



Gestion des vulnérabilités logicielles

François MAUFRAIS
Senior Solution Engineer
fmaufrais@flexerasoftware.com

Agenda Software Vulnerability Management

- Vulnérabilités logicielles
- Le Secunia Research Team
- Solutions :
 - Vulnerability Intelligence Manager
 - Corporate Software Inspector
- Software Composition Analysis



Statistics

- Top 200 des Editeurs
- Profitable & pérenne
- 770+ employés
- 80,000 Clients
- 20,000 applications *FlexEnabled*
- 200,000,000 PC's recevant des téléchargements et mises à jour

Highlights



- Couverture mondiale
 - Itasca, IL (HQ) USA
 - San Jose, Orinda, & San Fran CA USA
 - Minneapolis, MN USA
 - Maidenhead & Cheshire UK
 - Munich, Germany
 - Copenhagen, Denmark
 - Bucharest, Romania
 - Paris, France
 - Tokyo, Japan
 - Melbourne, Australia
- Plus de 25 expérience
- Standard de l'industrie
- Consultants de haut niveau

Performance

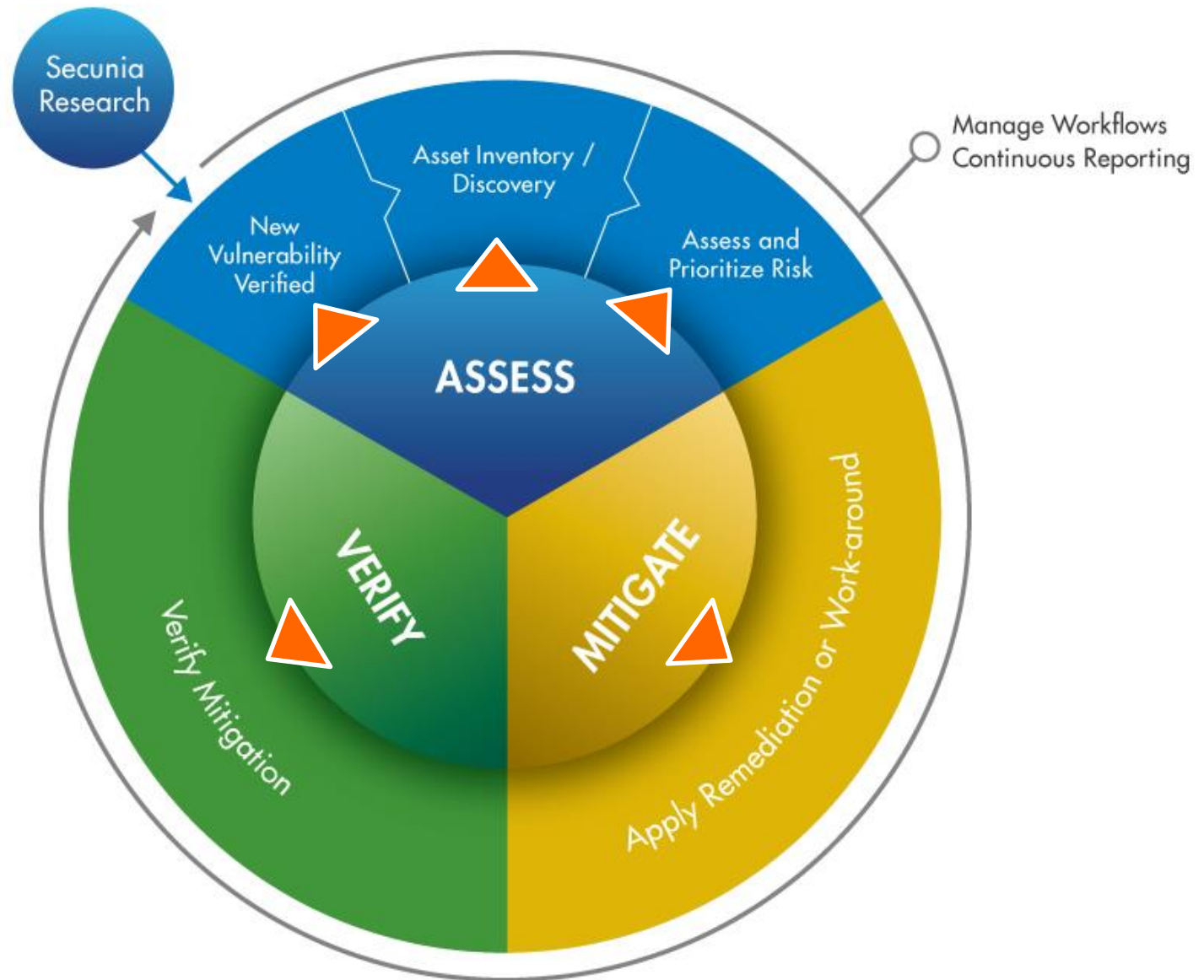
- **Market Leader**
 - Software Monetization (*FlexNet Producer Suites*)
 - Software License Optimization (*FlexNet Manager Suite, App Portal*)
 - Installation and Application Readiness (*InstallShield, AdminStudio,*)
- **Acquisitions To Date**
 - ManageSoft
 - Intraware, Inc.
 - LinkRight Tracker
 - Honico GmbH
 - SCCM Expert
 - Secunia (2015)
 - Palamida (2016)

Vulnérabilités Logicielles

Un risque permanent pour les uns

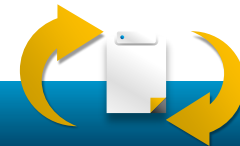
Un marché plus que rentable pour d'autres

Gérer les vulnérabilités logicielles est un cycle



Les challenges...

- Gestion des Vulnérabilités pas implementée correctement
- Collecte et vérification manuelle des données
- Flux d'information peu fiable, peu utile
- Flux d'information trop riche pour être traité correctement
- Pas de processus en place et de délégations locales
- Pas de traces écrites des audits et corrections
- Pas de documentation et de reporting
- Attente des rapports d'audits de vulnérabilité (position réactive vs proactive)



