acceis

Gwenn Feunteun

gwenn@acceis.fr

Largement inspiré d'un cours d'Odile PAPINI :
http://odile.papini.perso.esil.univmed.fr/sources/SSI.html

Architecture & sécurité réseau

La détection d'intrusion

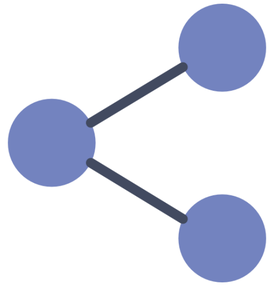
istic Informatique Électronique

acceis

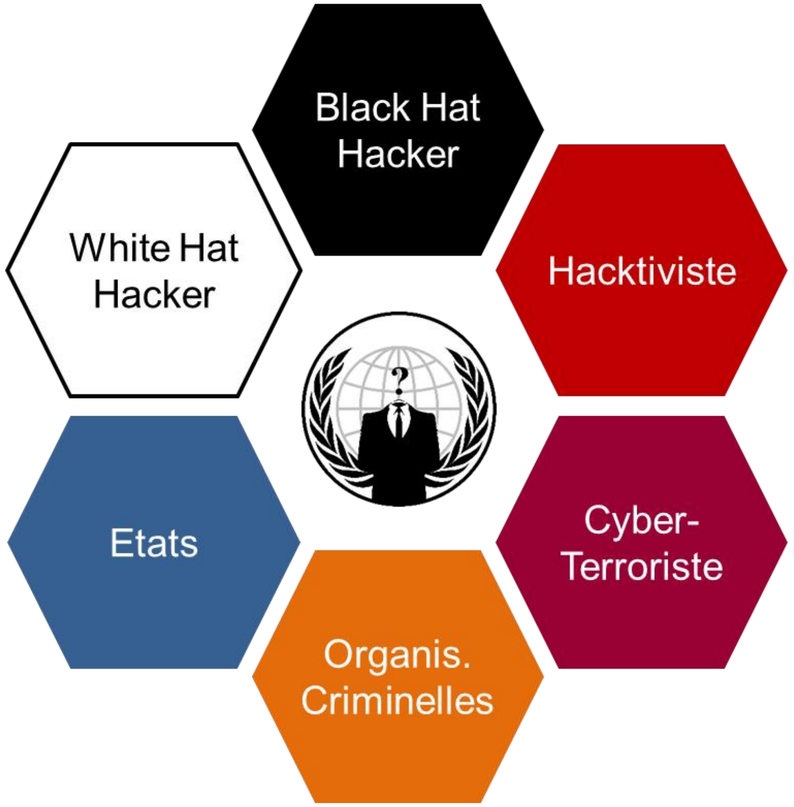
Introduction

- Les besoins de dématérialisation sont grandissants ;
- L'interconnexion des réseaux est croissante ;

➔ les points d'interconnexion avec l'extérieur et en particulier avec Internet sont autant d'accès qu'un attaquant peut tenter d'utiliser pour s'introduire dans un système d'information.



Sources d'intrusion



- Des origines, des motivations et des ressources variables

Canaux d’intrusion

- Des canaux d’intrusion variés, dépendant souvent des moyens et de la finalité.

Les motivations

- Les motivations et enjeux vont conditionner les méthodes employées.

Détection d’intrusion

Il faut donc mettre en œuvre des moyens permettant de détecter, voire de bloquer, les intrusions.

Détection des intrusions

≠

Détection des attaques

Systèmes de détection d'intrusion

La détection d'intrusion est opérée par des systèmes en charge d'identifier des actions pouvant être associées à des activités non légitimes en analysant les composant d'un système d'information et/ou leur activité.

Il existe généralement trois grandes familles distinctes de système de détection d'intrusion (*Intrusion Detection System* ou IDS) :

- Les **NIDS** (*Network Based Intrusion Detection System*), qui surveillent l'état de la sécurité au niveau du réseau.
- Les **HIDS** (*HostBased Intrusion Detection System*), qui surveillent l'état de la sécurité au niveau des hôtes.
- Les **IDS hybrides**, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes.
- Et d'autres, notamment les **SIEM**.

