[VULNIT]

Vulnerability
Identification Tool

Présentation de la solution

OSSIR – groupe Paris

15/06/2010

Sommaire

- ✓ Introduction
- ✓ Information et menaces
- ✓ Contrôles
- ✓ VulnIT, concept et architecture
- ✓ Démonstration
- ✓ Avenir
- ✓ Conclusion

Introduction

- ✓ Vincent Maury
- ✓ 28 ans, marié
- ✓ Ingénieur IT en 2004
- ✓ 4 ans d'audit IT (externe et interne)
  - Clients industriels, services, bancaires
- ✓ Outils existants
- ✓ Expérience du partage Windows

L'importance de l'information

- ✓ Croissance exponentielle de l'information
  - ➔ Tous les secteurs, toutes les tailles d'entreprise
- ✓ De plus en plus numérique
- ✓ Information connectée (Internet, Extranet)
  - ➔ Impact plus large, plus accessible

Vocabulaire

Potentialité

✓ Les menaces peuvent à l'occasion exploiter des vulnérabilités et contourner les mécanismes de sécurité pour voler des informations ou nuire.

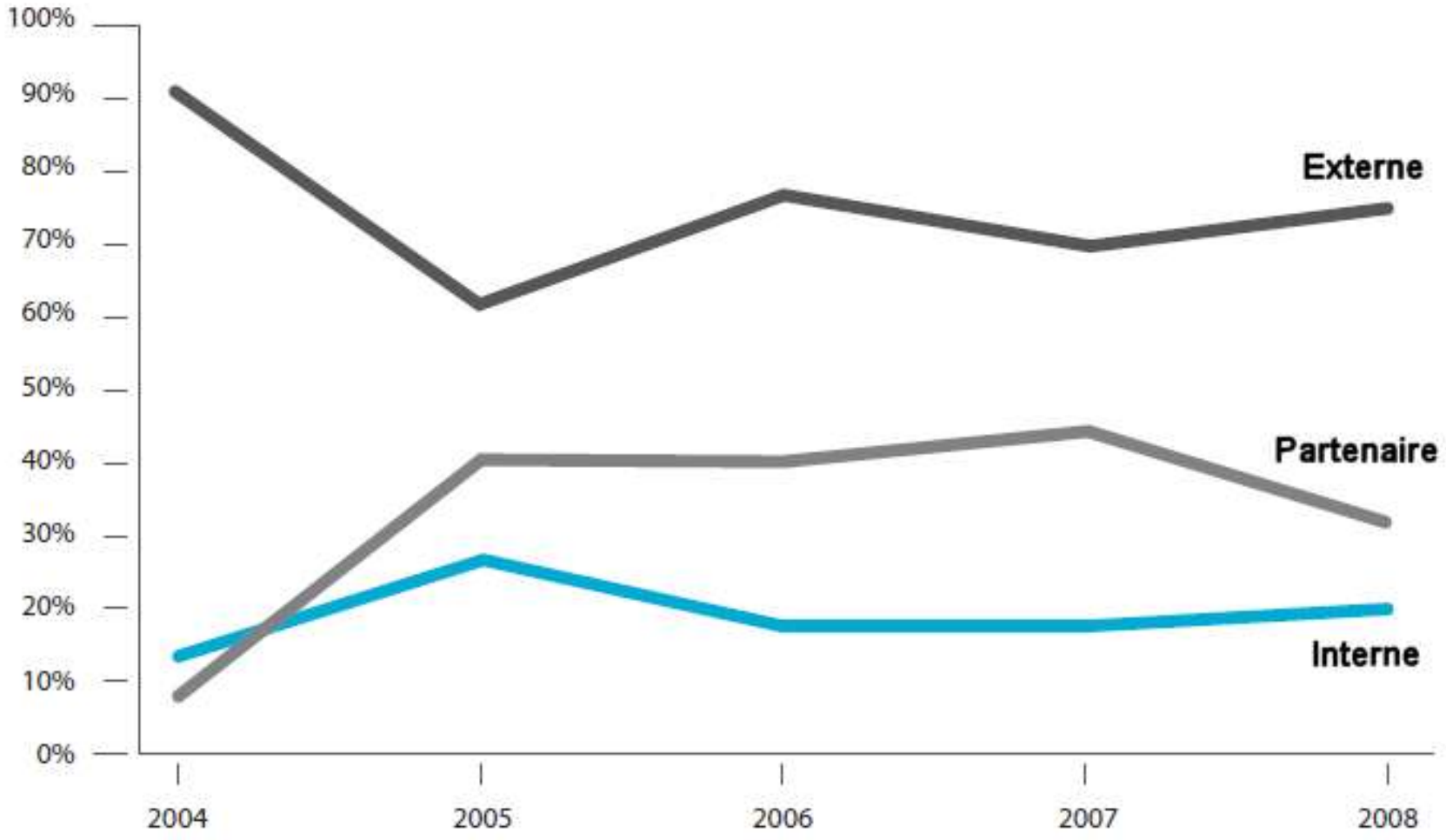
Contrôle

Impact

Les menaces

- ✓ Externes
  - Piratage, DDoS, trojan
- ✓ Internes
  - Par mégarde ou malintentionnée
- ✓ Partenaires
  - Prestataire, hébergeur, infogéreur

