

La Sécurité Applicative en DevSecOps avec JAZZ et APPSCAN





ABlogiX – Présentation

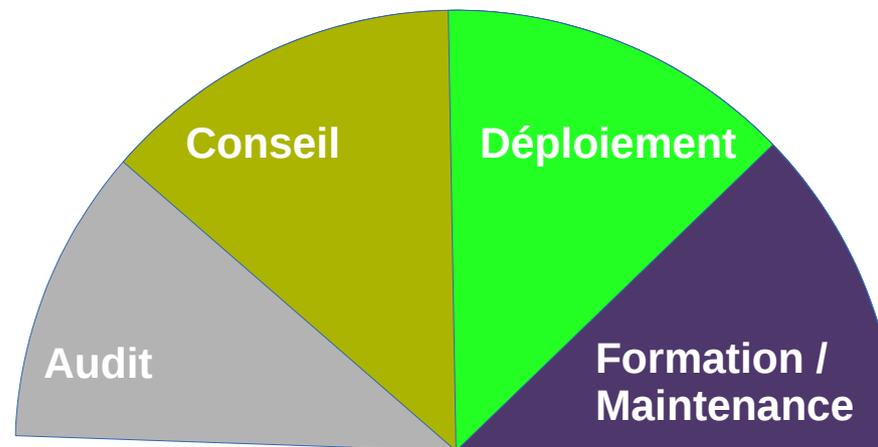
- Présentation
 - Nos activités
 - La Sécurité Applicative
 -





Nos activités

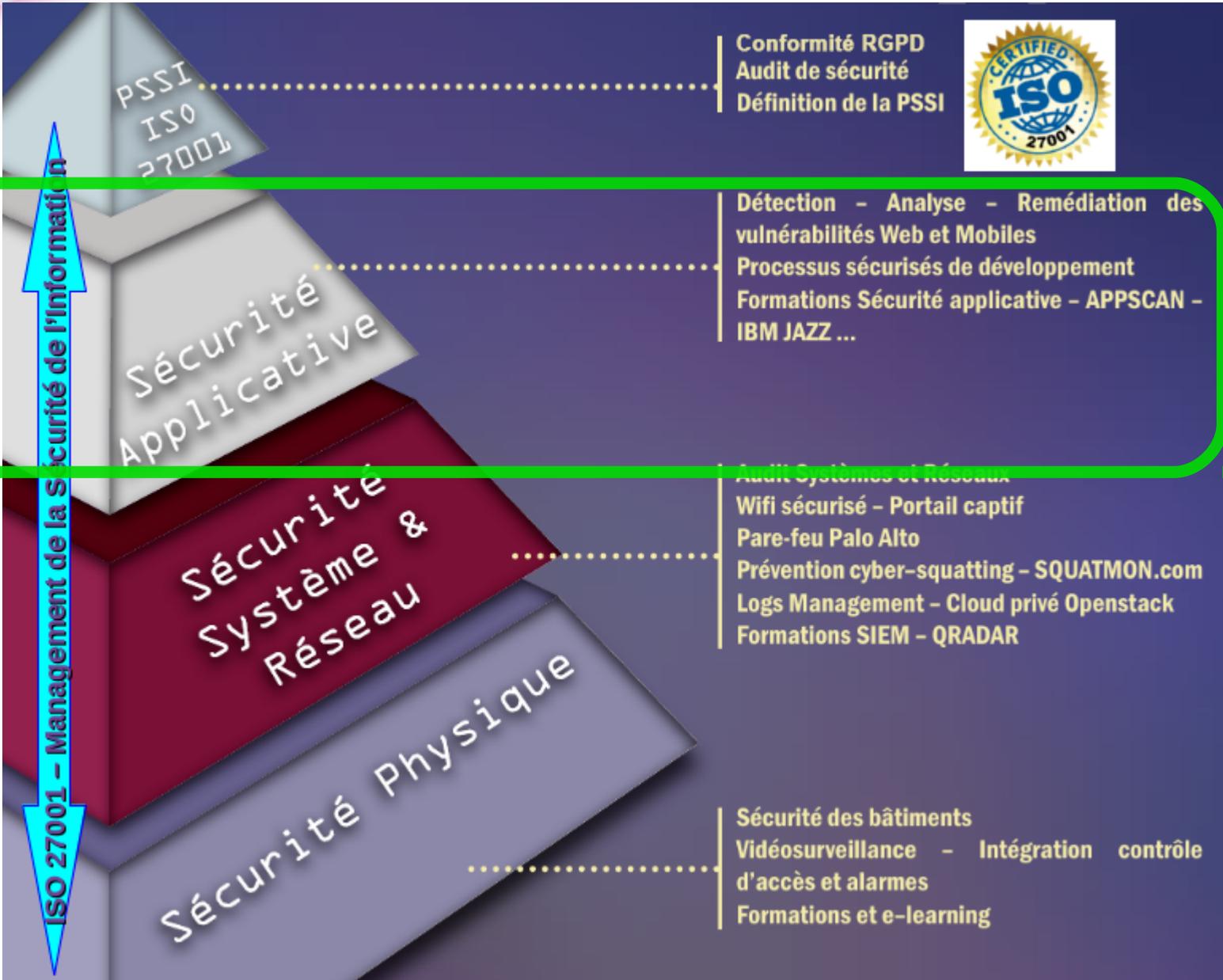
- ABlogiX est une société fondée en 2007 par Arnaud Bourlier
- 2 axes de compétences : **Qualité & Sécurité**
 - **Amélioration** des **processus** de « **développement logiciel et système** »
 - **Amélioration** de la **Sécurité du Système d'Information**