Secunia Research Team

Vulnerability Intelligence

Secunia Research

Software Vulnerability Management

L'une des bases de données de vulnérabilités les plus complètes du marché



**Base de données
sur les
vulnérabilités
recensées depuis
2003.**



**50 000+
programmes,
applications et
plug-ins
de milliers de
vendeurs de
logiciels.**



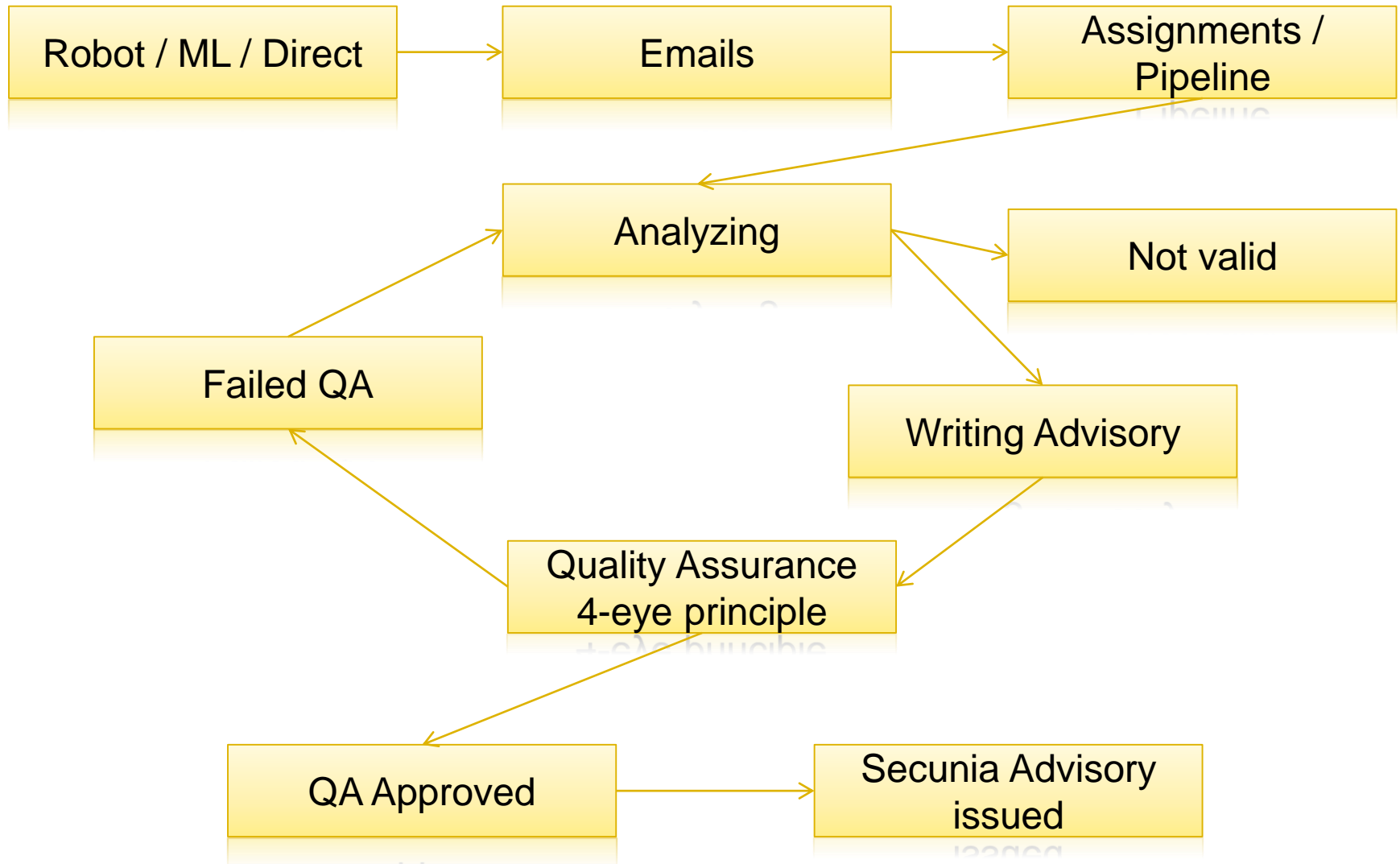
**100% CVE
compatible.**

**Les données sont
testées et vérifiées
par Secunia
Research..**



**Une base de
données unique
Propriété
intellectuelle
exclusive de Flexera
Software.**

Workflow d'analyse (simplifié)



Secunia Research Team

- **Où Secunia Research trouve-t-il les vulnérabilités?**
 - Vulnerability Tracker: des milliers de meta-crawlers qui recherchent dans des milliers de sources
 - De bonne relations avec les CERT éditeurs
 - De bonne relations avec la communauté
 - Des recherches internes pour la découverte et le compte-rendu de nouvelles vulnérabilités aux éditeurs

Activité du Secunia Research Team

- **300** – Quantité d'informations reçues chaque jour de notre propre robot web personnalisé et de plus de 1000 sources différentes. Notre réputation nous aide également ici, des contributeurs nous alertent spontanément.
- **80** – vulnérabilités méritent une analyse approfondie, dans l'intérêt de nos clients
- **25** – bulletins Secunia publiés sur ces 80 vulnérabilités en moyenne par jour
- **~5** – bulletins rejetés. Mais publiés pour des raisons de conformité réglementaire (certaines organisations doivent expliquer pourquoi un bulletin n'est pas retenu)

Vulnérabilités recensées, tous produits confondus en 2015: 16,081

DERNIER
RAPPORT



Source: “Flexera Software Vulnerability Review 2016.”

<http://www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/>

Les solutions

 FLEXERA SOFTWARE®
**Vulnerability
Intelligence Manager**

- **Solution intelligente de gestion des vulnérabilités**
- Evaluation des risques et reporting basés sur des informations vérifiées fournies par Secunia Research, couvrant l'ensemble des applications et systèmes

 FLEXERA SOFTWARE®
**Corporate
Software Inspector**

- **Gestion intelligente des correctifs de sécurité pour votre entreprise**
- Fait l'inventaire de vos logiciels, hiérarchise et gère les correctifs de sécurité

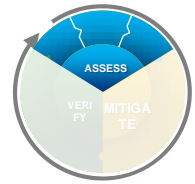
 FLEXERA SOFTWARE®
**Personal
Software Inspector**

- **Logiciel gratuit et automatisé de gestion des vulnérabilités pour les ordinateurs personnels**
- Installation automatique des mises à jour pour une protection efficace de votre PC et de vos données
- Plus de 7 millions de téléchargements

Note: Une des plus importantes sources de données pour Secunia Research



Vulnerability Intelligence Manager



VIM est une solution de recherche d'information en Cloud pour les spécialistes de sécurité

- Vue globale de toutes les vulnérabilités logicielles
- Délégation du travail de recherche et d'expertise à Secunia Research pour analyser et interpréter d'énorme quantité d'informations
- Evaluation réfléchie du risque par rapport à vos priorités
- Suggestions prise en compte en 72 heures
- Workflow pour déléguer le traitement
- Gestion de tickets pour suivre la résolution
- Intégration Imports & Exports par API
- Rapports périodiques et diffusables
- Compatibles avec les standards
 - SOX, PCI-DSS, NERC, HIPAA, ...