Répartition des menaces



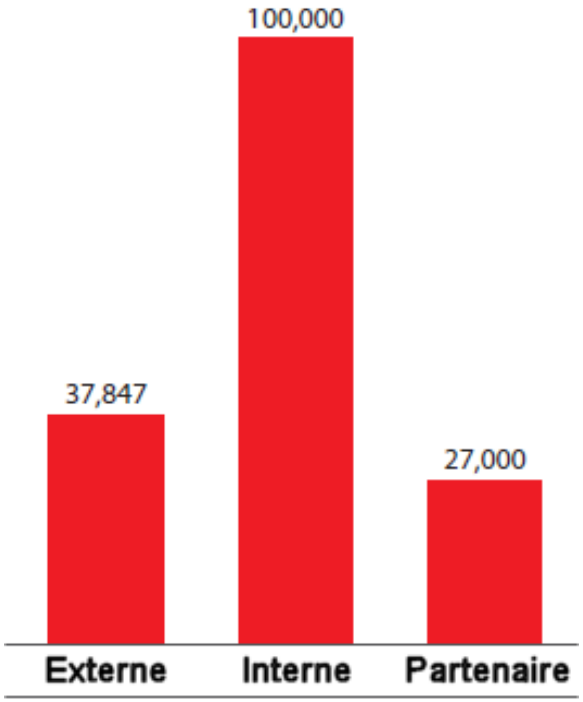
Source : Verizon Business (2009)

[VULNIT]

Impact

- ✓ Disponibilité de l'infrastructure
- ✓ Valeur du bien
  - Secret industriel, fichier client
- ✓ Règlementaire
  - PCI DSS, Loi Détraigne-Escoffier (art. 7)
- ✓ Image de l'entreprise
  - Défacement de site web
- ✓ Stratégique
  - Annonce marketing

Chiffrage



Nombre d'enregistrements compromis, par vol

Source : Verizon Business (2009)

Coût moyen d'une fuite de données en France : 2,53 millions de $

Source : Ponemon Institute (2010)

PCI DSS :
Les pénalités publiées par Visa sont de 25 k$ mensuels pour non-conformité et 500k$ d'amende pour compromission

Source : CLUSIF (2009)

[VULNIT]

Potentialité

- ✓ Probabilité d'occurrence de la menace
  - Exposition (banque vs. sidérurgie)
  - Exploitabilité des vulnérabilités

59% des organisations ont déjà perdu des données personnelles critiques (70% pour les plus de 75.000 salariés, 40% pour les moins de 500)

Source : Accenture (2010)

37% des entreprises de 200 salariés subissent des vols d'informations, 65% des sociétés de plus de 1.000 salariés

Source : CLUSIF (2009)

Les attaques ciblant les données de l'entreprise ont presque doublé en 2009 dans le monde (PWC, 2009)