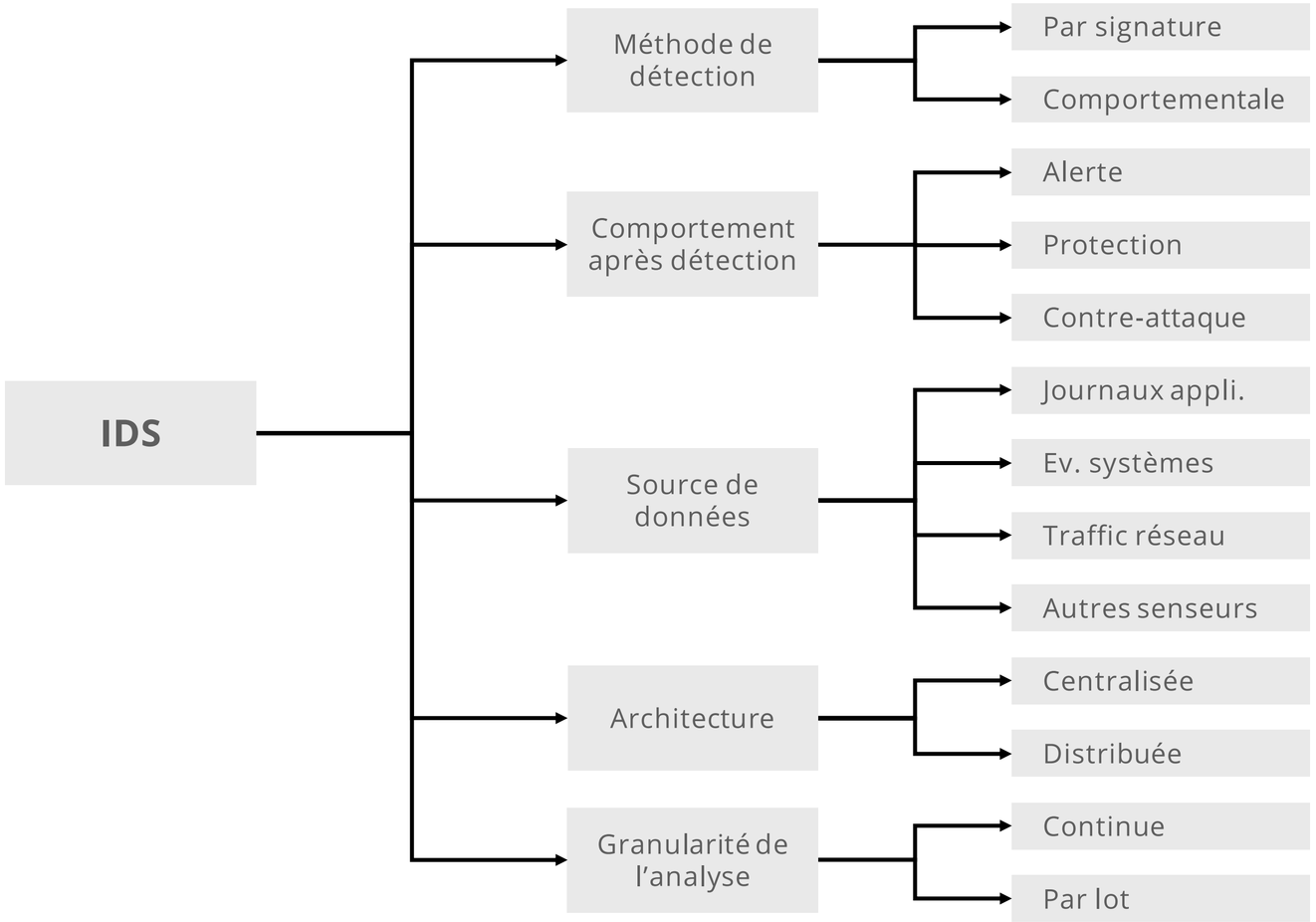
Une grande variété

- Logiciels vs. Matériels ;
- Dédiés vs. Associés à d'autre composants (comme un pare-feu par exemple) ;
- Libres vs. Payants ;
- « Passifs » vs. « Actifs » (capable de bloquer les tentatives d'intrusion. On parle alors d'IPS pour *Intrusion Prevention System*) ;
- Comportementaux vs. Basés sur des signatures.

Notions fondamentales

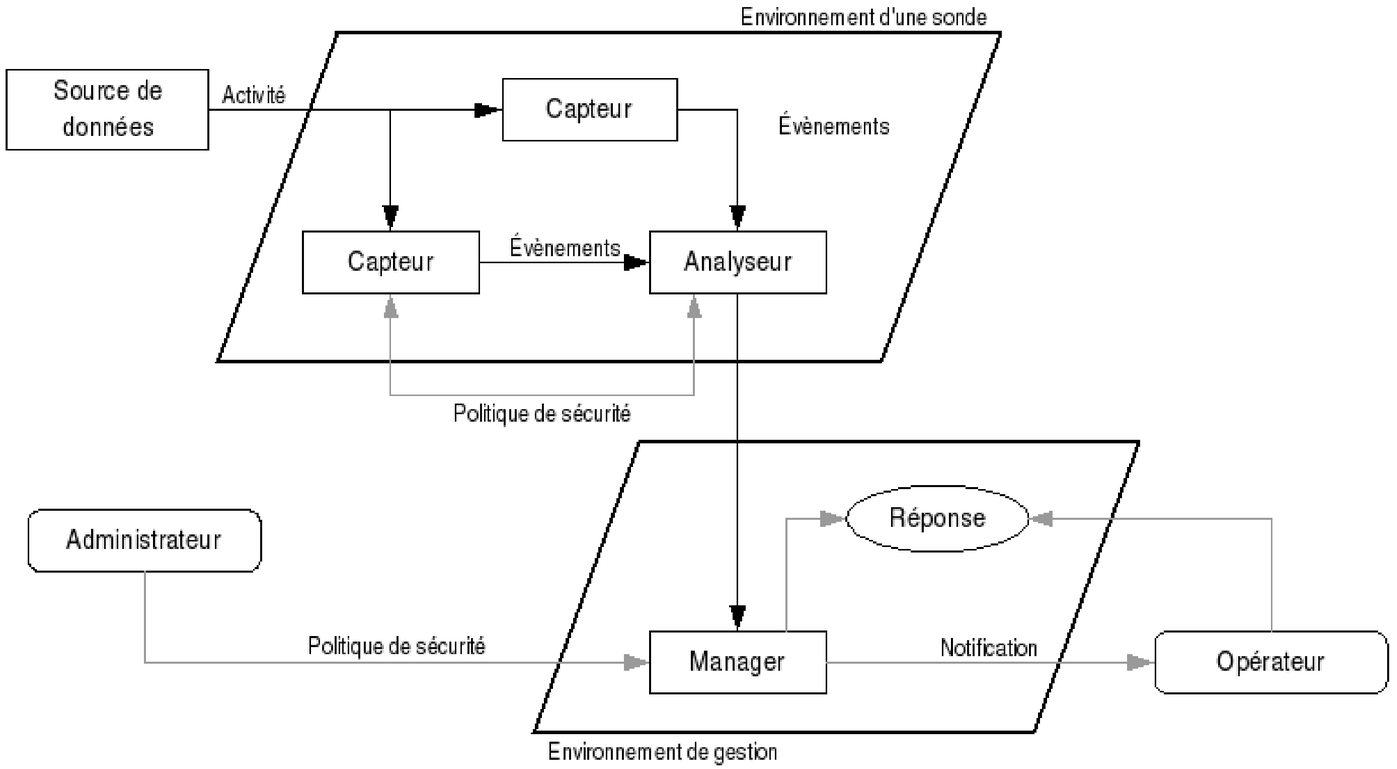
- **Vrai positif** : Considérer une activité malveillante comme telle ;
- **Faux positif** : Considérer une activité légitime comme étant malveillante.
- **Vrai négatif** : Considérer une activité légitime comme telle ;
- **Faux négatif** : Considéré une activité malveillante comme légitime ;
- **Sensibilité** : Capacité de détecter la plus infime activité malveillante
  ➔ beaucoup de faux positifs ;
- **Spécificité** : Capacité de détecter de manière fiable les activités malveillante
  ➔ beaucoup de faux négatifs.

