Source

Kamel Moulaoui kamel.moulaoui@fr.ibm.com

DevCon #5

Mars, 2018

IBM

Le mythe et les croyances subsistent

Nous réalisons de l'analyse de code

Nous auditons une fois par an une application par des testeurs

Nos développeurs ont suivi une formation sur la sécurité des applications

Nous utilisons un scanner de vulnérabilité réseau

Les menaces de sécurité des applications

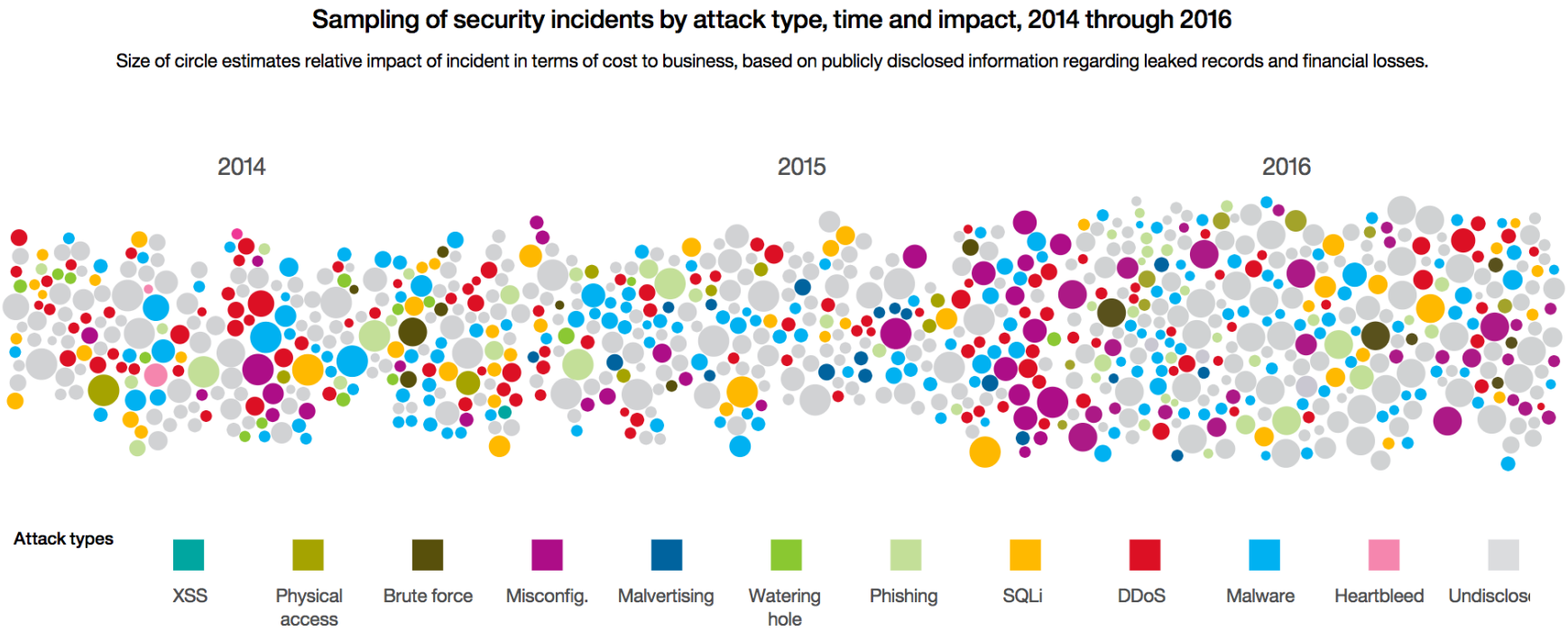


Figure 3: Sampling of security incidents by attack type, time and impact, 2014 through 2016.

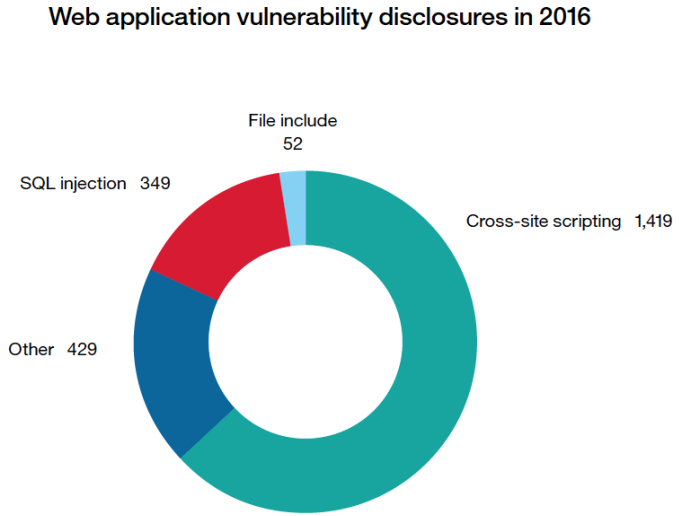


Figure 6: Web application vulnerability disclosures in 2016.

Anatomie d’une application et les contributions

Développements internes

Réutilisation de code existant

Développements sous-traités

Composants et librairies tiers

Et l'Open Source dans ces contributions ?

