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)

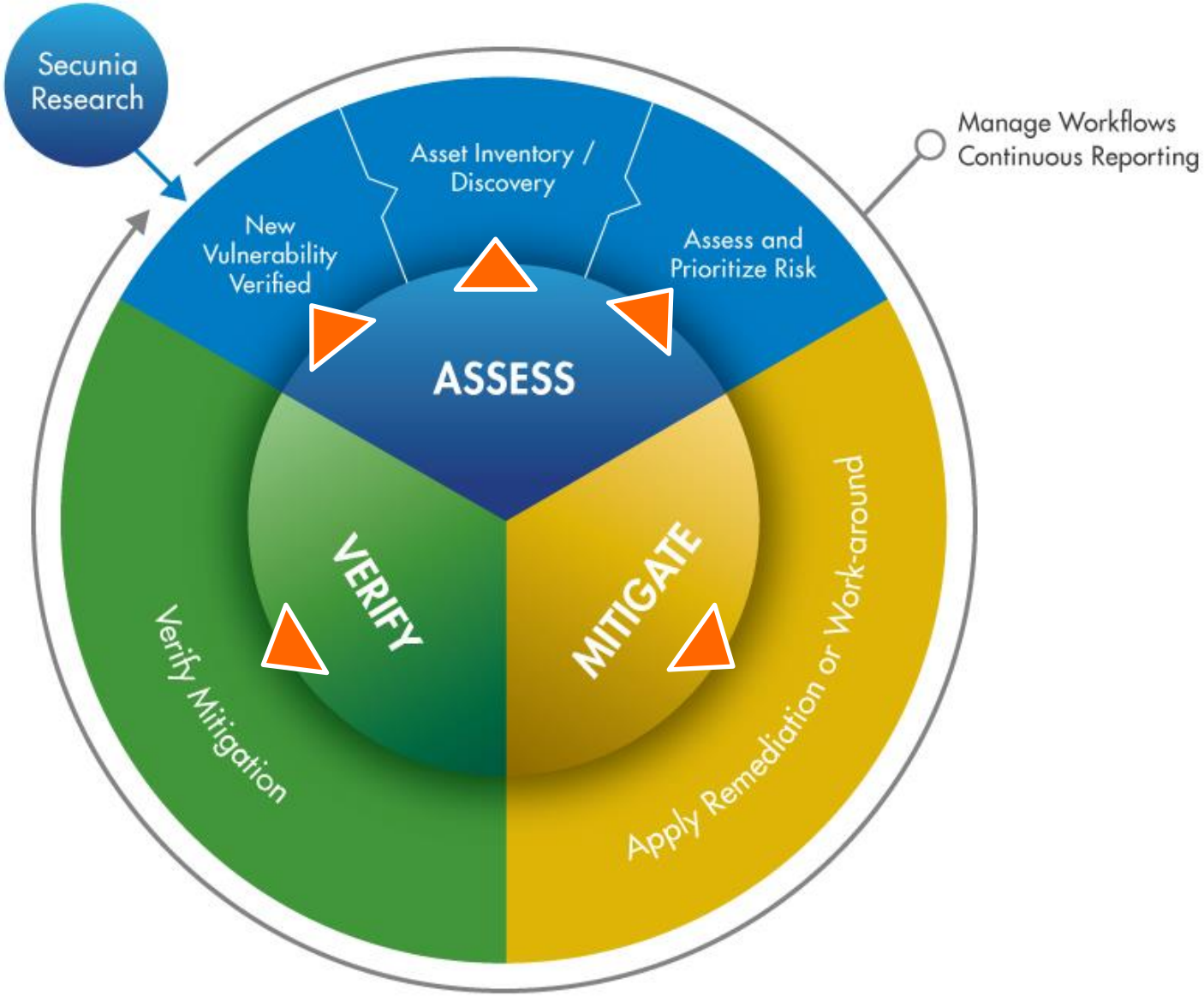
Vulnérabilités Logicielles

Un risque permanent pour les uns

Un marché plus que rentable pour d’autres

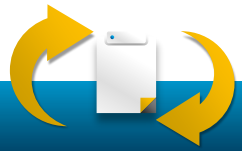
FLEXERA SOFTWARE

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 déléguations 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

FLEXERA SOFTWARE

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 appronfondie, 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 gére les correctifs de sécurité

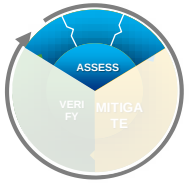
FLEXERA SOFTWARE®
Personal Software Inspector