Tableaux de bord et Rapports

Rapport d'évaluation des priorités & filtrage

Vulnerability Intelligence Manager Dashboard

- Dashboard
- Notification Center 1603
- Vulnerability Manager
- VulnTrack
- Policy Manager 3
- Analytics
- Auditor
- Settings
- User Profile

Latest advisories

SAID	Title	Criticality	Release date
SA74216	Cisco Aggregation Services Routers (ASR) 5000 Series IKEv2 Denial of Service Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74213	IBM Tivoli Netcool Configuration Manager Serialized Object Handling Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74166	SUSE update for MozillaFirefox and mozilla-nss	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74167	SUSE update for tomcat	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74168	SUSE update for java-1_8_0-ibm	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74172	SUSE update for java-1_7_0-ibm	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74154	Gentoo update for libmms	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74150	Gentoo update for docker	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74139	Magela update for phpmyadmin	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74214	IBM Tivoli Storage Manager Client Journal-Based Backup Buffer Overflow Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12

Latest advisories per asset list

SAID	Title	Criticality	Release date
SA74213	IBM Tivoli Netcool Configuration Manager Serialized Object Handling Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74214	IBM Tivoli Storage Manager Client Journal-Based Backup Buffer Overflow Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74240	Apache Tomcat NIO HTTP Connector Information Disclosure Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74131	IBM Security Access Manager for Web / Tivoli Access Manager for e-business Multiple Vulnerabilities	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74138	IBM Security Access Manager Products OpenSSH Security Bypass Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-12
SA74208	Cisco AnyConnect Secure Mobility Client Interprocess Communication Privilege Escalation Vulnerability	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	2016-12-09

Your latest assigned tickets

Id	Ticket created	Queue	Status	Priority	Affected Asset	SAID	Title
645	2016-12-12	Default	Open	Low	All IBM	SA74213	IBM Tivoli Netcool Configuration Manager Serialized Object Handling Vulnerability
644	2016-12-12	Default	Open	Medium	FNMS_import	SA74240	Apache Tomcat NIO HTTP Connector Information Disclosure Vulnerability

Open tickets split by advisory criticality

Criticality	Count
Rejected	2
Extremely critical	7
Highly critical	126
Moderately critical	221
Less critical	212
Not critical	68

Tickets split by status

Status	Count
Open	7
Waiting	126
Handled	221
Irrelevant	212
Waiting on Change Man...	68

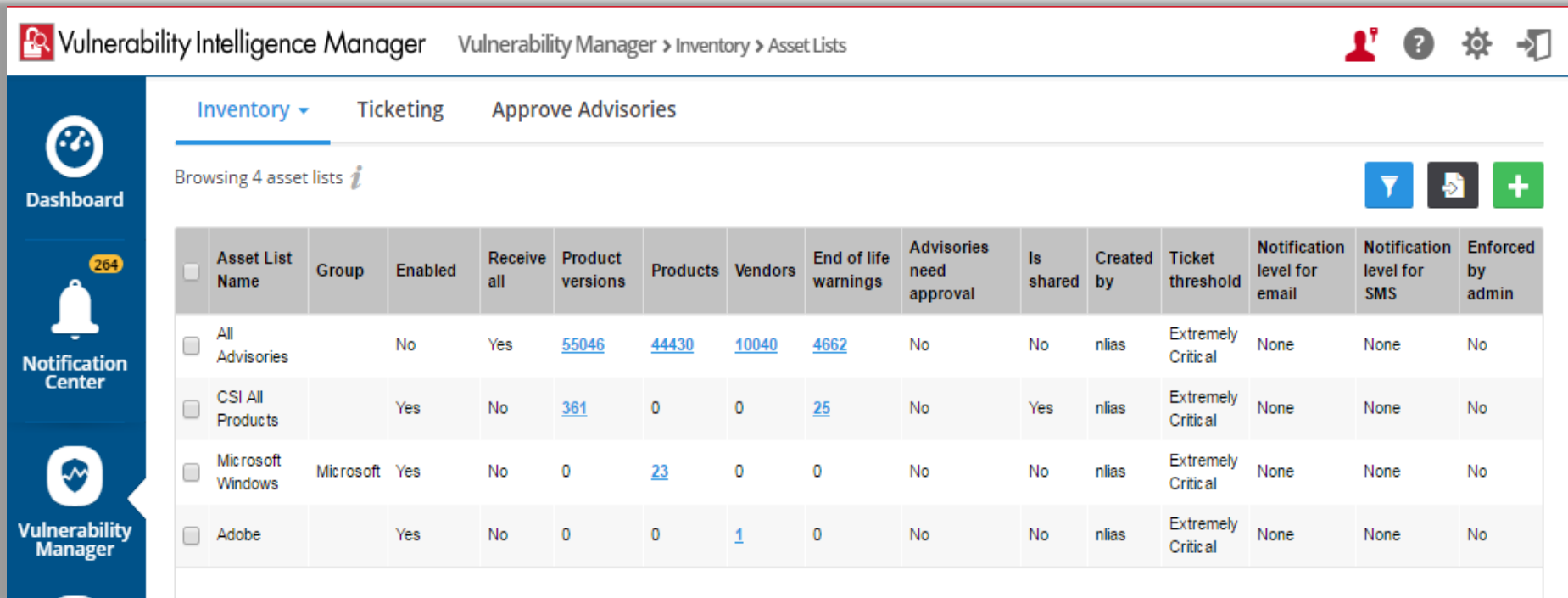
Advisories released last year

Menu

- Setup & Configuration
- Vulnerability Management
- Reporting
- Dashboard
- Action History
- Historic Advisories
- Report Configuration
- XML & RSS Intelligence Feeds
- Dashboard: My Profile
- Most Popular Advisories - Last 3 Hours
- The top-five most popular advisories, ranked by...
- Advisory**
- Oracle Java Three Vulnerabilities
- Red Hat update for java-1.5.0-ibm
- RealPlayer Multiple Vulnerabilities
- SUSE update for xan

Gérer le bon parc logiciel

- **Asset List** : configurer les groupes de logiciels qui vous concernent (par OS, Produit, éditeurs, ...)