Classification

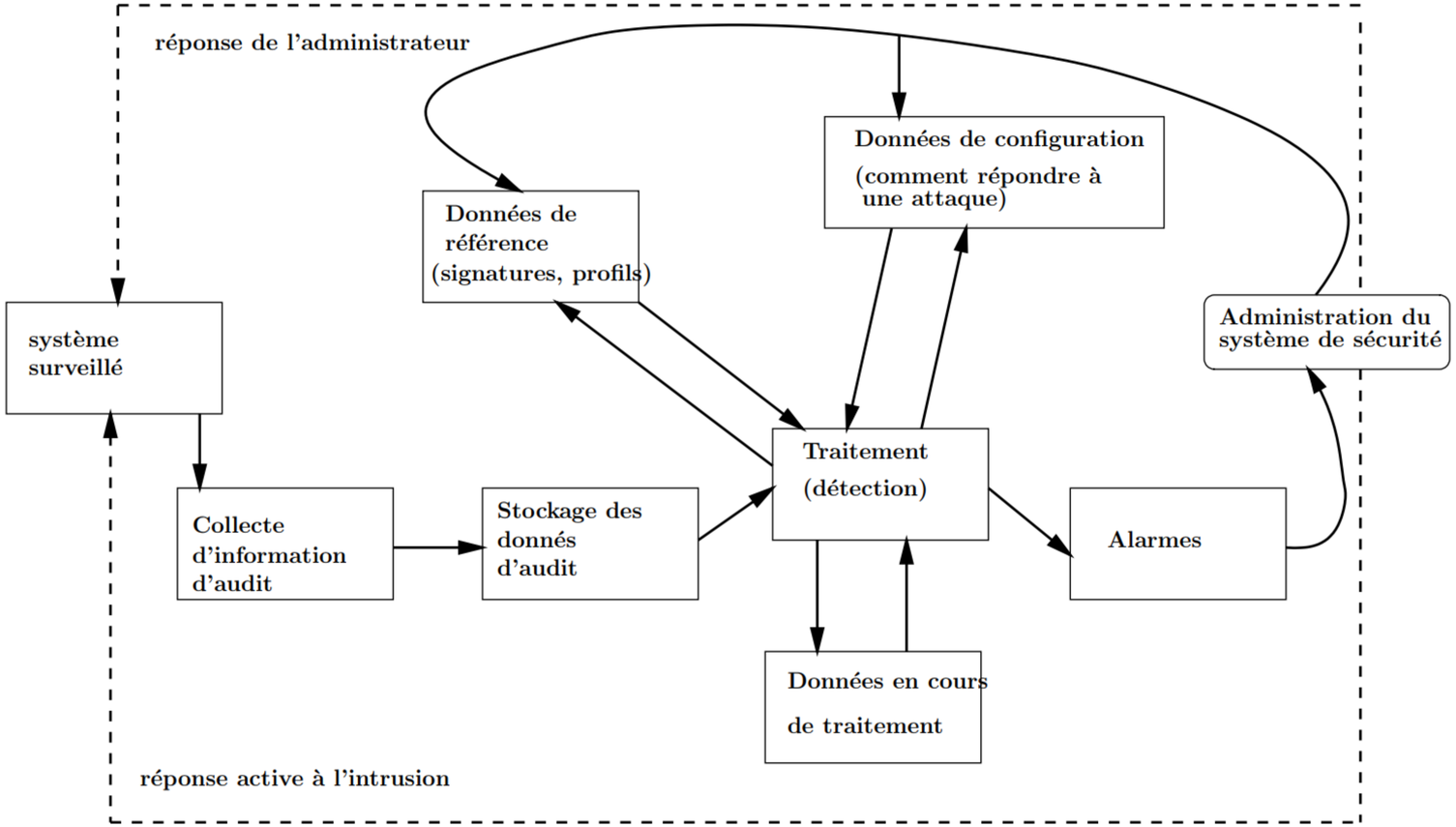


src L. Mé

Architecture IDWG

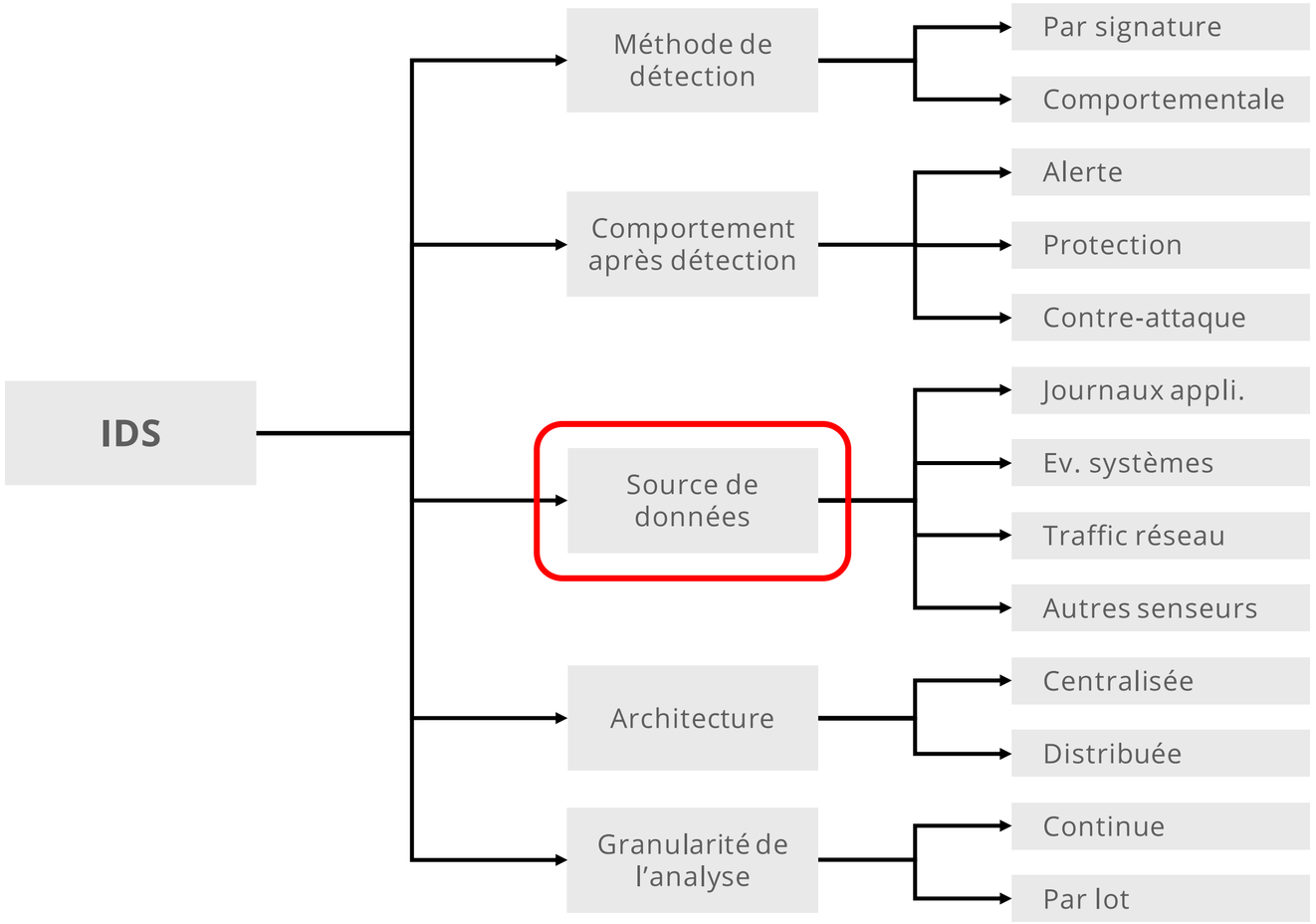


Modèle de fonctionnement



src O. Papini

Classification



src L. Mé

NIDS

Les Network-based IDS s'appuient sur une analyse du trafic réseau :

- Placés en coupure de flux, ils analysent ce qui passe, voire le bloque ;

  ↳ ⚠️ Si l'équipement à un problème (*fail-safe* ?).

- Connectés à un port « miroir » sur un commutateur ou reliés à un TAP réseau ;

- En recevant du trafic *Netflow* (exportation d'informations sur les flux réseau par les équipements, initialement Cisco).