Sommaire

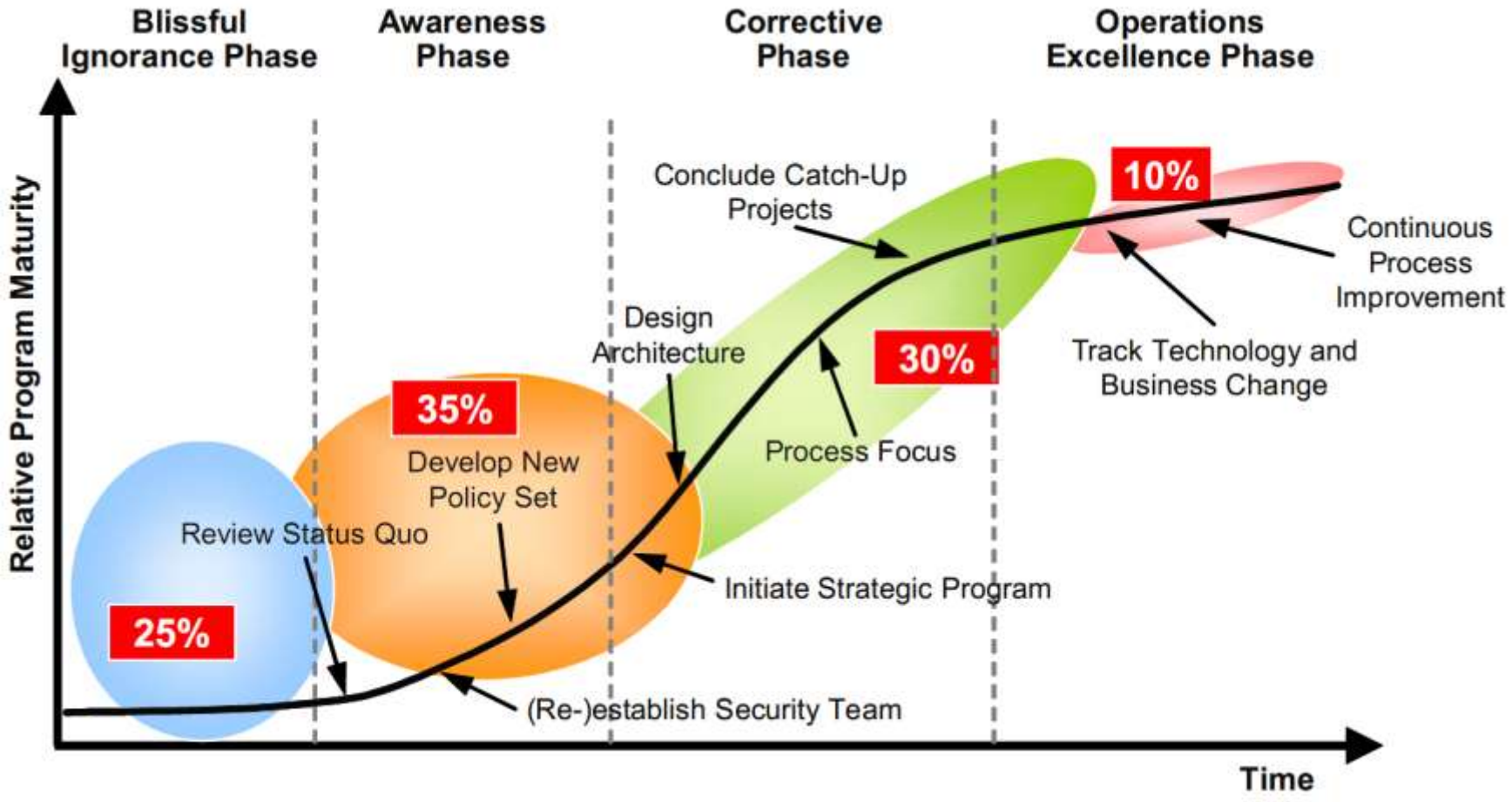
- ✓ Introduction
- ✓ Information et menaces
- ✓ Contrôles
- ✓ VulnIT, concept et architecture
- ✓ Démonstration
- ✓ Avenir
- ✓ Conclusion

Les contrôles

- ✓ A priori
  - Dissuasifs (log, sanction)
  - Préventifs (ACL, patching)
- ✓ A posteriori
  - Palliatifs (PSI, PCA)
  - Confinement