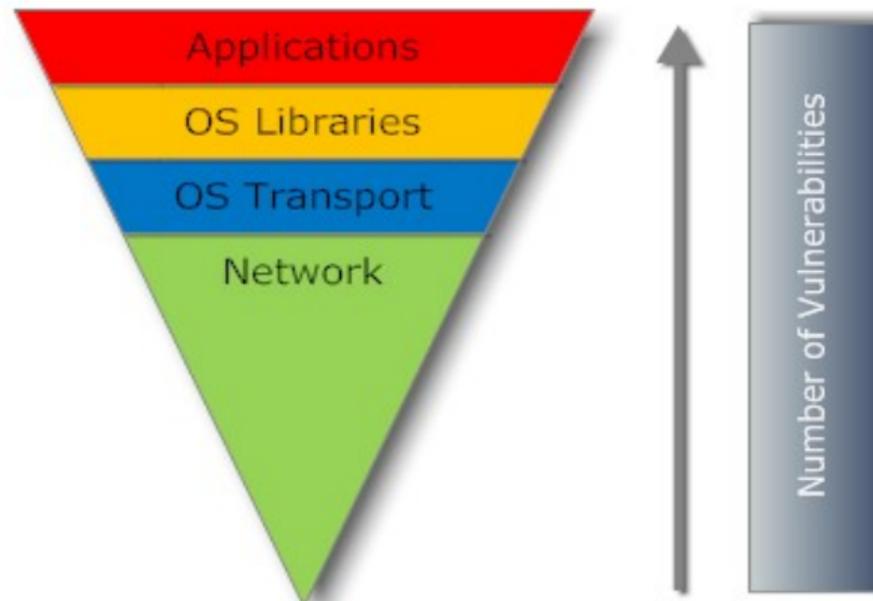
La Sécurité Applicative dans la pyramide de la SSI

Parmi les produits déployés :



Pourquoi les applications sont-elles si vulnérables ?

- Les développeurs se focalisent sur l'**aspect fonctionnel** pour respecter les **délais et budget** – mais pas nécessairement sur la **sécurité**
- Les **développeurs** ne sont généralement **pas formés aux pratiques de code sécurisé**
- **43 % des failles concernent les applications web** alors que la grande majorité des investissements en sécurité des entreprises concernent l'infrastructure et le réseau.



Différentes démarches complémentaires :

- **Audit** de sécurité de l'architecture logicielle (i.e. respect et robustesse des 3 « A »)
- **Scan** des vulnérabilités en mode statique et dynamique (Revue/Pentest/Automatique)
- **Déploiement** de Scanner DAST et SAST et intégration dans le Cycle de Développement
- **Formation** des développeurs (France & International) : *200 étudiants*
- ✓ Sécurité des applications – Identification/remédiation des vulnérabilités



4 techniques complémentaires :

Manuel

Tests d'intrusions manuels



```

{
connection = DatabaseUtilities.makeConnection(s);
}

ec.addElement(makeAccountLine(s));

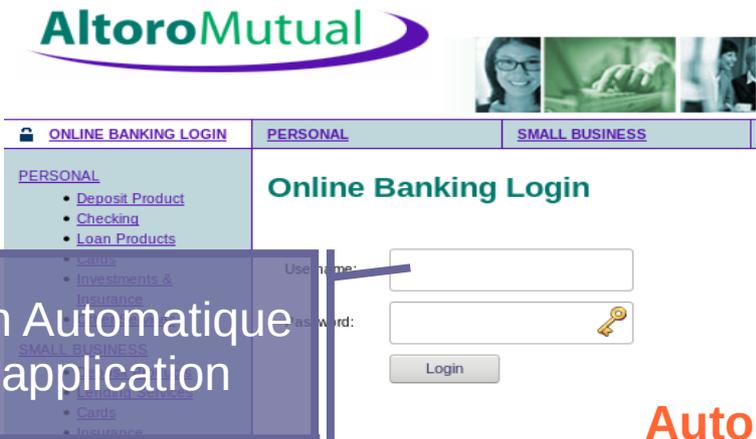
String query = "SELECT * FROM user_data WHERE last_name = '"
+ accountName + "'";
ec.addElement(new PRE(query));

try
{
Statement statement = connection.createStatement(
ResultSet.TYPE_SCROLL_INSENSITIVE,
ResultSet.CONCUR_READ_ONLY);
}
}
    
```

Audit et Revue Manuelle du Code Source

Exécution

Code



Scan Automatique d'application

Findings	Sev...	Classification	API
Findings (1,028)			
AccessControl (3)	High	Type I	System.D
Authentication.Credentials.Ui	High	Type II	System.D
CrossSiteScripting (145)	High	Type II	System.D
CrossSiteScripting.Reflected	High	Type I	System.D
ErrorHandling.RevealDetails.I	High	Type II	System.D
Info (560)	High	Type I	System.D
Injection.SQL (82)	High	Type II	System.D
Injection.SQL	High	Vulnerability	System.D
Logging.Required (30)	High	Vulnerability	System.D
Malicious.Trigger (6)	High	Type I	System.D
PrivilegeEscalation (1)	High	Type I	System.D
SessionManagement.Cookies	High	Type II	System.D
SessionManagement.Timeout	High	Type I	System.D
Validation.EncodingRequired	High	Type II	System.D
Validation.Required (163)	High	Type I	System.D
Validation.Required	High	Type II	System.D
Vulnerability	High	Vulnerability	System.D
Vulnerability	High	Vulnerability	System.D