- **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*

FLEXERA SOFTWARE®

Vulnerability Intelligence Manager

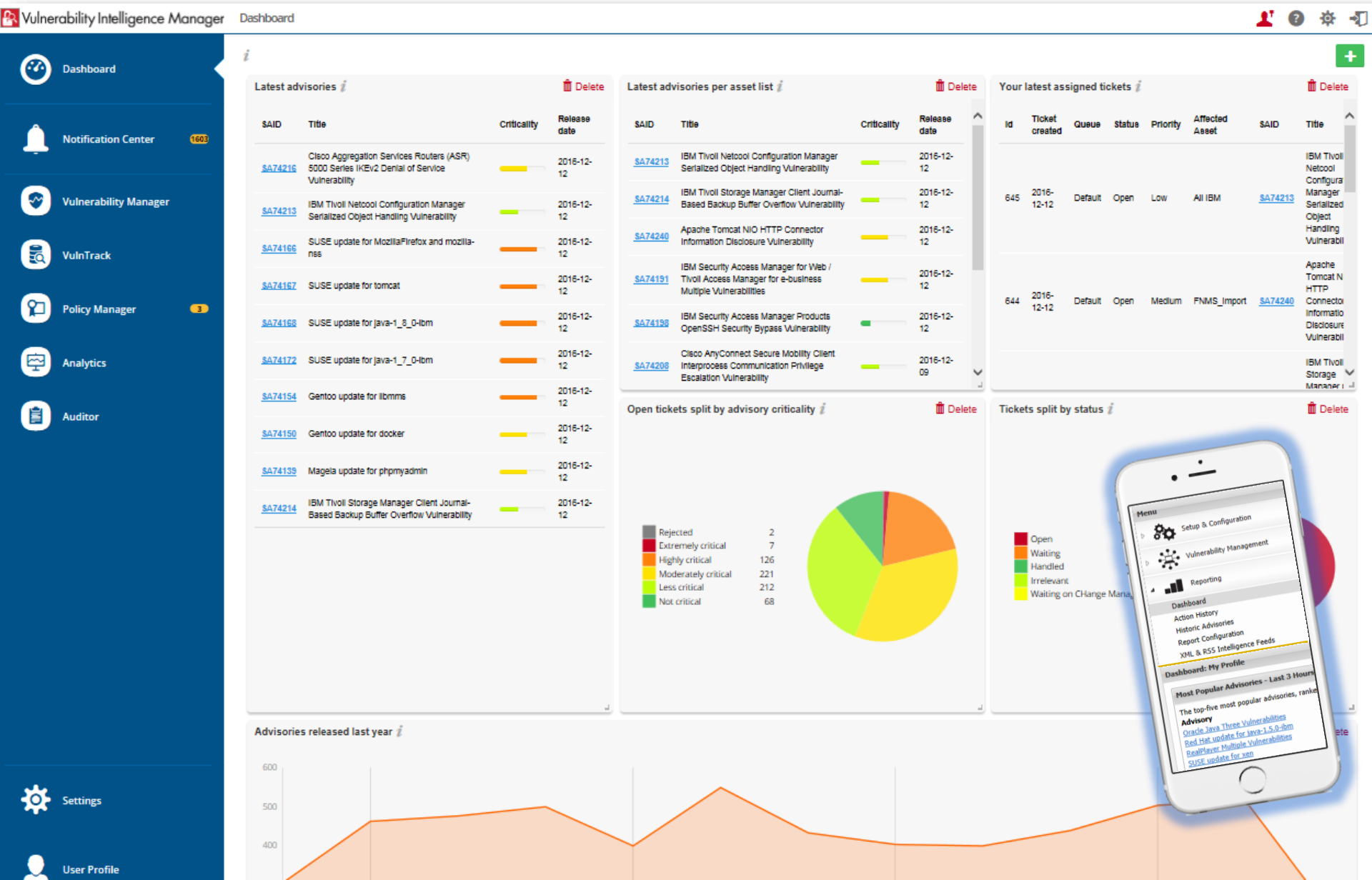


VIM est une solution de recherche d'information en Cloud pour les spécialistes de sécurité

