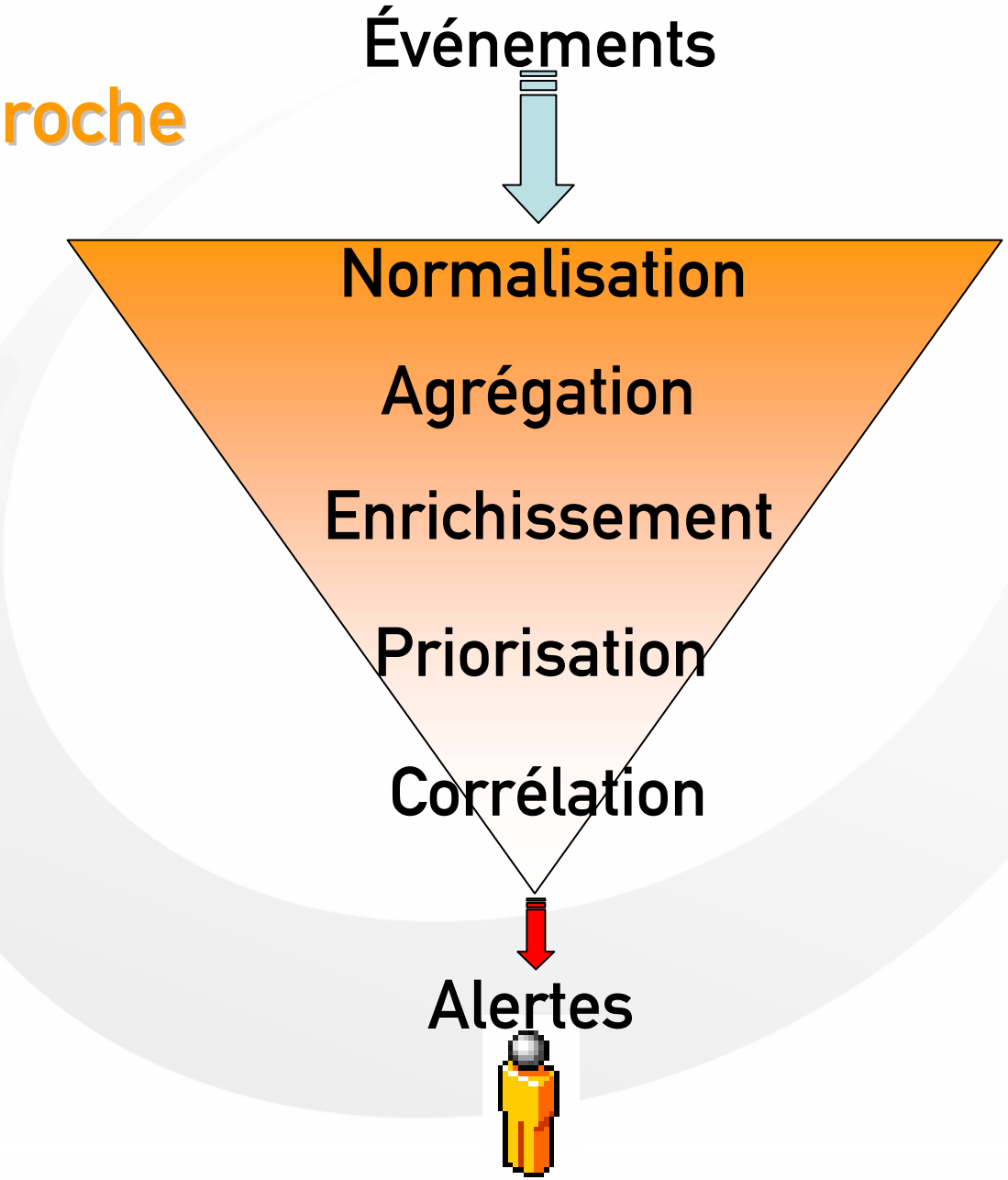
Corrélation et Analyse d'événements de sécurité

Auteur(s): Christophe BRIGUET

Contexte et besoin

- Équipements hétérogènes
- Trop d'information à gérer
- Pas de prise en compte de l'environnement
- Besoin de plus de visibilité
  - Supervision temps réel de la sécurité
  - Pilotage « à vue » du SI (tableaux de bord)

Notre approche



Normalisation des messages

- Analyse sémantique (lexicale)
  - Uniformisation du **contenu (nomenclature)**
  - Un même événement, différents messages !

Checkpoint : « *Port Scanning* »
NetASQ : « *Possible port scan* »
Snort : « *Portscan detected* »

- Analyse syntaxique
  - Uniformisation de la **forme**
  - Conversion en IDMEF* de chaque message

Permet un traitement optimisé des messages

* Intrusion Detection Message Exchange Format

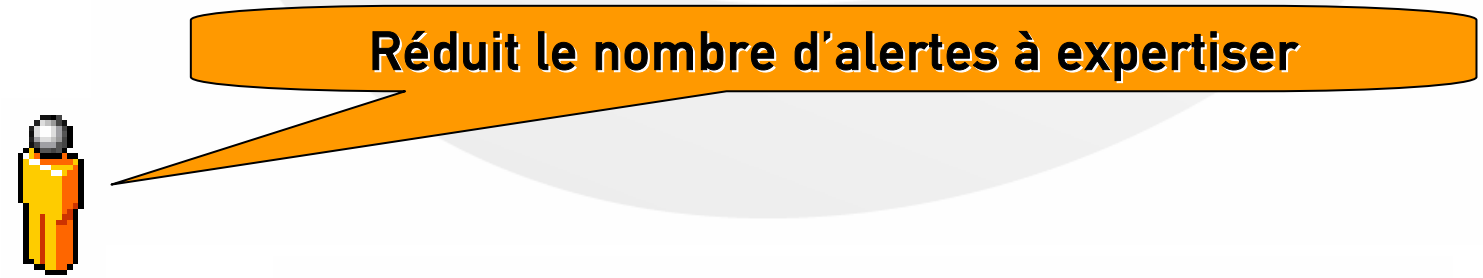
Agrégation d'événements

- Regroupement sur critères similaires
  (Ex: Même source, destination, signature)
- Sélection des critères suivant le type de message

Ex:

Exploit (IP source, IP destination, port destination)

Attack response (IP source, port source)



Enrichissement d'événements

- Prise en compte de l'environnement
- Analyse du contexte (vulnérabilité, criticité …)
- Utilisation d'une **base de connaissance**
  - Modélisation du périmètre (host, service, criticité …)
  - Nessus KB , ICAT, OSVDB (*mapping* Host / Service / n°CVE)

1. Augmente la pertinence des alertes
2. Enrichit la description de l'événement
3. Priorise les événements

Corrélation d'événements

- Basée sur des règles utilisant des scénarii prédéfinis (si… alors… sinon…)
- Ex:

  Si

  IDS-> "DoS attempt on *MyTarget*"

  Nagios-> "*MyTarget* System Status Down"

  Alors

  Correlator -> "Dos Attack Succeed on *MyTarget*"

1. Détection d'incident potentiel
2. Réduction du nombre d'alertes en les regroupant en fonction de scénarii prédéfinis

Pour conclure

- Étape indispensable pour …
  - Superviser efficacement
  - Obtenir des indicateurs (fiables) pour tableaux de bord
  - Industrialiser la notion de « contre mesure »
- D'autres mécanismes à implémenter (corrélation à base de prédicat …)

exaprotect
Technology

Merci de votre attention …

Contact: cbriguet@exaprotect.com