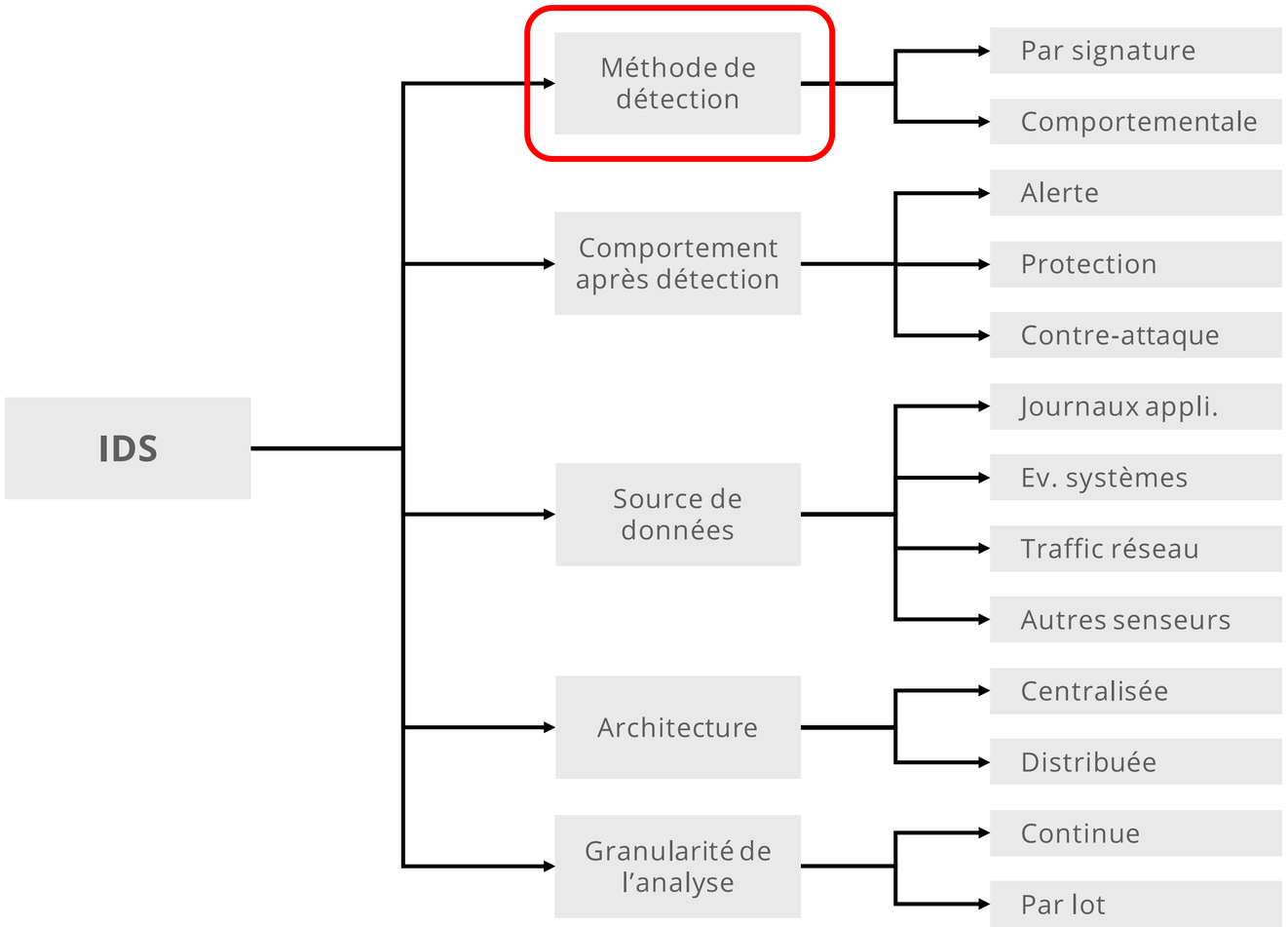
  ↳ Mode de fonctionnement relativement « passif ».

HIDS et hybrides

La frontière entre les Host-based IDS et les IDS hybrides sont plus floues. Leur analyse peut notamment être basée sur :

- L'intégrité des fichiers du système (via des contrôles planifiés ou en continue) ;
- Les événements des journaux d'activité ;
- Les événements systèmes (en particulier les appels de fonctions « sensibles ») ;
- L'activité réseau de l'équipement…

Classification



src L. Mé

Détection par modèles comportementaux

Détection d'anomalies via l'identification de déviations par rapport à un profil de référence, correspondant aux comportements « normaux ».

➔ **Phase d'apprentissage** pour définir le profil de référence.

Différentes approches pour la construction du profil :

- Probabiliste ;
- Statistique ;
- Réseaux de neurones…

Détection par modèles comportementaux

Probabiliste

Création du profil de fonctionnement d'une application à partir des événements observés. Une probabilité est liée à chaque séquence d'événements E_i → E_{i+1}. Une alerte est levée si :

- E_{i+1} n'est pas prévu par le profil ;
- E_{i+1} apparaît trop souvent ;
- E_{i+1} n'est pas l'événement attendu.

Détection par modèles comportementaux

Statistique

Création du profil en mesurant de manière régulière des éléments du système surveillé (occupation mémoire, heure de connexion, typologie de trafic, etc.), en leur attribuant des valeurs statistiques et ainsi en construisant une distribution de chaque variable selon un modèle statistique.

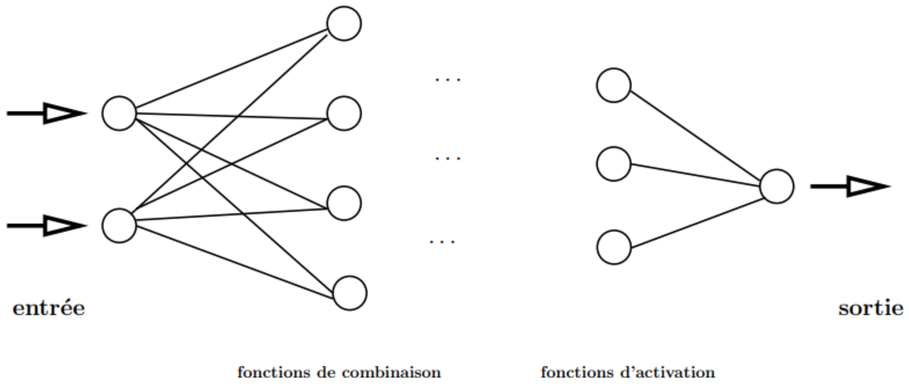
Le système mesure le taux de déviation entre les comportements courants et passés et déclenche une alerte si l'écart est trop important.