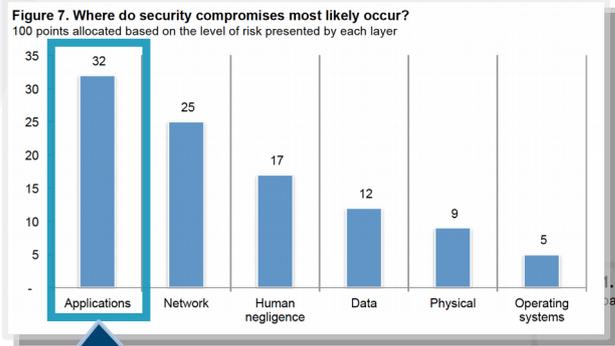
Analyse Statique Automatisée

Automatique

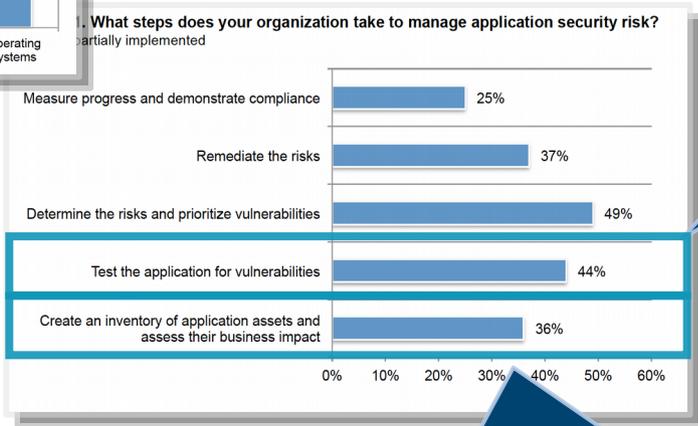


Etat de la situation sur la sécurité des applications

Seulement 11% des entreprises ont des programmes de sécurité applicatives complets
- Etude indépendante menée par Ponemon Institute LLC - mars 2016



Les applications sont les plus vulnérables aux menaces



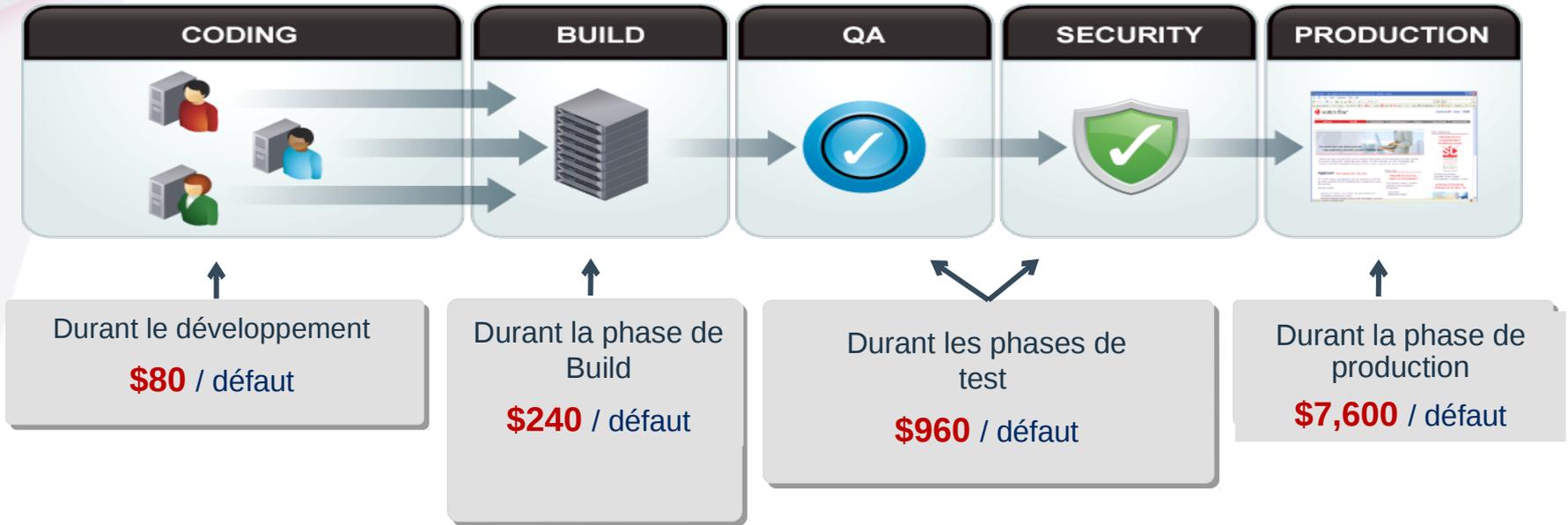
Que dire des 56% restants

64% ignorent le nombre d'applications dans leur société





Trouver les erreurs le plus tôt possible reste essentiel



80% des coûts de développement sont consacrés à l'identification et à la correction des défauts !

Source: National Institute of Standards and Technology

- Coût d'une violation de données 7,2 M \$
- 80 jours pour la détecter
- Plus de quatre mois (123 jours) à résoudre

Source: Ponemon Institute

3 facteurs de réussite essentiels: automatisation, traçabilité et complétude

Application Security Management

Utilisez une console unique pour gérer les risques liés aux applications, les résultats des tests et les rapports



Dynamic

Identifier les vulnérabilités dans les applications en cours d'exécution

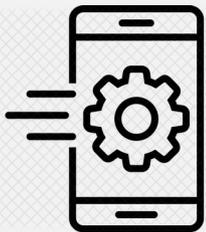
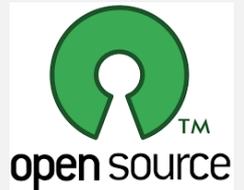
Static

Analyse de trace du code d'application



Open Source

Identifier les vulnérabilités introduites par les packages open source



Mobile

IAS test pour les binaires Mobile

APPSCAN on-Premise ou APPSCAN on-Cloud (ASoC)



APPSCAN : Un Dashboard unique pour l'Application Security Management

(one) Sign Out

Quel est l'état actuel de la Sécurité applicative? Quelles applications présentent le plus haut risque ?

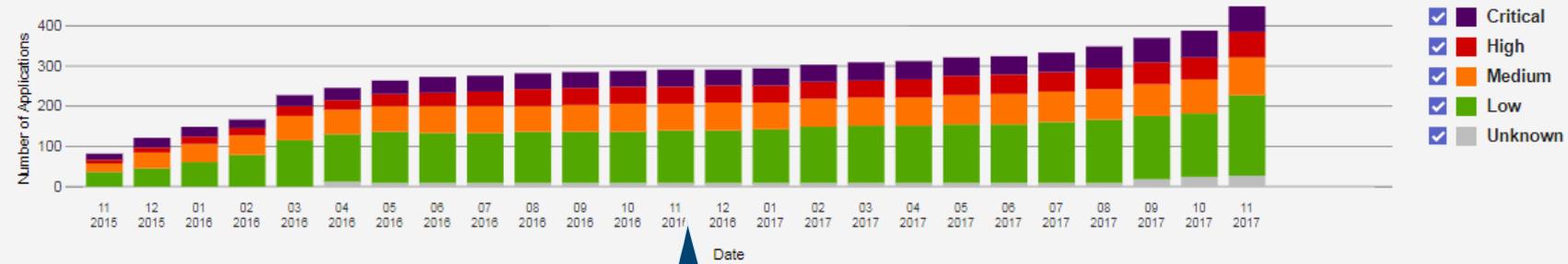
Combien d'applications de notre portfolio avons nous évalué ?

