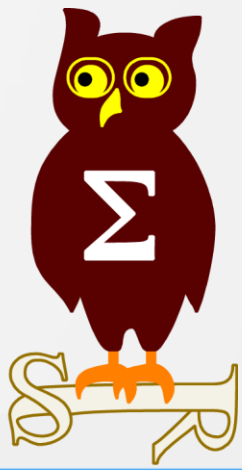


OS  
S  
I  
R



VOS DONNÉES  
SONT CE QUE VOUS AVEZ  
DE PLUS PRÉCIEUX

UNE SÉCURITÉ D'AVANCE

SECLUD

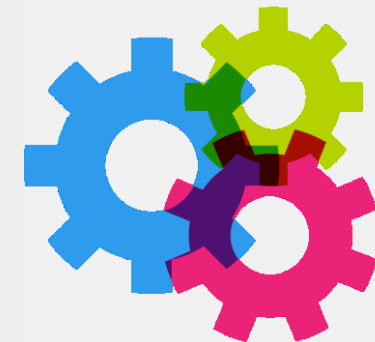
## Surveillance Continue et Adaptative avec « Elastic Detector » LE scanner de nouvelle génération

Frédéric DONNAT – Directeur Technique et Co-Fondateur  
[fred@secludit.com](mailto:fred@secludit.com)  
Téléphone 06 59 98 30 77

Les vulnérabilités représente la première porte empruntée des attaquants - (53% des attaques réussies, source Forrester).



Prévenir,  
vaut mieux que guérir...



# La sécurité : c'est notre expertise

- Membre fondateur du “Cloud Security Alliance”
- Membre du consortium “Secured Virtual Cloud”
- Technologie breveté
- **Mission: Détecter, Mesurer et Agir sur votre cyber risque**
- **Chronologie**
  - 2011: audit AWS EC2 ► Amélioration des procédures de sécurité et corrections
  - 2012: création d'un produit d'audit continu automatisé
    - Elastic Detector devient le haut de gamme des scanners de vulnérabilités
  - 2015: partenariat avec les fournisseurs de service ► Cloud responsable
  - 2016: 15 personnes dont 80% en R&D



SecludIT est cofinancée par l'Union européenne. L'Europe s'engage en PACA avec le fond européen de développement régional



Région  
Provence  
Alpes  
Côte d'Azur



## Témoignage de compétence : article Forbes



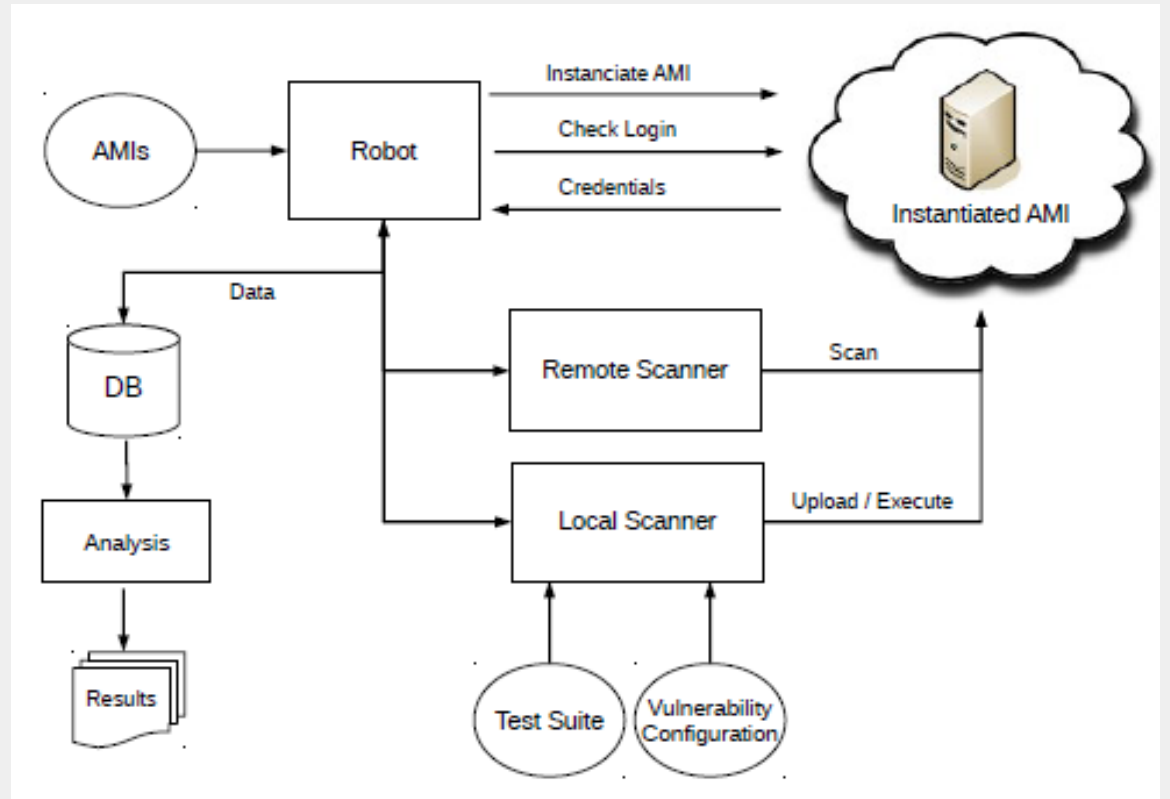
**Andy Greenberg**, Forbes Staff  
Covering the worlds of data security, privacy and hacker culture.  
[+ Follow](#)

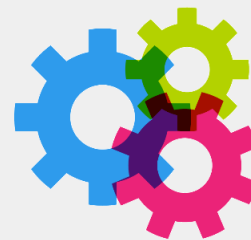
SECURITY | 11/08/2011 @ 1:26PM | 8,145 views

# Researchers Find Amazon Cloud Servers Teeming With Backdoors And Other People's Data

## Résultats de l'analyse : en bref...

- Analyse : +5 000 VMs
- Au moins 1 Vulnérabilité **Critique** sur :
  - 98% des VMs Windows
  - 58% des VMs Linux
- Accès super utilisateur sur 22% des VMs





Elastic  
Detector®

# Mesures de sécurités fréquemment rencontrées



➤ Évalue le risque

➤ Mesure l'impact

➤ Délivre les corrections

Les vulnérabilités représentent la première  
porte empruntée  
En automatique et en continu  
des attaquants - (53% des attaques  
réussies, source Forrester).

## Quels sont les risques encourus ?

---

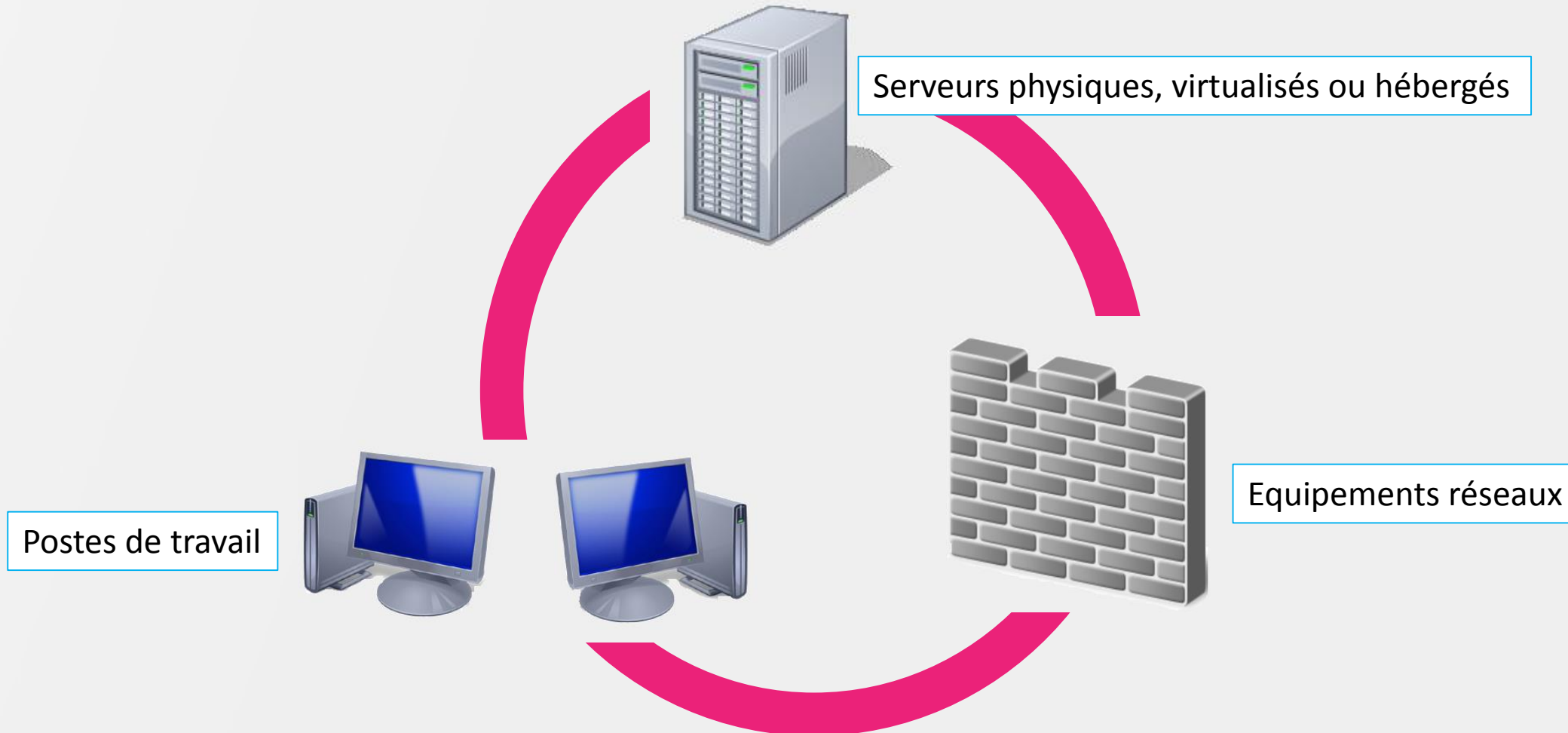
- Vol et violation de la confidentialité des données (perte de fichiers, Responsabilité pénale...)
- Indisponibilité du réseau informatique (arrêt d'activité, ROI impacté...)
- Risques médiatiques pour l'entreprise (Image, réputation...)
- Cyber extorsion (perte financière...)



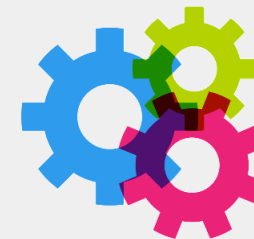
Elastic  
Detector®



# Un périmètre à surveiller







## Problématique

---

- Surveillance continue ?
- Audit de sécurité ? Tests d'intrusion ?
- Pilotage de la sécurité ? Quels outils ? Quels indicateurs ?
- Gestion du risque ? Quels outils ? Quels indicateurs ?
- Une solution ?

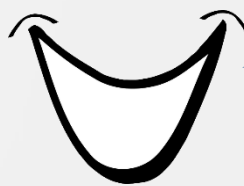
# Des innovations adaptées aux hébergements actuels

Votre parc est-il  
« élastique » ?


Faites vous régulièrement les  
tests de sécurité adaptés à vos  
serveurs ?

Pouvez-vous scanner à tout  
moment vos machines de production ?

Savez-vous extraire et donner  
la bonne information à la  
bonne personne ?



SecludIT – Copyright & confidentiel - 2016

<p><b>Auto-découverte</b> Réseaux et serveurs découverts automatiquement</p>	<ul style="list-style-type: none"> <li>• Périmètre de sécurité mis à jour des changements</li> <li>• Pas de configuration</li> <li>• Pas de risque d'erreur</li> </ul>
<p><b>Auto-checks</b> Tests de sécurité mis à jour et lancés automatiquement</p>	<ul style="list-style-type: none"> <li>• Nouveau serveurs immédiatement surveillés</li> <li>• Pas de configuration</li> <li>• Pas de risque d'omission</li> <li>• Base de tests jamais périmée</li> </ul>
<p><b>Sans agent</b> Pas de logiciel à déployer sur les serveurs</p>	<ul style="list-style-type: none"> <li>• Pas de coût de déploiement ni de maintenance</li> <li>• Pas de ressource utilisée</li> <li>• Pas de risque de cheval-de-Troie</li> </ul>
<p><b>Clonage</b> Analyse approfondie, de l'intérieur du serveur</p>	<ul style="list-style-type: none"> <li>• Analyse poussée sans impact sur la production</li> <li>• Serveurs dormants inclus</li> <li>• Moins de faux-positifs</li> </ul>
<p><b>Multi-cible</b> Utilisation Cloud, virtuelle, physique et hybride</p>	
<p><b>Reporting</b> Rapports détaillés et tableau de bord</p>	<ul style="list-style-type: none"> <li>• Synthèse</li> <li>• Rapports configurables</li> <li>• Alertes et réactivité</li> <li>• Archivage et tendances</li> </ul>

