Scénarios d'attaques et Détection d'Intrusions

Soutenance de stage de Master

Quack1

Julien IGUCHY-CARTIGNY

Adrien VERNOIS

Master CRYPTIS

Limoges, le 12 Septembre 2013

Introduction

Sécurité informatique

→ Recrudescence des intrusions

→ Importance de la détection

Objectifs du stage :

→ Compétences en détection d'intrusions et amélioration des scénarios

→ *« Peut-on détecter efficacement des intrusions ? »*

Plan

→ L'entreprise : Conix Security

→ La détection d'intrusions

→ Détection d'attaques Web

→ Certaines limites

→ Aller plus loin : la corrélation d’évènements

Conix

SSII créée en 1997

Paris

Plusieurs activités

Conix Security

- Audit
- Forensique
- Conseil
- Détection d'intrusions

La détection d'intrusions

Sécurité Informatique :

> *« Conserver, rétablir, et garantir la sécurité des systèmes d'information »*[*]

Principaux enjeux de la détection

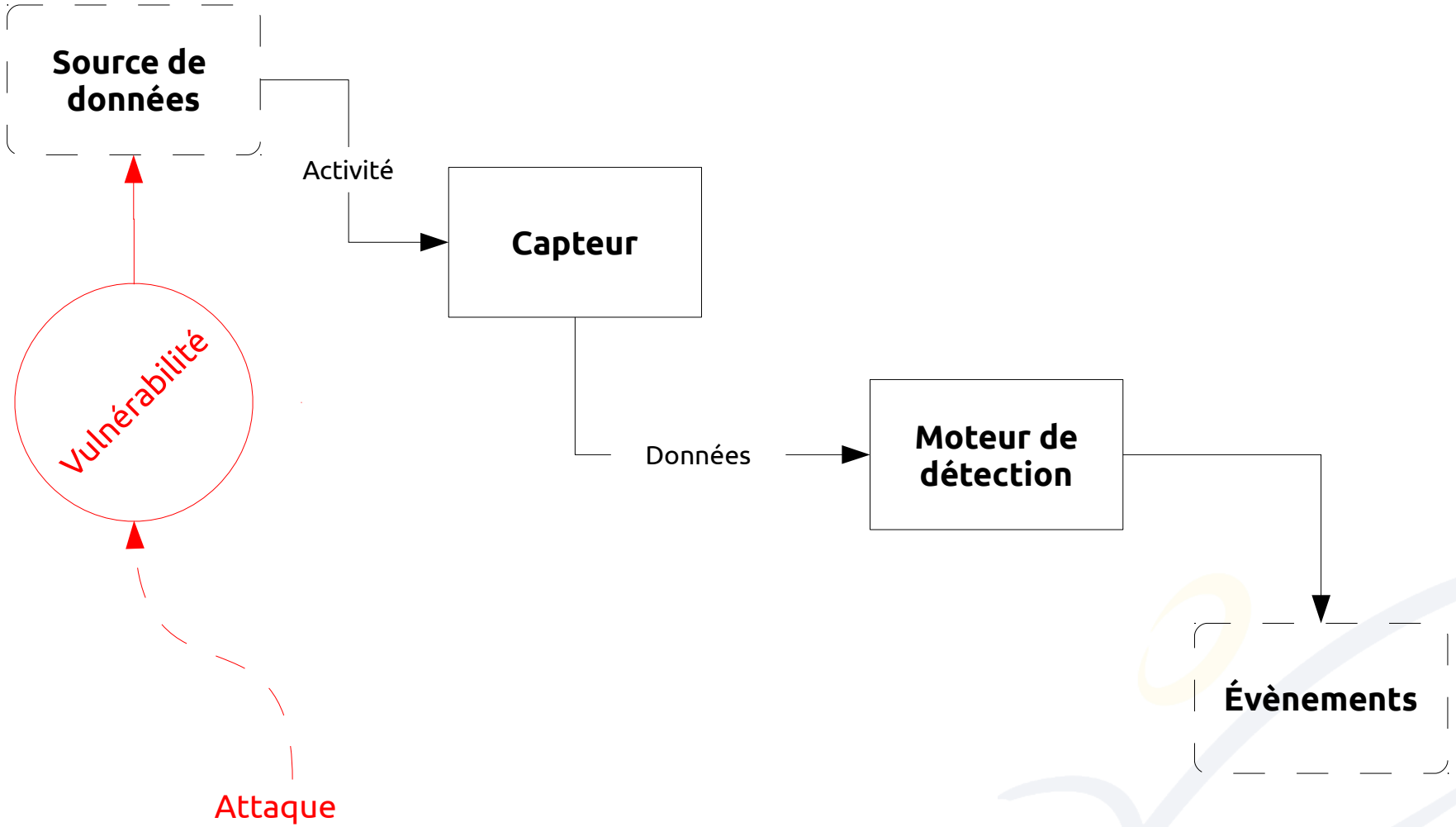
- Détecter les intrusions en « temps réel »
- Obtenir le niveau de sécurité du SI
- Résoudre rapidement les intrusions