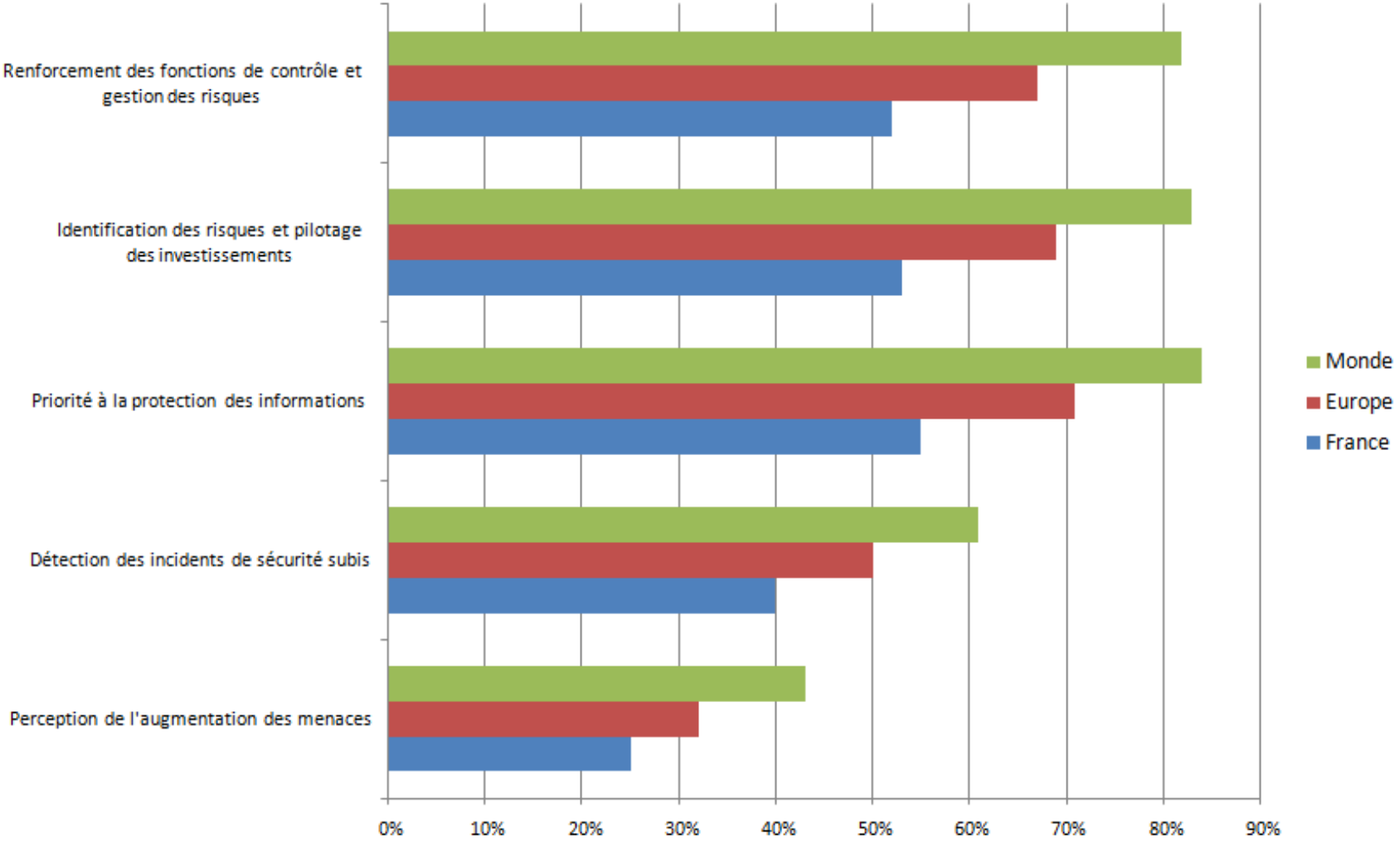
Mieux vaut prévenir que guérir

Prise de conscience



Source : Byrnes & Scholtz, 2005

Maturité française

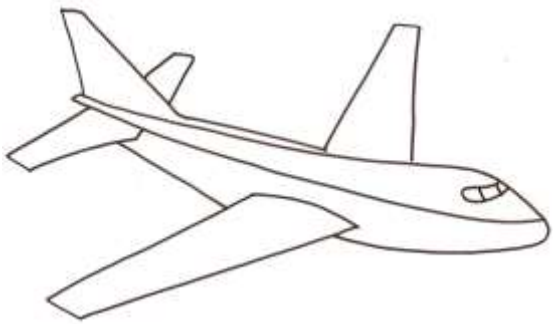


Source : PWC (2009)

[VULNIT]

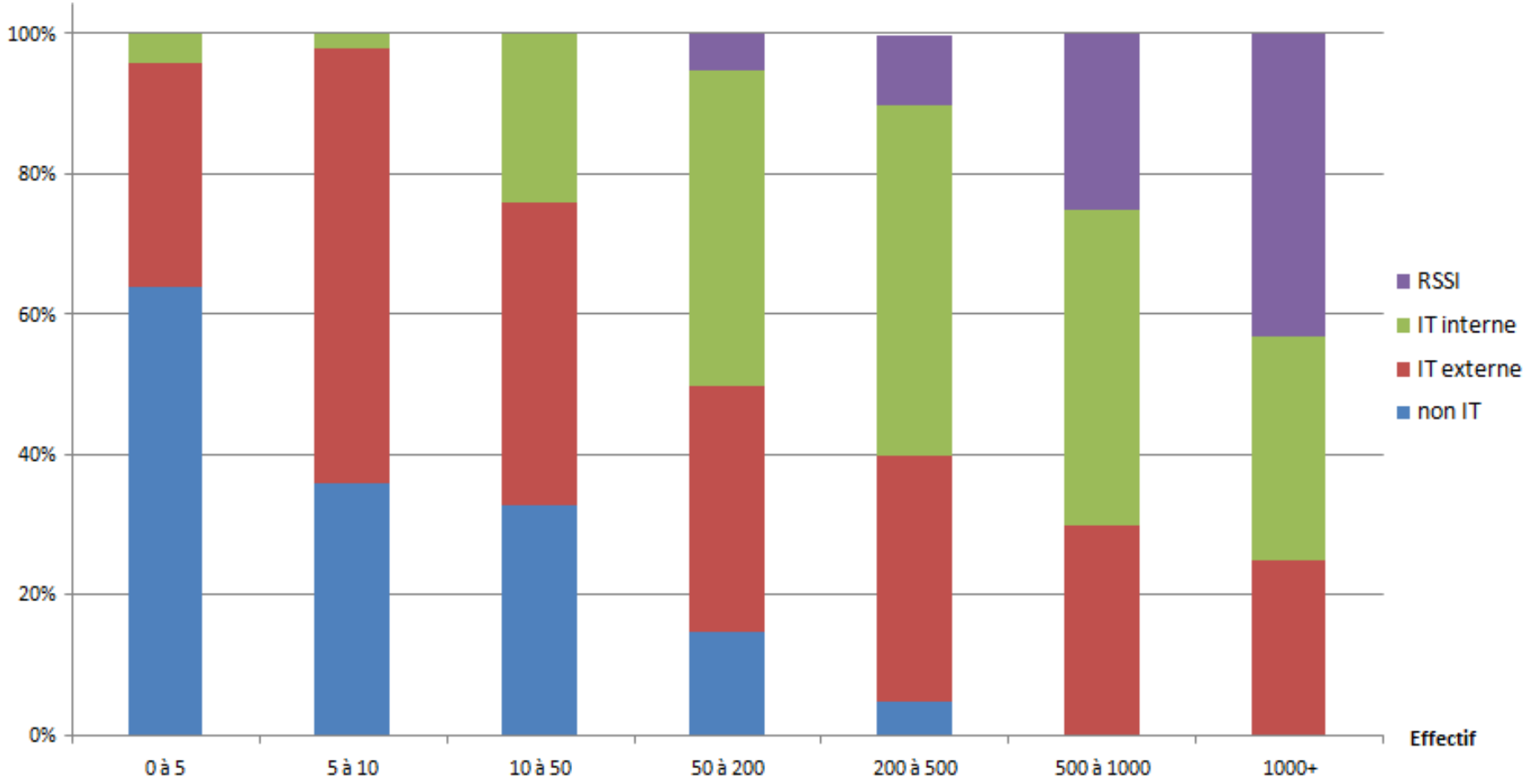
Y a-t-il un contrôleur…?