# Différenciateurs Majeurs d'Elastic Detector :

---

1. Automatisation Intensive / Connecteur APIs
  - Auto-Découverte
  - Pas d'agent
2. Technologie de « Clonage »
  - Pas d'impact sur la production
  - Isolation / Cloisonnement
3. Reporting : « La bonne information à la bonne personne »
  - Indicateur de risque pour le pilotage
  - Feuille de route « métier » pour la remédiation

# Technologie de Clonage



## Clonage de VM en 4 étapes

- Sélection et Clonage
- Cloisonnement & Isolation
- Reconfiguration
- Décommissionnement

## Bénéfices de la Recherche de Vulnérabilités

- Zéro impact sur la VM de production
- Analyse en profondeur (accès authentifié)

# A chacun ses informations

## Equipe dirigeante



- ANSSI
- OWASP
- PCI-DSS
- ISO



## DSI



- Application Web
- Application Mail
- Application Autre
- Frameworks
- Logiciel Tiers
- Logiciel malveillant
- Données
- Système d'exploitation
- Virtualisation
- Network



## Expert Sécurité



## Techniciens



Id	Titre	Statut	Impact	Complexité	Remarque	Remarque
1	...	...	...	...	...	...
2	...	...	...	...	...	...
3	...	...	...	...	...	...
4	...	...	...	...	...	...
5	...	...	...	...	...	...
6	...	...	...	...	...	...
7	...	...	...	...	...	...
8	...	...	...	...	...	...
9	...	...	...	...	...	...
10	...	...	...	...	...	...

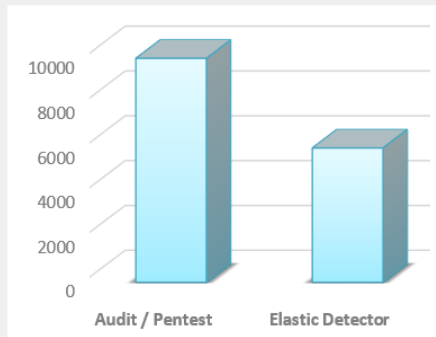
# Démonstration Elastic Detector

---



# Pourquoi choisir Elastic Detector ?

## 1 - Plus efficace et moins cher que l'audit et les Pentests

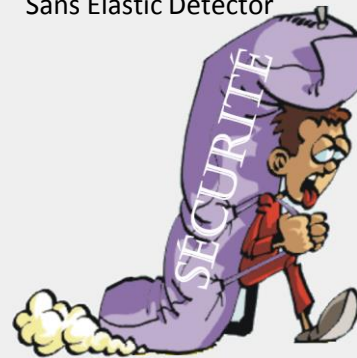


18 nouvelles vulnérabilités  
chaque jour



## 2 - Gain de temps & productivité

Sans Elastic Detector



Avec Elastic Detector



## 3 - L'un des meilleurs scanners du marché



Pas convaincu ?

**ESSAYEZ & COMPAREZ !**

## 4 - Rapidité, simplicité et lisibilité



Rapidement opérationnel



Interface intuitive

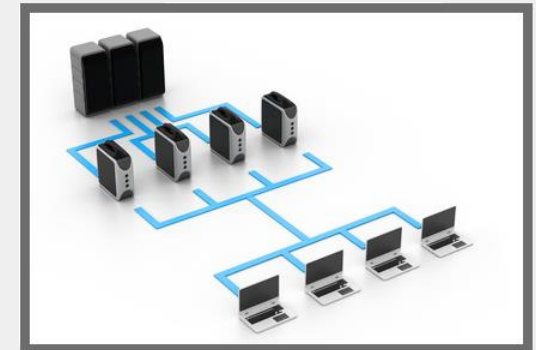


Des rapports  
clairs et compréhensibles

## Notre solution :

### Elastic Detector

- Surveillance automatique
- Surveillance continue
- Surveillance ponctuelle
- Mise à jour quotidienne automatique des tests de vulnérabilité
- Evaluation des risques
- Rapports différentiels
- Alertes
- Tableaux de bords adaptés





# Questions ?