Plusieurs types d'IDS

- Réseau (*NIDS*) – Snort, Bro, Suricata
- Système (*HIDS*) – OSSEC, GNU/Linux Audit, Windows Audit
- Données brutes – Logs d'applications, d'équipements réseaux

[*] https://fr.wikipedia.org/w/index.php?title=Portail:S%C3%A9curit%C3%A9_informatique

Fonctionnement d'un IDS



Détection d'attaques Web

Pourquoi ?

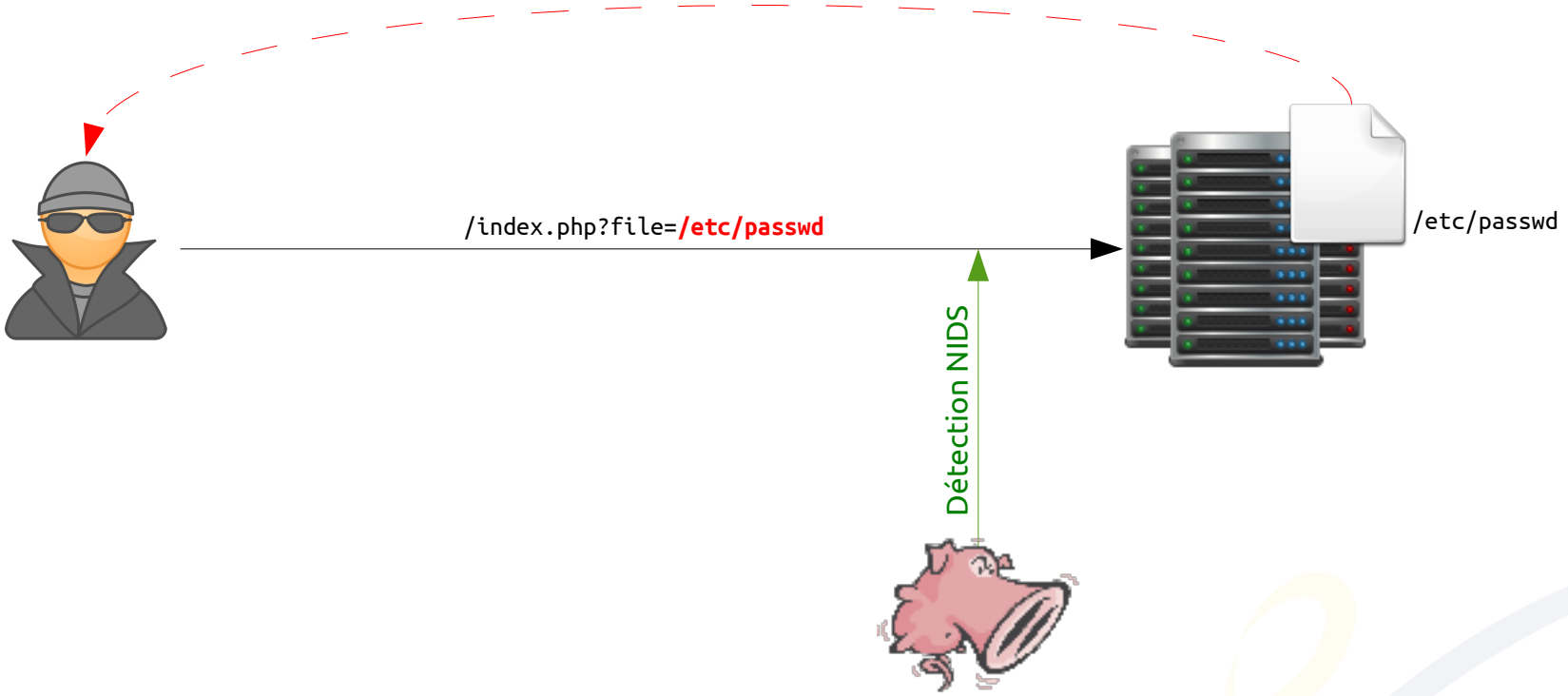
- Répandues – Facilité d'exploitation
- Facilité de détection