Introduit par les développeurs

Embarqué dans le code existant

Introduit dans le code sous-traité

Composants et librairies tiers provenant de l'Opens Source

Composants et librairies tiers provenant d'éditeurs

Forrester: *How To Leverage DevOps Trends To Strengthen Applications Dec. 2016*

"Approximately 80% to 90% of the code in modern applications is from open source components, and open source components that are at least two years old have three times the number of vulnerabilities. Even when developers are diligent about using newer third-party libraries, these libraries often use other libraries of their own, resulting in latent vulnerabilities that expose themselves at a later date.

Quelle stratégie adopter ?

Faut-il privilégier les tests statiques ou dynamiques ?

Une seule technique est elle suffisante ?

Qui va réaliser les tests ?

Faut-il automatiser les tests ?

Faut-il réaliser des tests sur toutes les applications

Comment gérer la sécurité du code Open Source embarqué ?

Quel effort organisationnel pour la réalisation des tests ?

Comment communiquer les résultats de test aux développeurs ?

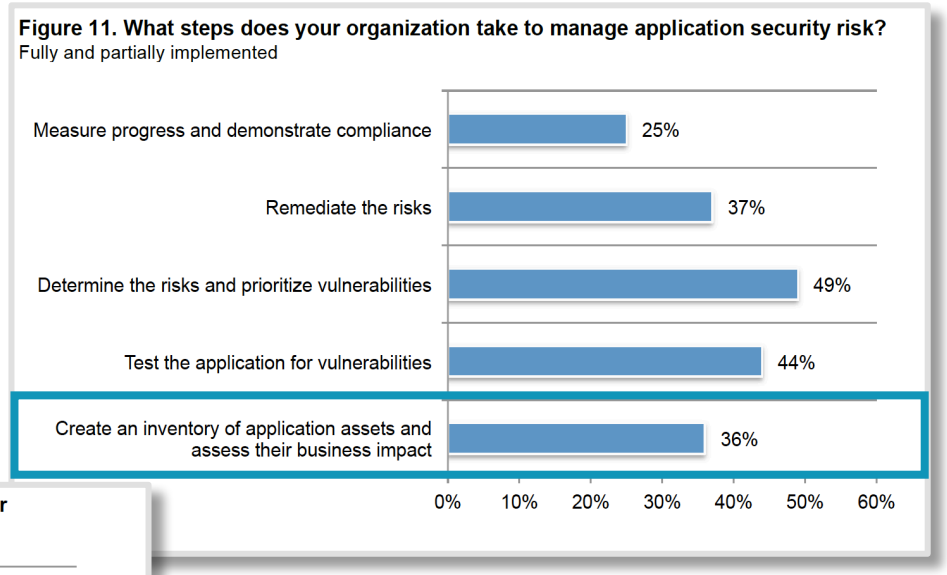
Nos application sont-elles conformes à la règlementation ?

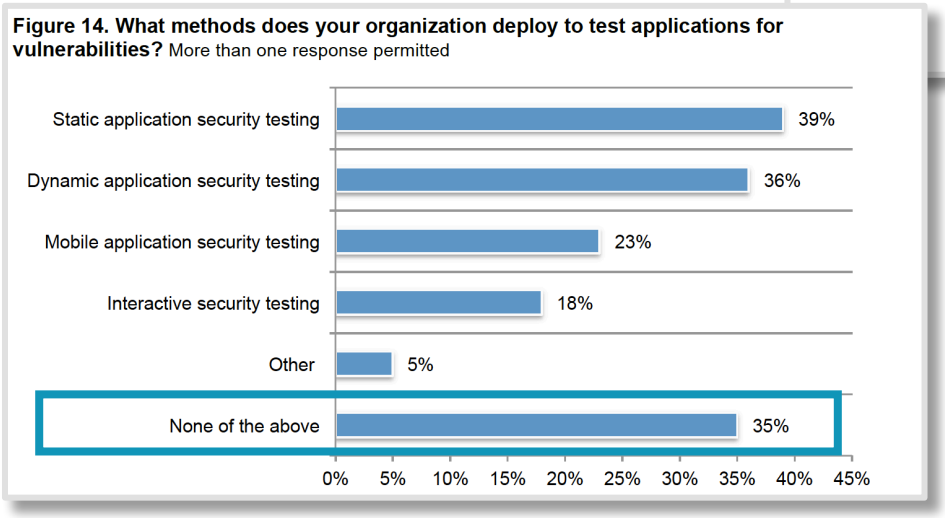
Le Constat:

Étude: Comment faire de la sécurité des applications une discipline gérée stratégiquement

Indépendamment menée par Ponemon Institute LLC - Mars 2016

Seulement "11% des sondés affirement que leur programme est mature et que le sujet est pleinement maitrisé"