All Business Units

Security Risk Rating [What's this?](#)



Chart type
Security Risk Rating



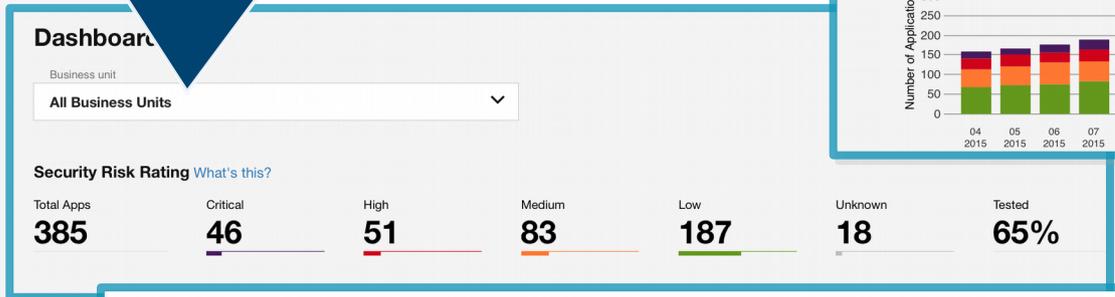
L'état de notre Sécurité Applicative s'améliore-t-elle?



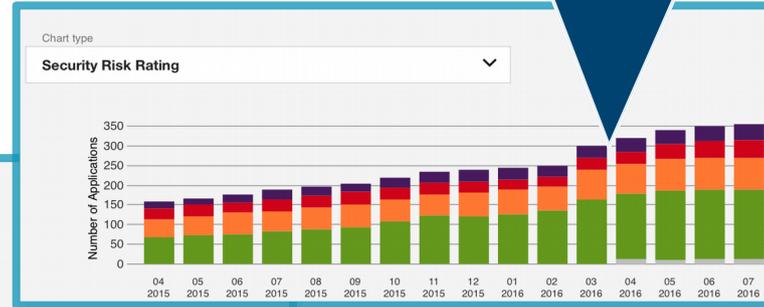
Dashboard principal de la Solution IBM ASoc

Gérez les risques de votre organisation

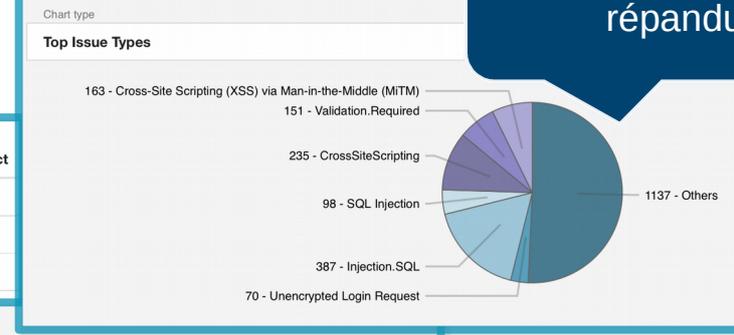
Quel est le statut actuel ?



Sommes-nous en train de réduire les risques ?



Quel est le risque le plus répandu ?



Risk Rating ↓	Name	New Issues	High Issues	Business Impact	Technology	Development Contact
Critical	Altoro 3.1 - Web	472	200	Critical Impact	Web	
High	Runzooace Vaia-Zap 1.0	5	1	Medium Impact	Web	Henrietta Rayfield
High	Findex Warmlex	3	1	High Impact	Web	Leo Ulman
High	Hotdomcon Zonzap 1.0	7	0	Medium Impact	Desktop	
High	Altoro 3.1 - IOS	47	11	High Impact	Mobile	
High	Altoro 3.1 - Android	82	33	High Impact	Mobile	
Medium	Lineace Quad Zimfan 1.0	5	1	Low Impact	Desktop	
Medium	Nimzenhow Dom-Dox 1.0	5	0	Low Impact	Web	
Medium	meding Freefax 1	1	0	Low Impact	Web	
Medium	Runzooace Vaia-Zap 1.0	1	0	Medium Impact	Web	

Les applications répertoriées



Évolution des risques applicatifs ?

Intégration dans les outils de développement



Secure code = Efficient Code



```
blockquote p { margin-bottom: 10px; }
strong, b { font-weight: bold; }
em, i, cite {
  font-style: normal;
  font-family: arial;
}
small { font-size: 100%; }
figure { margin: 10px 0; }
code, pre {
  font-family: monospace, consolas, sans-serif;
  font-weight: normal;
  font-style: normal;
}
pre {
  margin: 5px 0 20px 0;
  line-height: 1.3em;
  padding: 8px 10px;
  overflow: auto;
}
code { padding: 0 8px; }
pre { height: 1.5em; }
code { padding: 1px 6px; }
pre { padding: 0 2px; }
code { background-color: black; }
```