Analyse réseau

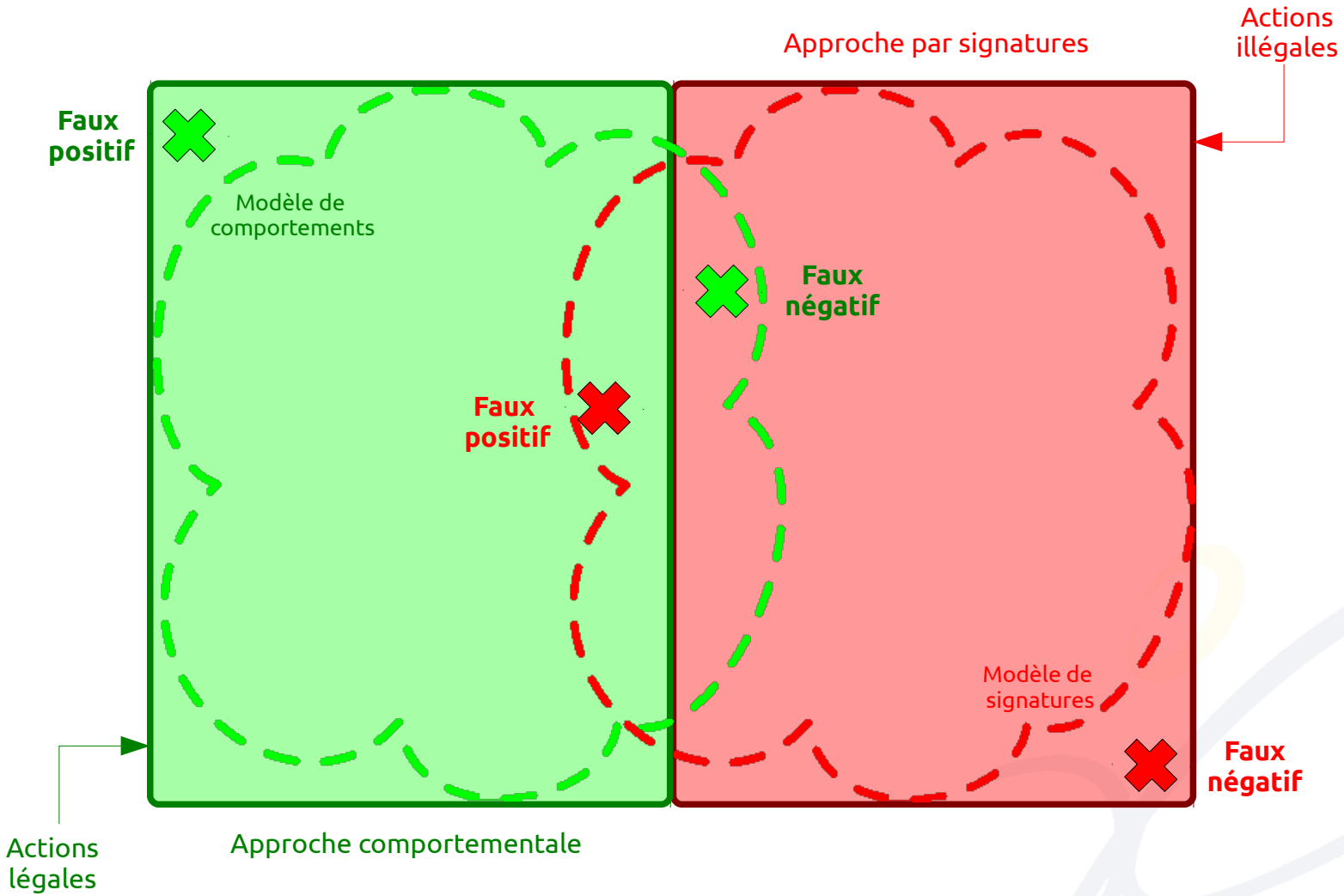
- Observation du comportement dans *Wireshark*
- Empreinte « unique » de l'outil
- Écriture d'une règle IDS