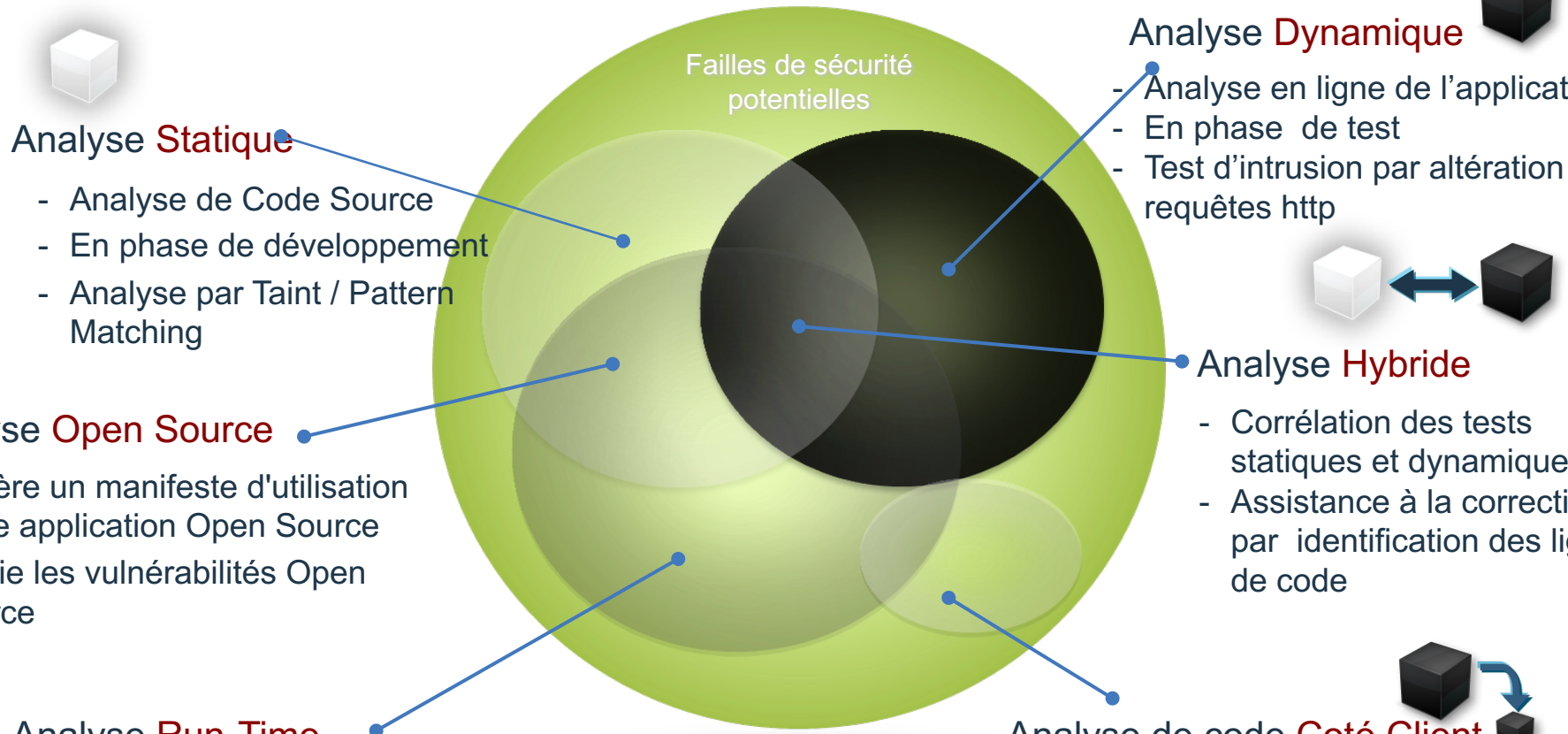




Résultats complets du sondage

L’approche et les innovations IBM

Une gamme complète de techniques d'évaluation des applications pour fournir une analyse de sécurité approfondie



Analyse Statique

- Analyse de Code Source
- En phase de développement
- Analyse par Taint / Pattern Matching

Analyse Dynamique

- Analyse en ligne de l'application
- En phase de test
- Test d'intrusion par altération des requêtes http

Analyse Open Source

- Génère un manifeste d'utilisation d'une application Open Source
- Vérifie les vulnérabilités Open Source

Analyse Hybride

- Corrélation des tests statiques et dynamiques
- Assistance à la correction par identification des lignes de code