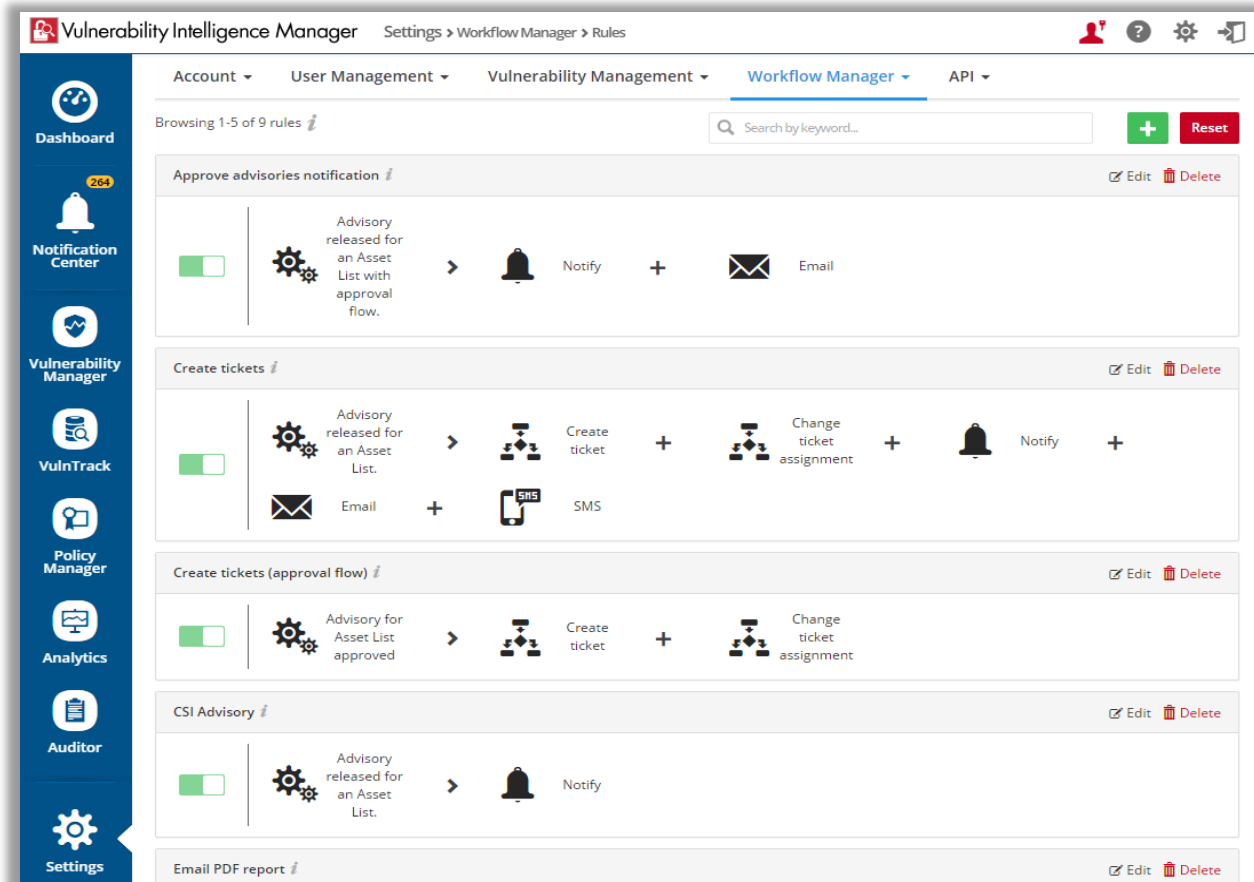
The screenshot displays the 'Vulnerability Intelligence Manager' interface. The breadcrumb navigation shows 'Vulnerability Manager > Inventory > Asset Lists'. The main content area is titled 'Inventory' and shows 'Browsing 4 asset lists'. A table lists the asset lists with columns for Name, Group, Enabled status, Receive all, Product versions, Products, Vendors, End of life warnings, Advisories need approval, Is shared, Created by, Ticket threshold, Notification level for email, Notification level for SMS, and Enforced by admin.

<input type="checkbox"/>	Asset List Name	Group	Enabled	Receive all	Product versions	Products	Vendors	End of life warnings	Advisories need approval	Is shared	Created by	Ticket threshold	Notification level for email	Notification level for SMS	Enforced by admin
<input type="checkbox"/>	All Advisories		No	Yes	55046	44430	10040	4662	No	No	nlias	Extremely Critical	None	None	No
<input type="checkbox"/>	CSI All Products		Yes	No	361	0	0	25	No	Yes	nlias	Extremely Critical	None	None	No
<input type="checkbox"/>	Microsoft Windows	Microsoft	Yes	No	0	23	0	0	No	No	nlias	Extremely Critical	None	None	No
<input type="checkbox"/>	Adobe		Yes	No	0	0	1	0	No	No	nlias	Extremely Critical	None	None	No

- Peut être importée (SCCM, FlexNet Manager...)
- L'Asset List peut être déléguée à des groupes

Gestion des incidents: workflows

Workflows personnalisés pour déclencher des notifications, approbations ou tickets d'incidents





Intégration avec ServiceNow. API disponible en standard.


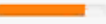



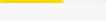

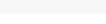
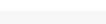


Gestion des incidents: Suivi des tickets, allocation de tâches, relances, ...

Advisory Database ▾ Products Database ▾

Browsing 1-20 of 60319 advisories *i*

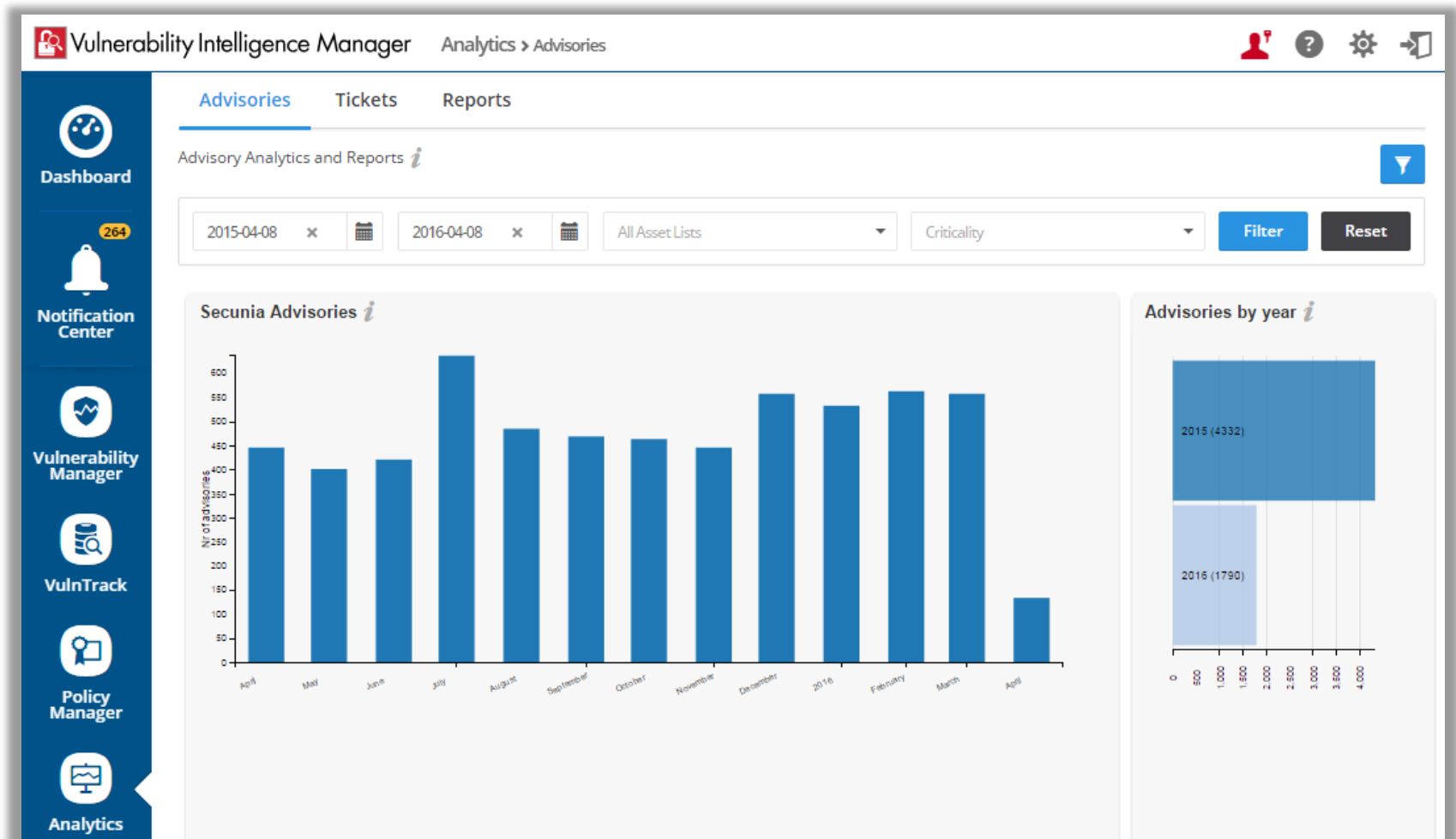
SAID From  To  Title Criticality ▾ Solutions... ▾ **Filter**