Détection par modèles comportementaux

Réseaux de neurones

Chaque utilisateur est identifié par son comportement (ses habitudes de travail, les applications qu'il utilise, etc). Le profil est établi au travers d'un réseau de neurones qui reconnaît une suites d'opérations effectuées par l'utilisateur.

Le but est de prédire l'action suivante de l'utilisateur et de lever une alerte en cas d'échec.



Détection par modèles comportementaux

- Capacité de détecter de nouvelles attaques ;
- Besoin de peu de maintenance.

- Sensibilité aux attaques lors de l'apprentissage ;
- Pas adapté aux changements d'entité modélisée ;
- Evolution des profils au cours du temps problématique.

Détection par signatures

Modélisation des caractéristiques d'une attaque = signature
➔ spécification des comportements interdits.

Une alarme est déclenchée si le scénario d'attaque est identifié dans la bibliothèque de signature.

Différentes approches pour la détection :

- Recherche de motifs ;
- Détection par inférence ;
- Vérification de modèles…

Détection par signatures

Recherche de motifs

Recherche de marqueurs dans un événement ou une série d'événements :

- Sur le contenu ;
- Sur les métadonnées :
  - Adresses sources et destinations ;
  - Nature du protocole et ports ;
  - Processus à l'origine ;
  - Type d'appels systèmes ;
  - Etc.

Détection par signatures

Recherche de motifs

La description des motifs se fait au travers de langages spécifiques :

- **STATL**, basé sur des transitions d'état. L'état caractérise un point de contrôle d'un système durant l'évolution de l'attaque, alors qu'une transition est une action qui, mises bout-à-bout conduisent à une intrusion.
- **ADeLe** est un langage de description procédural. Chaque attaque est définie de manière unique.
- **CISL** est l'acronyme de *Common Intrusion Specification Language.* Il s'agit de la principale composante du CIDF, le *Common Intrusion Detection Framework*), créé par le DARPA. Sa vocation est de pouvoir partager les informations concernant les intrusions.
- Et d'autres…

Détection par signatures

Détection par inférences

Basé sur le principe d'inférences de Bayes : détermination de la probabilité de réalisation d'une attaque comptes-tenus de l'occurrence d'événements précis. Si la probabilité est élevée, une alerte est levée.

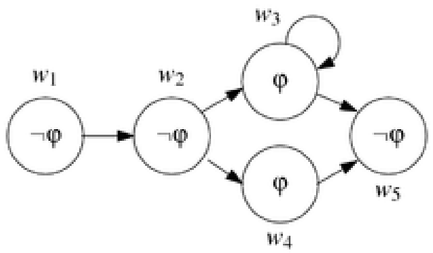
$$P(A|S) = \frac{P(s_1|A) \cdot P(s_2|A) \cdot [\dots] \cdot P(sn|A) \cdot P(A)}{P(S)}$$

- A : attaque, S : symptômes (événements donnés) ;
- P(X) : probabilité de l'occurrence de X (A ou S) ;
- P(A|S) : probabilité de A sachant S.

Détection par signatures

Vérification de modèles

La signatures est une séquences d'événements suivant une logique (modale) temporelle. L'attaque est modélisée par un système de transition d'états (un graphe orienté). La séquence d'événements est décrite en utilisant la sémantique de Kripke.