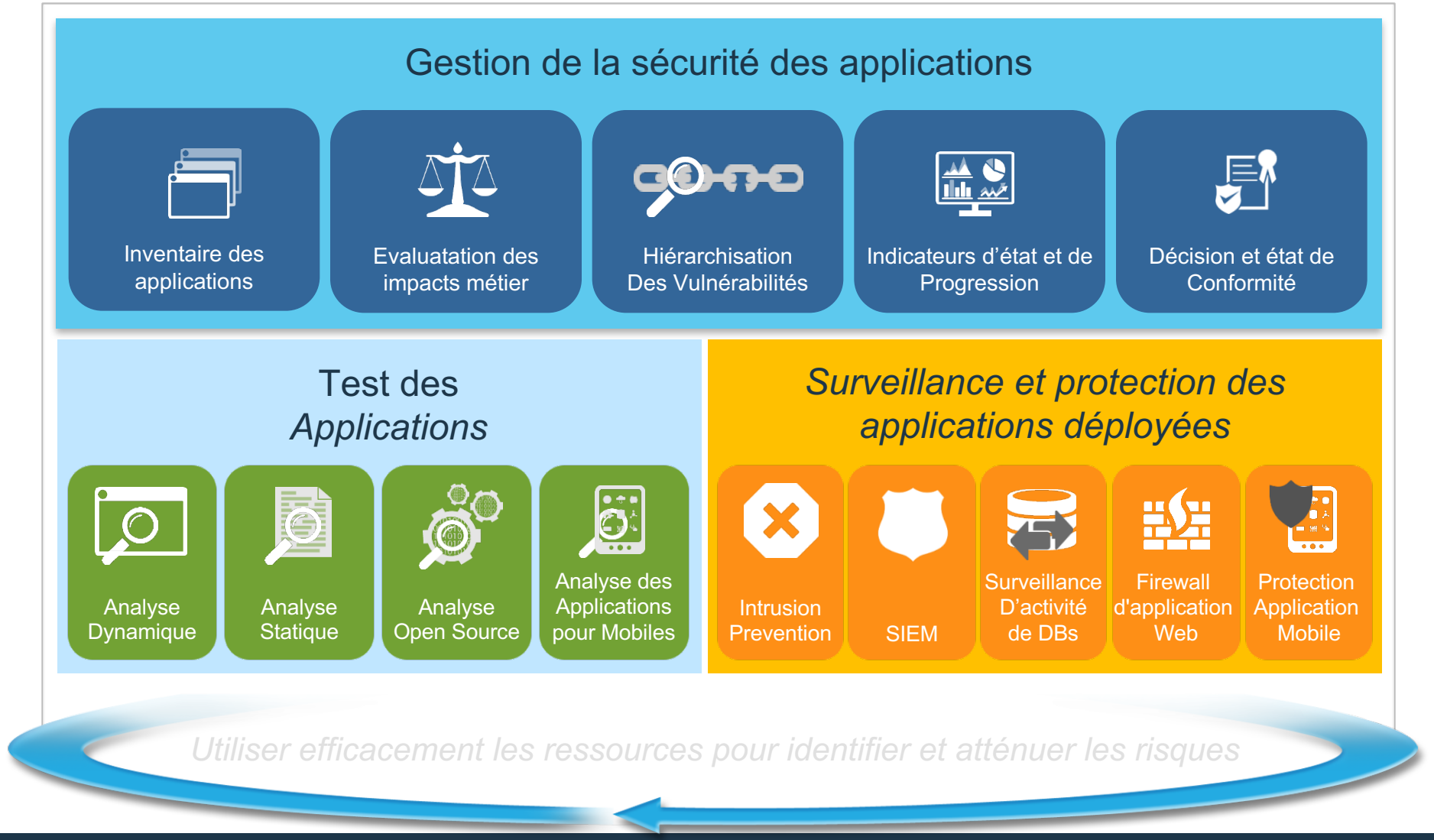
Analyse Run-Time

- Combine l'analyse dynamique et instrumentation du serveur d'application
- Plus de résultats, meilleur précision

Analyse de code Coté Client

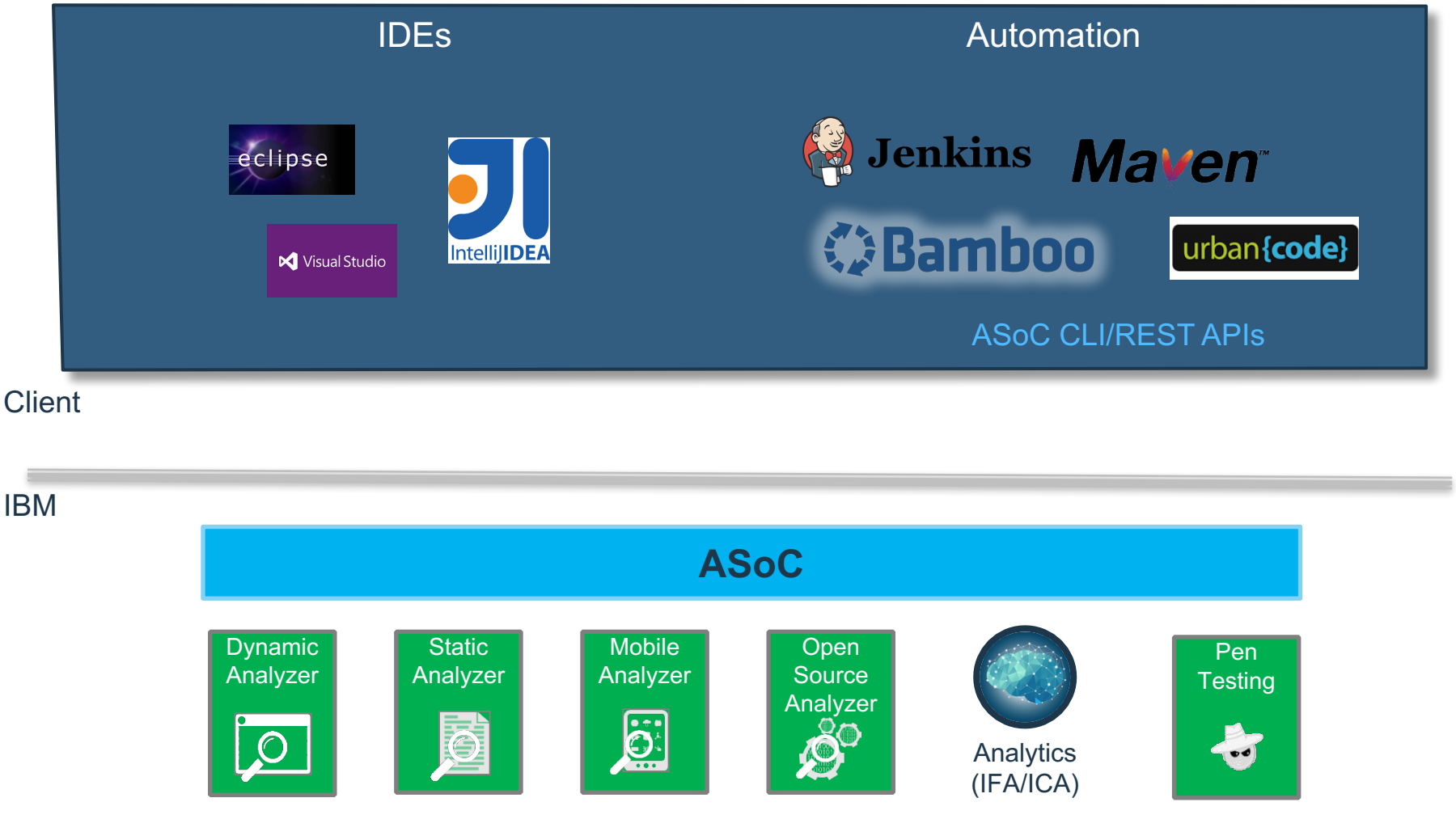
- Analyse du code javascript téléchargé et exécuté coté client