Where ▾ CVE CVSS Score M CVSS Score M Impact ▾

<input type="checkbox"/>	SAID	Release date	Modified date	Title	Criticality
<input type="checkbox"/>	SA67816	2015-12-16	2015-12-16	ISC BIND OpenSSL Weakness and Two Denial of Service Vulnerabilities	
<input type="checkbox"/>	SA67986	2015-12-16	2015-12-16	Cyberfox Multiple Vulnerabilities	
<input type="checkbox"/>	SA67948	2015-12-16	2015-12-16	Red Hat update for Red Hat Satellite	
<input type="checkbox"/>	SA67942	2015-12-16	2015-12-16	Oracle Linux update for libreoffice	
<input type="checkbox"/>	SA67968	2015-12-16	2015-12-16	IBM Forms Server Two Spoofing Security Issues and Security Bypass Vulnerability	
<input type="checkbox"/>	SA67826	2015-12-16	2015-12-16	Cisco Unified Communications Manager Identity Management Subsystem Denial of Service Vulnerability	
<input type="checkbox"/>	SA67987	2015-12-16	2015-12-16	IBM Tivoli Netcool Configuration Manager Multiple Vulnerabilities	
<input type="checkbox"/>	SA68014	2015-12-16	2015-12-16	QEMU VMXNET3 NIC Information Disclosure Vulnerability	
<input type="checkbox"/>	SA67803	2015-12-16	2015-12-16	Mozilla Firefox ESR Multiple Vulnerabilities	
<input type="checkbox"/>	SA67802	2015-12-16	2015-12-16	Mozilla Firefox Multiple Vulnerabilities	
<input type="checkbox"/>	SA67890	2015-12-16	2015-12-16	TYPO3 Multiple Vulnerabilities	

Suivi analytique

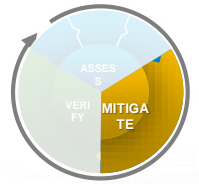
- Aperçu graphique de l'activité et de la santé de la gestion de la vulnérabilité dans votre organisation





FLEXERA SOFTWARE®

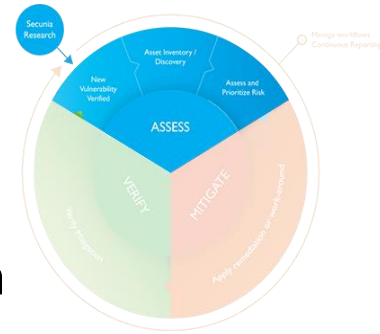
Corporate Software Inspector



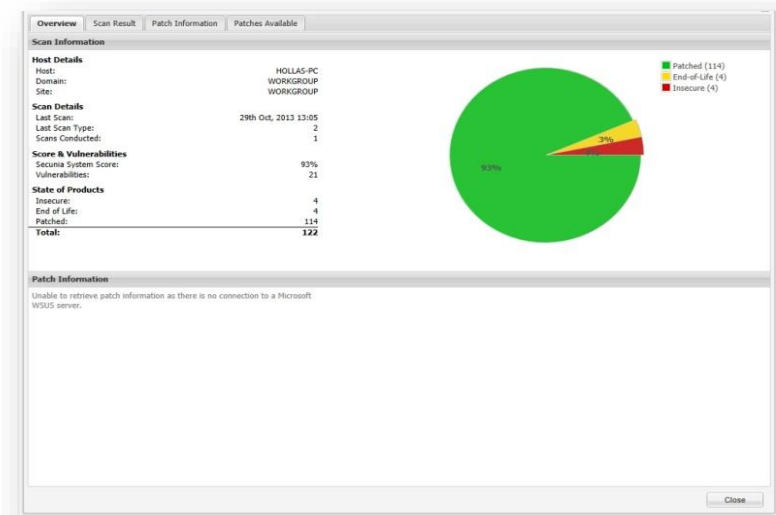
- Identifie et gère les les vulnérabilités logicielles pour créer et déployer les patches de sécurité
- Tire partie de la base de connaissance de Secunia Research



Corporate Software Inspector: évaluation

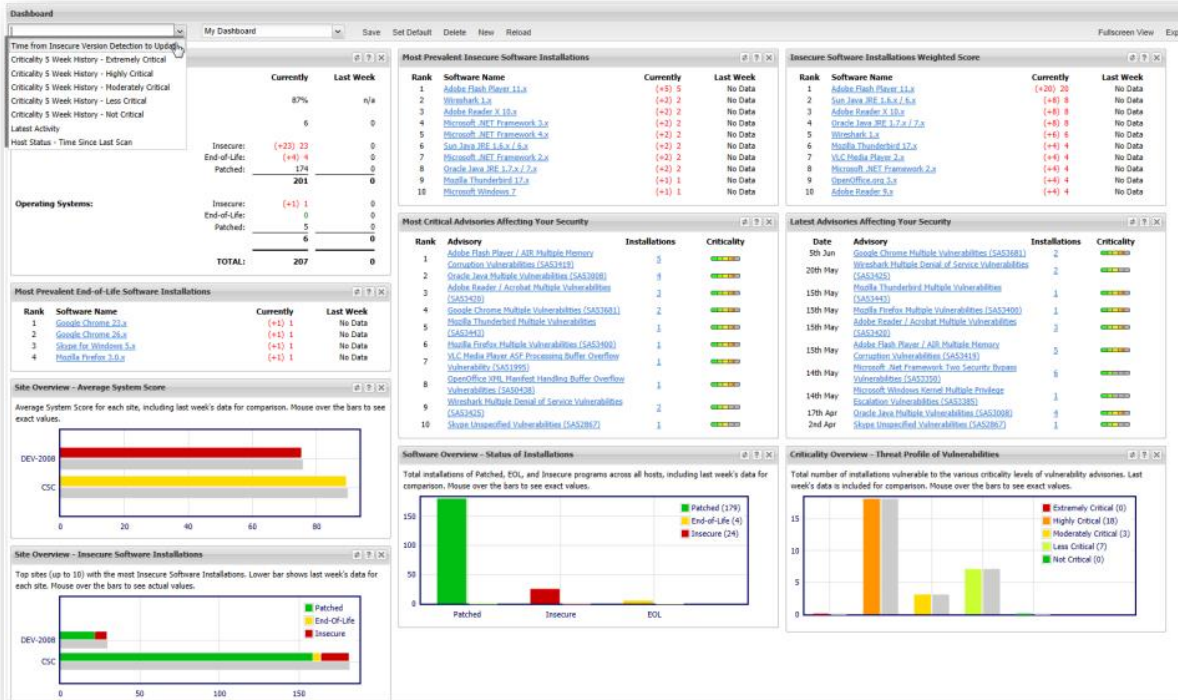


- Nouvelle vulnérabilité :
 - Alertes reçues régulièrement de Secunia Research
- Inventaire/Découverte:
 - Intégration avec l'inventaire MS System Center pour une recherche sans scan
 - Scanner Non-intrusif, authentifié pour la découverte
 - Scanner de logiciels: 20,000+ applications
 - Niveau de Patch et criticité pour 20,000+ applications
- Etablir le risque et l'évaluer
 - Accès aux bulletins Secunia
 - Indication de la criticité
 - Application de coefficients
 - Alertes de vulnérabilité sans scan