- ✓ Quid des contrôles ?
  - 87% des vols de données auraient pu être évités par des contrôles simples (Verizon Business, 2009)
- ✓ Le RSSI (Responsable de la Sécurité du SI)
  - 21% des entreprises de plus de 200 salariés, 43% pour celles de plus de 2000 salariés (CLUSIF, 2008)
  - 60% des entreprises ne savent pas dire s'ils ont subi des incidents de sécurité (PWC, 2009)



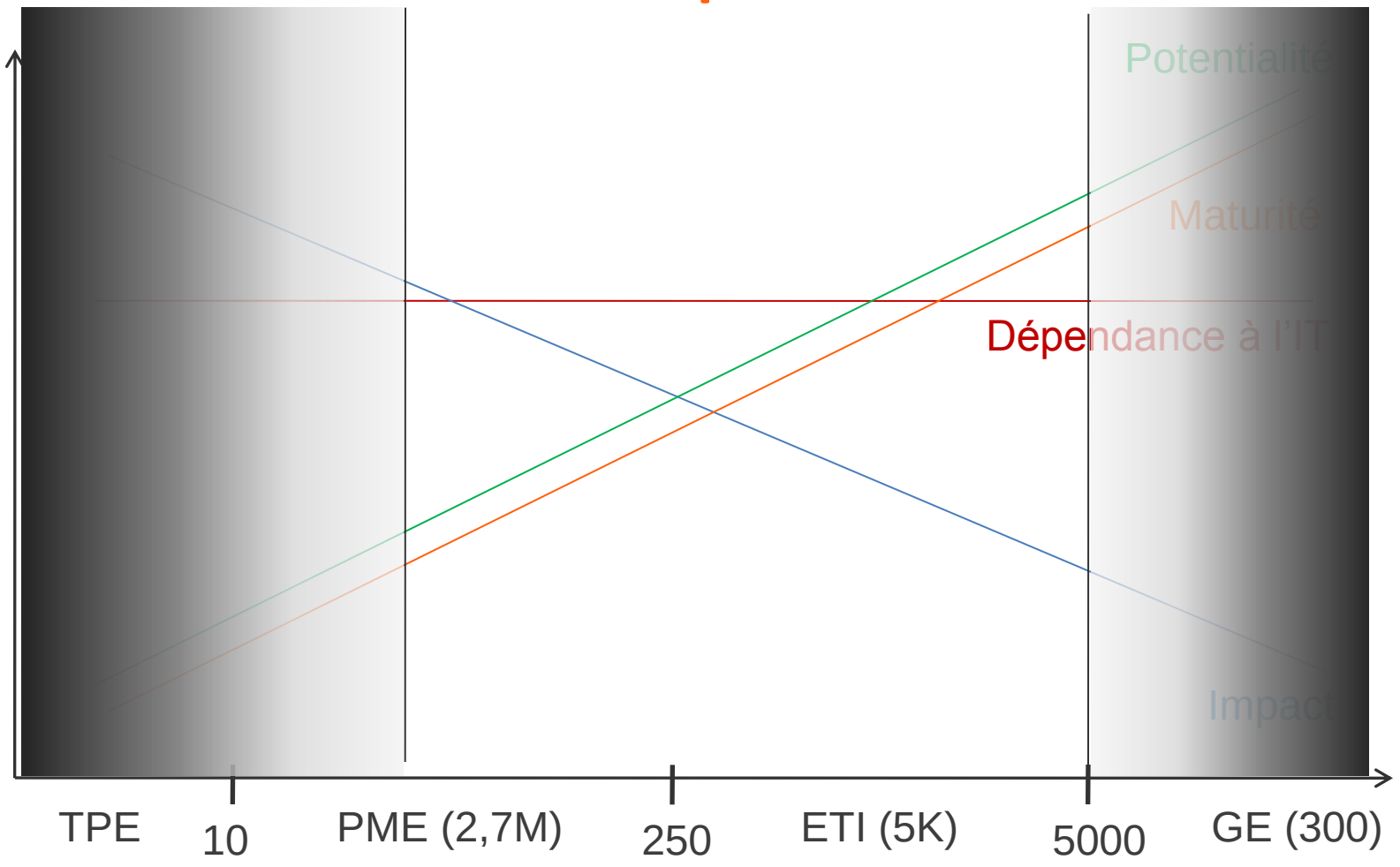
[VULNIT]

Qui est le RSSI ?