Framework IBM pour la Sécurité des Applications



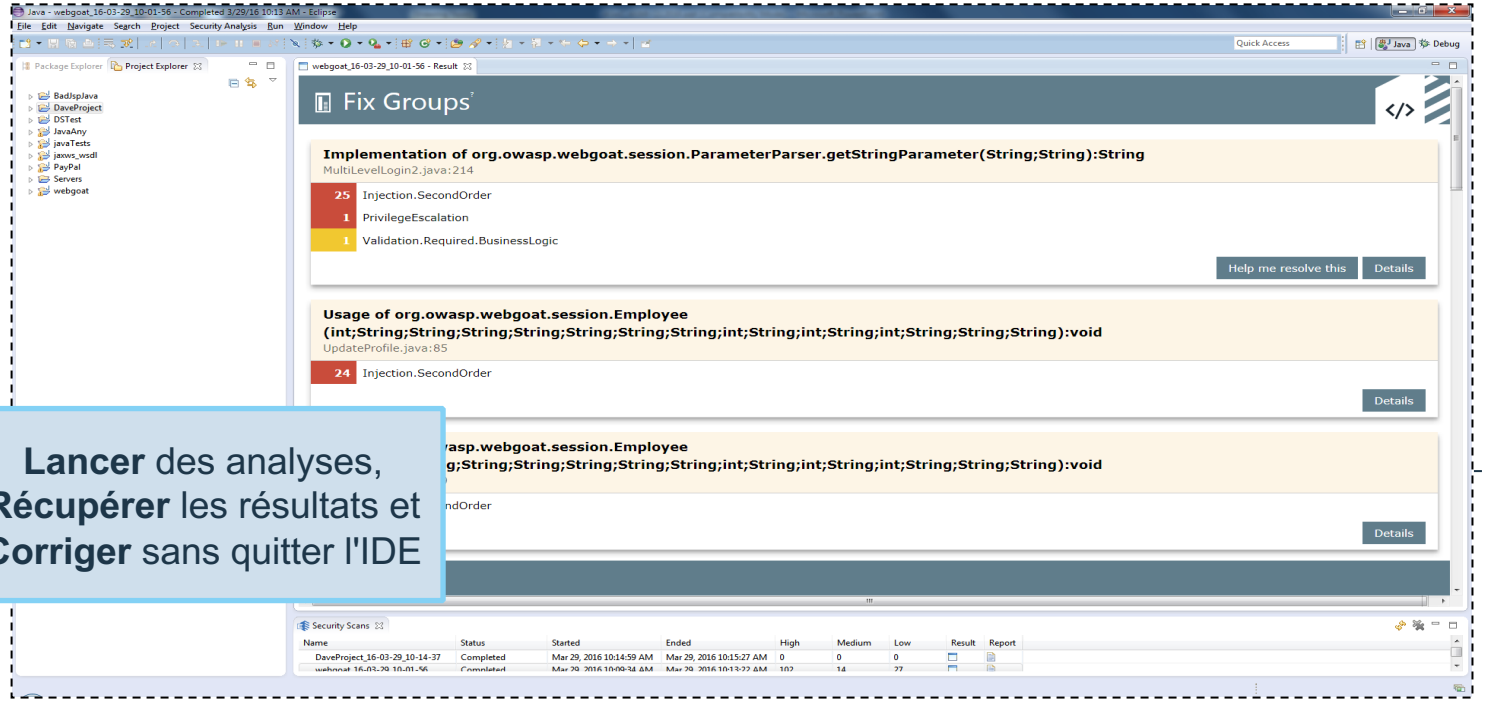
DevOps – Automation

Intégration dans les outils / processus de développement existants

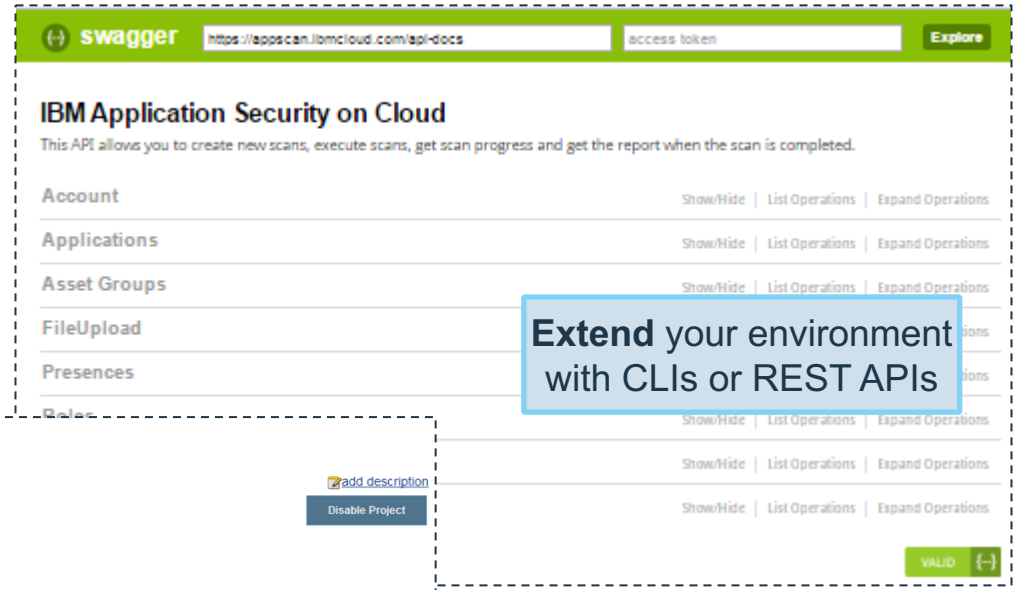