Exemple : Détection d'une attaque Web simple

« Local File Inclusion »



Limites de la détection : fiabilité vs pertinence



Limites de la détection : contournement

Détection d'un outil

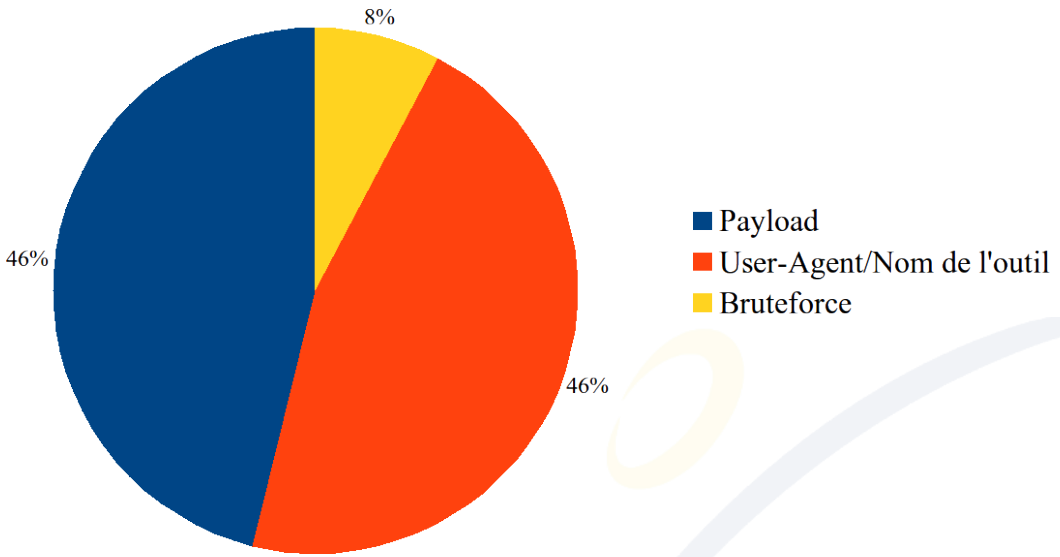
- Règle spécifique à l'outil
- 1 outil → Plusieurs règles

Contournement d'IDS

- Modification du *User-Agent*
- Modification du *payload*
- Encodage des caractères
- Délai entre chaque tentative