Security scans should be part of my nightly build



DAST Scan = Regression Testing

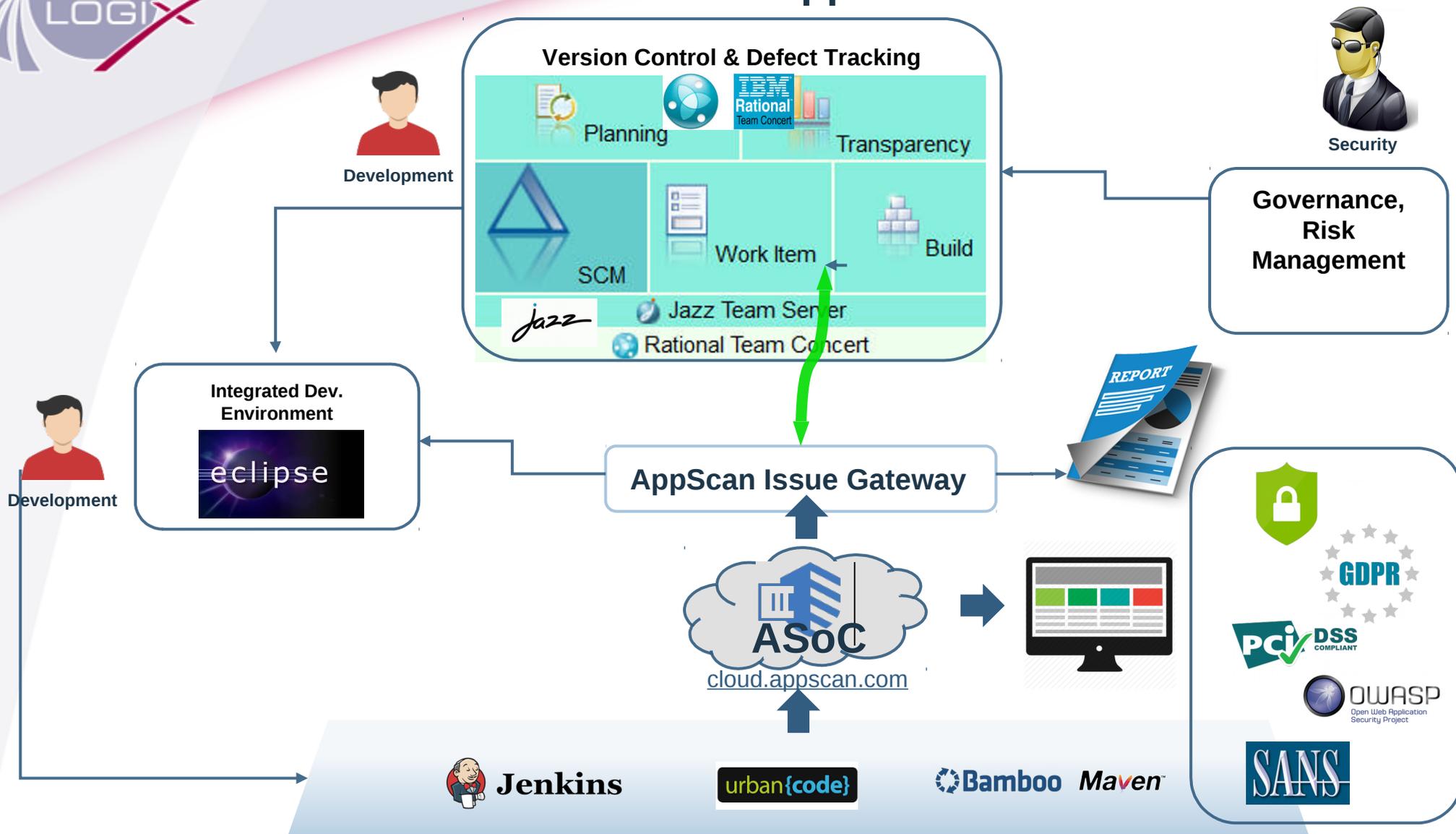
Security vulnerability = Defect



https://www.ibm.com/support/knowledgecenter/fr/SSYJJF_1.0.0/ApplicationSecurityonCloud/appseccloud_rest_apis.html

L'interface d'API REST intégrée vous permet de visualiser les services Web RESTful. La documentation API est élaborée à l'aide de Swagger. Vous pouvez y tester des opérations API et consulter instantanément les résultats afin d'examiner vos applications plus rapidement.

DevSecOps : Intégration de ASoC dans le Cycle de Développement



- **ASoC** : AppScan on Cloud is available at : <https://cloud.appscan.com>
- <https://jazz.net> met à disposition l'outil collaboratif JAZZ RTC de Gestion de Version & de Gestion des Changements.
- APPSCAN.Issue.Gateway : disponible sur <https://github.com/hclproducts/appscan-issue-gateway> permet de fournir l'intégration entre JAZZ RTC et ASoC



ASoC – Intégration avec JAZZ RTC

- Création d'un projet « demo »
- Exécution du scan

IBM Application Security on Cloud

Documentation What's New Support Forum Contact Support Arnaud Bourlier (Sarl ABlogiX) Sign Out

My Applications **DevSecOps** x

Details **Scans** **Compliance** [Application Reports](#) [Create Scan](#) ⓘ

High Risk Rating
76 New Issues
76 Total Issues
76 Non-compliant Issues

1
● 1 Completed
● 0 Running
● 0 Failed
● 0 Queued

N/A No Policies Associated

[Scan History](#) [Issue Management](#) [Policies](#)

Filter ▾ Search 🔍

demo		Scanned by: Arnaud Bourlier	Total Issues	High	Med	Low	Info	
	Scan start: 5/27/2019, 12:06:58 PM Scan end: 5/27/2019, 12:08:21 PM Duration: 1.4 minutes		76	68	7	1	0	ⓘ ↻ ⬇️ 🗑️

1 - 1 of 1 | items per page: 5 10 20 50

First Previous **1** Next Last



ASoC – Intégration avec JAZZ RTC

- Le Build RTC est déclenché manuellement ou sur évènement

Builds > Build Engines > DevSecOps1 > Moteur DevSecOps1 >

Build Engine

ID: Moteur DevSecOps1

Overview [Hudson/Jenkins](#)

General Information

This build engine registration represents a Jazz Build Engine or

Description:

Activation

Only active engines can execute builds.

Active

Build Request Processing

Configure whether the process represented by this build engine within a given threshold.