Test de sécurité des applications entre les mains des développeurs

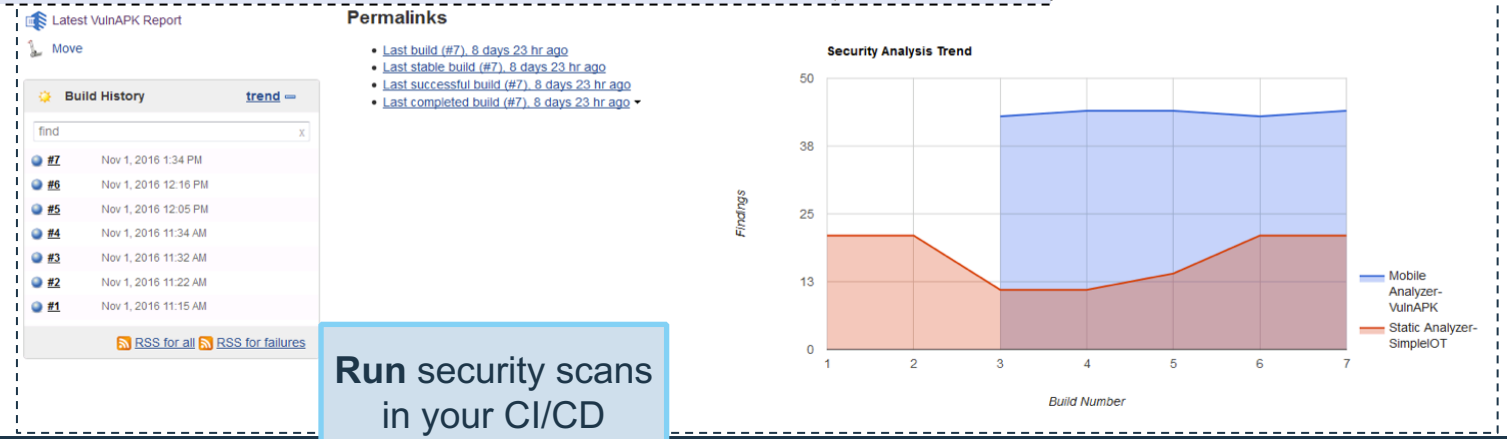
Streamlined Automation for DevOps: IDEs & Continuous Integration Frameworks



Lancer des analyses, **Récupérer** les résultats et **Corriger** sans quitter l'IDE