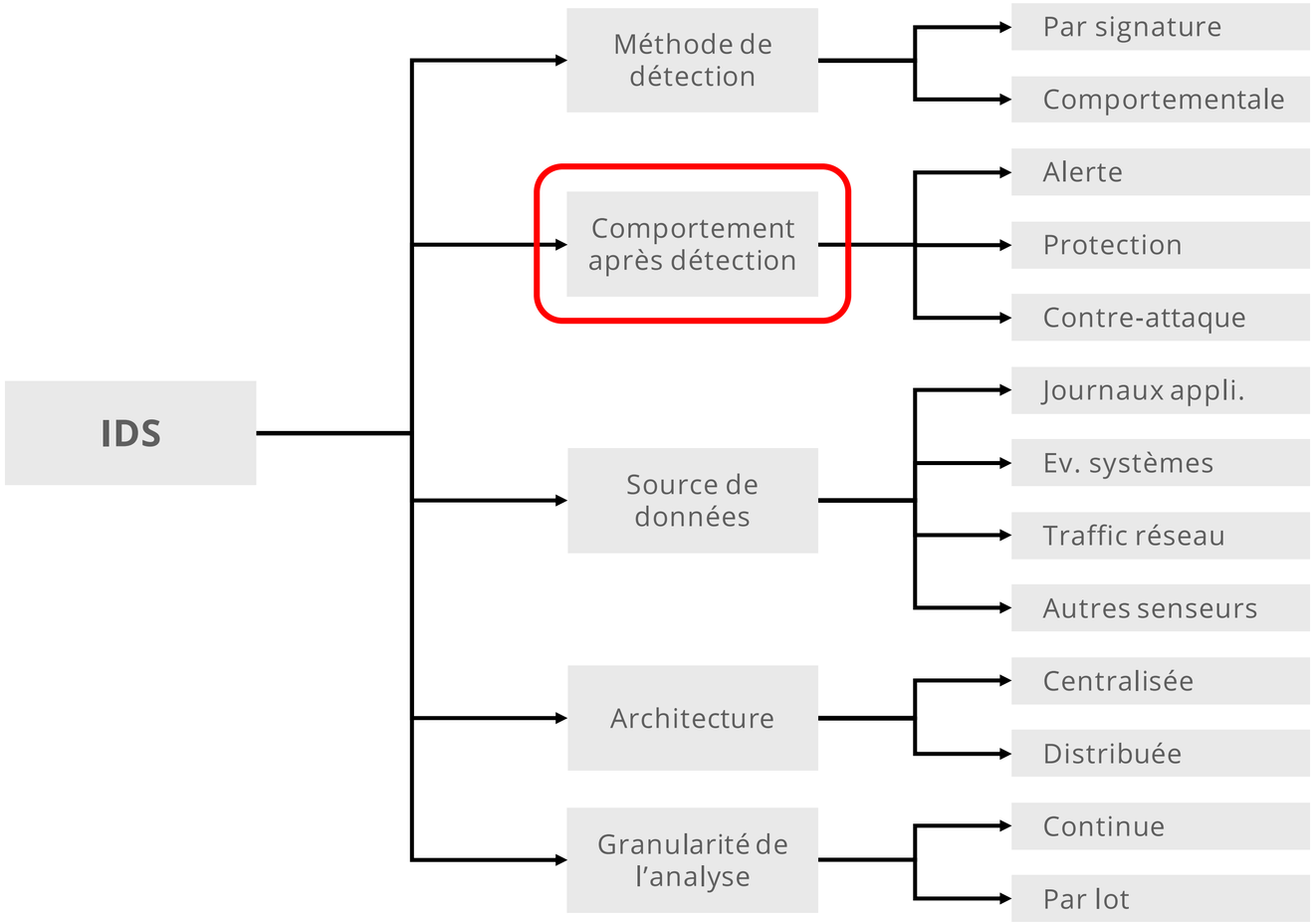
$\mathcal{M}, w_1 \models \neg\varphi$
$\mathcal{M}, w_1 \models \Box\Box\varphi$
$\mathcal{M}, w_2 \models \Box\varphi$
$\mathcal{M}, w_3 \models \Diamond\varphi$
$\mathcal{M}, w_5 \models \Box\varphi$
$\mathcal{M}, w_5 \models \Box\neg\varphi$

Détection par signatures

- Détection fiable des attaques connues.

- Seules les attaques pour lesquelles il y a des signatures sont détectée :
  - ↳ Maintenance lourde (il faut souvent mettre à jour les bases) ;
  - ↳ Relativement facile de passer inaperçu en modifiant la charge.

Classification



src L. Mé

Alerte

- Par la **journalisation** de l'événement (*log*), permettant notamment d'alimenter des outils tiers qui agrègent des événements venant de différentes sources pour les corréler (des SIEM par exemple) ;
- Par un indicateur niveau d'une **console de supervision** ;
- Par l'envoi **d'emails** ;
- Via des ***traps* SNMP**, des informations envoyées en utilisant le protocole SNMP depuis un équipement supervisé vers un serveur de supervision (UDP 162) ;

Plusieurs alertes consécutives de même nature peuvent être regroupées afin de faciliter leur traitement et, en particulier, ne pas « noyer » l'opérateur en charge de leur traitement.