Build engine process polls for requests

Monitor the last contact time

Threshold (in minutes): *

Properties

Name
com.ibm.rational.connector.hudson.connectionTimee



DevSecOps1

[Project Dashboards](#) > [Work Items](#) > [Plans](#) > [Source Control](#) > [Builds](#) > [Reports](#)

Builds > Build Definitions > DevSecOps1 > DevSecOps1 build >

Build DevSecOps1 build N° 10



Completed

Duration: 12 seconds

Start time: 5 hours ago at 12:11

Completed: 5 hours ago at 12:11

Time in queue: 9 seconds

Overview

[Activities](#)

[External Links](#)

[Logs](#)

[Work Items](#)

General Information

Requested by: Arnaud Bourlier

Build Definition: DevSecOps1 build

Build Engine: Moteur DevSecOps1

Build History: 8 builds

Tags:

Deletion allowed

Contribution Summary

External Links: 1 link

Logs: 1 log



ASoC – Intégration avec JAZZ RTC

- les vulnérabilités identifiées sont détaillées sous l'onglet « Issue Management »
- RTC déclenche la création des Issues vers des Work Items

IBM Application Security on Cloud

Documentation What's New Support Forum Contact Support Arnaud Bourlier (Sarl ABlogiX) Sign Out

My Applications DevSecOps x

Details

High Risk Rating

76 New Issues
76 Total Issues
76 Non-compliant Issues

Scans

1

1 Completed
0 Running
0 Failed
0 Queued

Compliance

N/A No Policies Associated

Application Reports Create Scan

Scan History **Issue Management** Policies

Filter Search Column Selection

New Open In Progress Fixed Noise Passed Filtered Security Report Import Issues

Status	Location	CVSS	Issue Type	Severity ↓	Scan Name	Last Comment	
New	static\personal_investments.htm		CrossSiteScripting.Reflected	Medium	demo	May 27, 2019	<input type="checkbox"/>
New	.._Altor406859087\d\WEB-INF\lib\commons-codec-1.6.jar		OpenSource	Medium	demo	May 27, 2019	<input type="checkbox"/>
New	.._Altor406859087\d\WEB-INF\lib\derby.jar		OpenSource	Medium	demo	May 27, 2019	<input type="checkbox"/>
New	com.ibm.security.appscan.althoromutual.util.DBUtil.getConnection():Connection		Authentication.Entity	Medium	demo	May 27, 2019	<input type="checkbox"/>
New	com.ibm.security.appscan.althoromutual.util.DBUtil.initDB():void		Authentication.Entity	Medium	demo	May 27, 2019	<input type="checkbox"/>
New	.._Altor406859087\d\WEB-INF\lib\commons-codec-1.6.jar		OpenSource	Low	demo	May 27, 2019	<input type="checkbox"/>

First Previous ... 6 7 8 Next Last

71 - 76 of 76 | items per page: 10 15 25 50



ASoC – Intégration avec JAZZ RTC

- L'Issue « Open Source » a généré un WorkItem « 217 »
- La Description de l'Issue contient une trace du WorkItem créé « 217 »

217

ASoC scanner issue : OpenSource.

➔ Nouveau



27 May 2019 12:14:01

OpenSource

.._Altor406859087\d\WEB-INF\lib\commons-codec-1.6.jar

Overview

Details

Discussion (1)

History

Fix Recommendations

Discussion

🗨️ Add Comment

Write your comment here...

Save

Arnaud Bourlier 5/27/2019, 12:14:11 PM

AppScan Issue Gateway created the following issue:
<https://localhost:9443/ccm/resource/itemName/com.ibm.team.workitem.WorkItem/217>



ASoC – Intégration avec JAZZ RTC

- Le WorkItem « 217 » a été créé sous la Project Area RTC
- La Description de l'Issue « 217 » contient une trace du WorkItem créé « xx »

DevSecOps1

Project Dashboards ▾ Work Items ▾ Plans ▾ Source Control ▾ Builds ▾ Reports ▾

Work Items > Queries > Issues >

Incident 217 ?

Récapitulatif: * ASoC scanner issue : OpenSource.

Présentation | Liens | Approbations | Historique | Suivi temporel

Détails

Type: Incident

Gravité: Normale

Trouvé dans: Unassigned

Date de création: 27 May 2019 12:13:55

Créé par: Arnaud Bourlier

Project Area: DevSecOps1

Team Area: DevSecOps1

Classé dans: * Catégorie 2

Etiquettes:

Description

Web Security issue:
Scanner: ASoC.



ASoC – Intégration avec JAZZ RTC

- Le WorkItem « 217 » a été créé sous la Project Area RTC

Change and Configuration Management (Jazz)

La description de l'Issue « 217 » contient une trace du Workitem créé « xx »

DevSecOps1

Project Dashboards ▾ Work Items ▾ Plans ▾ Source Control ▾ Builds ▾ Reports ▾

Work Items > Queries > Issues >

Incident 217

Récapitulatif * ASoC scanner issue : OpenSource.

Présentation **Liens** Approbations Historique Suivi temporel

Pièces jointes

Drop files to add them or click here to browse.

73: IssueDetails-ed6b41...

Liens

Add Related ▾

Attachments

73: IssueDetails-ed6b4157-6780-e911-84e5-002590ac753d.html (Taille : 105 Ko)

Le rapport de cette Issue a été joint au Workitem
Il contient les détails de la vulnérabilité et les conseils pour la remédiation



ASoC – Intégration avec JAZZ RTC

- Le rapport de cette vulnérabilité donne les détails



IBM A
Appli

Name: Sing

Security Report for
Business Impact: H
Created: Monday, M
Contains: 1 issues (

Summ

Total security is

Issue Types: 1

OpenSource

Issues

L SAST: OpenSource 1

Issue 1 of 1

Issue ID:	-557898642
Severity:	Low
Status	New
Classification	Definitive
Location	.._Altor406859087\d\WEB-INF\lib\commons-codec-1.6.jar
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Monday, May 27, 2019
Last Updated	Monday, May 27, 2019
File:	.._Altor406859087\d\WEB-INF\lib\commons-codec-1.6.jar
Name:	2009-0001
Description:	Not all "business" method implementations of public API in Apache Commons Codec 1.x are thread safe, which might disclose the wrong data or allow an attacker to change non-private fields. Updated 2018-10-07 - an additional review by WhiteSource research team could not indicate on a clear security vulnerability
URL:	https://issues.apache.org/jira/browse/CODEC-55

Issue 1 of 1 - Details

Issue 1 of 1 - Audit Trail

05/27/2019 10:07:24

IssueTypeName: → OpenSource
Status: → New
Location: → .._Altor406859087\d\WEB-INF\lib\commons-codec-1.6.jar
Severity: → Low
Scanner: → AppScan Static Analyzer

Application Security Advisor

- **Intelligent Code Analytics (ICA)**

Étend la couverture des analyses et élimine les **Faux Négatifs** en générant des Politiques de Sécurité pour **TOUT** framework utilisé par une application durant l'analyse des traces.