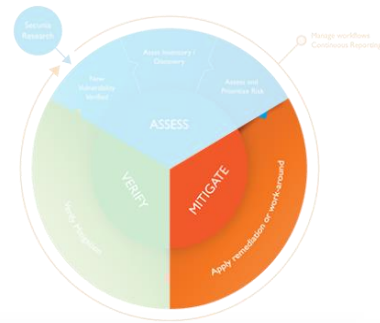
Aide à la décision : évaluation de la criticité

- Criticité déterminée par le Secunia Research Team



Name	Version	State	SAID	Criticality	Issued	Vulnerabilities
Adobe Flash Player 13.x	13.0.0.223 (NPA...	End-Of-Life	SA67114		30 days ago	17
Adobe Flash Player 13.x	13.0.0.223 (NPA...	End-Of-Life	SA67114		30 days ago	17
Adobe Reader XI 11.x	11.0.0.7.79	Insecure	SA66814		58 days ago	57
Apple QuickTime 7.x	7.74.80.86	Insecure	SA66145		111 days ago	9
Mozilla Firefox 18.x	18.0.0.4744	End-Of-Life	SA67179		36 days ago	19
Oracle Java JRE 1.6.x / 6.x	6.0.450.6	End-Of-Life	SA67038		50 days ago	25
Oracle Java JRE 1.7.x / 7.x	7.0.150.3	End-Of-Life	SA67038		50 days ago	25
RealPlayer 1.x	12.0.0.297	End-Of-Life	SA59238		525 days ago	1
VLC Media Player 2.x	2.1.2.0	Insecure	SA62720		311 days ago	5

Corporate Software Inspector: Appliquer



- Appliquer le correctif ou le contournement

- Contenu:

- Patches pre-testés
 - Contenu Non-Microsoft riche
 - Ajout de ses propres Packages

- Packaging:

- désactivation adware, EULA, raccourcis, ...configuration en 1 click

- Priorisation:

- Listes de priorité basée sur la criticité ou des Smart Groups

- Integration pour le déploiement:

- **Microsoft WSUS, SCCM, Symantec Altiris**

- SC2012 Plugin:

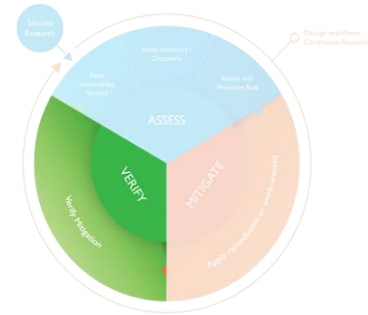
- Patching directement depuis la console Microsoft System Center

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected	Insecure	End-Of-Life	Patched
Product: Adobe AIR 3.x (1 Item)									
Adobe AIR 3.0	Adobe	3.8.0.870	Windows 32-bit	SAS3975	Low	2 days ago	1	0	0
Product: Adobe AIR 3.0 (ActiveX) (1 Item)									
Adobe AIR 3.0 (ActiveX)	Adobe	11.8.800.94	Windows 32-bit	SAS3975	Low	2 days ago	1	0	0
Product: Apple iTunes 10.x (1 Item)									
Apple iTunes 10.x	Apple	10.7	Windows 32-bit	SAS0618	Low	2 days ago	1	0	0
Product: Apple QuickTime 7.x (1 Item)									
Apple QuickTime 7.x	Apple	7.7.4	Windows 32-bit	SAS3320	Low	2 days ago	2	0	0
Product: Mozilla Firefox 20.x (1 Item)									
Mozilla Firefox 20.x	Mozilla Foundation	22.x	Windows 32-bit	SAS3970	Low	2 days ago	0	1	0
Product: Mozilla Firefox 21.x (1 Item)									
Mozilla Firefox 21.x	Mozilla Foundation	22.x	Windows 32-bit	SAS3970	Low	2 days ago	0	1	0
Product: Oracle Java JRE 1.7.x / 7.x (1 Item)									
Oracle Java JRE 1.7.0_75	Oracle Corporation	7u25	Windows 32-bit	SAS3846	Low	2 days ago	1	0	0

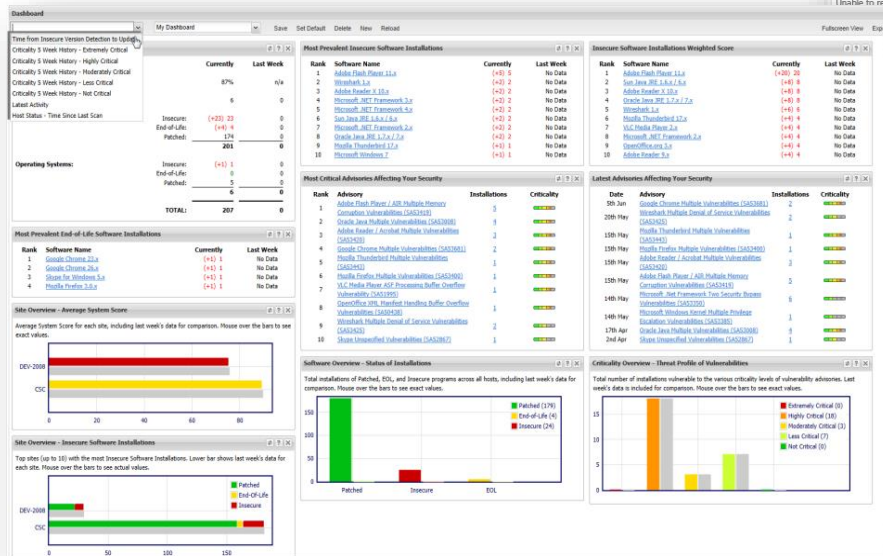
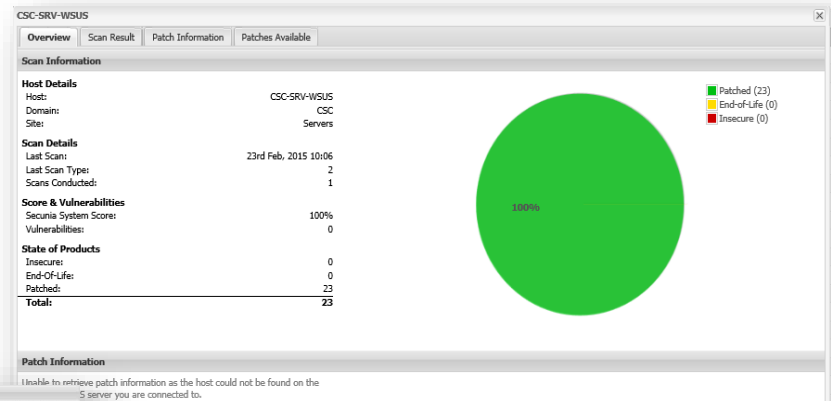
Name	Version	State	SAID	Criticality	Issued	Vulnerabilities
Google Chrome 42.x	42.0.2284.415	Patched	-	-	-	-
Microsoft .NET Framework 2.0	2.0.50727.5483	Patched	-	-	-	-
Microsoft .NET Framework 2.0	2.0.50727.5483	Patched	-	-	-	-
Microsoft .NET Framework 4.0	4.0.30319.1	Patched	-	-	-	-
Microsoft .NET Framework 4.0	4.0.30319.1	Patched	-	-	-	-
Microsoft Internet Explorer 9.x	9.0.8112.16609	Patched	-	-	-	-
Microsoft Internet Explorer 9.x	9.0.8112.16609	Patched	-	-	-	-
Microsoft SQL Server 2005	2005.90.2000.9	Patched	-	-	-	-
Microsoft Visual C++ 2005 Redistributable Package (x86)	8.0.50727.4195	Patched	-	-	-	-
Microsoft Visual C++ 2005 Redistributable Package (x86)	8.0.50727.4195	Patched	-	-	-	-
Microsoft Visual C++ 2008 Redistributable Package	9.0.30729.6161	Patched	-	-	-	-
Microsoft Visual C++ 2008 Redistributable Package	9.0.30729.6161	Patched	-	-	-	-
Microsoft Windows Server 2008	Windows Server	Patched	-	-	-	-
Microsoft Windows Server Update Services (WSUS) 3.x	3.1.7600.226	Patched	-	-	-	-
Microsoft .NET Core Services (MSDN) 3.x	8.116.7601.18576	Patched	-	-	-	-
Microsoft .NET Core Services (MSDN) 3.x	8.116.7601.18576	Patched	-	-	-	-
Microsoft .NET Core Services (MSDN) 6.x	6.30.7601.18431	Patched	-	-	-	-
Microsoft .NET Core Services (MSDN) 6.x	6.30.7601.18431	Patched	-	-	-	-
Secunia CSI (Corporate Software Inspector) Plugin 7.x	7.0.0.5001	Patched	-	-	-	-
Secunia CSI Agent 7.x	7.0.0.5002	Patched	-	-	-	-
VMware Tools 5.x	5.0.1.18551	Patched	-	-	-	-
Windows PowerShell 2.x	6.1.7600.16385	Patched	-	-	-	-
Windows PowerShell 2.x	6.1.7600.16385	Patched	-	-	-	-