Extend your environment with CLIs or REST APIs



Run security scans in your CI/CD

IBM Open Source Analyzer

ASoC Open Source Analyzer

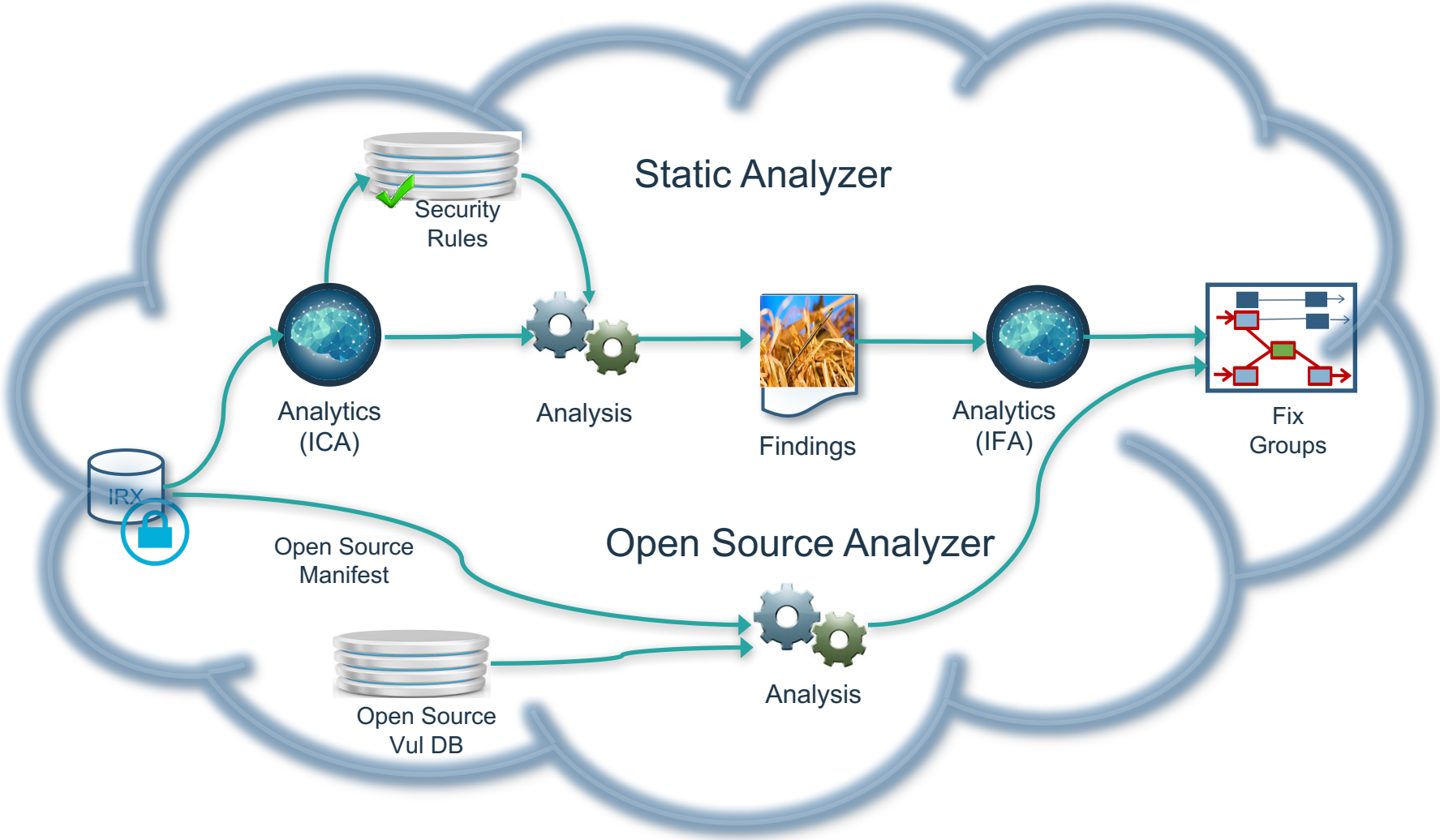
- Génère un manifeste d'utilisation d'une application Open Source
- Vérifie les vulnérabilités Open Source
- Référentiel leader de l'industrie avec plus de 230k vulnérabilités
- Proposition d'instructions de correction sur la version OSS vers laquelle il faut migrer
- Intégré dans l'environnement de test de sécurité des applications

IBM Application Security on Cloud: Static Analyzer/Open Source Analyzer

IDEs

Build CI/CD

ASoC CLI



Les capacités cognitives au service des tests de sécurité des applications

AppScan Cognitive Application Security Advisor

- **Intelligent Code Analytics**

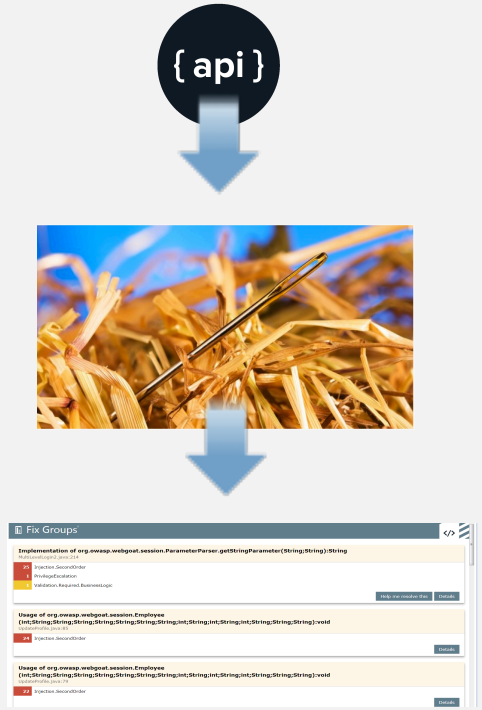
  Étend la couverture de l'analyse et élimine **les faux négatifs** en générant des règles de sécurité pour TOUT framework utilisé par une application pendant l'analyse.

- **Intelligent Findings Analytics**

  Réduit **les faux positifs** jusqu'à 99% et élimine les longues procédures de revue manuelle en fournissant une revue entièrement automatisée des résultats des tests de sécurité des applications.

- **Simple Fix Group recommendations**

  Fournit des recommandations de correction qui aident les équipes de développement à résoudre plusieurs vulnérabilités avec une seule correction de code.