- **Intelligent Finding Analytics (IFA)**

Réduit les **Faux Positifs** jusqu'à 98% & élimine les longs processus de revues des rapports en fournissant des revues automatisées complètes des anomalies des tests de Sécurité Applicative.

- **Simple Fix Group recommendations**

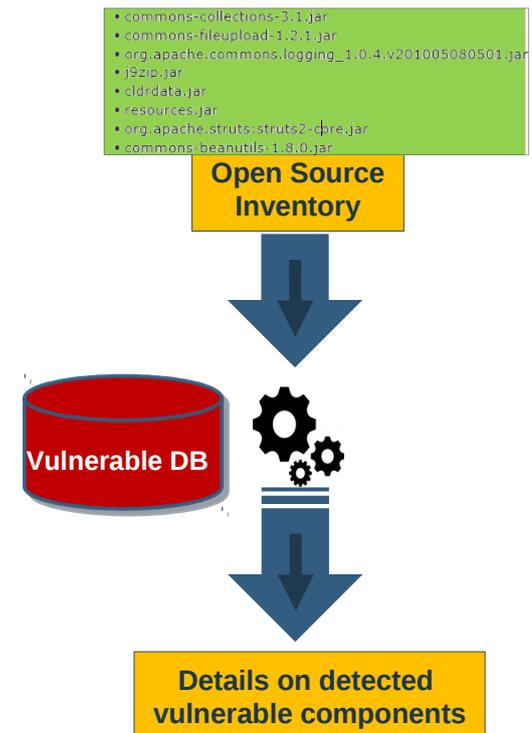
Fournit des recommandations de correctifs qui aident l'équipe de développement à résoudre de multiples vulnérabilités avec un seul correctif.



Etape 1: Analyse Open Source

L'outil d'analyse open source construit une liste de tous les composants de l'application et vérifie si l'un de ceux-ci présente des vulnérabilités.

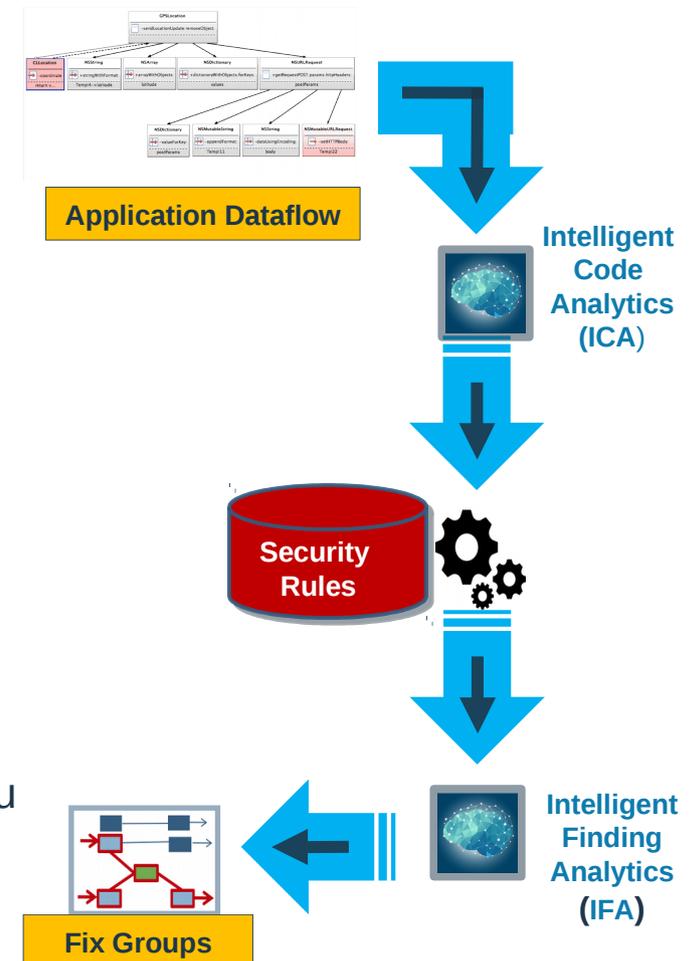
- Configuration minimale requise pour effectuer une analyse.
- Les analyses sont extrêmement rapides et claires
 - *Environ 80% à 90% des défauts du code des applications actuelles proviennent des composants open source.
- IBM ASoc trouve rapidement les sites vulnérables avec Google Dork ou des outils conçus par les pirates pour détecter les nouveaux CVE publiés.



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

L'**analyse statique** a pour but de rechercher les vulnérabilités dans le code de l'application elle-même. L'une des méthodes consiste à détecter les flux de données qui ne sont pas désinfectés.