- 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, …

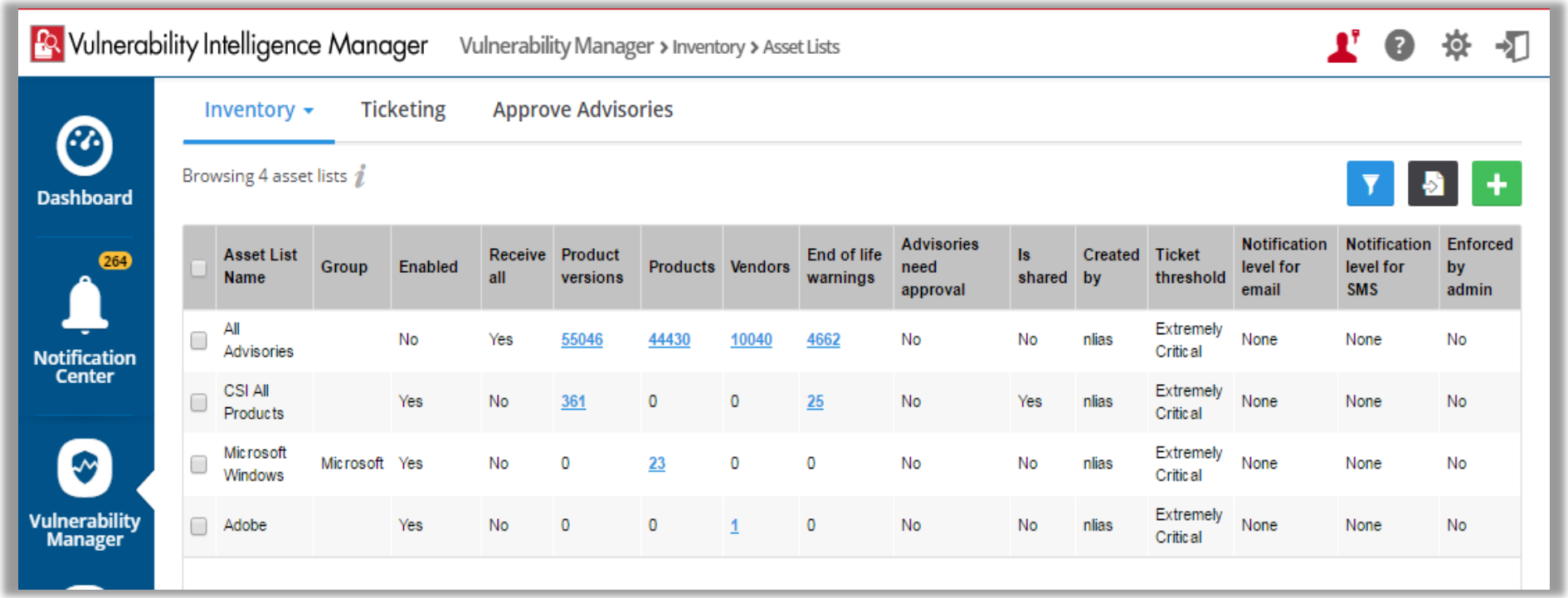
Tableaux de bord et Rapports

Rapport d'évaluation des priorités & filtrage



Gérer le bon parc logiciel

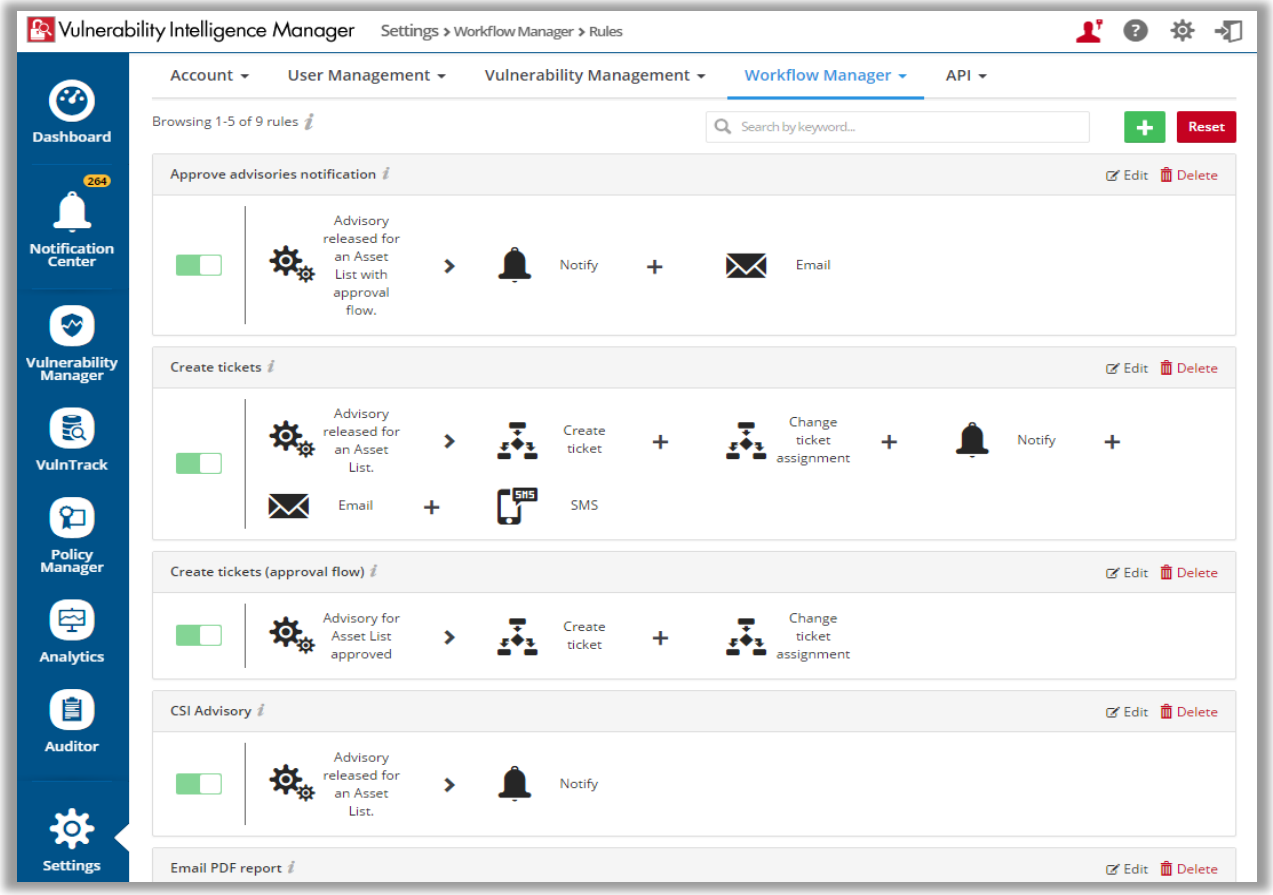
- ***Asset List*** : configurer les groupes de logiciels qui vous concernent (par OS, Produit, éditeurs, …)



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

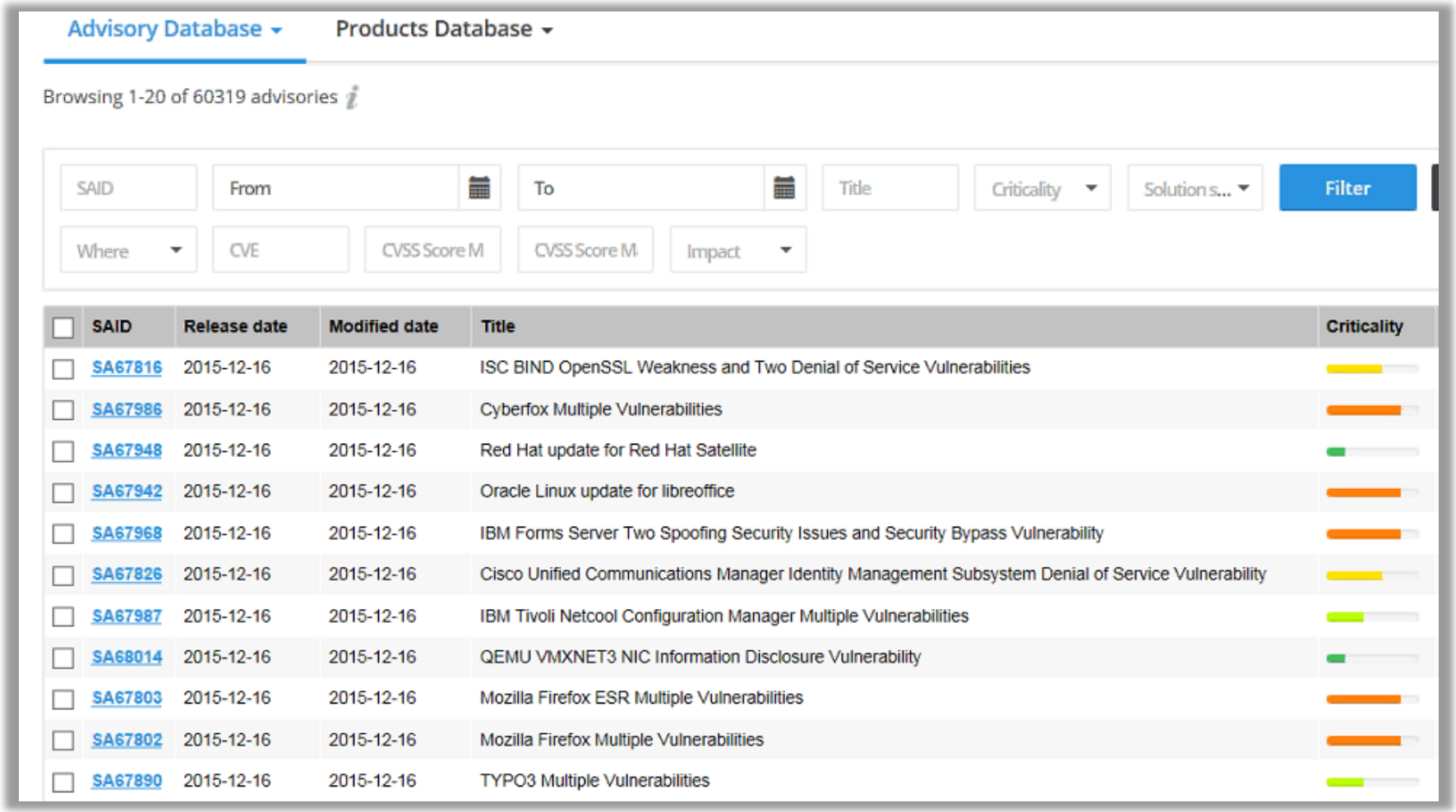
Gestion des incidents: workflows

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



Intégration avec ServiceNow. API disponible en standard.

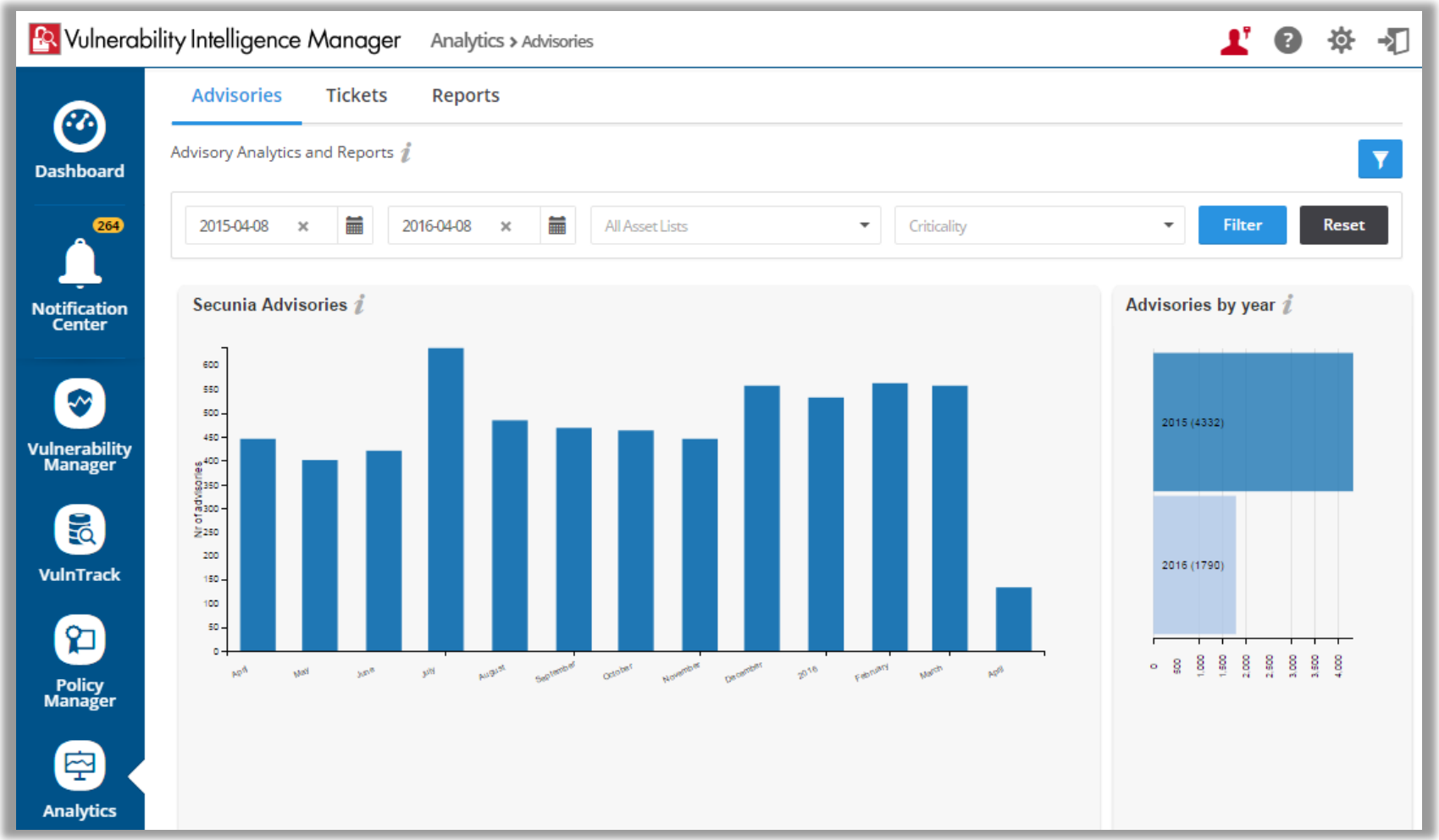
Gestion des incidents: Suivi des tickets, allocation de tâches, relances, …



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

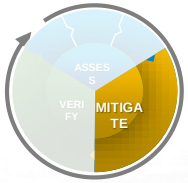
Suivi analytique

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

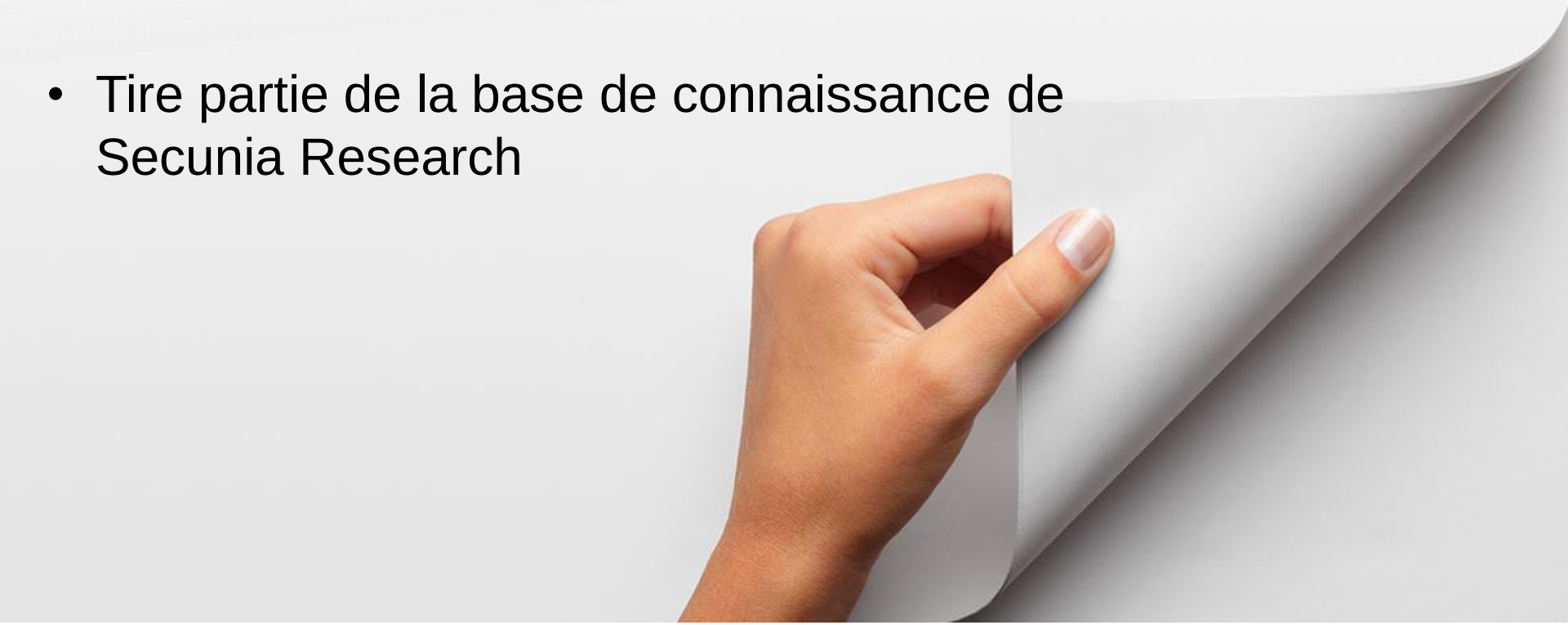


FLEXERA SOFTWARE®

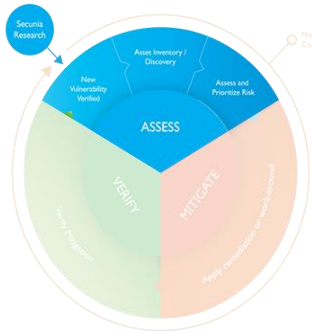
Corporate Software Inspector



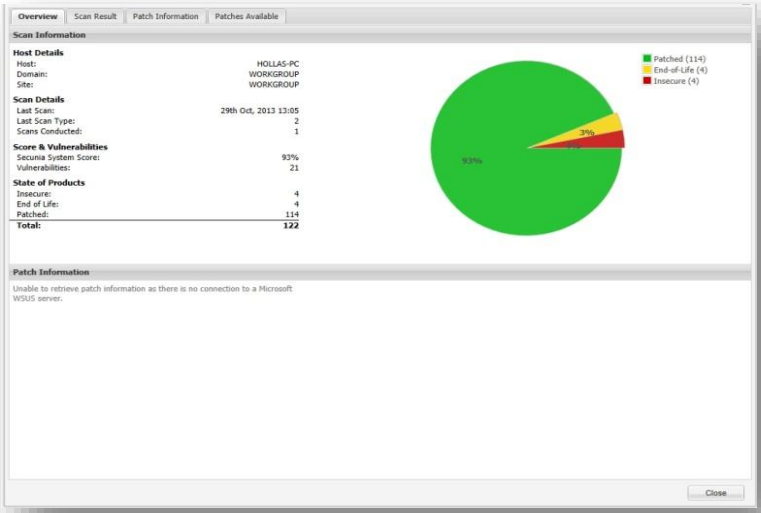
- Identifie et gère les les vulnerabilités logicielles pour créer et déployer les patches de sécurité
- Tire partie de la base de connaissance de Secunia Research



Corporate Software Inspector: évaluation

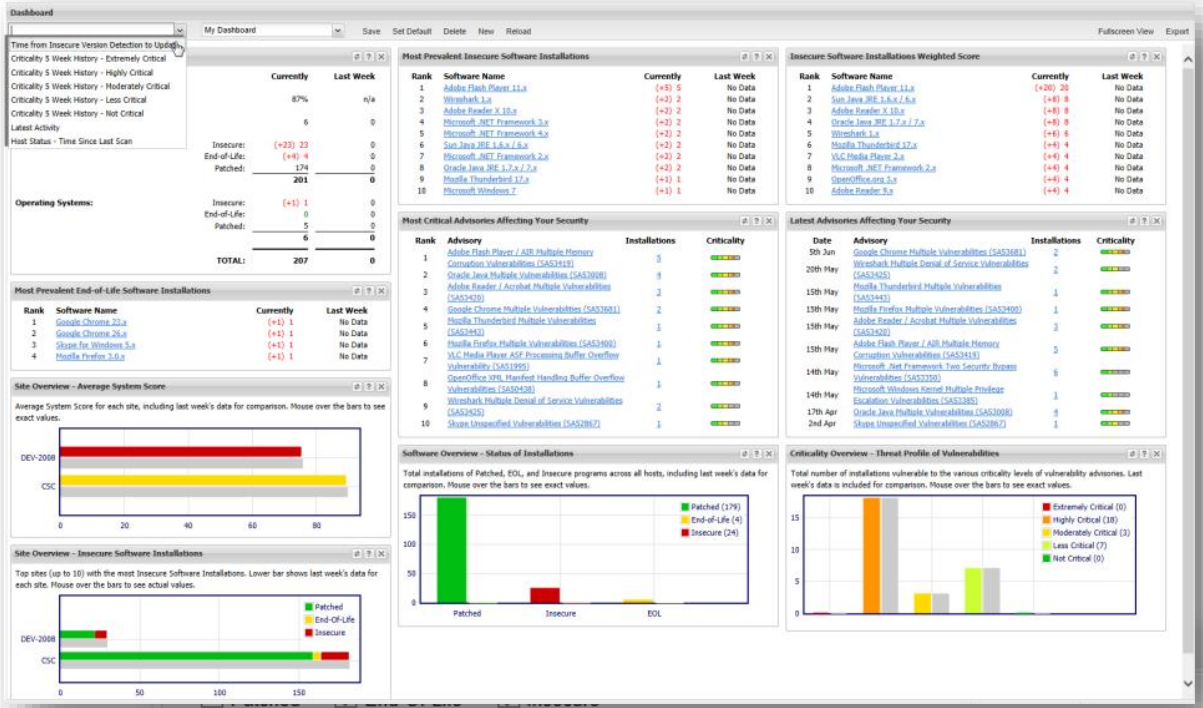


- Nouvelle vulnérabilité :
  - Alertes reçues régulièrememement de Secunia Research
- Inventaire/Découverte:
  - Intégration avec l'inventaire MS System Center pour une recherché sans scan
  - Scanner Non-intrusif, authentifié pour la découverte
  - Scanner de logiciels: 20,000+ applications
  - Niveau 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



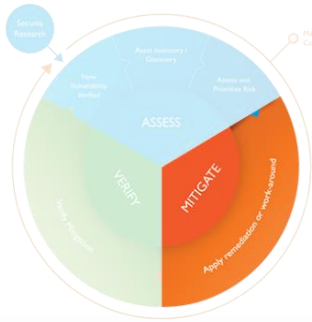
Aide à la decision : évaluation de la criticité

- Criticité déterminée par le Secunia Research Team

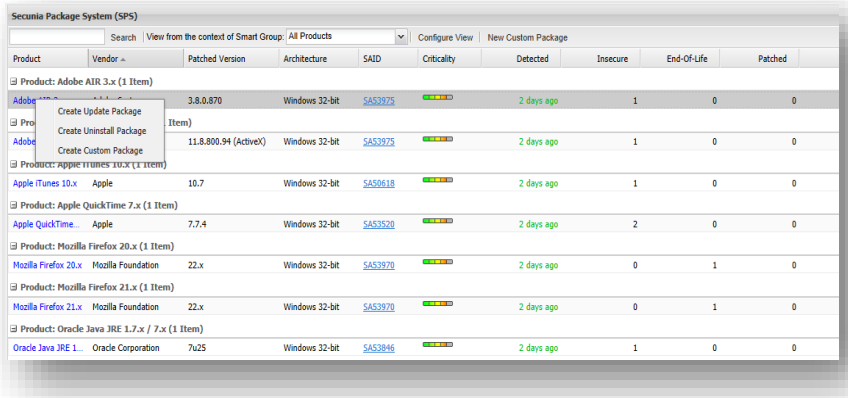


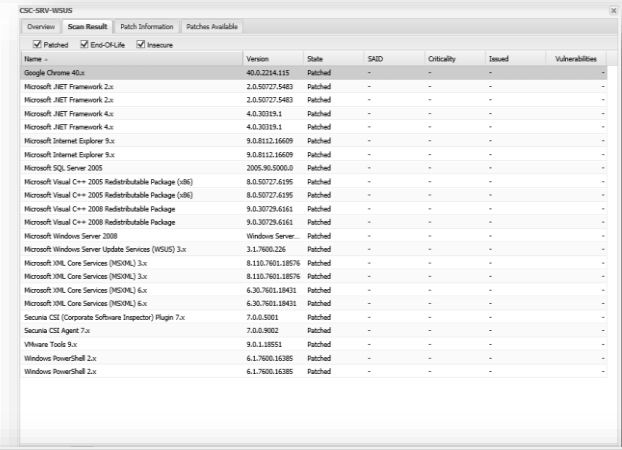
Name	Version	State	SAID	Criticality	Issued	Vulnerabilities
Adobe Flash Player 13.x	13.0.0.223 (NPA...	End-Of-Life	SA67114		30 days ago	17
Adobe Flash Player 13.x	13.0.0.223 (NPA...	End-Of-Life	SA67114		30 days ago	17
Adobe Reader XI 11.x	11.0.07.79	Insecure	SA66814		58 days ago	57
Apple QuickTime 7.x	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

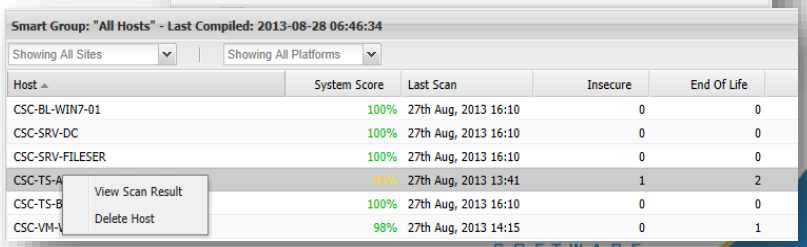
Corporate Software Inspector: Appliquer



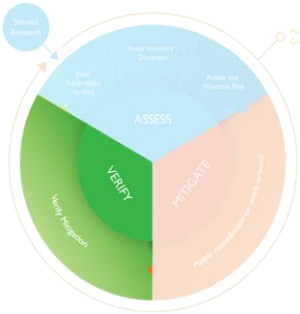
- Appliquer le correctif ou le contournement
  - Contenu:
    - Patches pre-testés
    - Contenu Non-Microsoft riche
    - Ajout de ses propres Packages
  - Packaging:
    - désactivation adware, EULA, raccourcis, …configuration en 1 click
  - Priorisation:
    - Listes de priorité basée sur la criticité ou des Smart Groups
  - Integration pour le déploiement:
    - **Microsoft WSUS**, **SCCM**, Symantec Altiris
  - SC2012 Plugin:
    - Patching directement depuis la console Microsoft System Center



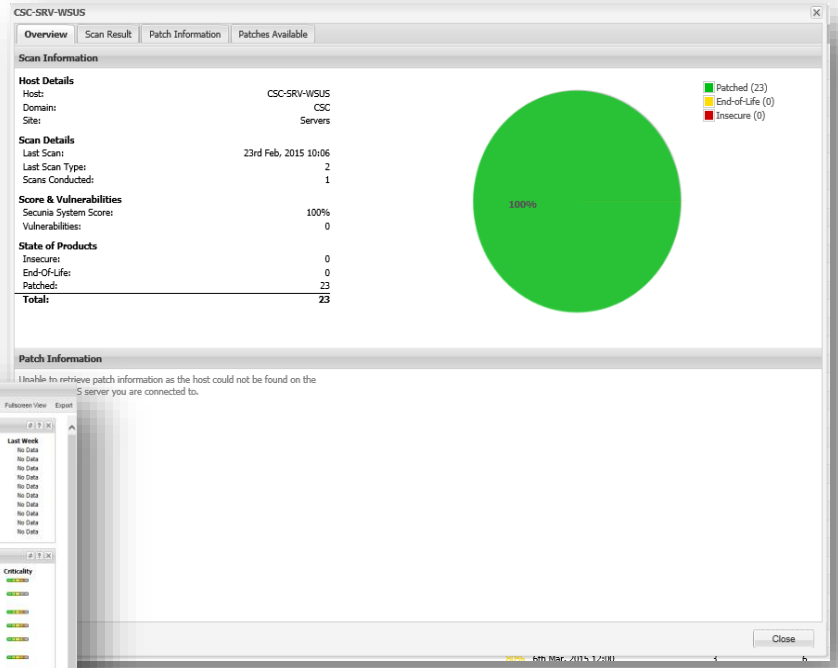


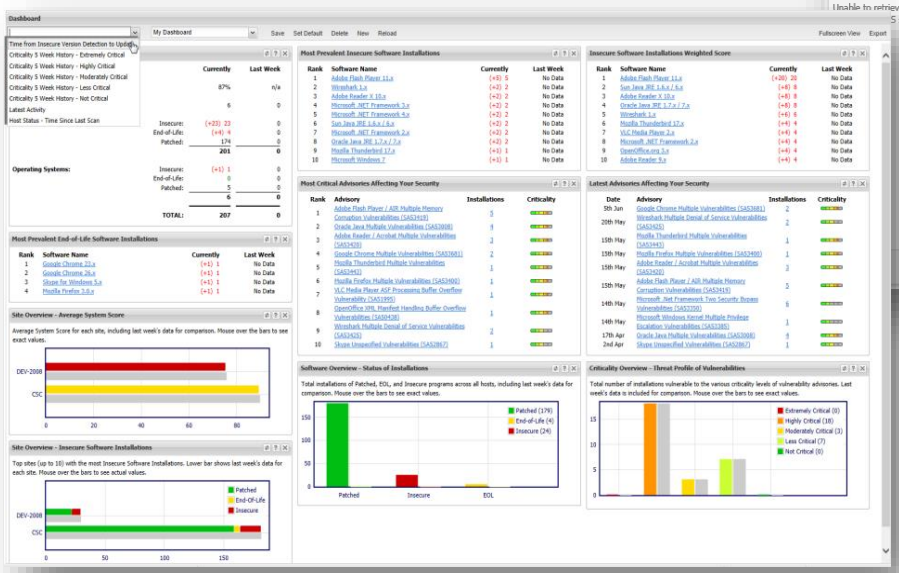


Corporate Software Inspector: Vérification



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



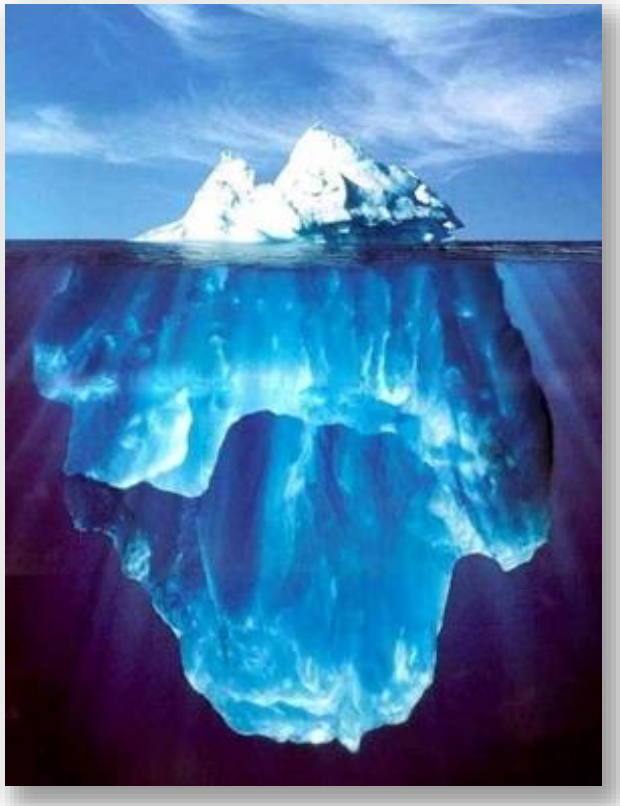


Et la vulnérabilité dans nos propres logiciels?

SOFTWARE COMPOSITION ANALYSIS

FLEXERA® SOFTWARE

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 utilsé

- 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 chaine de tracabilité est souvent rompue

mozilla

CPAN

Java.net

sourceforge

The Apache Software Foundation http://xml.apache.org

github SOCIAL CODING

CodePlex

Commercial

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

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."

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

FLEXERA SOFTWARE

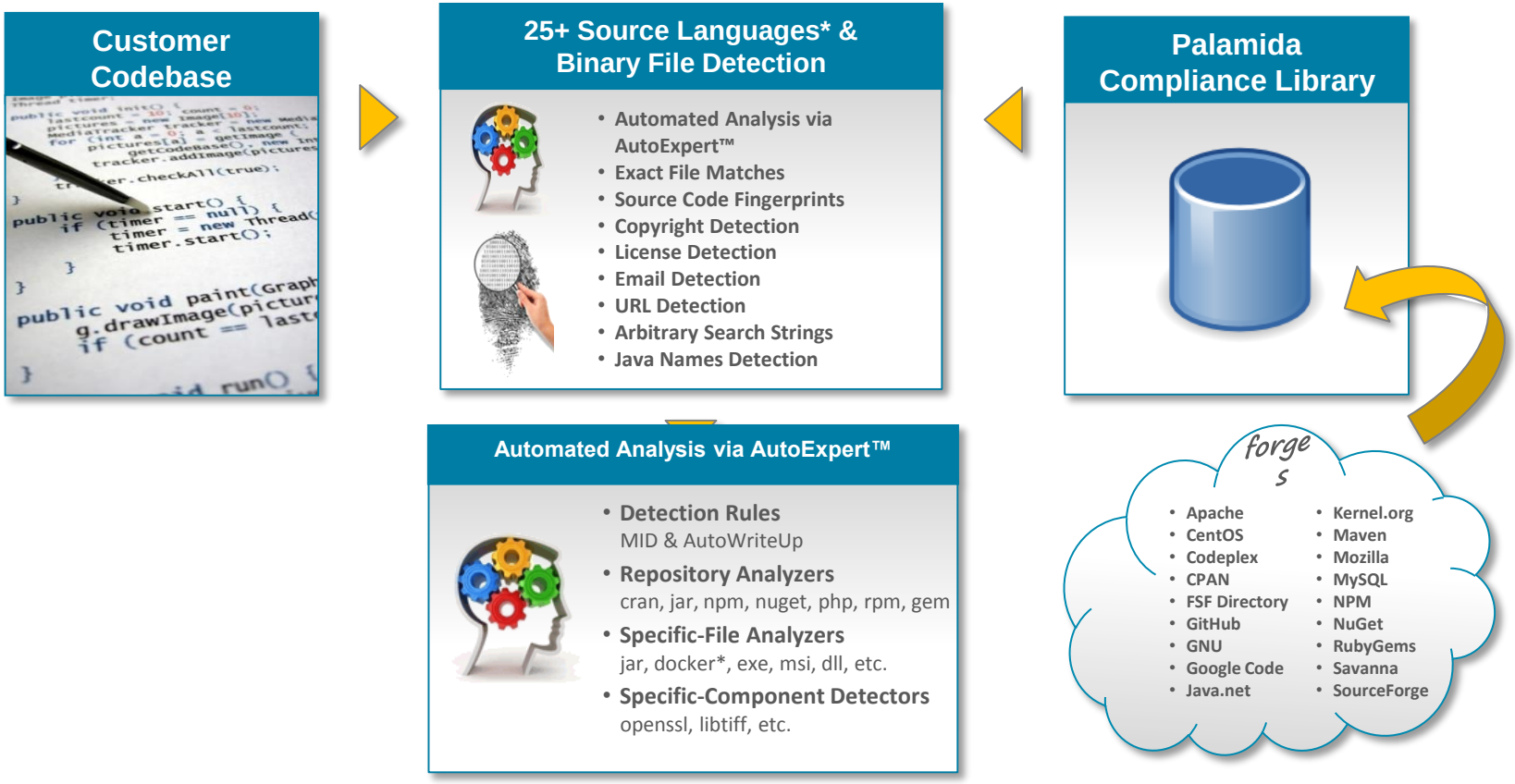
Products and Services

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)



*** 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

SCAN

Exact File Matches
Source Code Matches
License Detection
Copyright Detection
Email Detection
URL Detection
Arbitrary Search Strings
Java Names Detection

ANALYSIS

Automated (AutoExpert

Manual (GuidedAudi

Examine Files with Evidence
Associate to Inventory Items (BoM)
Mark Files as Reviewed
Publish Findings

INVENTORY

Bill of Materials Items
Component
Version
License
Security Vulnerabilities
Legal Obligations
Audit Notes
Third-Party Notices

INVENTORY REVIEW

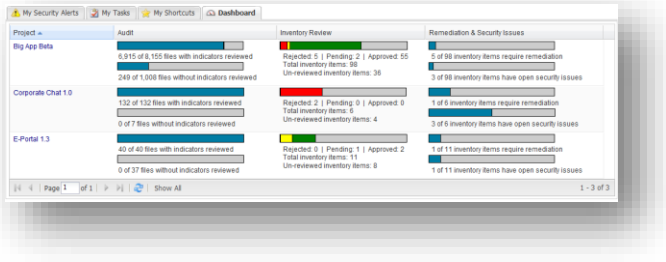
Legal / Security / OSRB

REQUEST WORKFLOW

Create / Associate Requests to Inventory Items

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

Pour plus d'information: www.flexerasoftware.fr

François MAUFRAIS - fmaufrais@flexerasoftware.com

Christian HINDRE – chindre@flexerasoftware.com