Solutions

- Expression régulières
- Corrélation d'évènements



Aller plus loin :
La corrélation d'évènements

Règle IDS unique → Peu utile mais précise

Plusieurs règles → Plus d'informations

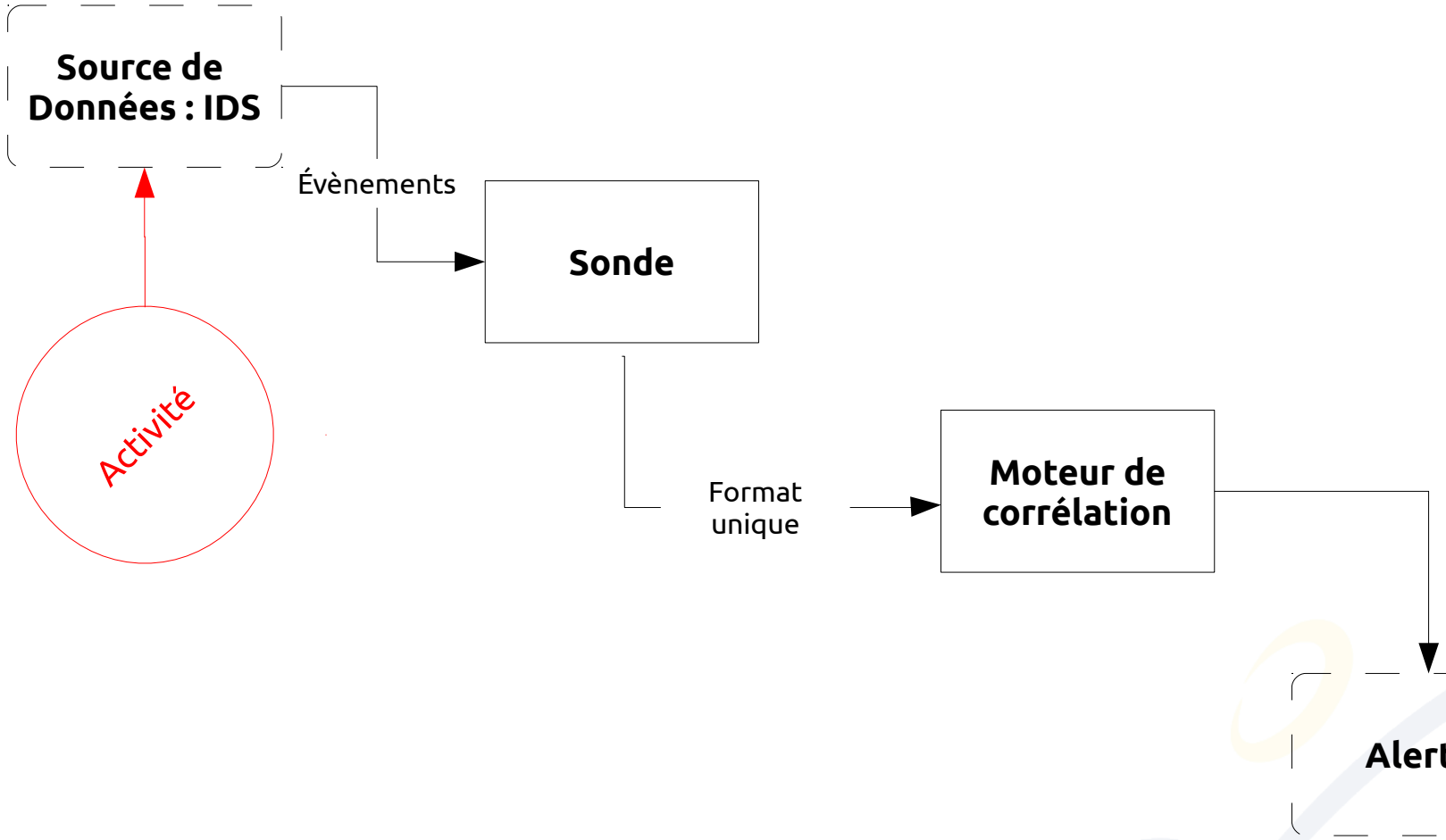
→ Nécéssité de corréler

- Qualifier les incidents avec plus de critères
- Supprimer les faux-positifs
- Mieux apprécier la criticité des évènements