Host	System Score	Last Scan	Insecure	End Of Life
CSC-BL-WIN7-01	100%	27th Aug, 2013 16:10	0	0
CSC-SRV-DC	100%	27th Aug, 2013 16:10	0	0
CSC-SRV-FILESER	100%	27th Aug, 2013 16:10	0	0
CSC-TS-A	93%	27th Aug, 2013 13:41	1	2
CSC-TS-B	100%	27th Aug, 2013 16:10	0	0
CSC-VM-1	98%	27th Aug, 2013 14:15	0	1

Corporate Software Inspector: Vérification



- Vérifier que la solution Adversio est appliquée:
 - Vue tableau de bord
 - Rapport de type *Executive Summary*
 - Statistiques par Site
 - Statistiques par Machine
 - Statistiques par Produit
 - Scans réguliers

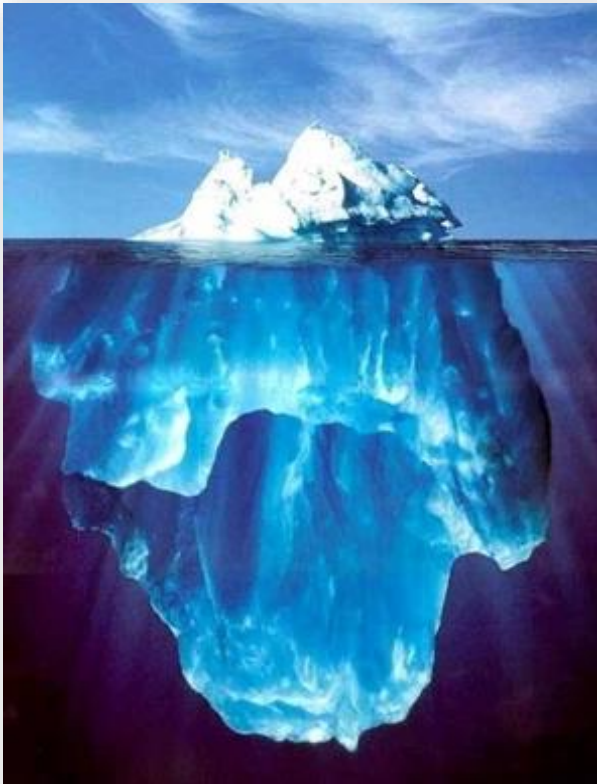


Et la vulnérabilité dans nos propres logiciels?

SOFTWARE COMPOSITION ANALYSIS



Statut de of OSS in the Software Industry



- **50% - 90%** du code des développements internes est externe
- Mais les organisations savent typiquement **moins de 10%** de ce qui est utilisé
- Un contenu externs non maîtrisé mène à:
 - **Risques de Vulnérabilité** Open Source
 - **Violations de propriété intellectuelle**
 - **Problème du contrôle des exports**
 - Prolifération des versions de composants
 - ...

Risques introduits par la "Software Supply Chain"

La chaîne de traçabilité est souvent rompue



FANTEC guilty of GPL infringement in Germany

[Posted June 26, 2013 by corbet]

The Free Software Foundation Europe [announces](#) that Harald Welte has won a GPL infringement case against FANTEC in Germany.

"The court decided that FANTEC acted negligently: they would have had to ensure to distribute the software under the conditions of the GPLv2. The court made explicit that it is insufficient for FANTEC to rely on the assurance of license compliance of their suppliers. FANTEC itself is required to ascertain that no rights of third parties are violated."

Est-ce que ce logiciel est sous votre contrôle depuis sa création ?

Heartbleed

Open SSL

Heartbleed is a [security bug](#) in the [open-source OpenSSL cryptography](#) library, widely used to implement the Internet's [Transport Layer Security](#) (TLS) protocol. A fixed version of [OpenSSL](#) was released on April 7, 2014, at the same time as Heartbleed was publicly disclosed. At that time, some 17 percent (around half a million) of the Internet's secure [web servers](#) certified by [trusted authorities](#) were believed to be vulnerable to the attack, allowing theft of the servers' [private keys](#) and users' session cookies and passwords.

