

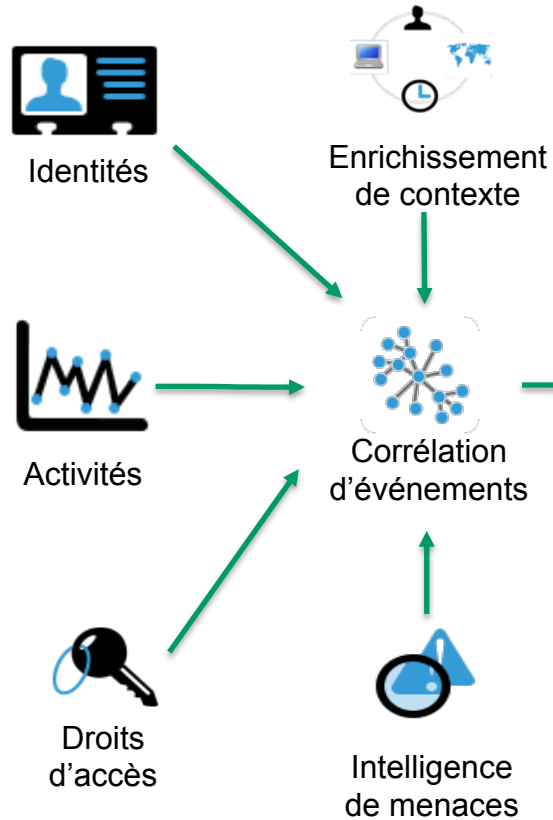
Analytique en cybersécurité

Objectif

Détecter et éliminer le plus rapidement possible les **menaces** qui peuvent impacter la sécurité de nos systèmes d'informations.

Besoins

- Surveillance
- Processus
- Irritants



Techniques de base

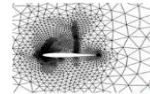
A+B

Règles logiques



Recherches manuelles

Techniques d'analytique



Analyse de comportements



Analyse par les paires

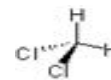


Rareté de l'événement



Comportement robotique

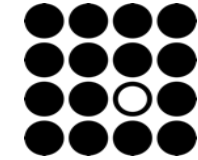
Techniques d'analytique avancée



Analyse prédictive



Analyse sentimentale



- Détection d'anomalies
- Présentation des résultats



Analyse

Orchestration
Automatisation



- Enquêtes & réponses aux incidents de sécurité
- Aide à la décision