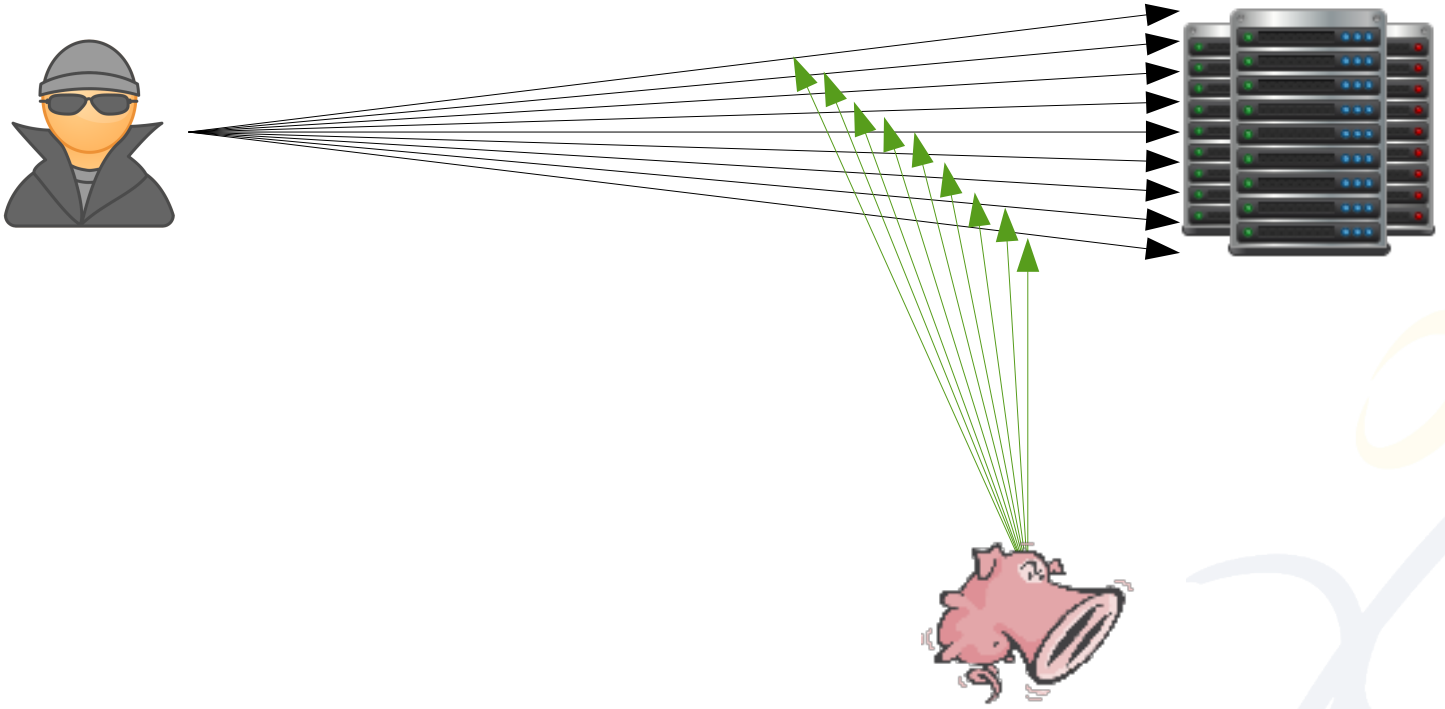
⇒ SIEM → OSSIM

- ⇒ Scénarios d'attaques évolués

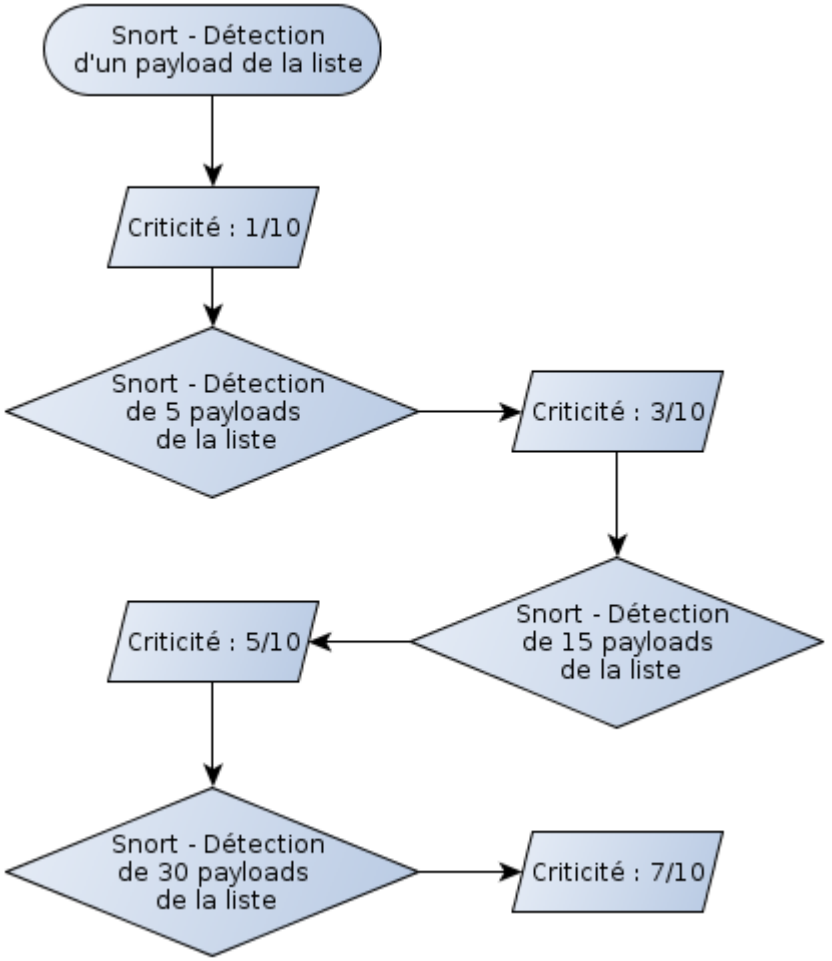
Fonctionnement d'un SIEM



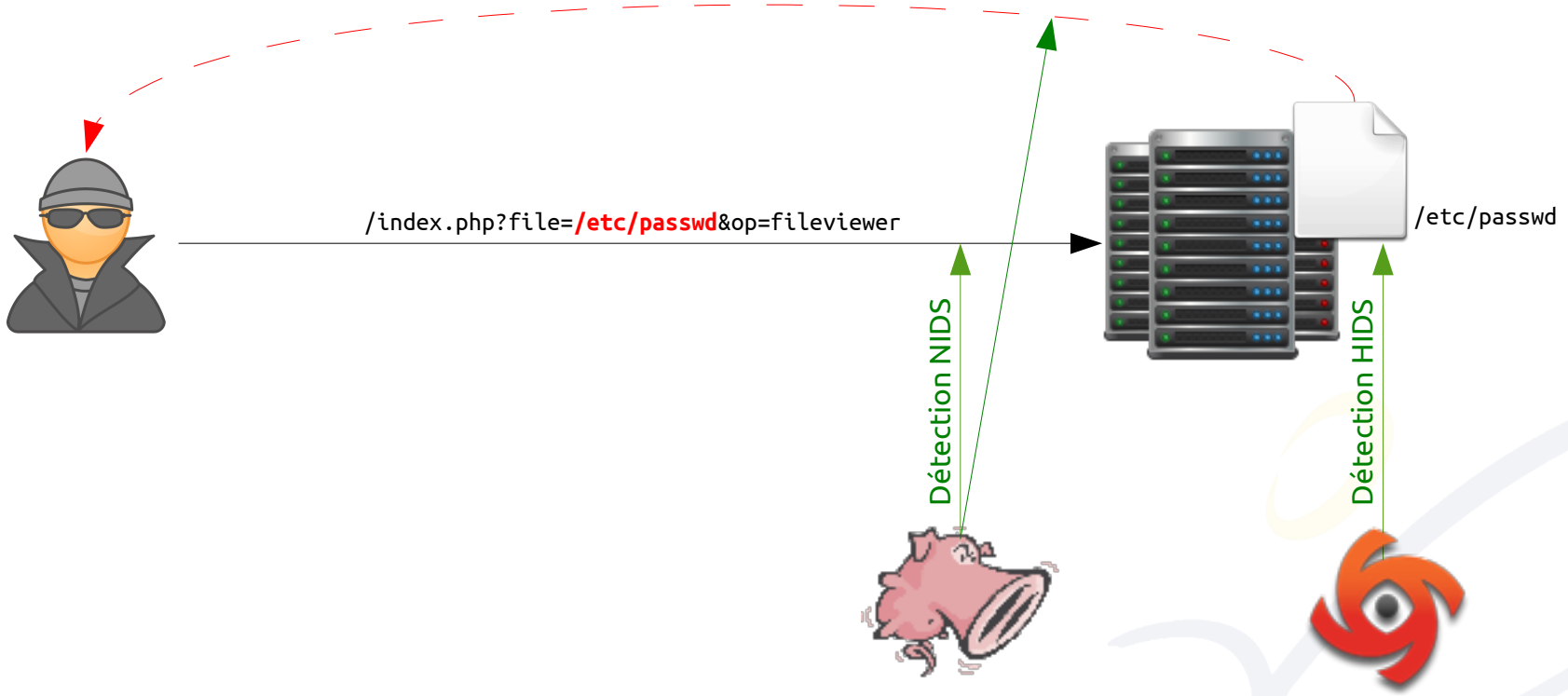
Corrélation : Attaques par un outil automatique



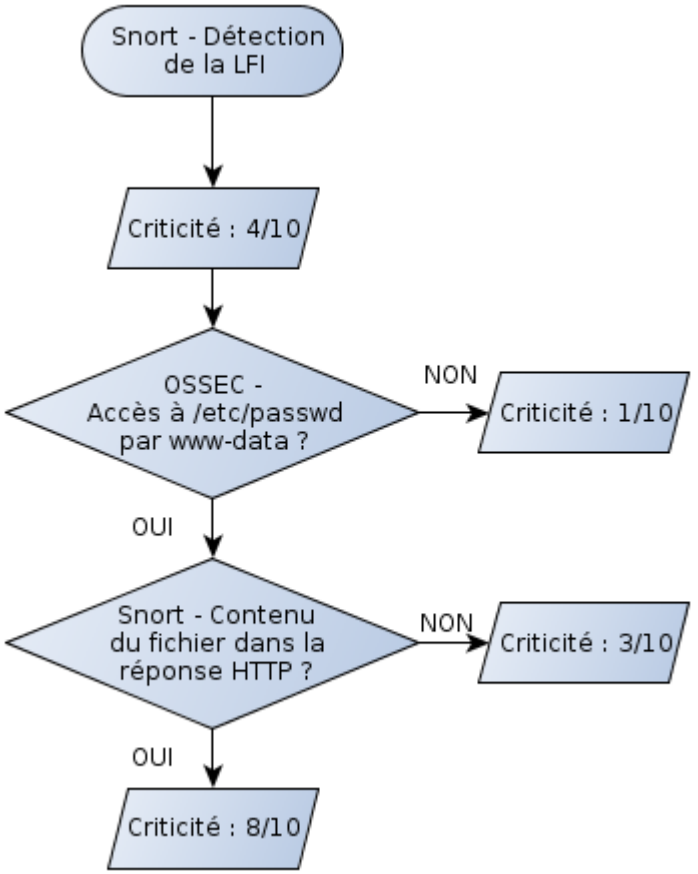
Corrélation : Attaques par un outil automatique



Cross-Corrélation : Attaque par « *Local File Inclusion* »



Cross-Corrélation : Attaque par « *Local File Inclusion* »



IDS / SIEM : Solution à toute épreuve ?

Solution IDS seule ?

- Règles précises
- Difficulté de traitement

Solution SIEM ?

- Sources illimitées
- Corrélation efficace

Mais …

- Difficulté de modélisation des scénarios
- Faux-positifs
- Attaques inconnues
- Flux chiffrés
- Traitement humain nécéssaire

NIDS		HIDS		SIEM	
Monitoring du trafic réseau	✓	Accès aux fichiers	✓	Corrélation des évènements	✓
Contexte	✗	Intégrité des fichiers et dossiers	✓	Reporting	✓
Détection précise des *payloads*	✓	Processus séparés	✓	Contexte	✓ ✗
Utilisation possible de *payloads* génériques	✓ ✗	Accès réseau des processus	✗	Faux-positifs/négatifs	✓ ✗
Utilisateur source de l'évènement	✗	Édition de paramètres systèmes	✓	Temps de maintenance/gestion	✓ ✗
Logiciels utilisés	✗	Utilisateurs	✓	Attaques multi-niveaux	✓
Adresses IP	✓				

« Catch the vulnerability, not the exploit »

Conclusion

→ Détection universelle

Détection complexe

Ressources supplémentaires nécéssaires

→ D'autres approches ?

→ Stage très intéressant

Forte montée en compétences

Rédaction d'un article dans le MISC #69

CDI dès septembre

Merci