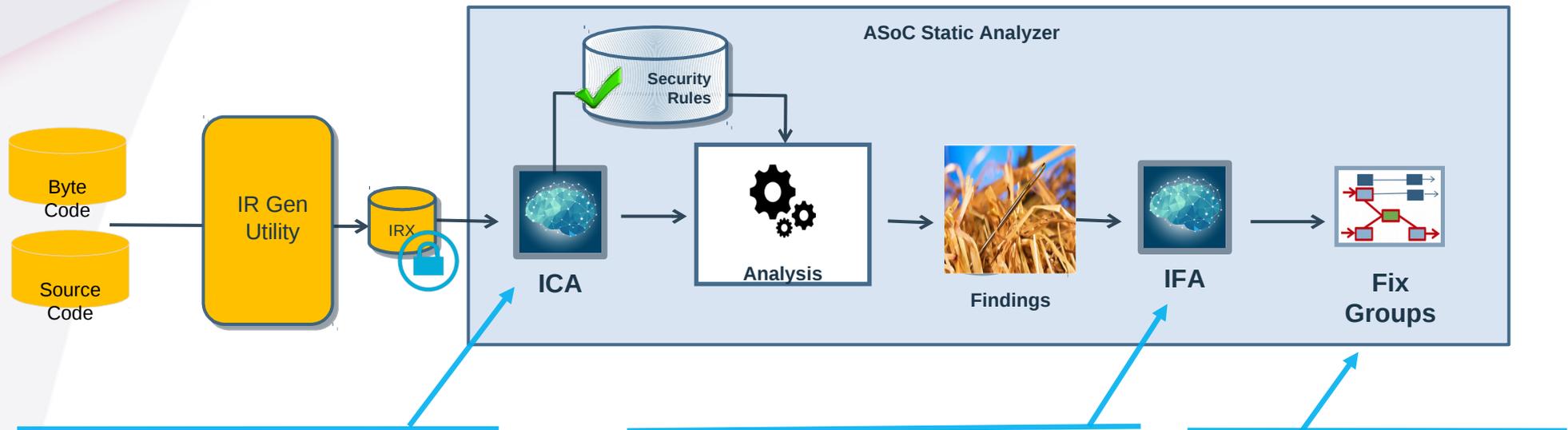
- Une petite configuration est nécessaire pour effectuer une analyse.
- L'analyse de petites applications / micro-services s'effectue en moins de 2 minutes.
- Les vulnérabilités signalées orientent généralement le développeur vers le code à corriger via l'interface de ses outils de développement.
- Des résultats très précis grâce à l'intelligence cognitive et au machine learning.





ASoC – L'analyse Applicative en 3 phases

Les fonctionnalités cognitives pour le Static Analyzer



Intelligent Code Analytics (ICA)

- Élimine les Faux Négatifs
- couvre les mises-à-jour des Langages
 - couvre tous les Frameworks

Intelligent Finding Analytics (IFA)

- Élimine les Faux Positifs & anomalies in-intéressantes
- A donné un gain jusqu'à 98.91% sur un cas d'usage client

Identifie les endroits optimaux dans le code source pour corriger de multiple Vulnérabilités

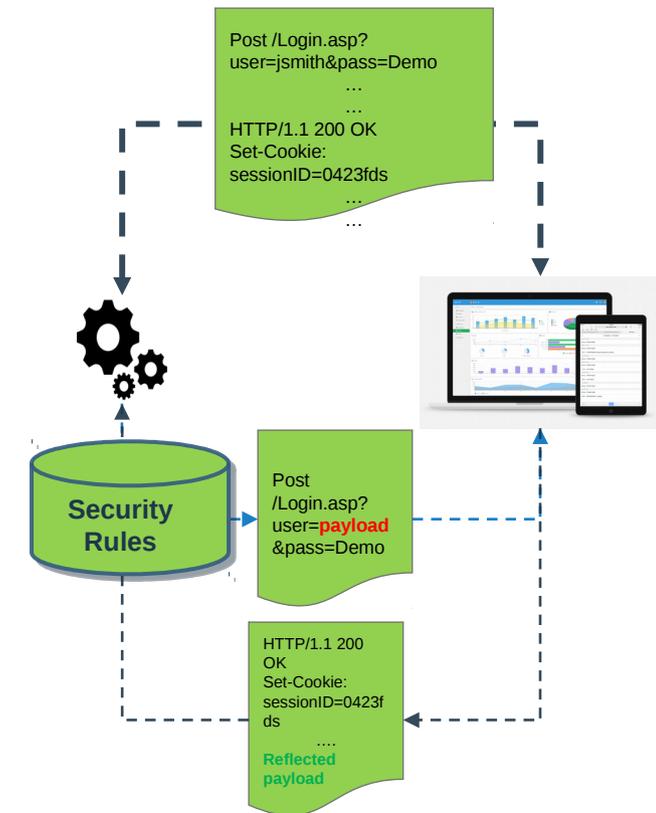
Etape 3: Analyse Dynamique

L'**analyse dynamique** vise à identifier des vulnérabilités dans une application en cours d'exécution.

La 1ère étape consiste à collecter des informations sur l'application

La 2nd consiste à envoyer des requêtes HTTP modifiées à l'application et en examiner les réponses.

- Peu de configuration nécessaire à son exécution.
- Détermine les vecteurs d'attaque basés sur la politique choisie du test
- Génère un rapport incluant des conseils et des recommandations sur les corrections à réaliser.





Depuis ASoC – Choix de génération de rapports

- Les principaux standards sont disponibles

Rapports d'application

Il n'est possible de générer qu'un rapport à la fois.

Rapport de sécurité | Norme du secteur | Conformité aux règle...

Tous les problèmes de l'application (352)
Remarque : ce rapport inclura tous les problèmes.

Filter les problèmes par conformité

Inclure tous les problèmes
 Inclure uniquement les problèmes de non conformité

Inclure les métadonnées

Table des matières
 Récapitulatif du rapport

Aperçu (toujours inclus si l'un des champs ci-dessous est sélectionné)
 Détails
 Discussion
 Historique
 Conseils
 Corrections recommandées

Nom du rapport: ABx-demo-ASOC_20190301_13:36:43 | Format: .pdf

Notes

Rapports d'application

Il n'est possible de générer qu'un rapport à la fois.

Rapport de sécurité | **Norme du secteur** | Conformité aux règle...

- CWE/SANS Top 25 Most Dangerous Errors
- International Standard - ISO 27001
- International Standard - ISO 27002
- NIST Special Publication 800-53
- OWASP Top 10 2017
- OWASP Top 10 Mobile 2016
- WASC Threat Classification v2.0

Nom du rapport: ABx-demo-ASOC_20190301_13:36:43 | Format: .pdf

Notes



A votre disposition pour répondre à vos questions

ABlogiX

+33 2 85 29 43 43

arnaud.bourlier@ablogix.fr

www.ablogix.fr

[@ABlogiX](#)