ICA - **I**ntelligent **C**ode **A**nalysis

Fait:
Les développeurs **dépendent** grandement des **APIs** existantes

Problèmes:
La Sécurité du code scanné nécessite de **comprendre** ces APIs pour pouvoir réaliser une bonne couverture. Les APIs non connues laisse des **angles morts**

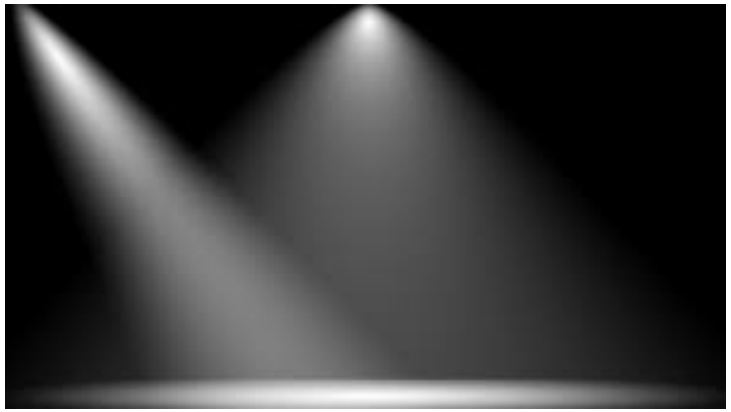
Solution:
Découvrir **manuellement** les informations des APIs et les ajouter à l'outil

ICA - **I**ntelligent **C**ode **A**nalysis

Introduction de **ICA** – nom de code “KRIS”

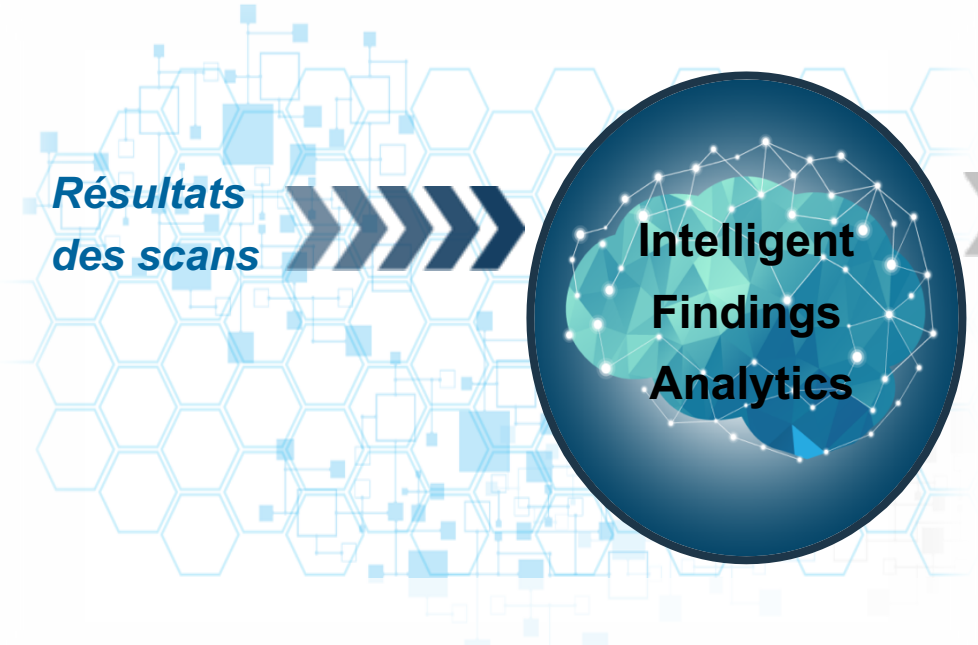
Notre nouveau moteur de Sécurité Cognitive ASoC analysera **tout framework** utilisé dans votre application pour une analyse complète du code développé et du framework.

- Plus **d’angle mort**
- **100% de couverture :** code développé et framework quelque soit son langage



IFA : Utiliser les technologies Cognitives pour l'analyse des vulnérabilités

*Machine learning with Intelligent Findings Analytics**



Résultats enrichis

- Réduit les faux positifs
- Minimise les "scenarios d'attaques improbables"
- Fournit des recommandations de "correction" permettant de résoudre plusieurs vulnérabilités

- Construit avec Watson Machine Learning
- Entrainé par les experts IBM Security
- Totalement automatisé

* Patents pending

IFA - Intelligent Findings Analytics

- **Moyenne de 90-95% de réduction de le charge de travail des analystes**
- Egale voire dépasse les compétences des experts
- Retourne des résultats en quelques secondes au lieu des heures voire jours habituels
- Intégration transparente dans le chaine de développement
- Résout en moyenne de 5 à 50% des problèmes en un seul endroit du code

		IFA	
Exemples d'applications réelles	**Scan Constatations**	**Vulnerabilities**	**Recommandations de correction**
Application 1	55,132	14,050	60
Application 2	12,480	1,057	35
Application 3	247,350	1,271	103

Moins de **1%**!!

Demo

https://www.youtube.com/watch?v=IdGnbh2yook
https://www.youtube.com/watch?v=rJe9dE-fHKA

En savoir plus sur IBM Application Security

Visit the
IBM Application Security Website

Watch AppScan Demo
http://www.youtube.com/watch?v=K6upeqbtdf4

Watch the videos on the
IBM Application Security YouTube Channel

Watch the AppScan Overview Video
How to Protect My Business from
Web and Mobile Application Attacks?

Read new Application Security blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

IBM Security

Merci

Suivez nous sur :

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM