SCAP & XCCDF/OVAL

Standardisation des Opérations de Sécurité et des Validations de Conformité

Benjamin Marandel

Ingénieur Avant-Vente
pour McAfee

Qu'est-ce que SCAP ?

- Secure Content Automation Protocol :
  est un ensemble de normes ouvertes sélectionnées qui énumère les défauts des logiciels et les problèmes de configuration liés à la sécurité, les noms de produits, les systèmes de mesure pour déterminer la présence de vulnérabilités et fournit des mécanismes de classement (score) des résultats de ces mesures afin d'évaluer l'impact de la découverte de problèmes de sécurité. SCAP définit, également, la manière dont ces normes sont combinées.

SCAP : un ensemble riche ?

CVE	cve.mitre.org	Common Vulnerabilities and Exposures	Identifiants standard et dictionnaire des défauts de logiciels liés à la sécurité.
CCE	cce.mitre.org	Common Configuration Enumeration	Identifiants standard et dictionnaire des problèmes de configuration liés à la sécurité.
CPE	cpe.mitre.org	Common Platform Enumeration	Identifiants standard et dictionnaire des plates-formes et/ou noms de produits.
XCCDF	xccdf.nist.org	eXtensible Checklist Configuration Description Format	Standard XML pour la spécification des listes de tests et la publication des résultats des tests.
OVAL	oval.mitre.org	Open Vulnerability Assessment Language	Standard XML pour les procédures de test des défauts liés à la sécurité des logiciels, des problèmes de conf. et des correctifs.
CVSS	www.first.org/cvss	Common Vulnerability Scoring System	Standard pour la transmission et la notation de l'impact des vulnérabilités.

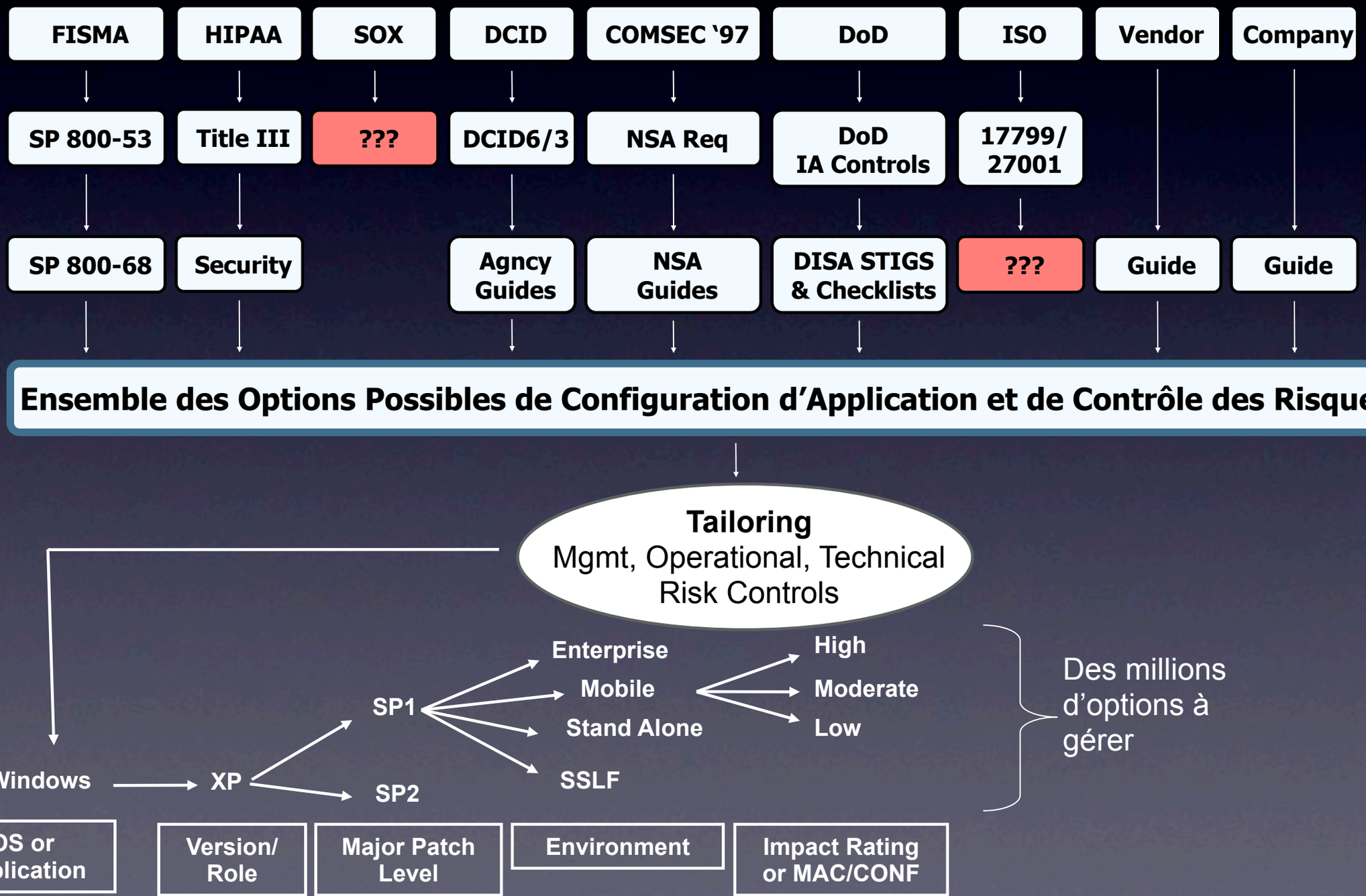
SCAP : mais encore...

Fonctions	Avantages
Standardise **comment** les ordinateurs communiquent les informations sur leurs vulnérabilités - le protocole	•Permet l'interopérabilité des produits et des services de divers fabricants.
Standardise **quelles** informations sur les vulnérabilités communiquent les ordinateurs - le contenu	•Autorise la répétabilité à travers les produits et les services de divers fabricants. •Réduit la variance du contenu dans les décisions et actions opérationnelles.
Basé sur des **standards ouverts**	•Guide la réflexion collective pour la création et l'évolution du contenu. •S'adapte à une vaste gamme de cas d'utilisation.
Utilise les **normes** de gestion des configurations et des équipements	•Mobilise l'inventaire des équipements et les informations de configuration pour la gestion des vulnérabilités et de la conformité.
Applicable à **différents** Framework de gestion du risque	•Réduit le temps, l'effort, et les coûts des processus de gestion des risques.
Traçabilité détaillée de multiples mandats et directives de sécurité	•Automatise en partie l'établissement de rapport et la démonstration de la conformité. •Réduit les chances d'erreur d'interprétation entre les auditeurs et les équipe opérationnelles.
Concentré sur des contrôles de sécurité **réels**	•Automatise l'établissement de rapport et la démonstration de la conformité.

SCAP : cas d'utilisation...

- Validation des Politiques et de la Conformité (Premier objectif à aujourd'hui)
- Détection des Vulnérabilités
- Gestion des équipements
- Suivit des Risques et des Réponses
- Fournisseurs et Clients de Produits de Sécurité
- Publication de Menaces et Alertes
- Autres …

Gestion de la Conformité et des Configuration



Présentation du Process FDCC
(NIST Federal Desktop Core Configuration)

Contenu SCAP extrait de la NVD par le NIST

Tous les Départements sont évalués sur la même base de Références.

Outils Certifiés (Publique et Privé)

Résultats

Contenu SCAP signé numériquement

Départements

Résultats avec Dérives

Etats Généraux

Pourquoi devrais je m'en préoccuper ?

- La révolution engendrée par des contenus structurés dans d'autres industries :
  - ISBN, UPC/Barcode, etc...
- L'Interopérabilité versus les contenus propriétaires.
- Fermé au niveau de l'Organisation mais Ouvert au niveau de l'Information.

SCAP : couverture des besoins

	Enumération	Evaluation	Notation	Rapport	Contenu
CVE cve.mitre.org	•				•
CCE	•				•
CPE common platform enumeration	•				•
XCCDF security benchmark automation		•		•	•
OVAL		•			•
CVSS			•		•

CVE et CVSS

- Common Vulnerabilities and Exposures
  - Nomage commun des vulnérabilités
  - Peut de valeure de nom ne sont pas communes
  - Utilisé à travers toute l'industrie de la sécurité d'aujourd'hui

- Common Vulnerability Scoring System
  - Nous pouvons tous utiliser le même fonction de classement
  - Un système de notation commun mais pas une note commune
  - Lié à un défaut de logiciel unique identifié par un nom CVE

Sans CCE

NSA Solaris Guide (XCCDF)
Configure SSH

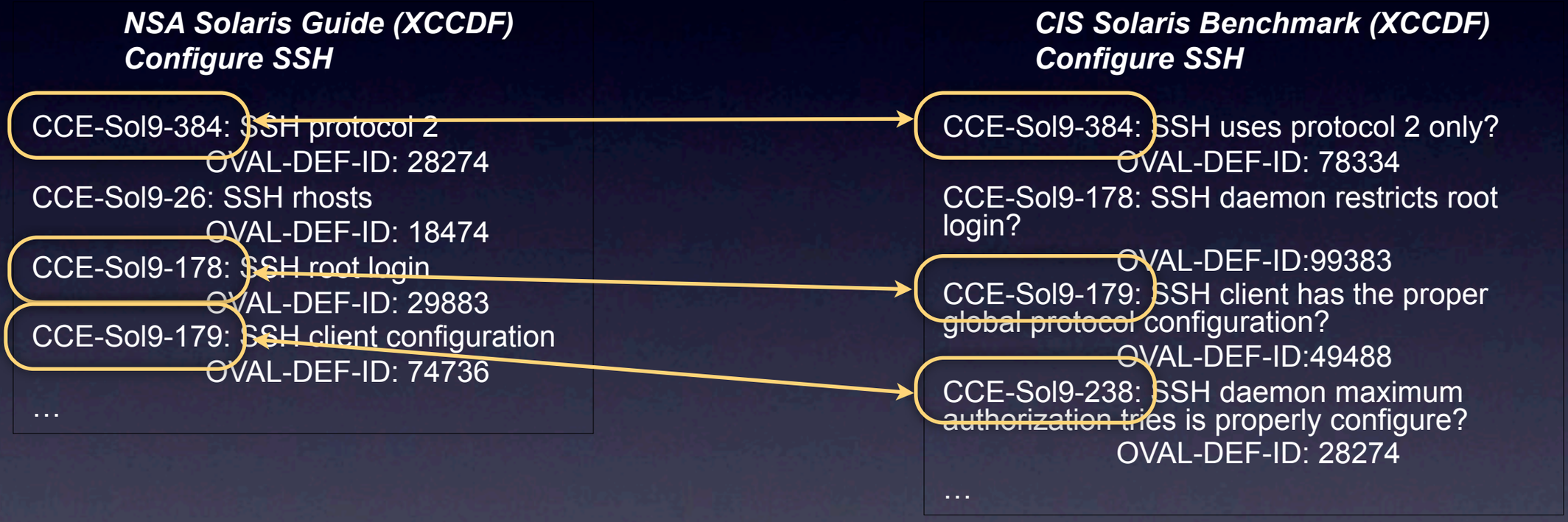
NSA-CC: SSH protocol 2
OVAL-DEF-ID: 28274
NSA-CD: SSH rhosts
OVAL-DEF-ID: 18474
NSA-CE: SSH root login
OVAL-DEF-ID: 29883
NSA-CF: SSH client configuration
OVAL-DEF-ID: 74736
…

CIS Solaris Benchmark (XCCDF)
Configure SSH

CIS-54: SSH uses protocol 2 only?
OVAL-DEF-ID: 78334
CIS-55: SSH daemon restricts root login?
OVAL-DEF-ID:99383
CIS-56: SSH client has the proper global protocol configuration?
OVAL-DEF-ID:49488
CIS-57: SSH daemon maximum authorization tries is properly configure?
OVAL-DEF-ID: 28274
…

Aucuns moyens de corréler les pré-requis de configuration individuellement.

Avec CCE



Common Configuration Enumeration permet de s’y retrouver.

CPE

- Common Platform Enumeration
- Nom CPE
  - Identifie un type de plate-forme
  - N'est pas fait pour identifier un système
  - Idéalement associé avec une Définition d'Inventaire OVAL
  - Comparaison faites sur un ID commun et non sur une chaîne de caractères
- Langage CPE
  - Utilisé en combinant les noms CPE pour identifier des plates-formes complexes
- Dictionnaire CPE
  - Liste des noms CPE connus
- Augmente la valeur de tous les processus IT
  - CMDB d'ITIL
  - Systèmes IT internes
  - Audits
  - Inventaire d'équipement

XCCDF

- eXtensible Configuration Checklist Description Format

- Conçu pour supporter :
  - L'Echange d'Information
  - La Génération de Documents
  - La Personnalisation selon son Organisation et sa Situation
  - Des Tests Automatiques de Conformité
  - La Notation de la Conformité

- Publié comme NIST IR 7275

- Favoriser la plus large application des bonnes pratiques en matière de sécurité

Processus OVAL

1

Bulletins de Sécurité
Les fabricants et les organisations leader dans la sécurité publient des bulletins de sécurité qui préviennent de menaces courantes et de vulnérabilités systèmes.

Politique de Configuration
Les agences gouvernementale telle que la NSA ou le NIST développe une politique des «Meilleures Pratiques» pour la sécurité des systèmes.

2

Les Définitions sont générées
Les détails spécifiques de configuration d'une machine provenants des Bulletins et des Politiques sont extrais et codés en Définition OVAL.

3

Données collectées depuis les ordinateurs
Les définitions OVAL sont structurées pour indiquer quelles informations de configuration doivent être récupérées sur chaque système.

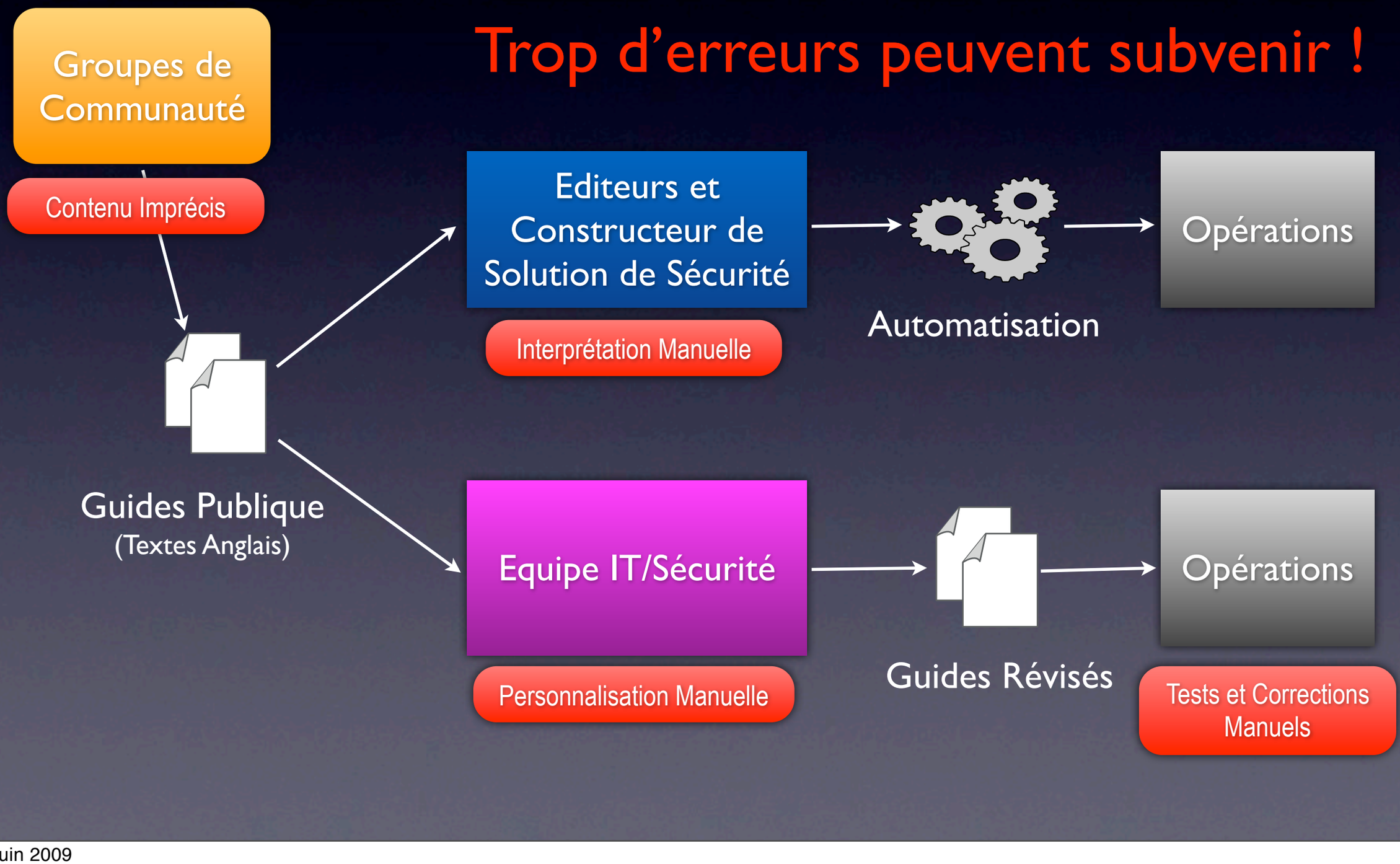
4

Analyse
Les définitions OVAL (étape 2) et les Caractéristiques des Systèmes (étape 3) sont comparés pour déterminer si le système courant est dans un état vulnérable ou pas.

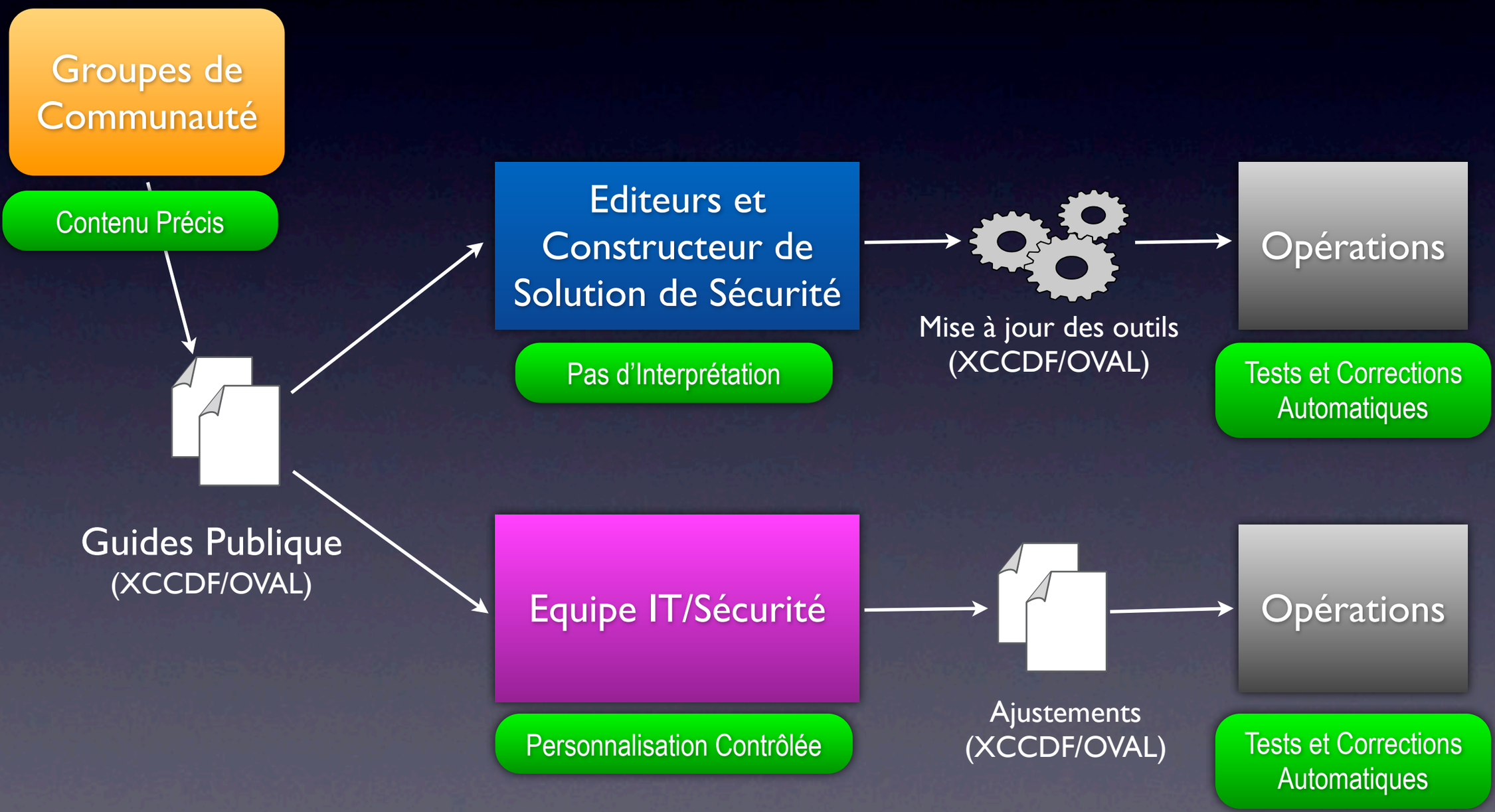
5

Résultats d'Analyse
Les résultats d'analyse sont formatés en tant que document de Résultats OVAL.

Sans XCCDF/OVAL

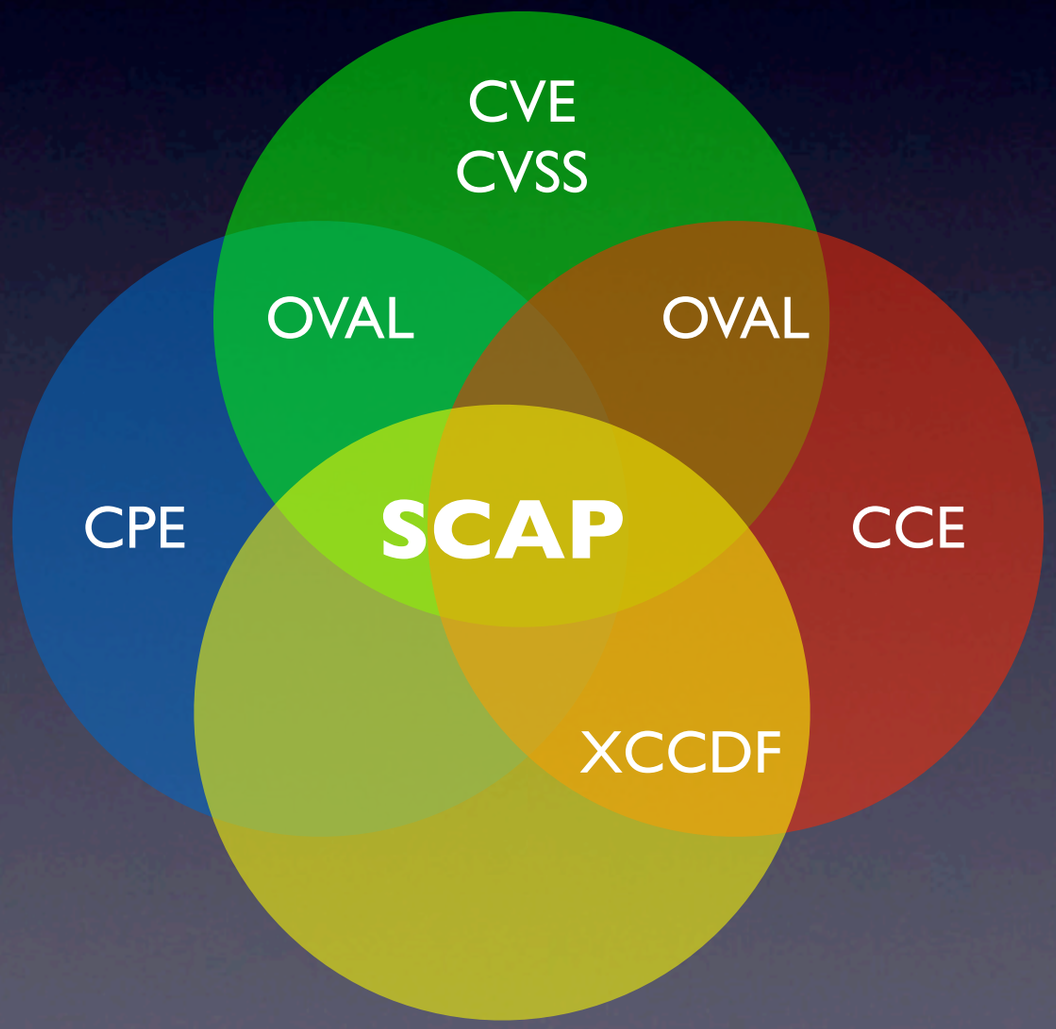


Avec XCCDF/OVAL



Intégré les équipes IT et Sécurité au travers de SCAP

Gestion des Vulnérabilités



Gestion des Equipements

Gestion des Configurations

Gestion de la Conformité

Comment SCAP va changer les audits...

Dans un future pas si lointain que çà...

- Le Management / l'IT / la Sécurité n'auront pas à stopper leurs projets en cours pour se préparer à un audit externe.
- Les Auditeurs n'auront pas besoin d'apporter leurs propres outils pour réaliser un audit directe des équipements réseaux.
- Seules les Références de Test signées et approuvées par l'Auditeur seront exécutées sur le réseau.
- L'équipe IT garde la main sur les Références signées de l'auditeur, le fichier signé des paramètres d'ajustement et l'accès aux fichiers signés de résultats.
- L'auditeur peut revoir les Références et les Résultats, vérifier les signatures et déterminer si il y a des zones qui devraient être auditées / validées puis améliorer les Références de Test.
- Ces améliorations sont en suite distribué et dorénavant les nouveaux équipement sont validés.
- Le Management et les équipe IT/Sécurité ont désormais une vue continue sur l'état des équipement du SI.

SCAP : résumé...

- SCAP offre aux entreprises un moyen d'évaluer la sécurité des failles et les erreurs de configuration des logiciels dans l'entreprise de manière transparente, interopérable, reproductible et automatisable.

- Les économies réalisées grâce à l'utilisation de SCAP permettent aux équipes IT/Sécurité de passer plus de temps sur d'autres aspects important de la sécurité du Système d'Information.

- En associant la Conformité aux aspects de Configuration, SCAP fait des rapports de conformité un sous-produit des «Meilleurs Pratiques» de Sécurité et fournit aux entreprises la capacité de voir la vraie posture de sécurité de leur Système d'Information.

SCAP : Implication de McAfee

- **OVAL (Open Vulnerability & Assessment Language)**
  - Carl Banzhof et Kent Landfield sont membres actifs du Comité de Direction OVAL
  - Produits Certifiés OVAL
- **CVE (Common Vulnerabilities & Exposures) Standard**
  - Kent Landfield est l'un des membres fondateurs du Comité Editorial CVE
  - Produits Certifiés Compatible CVE
- **CCE (Common Configuration Enumeration)**
  - Participation aux premiers travaux de définition du CCE
  - Membres du Groupe de Travail du CCE
- **CPE (Common Platform Enumeration)**
  - Participation actives à la revue des spécifications et à l'ajout de contenu dans le dictionnaire.
- **NIST**
  - Premier candidat à la NIST Security Configuration Checklists Repository
  - Participation à la NIST "Workshop on State of the Art in Software Assurance Tools"
  - Présent à la 2de Security Automation Conference and Workshop in Sept. 2006
  - Présent à la 3me Annual IT Security Automation Conference in Sept. 2007
  - Présent à la 4me Annual IT Security Automation Conference in Sept. 2008
  - A participé aux travaux de spécification des procédures de Validation / Certification SCAP
- **XCCDF (Extensible Checklist Configuration Description Format)**
  - Participation passé et courante aux travaux et efforts du projet NIST/NSA XCCDF

Questions / Réponses

Diapositives Complémentaires

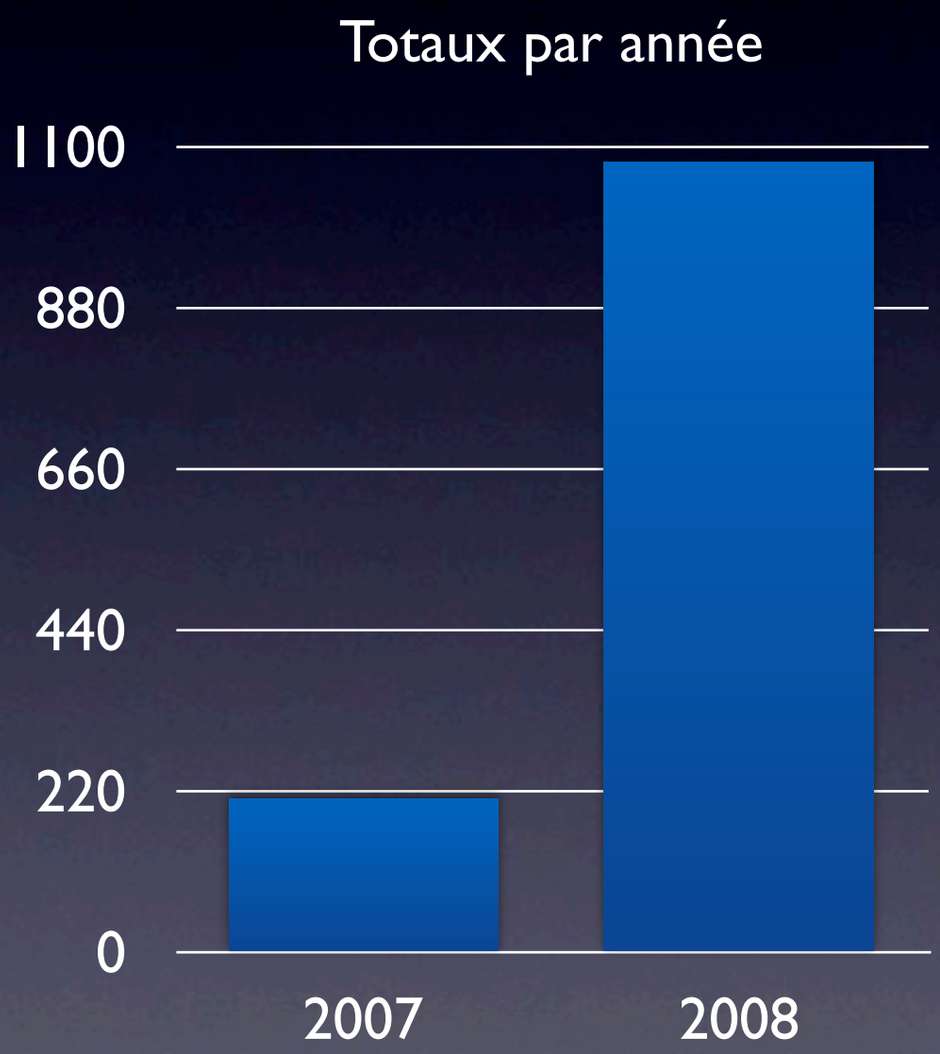
Example : OVAL

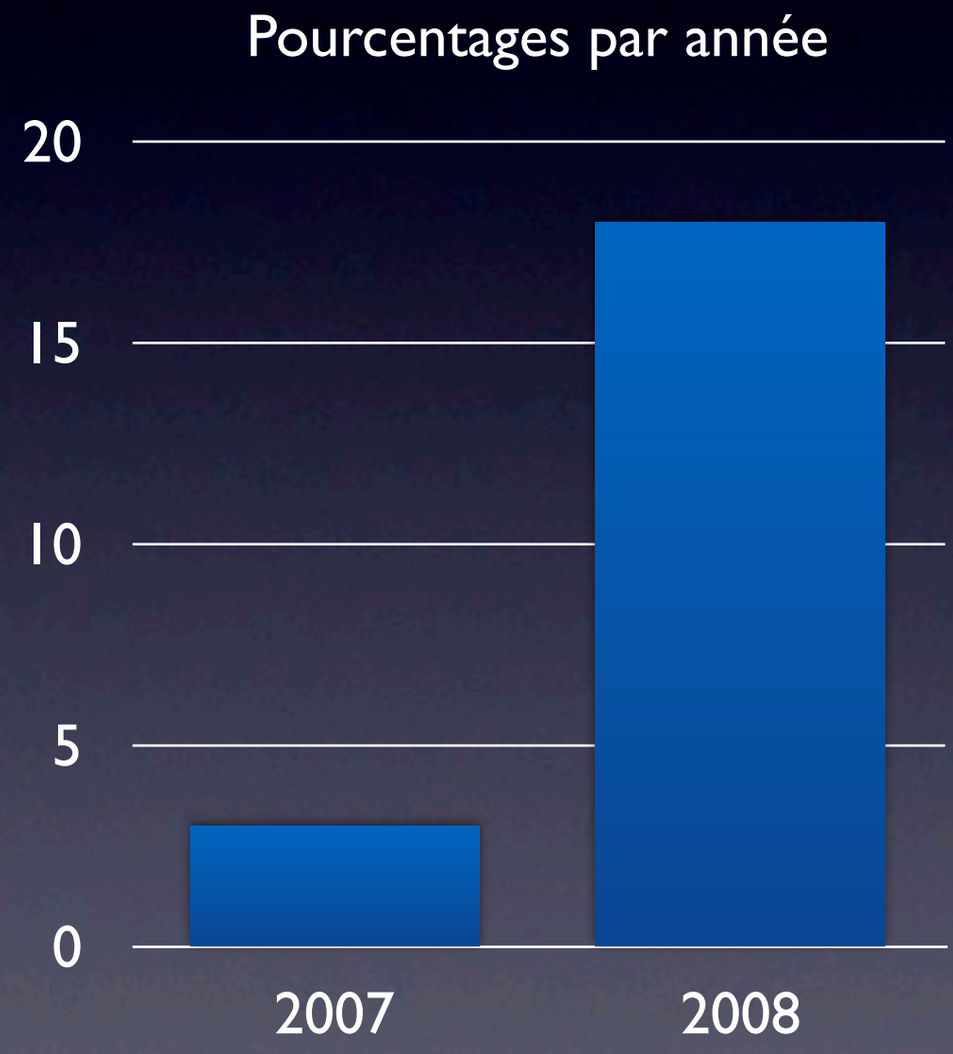
```
<oval_definitions …>
 <generator>…</generator>
 <definitions>
  <definition id="oval:org.mitre.oval.tutorial:def:1" version="1" class="miscellaneous">
   <metadata>
    <title>Hello World Example</title>
    <affected family="windows"/>
    <description>This definition is used to introduce the OVAL Language to individuals interested in writing OVAL Content.</description>
   </metadata>
   <criteria comment="Software section" operator="AND">
    <criterion comment="The oval example registry key has a value of &amp;quot;Hello World&amp;quot;" test_ref="oval:org.mitre.oval.tutorial:tst:1"/>
   </criteria>
  </definition>
 </definitions>
 <tests>
  <registry_test id="oval:org.mitre.oval.tutorial:tst:1" version="1" check="at least one" comment="The oval example registry key has a value of
   &amp;quot;Hello World&amp;quot;" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <object object_ref="oval:org.mitre.oval.tutorial:obj:1"/>
   <state state_ref="oval:org.mitre.oval.tutorial:ste:1"/>
  </registry_test>
 </tests>
 <objects>
  <registry_object id="oval:org.mitre.oval.tutorial:obj:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key operation="equals">SOFTWARE\oval</key>
   <name operation="equals">example</name>
  </registry_object>
 </objects>
 <states>
  <registry_state id="oval:org.mitre.oval.tutorial:ste:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <value operation="equals">Hello World</value>
  </registry_state>
 </states>
</oval_definitions>
```

Prédictions des Menaces 2009

Technologie Artemis

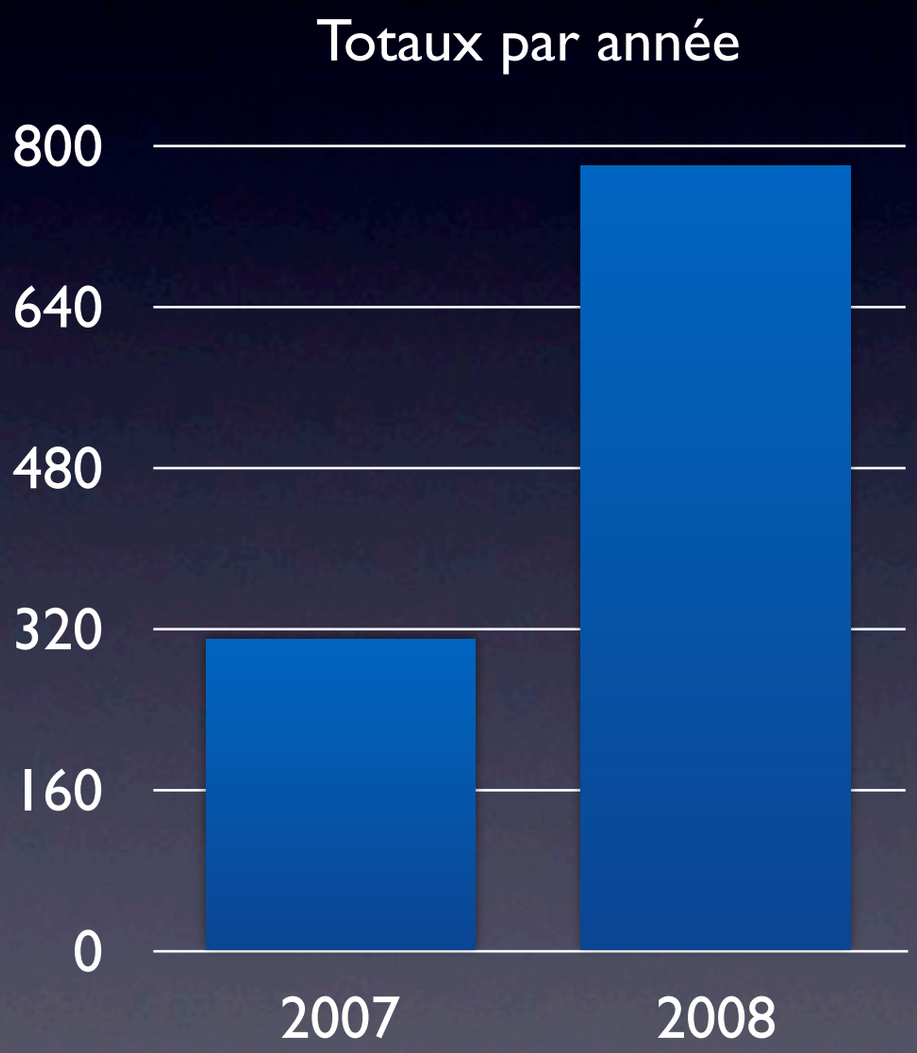
Attaques par Injection SQL

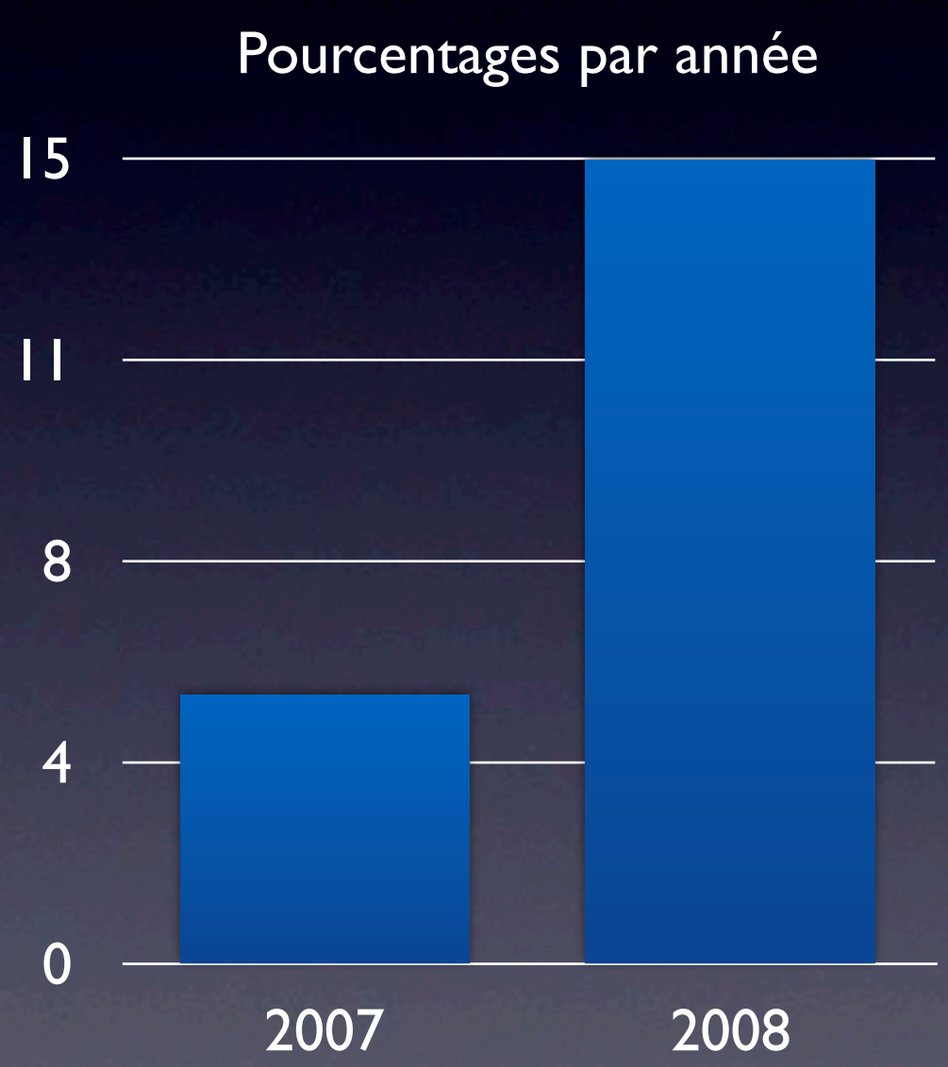




En nombre de vulnérabilités - Source : NIST, Compter Security Division

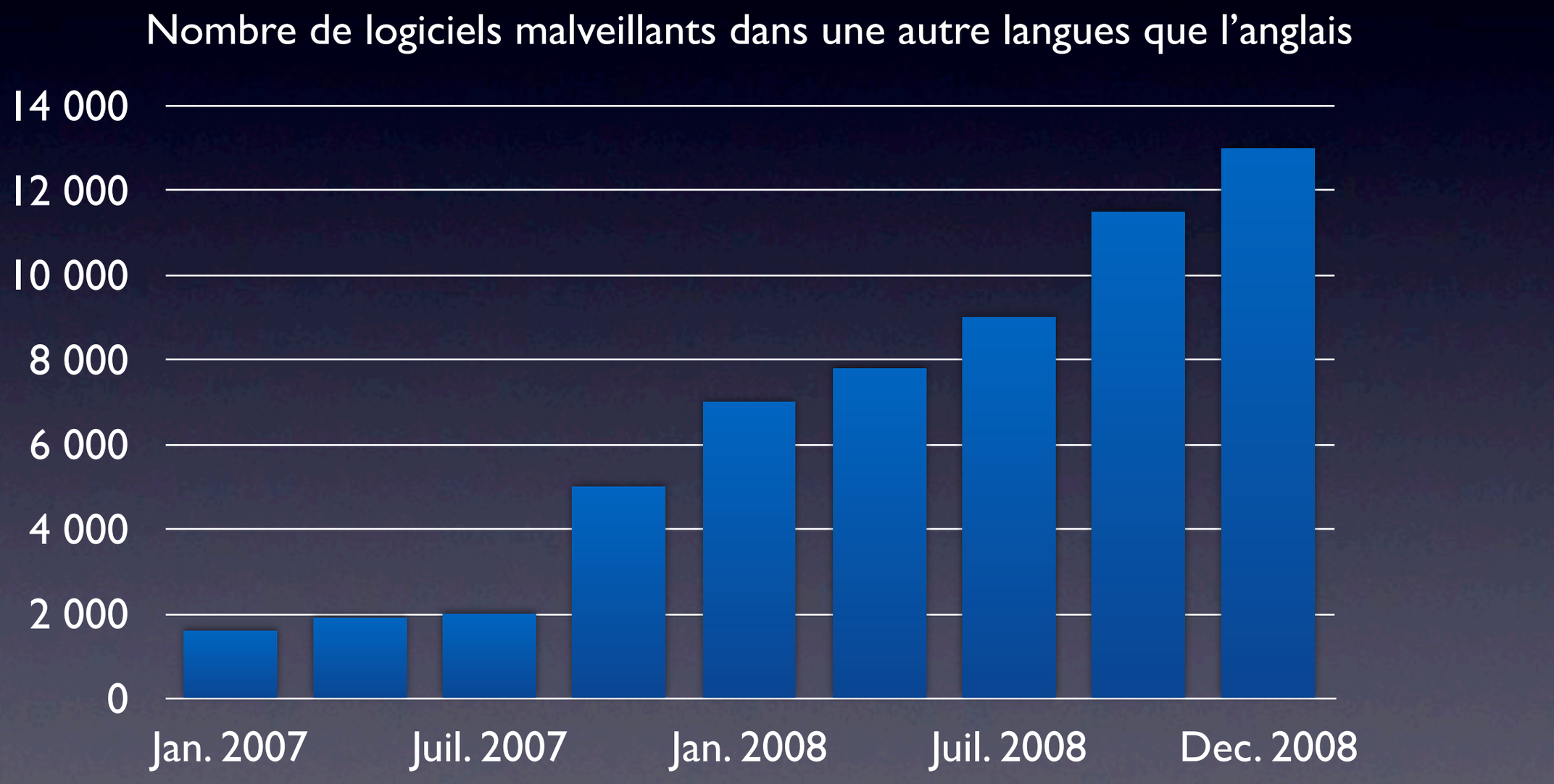
Exécution Forcée de Scripts





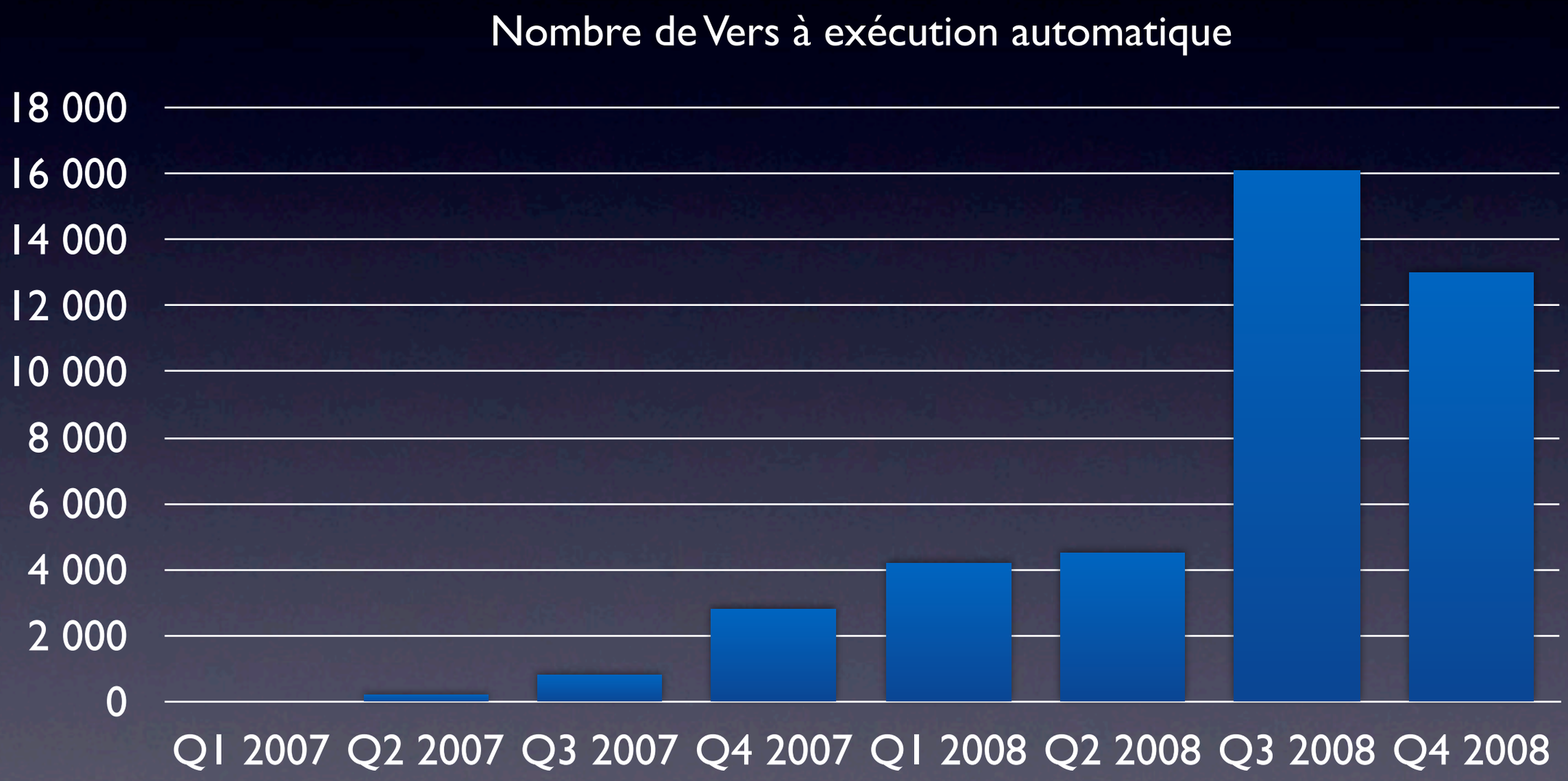
En nombre de vulnérabilités - Source : NIST, Compter Security Division

Augmentation du support des langues étrangères



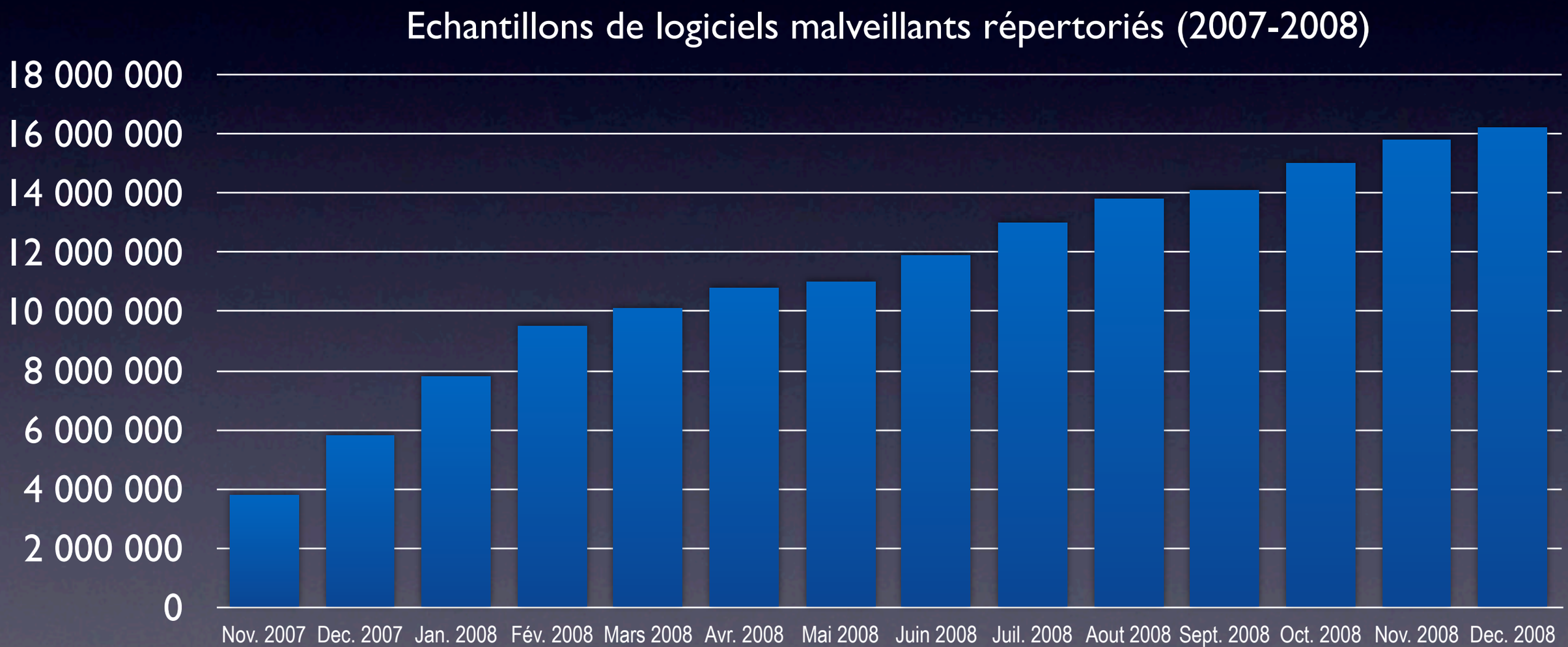
Source : McAfee, Avert Labs

Clé USB,
La nouvelle Disquette ?



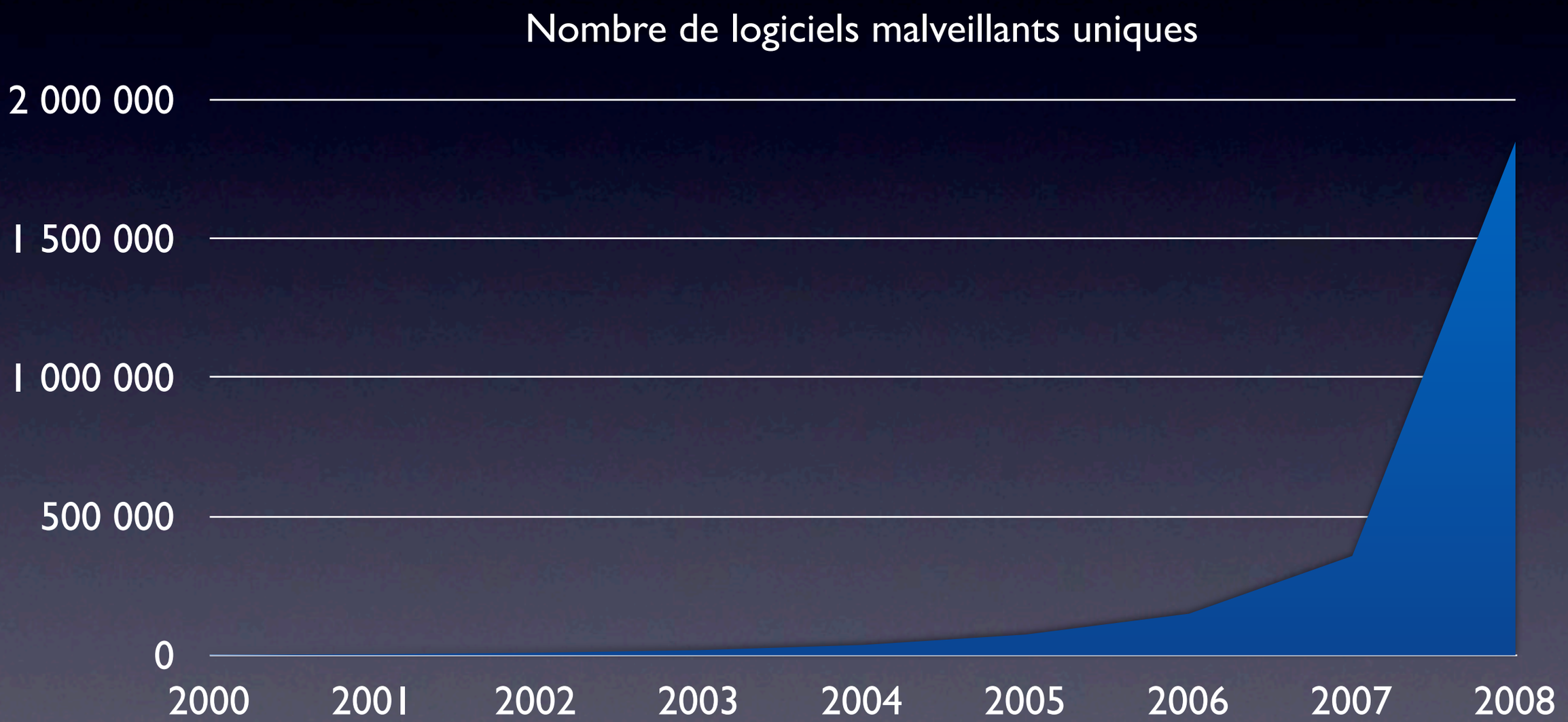
Source : McAfee, Avert Labs

Augmentation des soumissions



Source : McAfee, Avert Labs

Augmentations des menaces



Source : McAfee, Avert Labs

Conséquences

- Taille de la base de signature : 56Mo
- Problème de performance
- Problème de détection
- Manque de réactivité

Analyse Heuristique

- Exemple de règles heuristiques :
  - Fonctions de copie automatique dans Windows
  - Fonctions de renvoie par email
  - Fonctions d'ouverture de port
  - Fonctions d'exécution automatique
  - Fonctions de désinstallation de logiciels anti-virus
  - Fonctions d'énumération des processus en cours d'exécution
  - Fonctions de recherche dynamique de pointeur vers des API
  - Fonctions d'écriture en zone mémoire d'autres processus
  - Contient la liste des programme exécutable d'anti-virus
  - Contient une liste de ressources Peer-To-Peer
  - Contient un autre programme exécutable, etc...
- Le moteur à besoin de détecter 100% des conditions pour déterminer la présence d'un virus.

Technologie Artemis

1

Analyse du Fichier
L'anti-virus effectue sont analyse à partir de ses signatures et des ses moteurs heuristiques.

2

Résultat Suspect
Aucune menace détectée avec les fichiers de signatures, mais le fichier est jugé «suspect».

3

Nouvelle Empreinte
Une empreinte du fichier est créée et envoyée à l'aide de McAfee Artemis (DNS).

4

Base de données McAfee
McAfee Artemis examine cette empreinte et d'autres données statistiques par rapport à sa base de connaissance.

5

Analyse Artemis
McAfee Artemis identifie la menace et prévient le client.

6

Bloque la Manace
L'anti-virus traite les informations et bloque la menace.

Questions / Réponses

Ressources McAfee

- The Rise of AutoRun-Based Malware
  http://www.mcafee.com/us/local_content/white_papers/wp_autorun_malware_v6.5_fr.pdf
- Web browser : An Emerging platform nder attack
  http://www.mcafee.com/us/local_content/white_papers/wp_webw_browsers_w_fr.pdf
- Threats Report Q1 2009
  http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409fr_s_fnl.pdf
- Threats Predictions 2009 Report
  http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report_fr.pdf
- Artemis Technology

  http://www.mcafee.com/us/enterprise/products/artemis_technology/index.html