Heartbleed is registered in the [Common Vulnerabilities and Exposures](#) system as CVE-2014-0160

[Wikipedia](#)



Products and Services

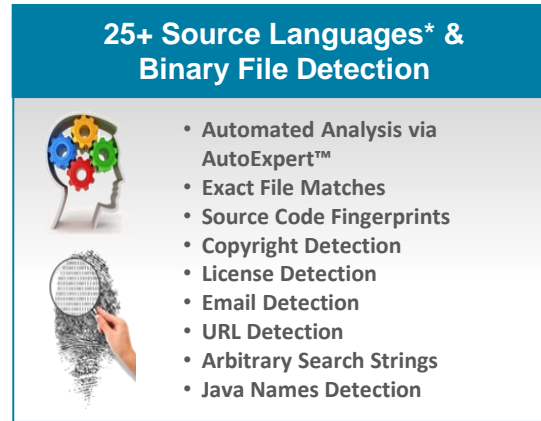
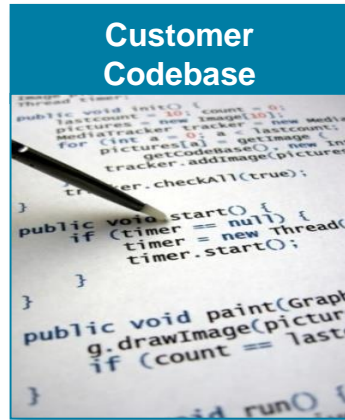
Software Solution for Software Composition Analysis: Software BOM, IP Compliance, Vulnerability and Export Reports

Professional Services Practice: M&A due diligence, product IP baseline analysis, inbound source audit

Over 400 customers worldwide in Technology, Finance, Manufacturing, Defense, Telecommunications and Entertainment

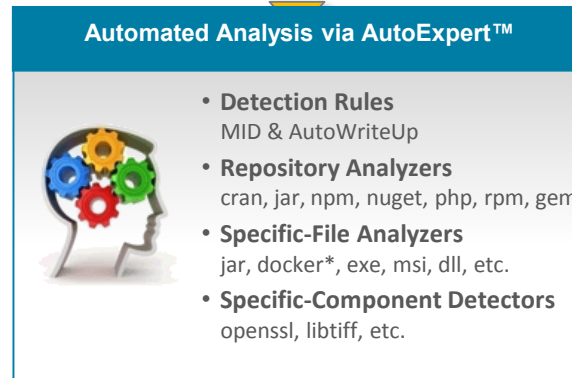
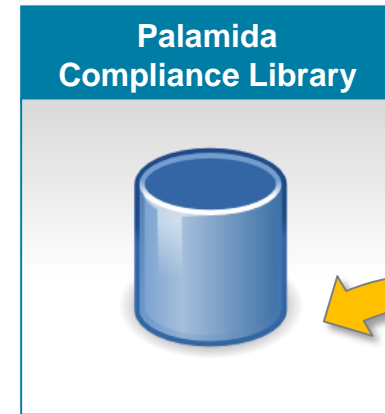


Technologie spécifique (brevetée)



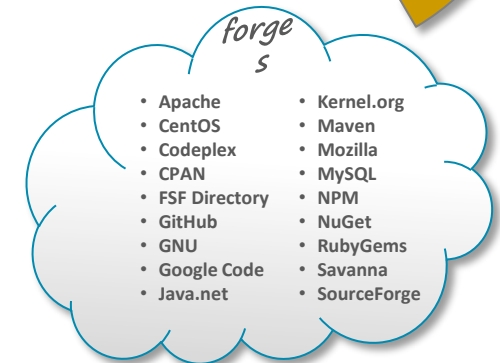
25+ Source Languages* & Binary File Detection

- Automated Analysis via AutoExpert™
- Exact File Matches
- Source Code Fingerprints
- Copyright Detection
- License Detection
- Email Detection
- URL Detection
- Arbitrary Search Strings
- Java Names Detection



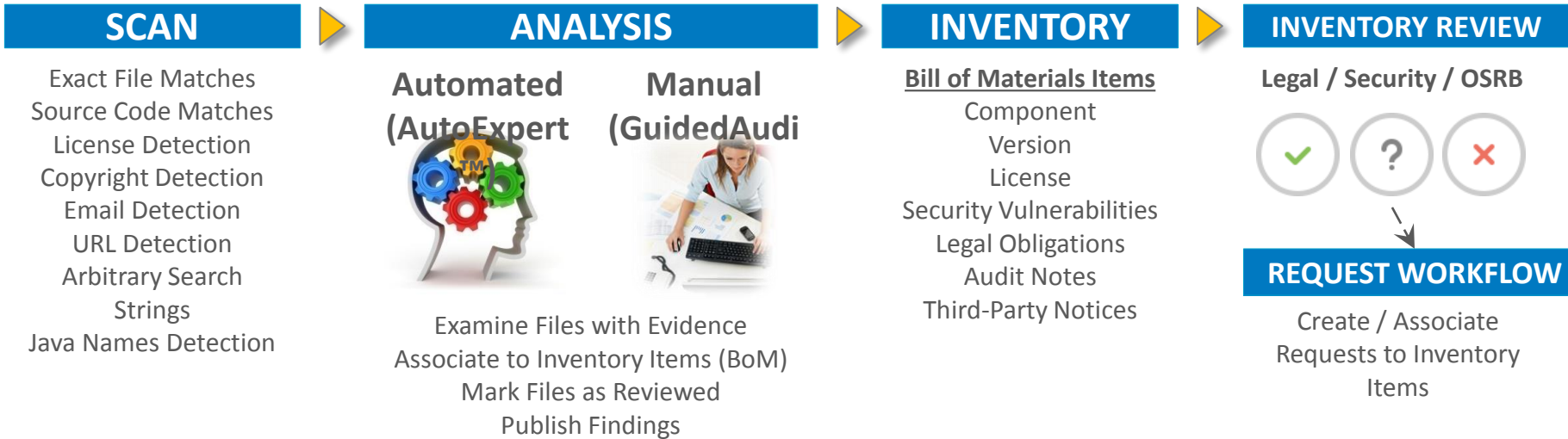
Automated Analysis via AutoExpert™

- **Detection Rules**
MID & AutoWriteUp
- **Repository Analyzers**
cran, jar, npm, nuget, php, rpm, gem
- **Specific-File Analyzers**
jar, docker*, exe, msi, dll, etc.
- **Specific-Component Detectors**
openssl, libtiff, etc.



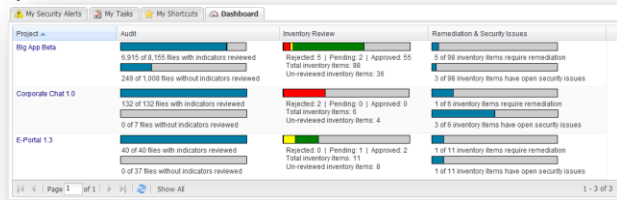
* **Source Languages:** Ada, ASP, C#, C/C++, Delphi, Erlang, F#, Fortran, Go, Java, JavaScript, Lua, Node.js, PHP, Perl, Python, Ruby, Scala, ShellScript, Swift, Tcl, Verilog, Visual Basic, and VHDL

Solution intégrée



REPORTS

Third-Party Indicators Report
Evidence



Analyzer Report
Evidence Rank Report

Palamida Report
Audit Report
Usage Reports
CVE/Vulnerability Report
Obligations Report
Third-Party Notices Report

Requests Report
Usage Reports
Obligations Report
Third-Party Notices Report

Merci



Pour plus d'information: www.flexerasoftware.fr

François MAUFRAIS - fmaufrais@flexerasoftware.com

Christian HINDRE – chindre@flexerasoftware.com