Sources : CLUSIF et ENE (2008)

Checkpoint



[VulnIT]

3 problèmes

Manque de temps

Manque de moyens

Manque de compétences

[VULNIT]

La solution VulnIT

Manque de temps

Automatique

Manque de moyens

Abordable

Manque de compétences

Accessible

[VULNIT]

Sommaire

- ✓ Introduction
- ✓ Information et menaces
- ✓ Contrôles
- ✓ VulnIT, concept et architecture
- ✓ Démonstration
- ✓ Avenir
- ✓ Conclusion

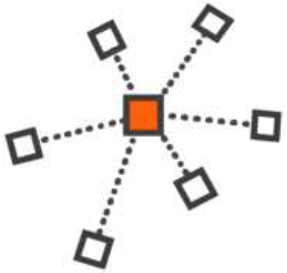
Concept Plug & Audit

- ✓ Live USB
  - Clé USB bootable
  - Environnement intégré
- ✓ Avantages
  - Automatique
  - Portable
  - Sans installation

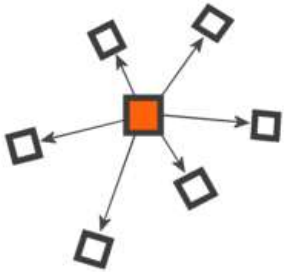
Plug & Audit

Démarche « black box »

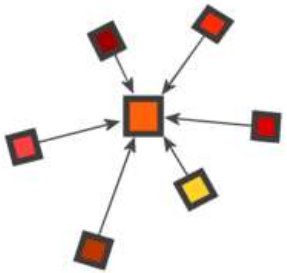
- ✓ Identifier
  - Serveurs, services, architectures



- ✓ Tester
  - De manière adéquate et ciblée



- ✓ Consolider
  - Un rapport homogène et cohérent



Architecture

- ✓ Outils open-source
  - Communauté d'experts
  - Nombreux, ciblés
  - Difficiles d'approche

- ✓ Plateforme VulnIT
  - Intégration d'un panel d'outils
  - Transparent pour l'utilisateur

netcat, dig, fping, smbclient, medusa, snmpwalk, rpcclient, nbtscan, tnscmd...

Tests de sécurité

- ✓ Bases de données (authentification),
- ✓ Partages de fichiers (Windows, FTP),
- ✓ Connexion à distance (SSH, Telnet),
- ✓ Messagerie (relai de spam),
- ✓ DNS (transfert de zones),
- ✓ Supervision (SNMP).

Diagramme macro

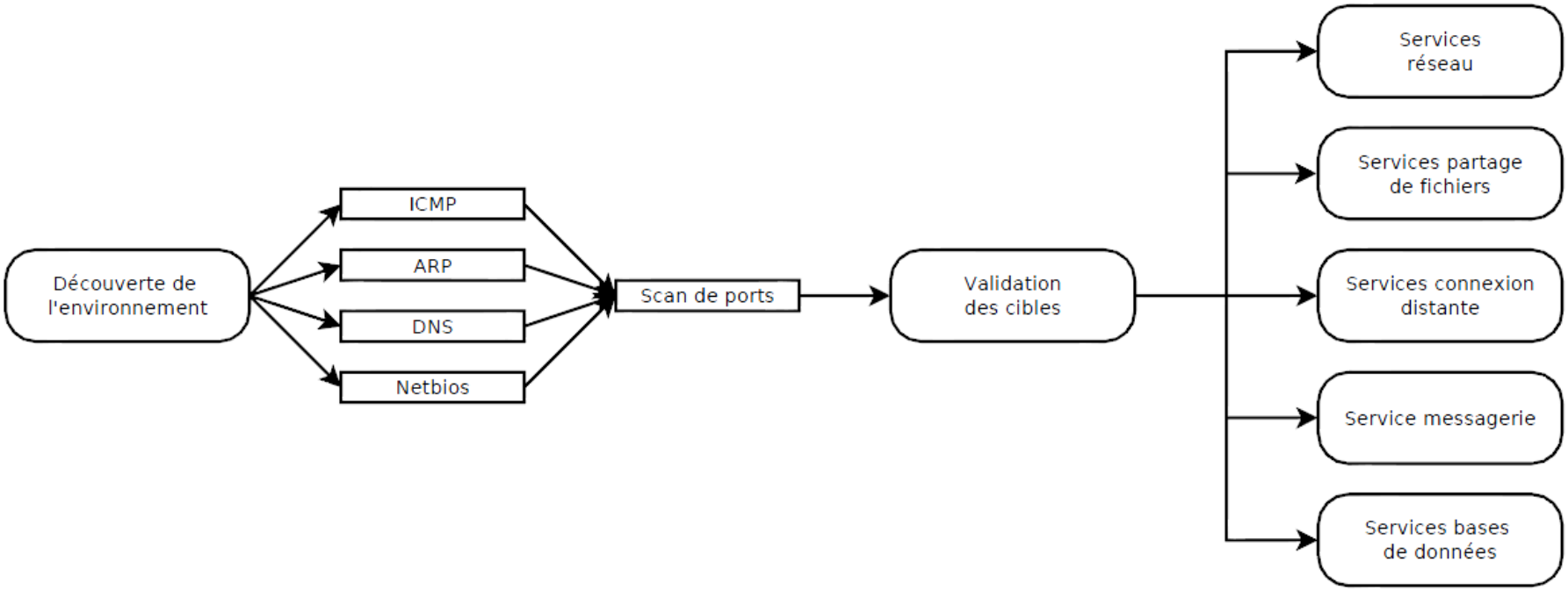


Diagramme micro

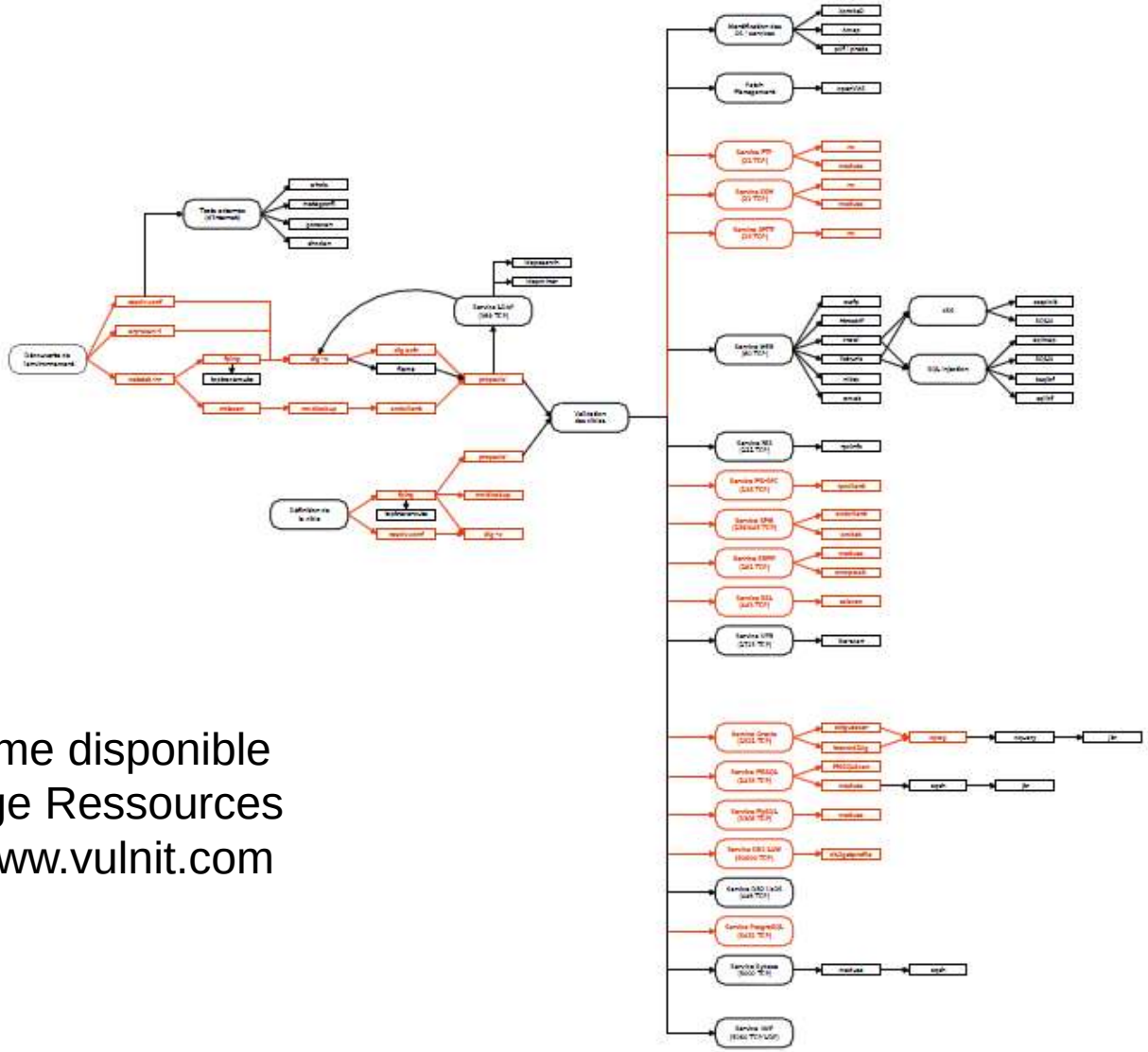


Diagramme disponible
sur la page Ressources
du site www.vulnit.com

Démonstration

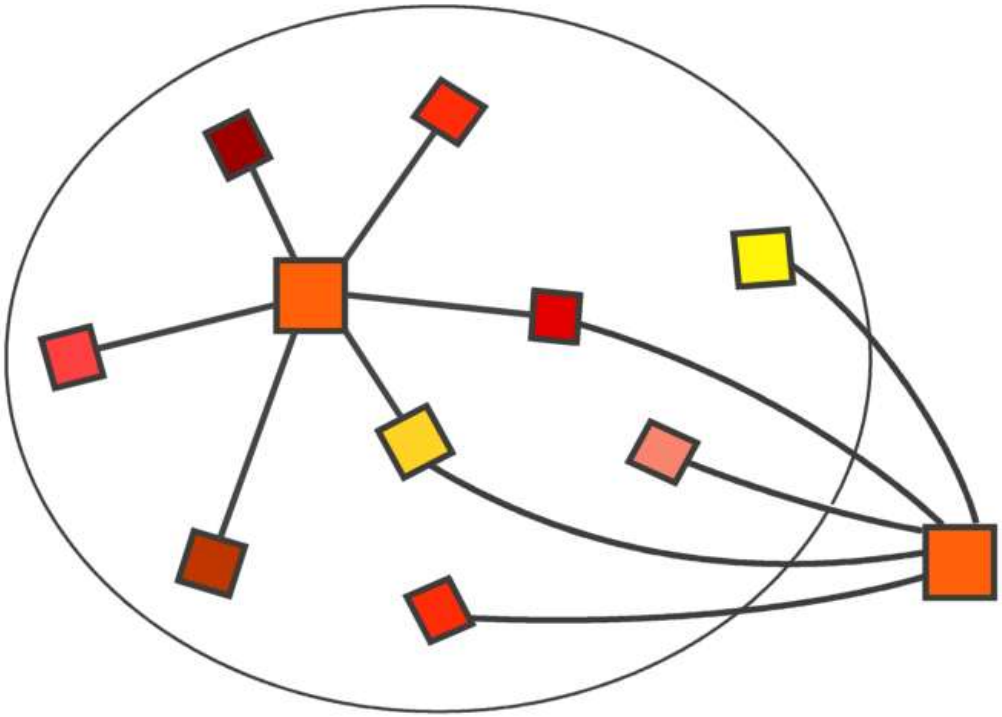
Démonstration et exemple de rapport d'audit consultables sur la page d'accueil du site www.vulnit.com

Sommaire

- ✓ Introduction
- ✓ Information et menaces
- ✓ Contrôles
- ✓ VulnIT, concept et architecture
- ✓ Démonstration
- ✓ Avenir
- ✓ Conclusion

Mais encore…?

- ✓ Evolution
  - Patch management (OpenVAS)
  - Web (SQLi, XSS)
  - Wifi
  - VoIP
- ✓ SaaS
  - Nouvelles cibles
  - Nouveaux tests



[VULNIT]

Limites

- ✓Test applicatif difficilement automatisable
- ✓Test boîte noire vs. revue de configuration

Source : Livre blanc SSI, Groupe 4

[VULNIT]

Concurrence

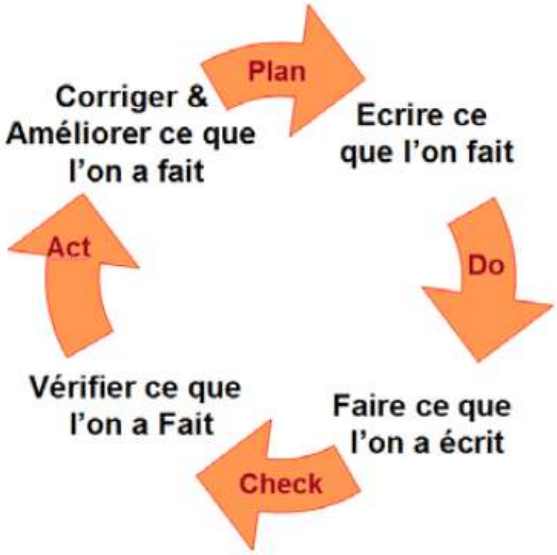
- ✓ Outils experts et onéreux
  - IBM, HP (20K$ a minima)
- ✓ Concurrence directe
  - Nessus, Qualys
- ✓ Concurrence étrangère
  - Support technique
- ✓ Traçabilité
  - Traces d'audit

Les plus connus

	VulnIT	Nessus	Qualys
Société	Française	Américaine (Maryland)	Américaine (Californie)
Approche	Plug & Audit	Installable	SaaS
Support	Clé USB	Logiciel téléchargeable	Appliance + web
Scan de ports	Oui	Oui	Oui
Tests ACL DB	Oui	Oui	Oui
Patch Mngt	V2	Oui	Oui
Wifi	V2	Non	Non
Licence	À la clé	À l'utilisateur	À l'utilisation
Prix	990 / 1490 €	1200 $	2500 $ + variable

Conclusion

- ✓ Importance information
  - menaces et vulnérabilités
  - contrôle
- ✓ Solution innovante et accessible
  - Plug & Audit
  - Rapport d'audit
- ✓ Contrôle doit s'inscrire dans une démarche (ISO…)



Pour en savoir plus

- ✓ Un site web
  - www.vulnit.com
- ✓ Une adresse
  - contact@vulnit.com
- ✓ Un téléphone
  - 01 55 94 92 71

Merci

[VULNIT]