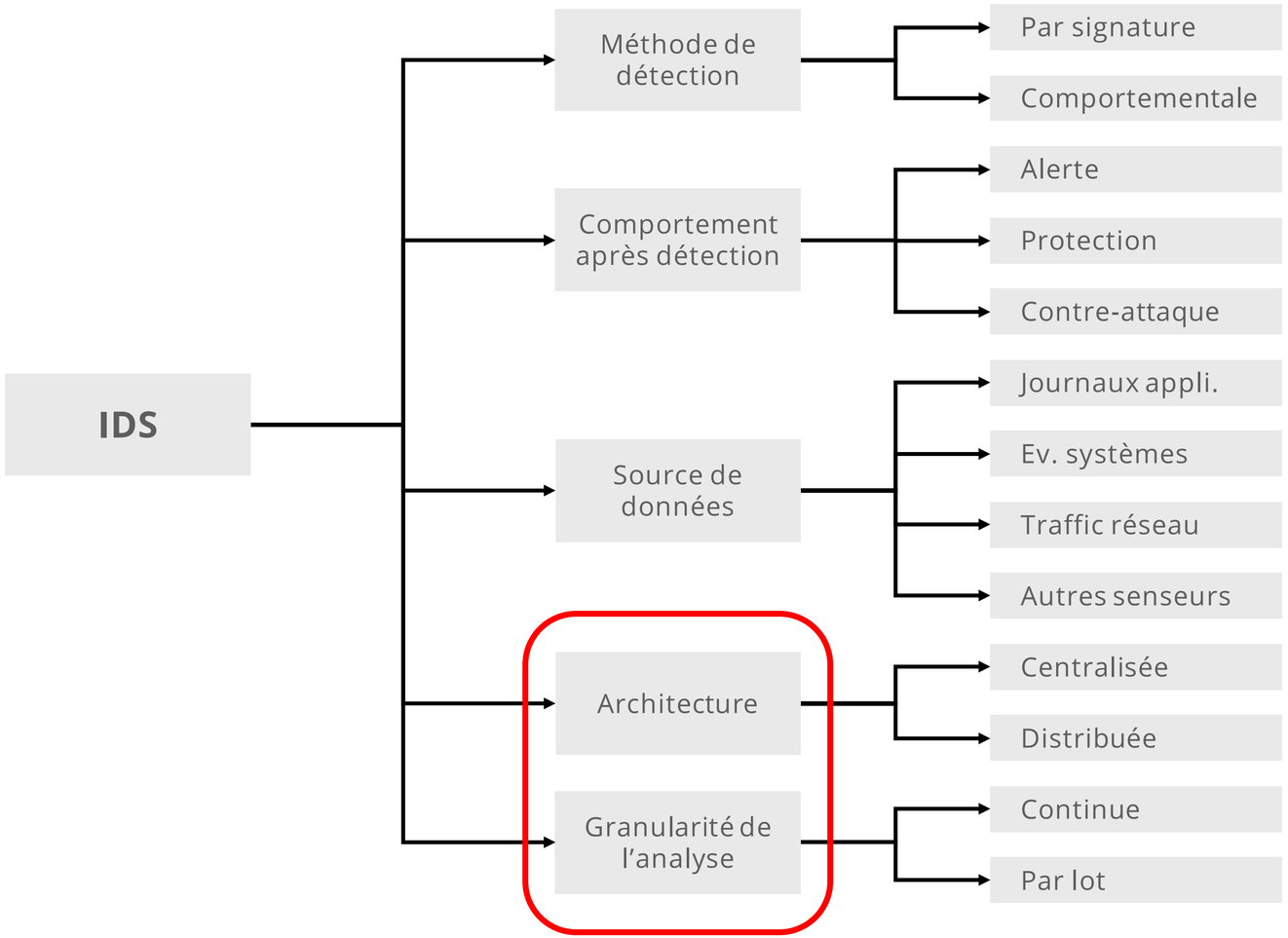
Protection

Dépend de la nature de l'IDS (H ou N) et de sa mise en œuvre :

- NIDS en coupure : bloque la communication et/ou envoie un RST pour terminer la connexion ;
- Autres NIDS : envoie un RST via un autre lien vers le réseau surveillé, mais le trafic dangereux est potentiellement quand-même arrivé à destination ;
- HIDS : « hook » les appels systèmes dangereux.

La contre-attaque est interdite.

Classification



src L. Mé

Architecture

Dépend de la nature de l'IDS (H ou N) et de sa mise en œuvre :

- NIDS en coupure : bloque la communication et/ou envoie un RST pour terminer la connexion ;
- Autres NIDS : envoie un RST via un autre lien vers le réseau surveillé, mais le trafic dangereux est potentiellement quand-même arrivé à destination ;
- HIDS : « hook » les appels systèmes dangereux.

La contre-attaque est interdite.

Produits, HIDS

Package	Year[1]	Ubuntu[2]	CentOS[3]	File	Network	Logs	Config	Sane defaults	Notes
unhide[14]	2012	Yes[15]	Yes[16]	No	No	No			proc ps compare
tripwire	2013	Yes[32]	Yes[33]	Yes	No	No			
Epylog[23]	2014	Yes[24]	Yes[25]	No	No	Yes			
Snort	2015	Yes[8]	Yes[9]	No	Yes	No			
SWATCH[26]	2015	Yes[27]	Yes[28]	No	No	Yes			
Samhain	2016	Yes[6]	No	Yes	No	Partial[7]		No	
aide	2016	Yes[30]	Yes[31]	Yes	No	No		No	
OSSEC	2017	Yes[4]	Yes[5]	Yes	Yes	Yes	Yes		
chkrootkit	2017	Yes[10]	No	Yes	No	Partial[11]			
rkhunter	2017	Yes[12]	Yes[13]	Yes	No	No	Yes	Yes	Ubuntu 18.04 LTS has some problems.
Sguil	2017	No	No	No	Yes	No			
Logwatch[17]	2017	Yes[18]	Yes[19]	No	No	Yes		No	
Logcheck[20]	2017	Yes[21]	Yes[22]	No	No	Yes		No	
sagan	2017	Yes[29]	No	No	No	Yes			

Proprietary software [edit]

Package	Year[34]	Linux	Windows	File	Network	Logs	Config	Notes
Lacework	2018	Yes	No	Yes	Yes	Yes	Yes	
Verisys	2018	Yes	Yes	Yes	Yes		Yes	
Nessus	2017	Yes	Yes				Yes	

Produits, NIDS

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems

Source: Gartner (January 2018)

Produits, NIDS Libres

Quelques-uns :

- **Snort** : appartient actuellement à Sourcefire, Snort est un des plus actifs NIDS Open Source et possède une communauté importante contribuant à son succès.

- **Suricata** : souvent considéré comme le successeur de Snort, d'ailleurs les outils valables pour Snort sont généralement compatibles. Il propose des performances élevées grâce au *multithreading*.

- **Bro NIDS** : conçu et maintenu par des centres de recherches. Utilise une approche comportementale pour la détection en concevant une cartographie du réseau afin d'en générer un modèle. Ce modèle est comparé en temps réel au flux de données et toute déviance lève une alerte.

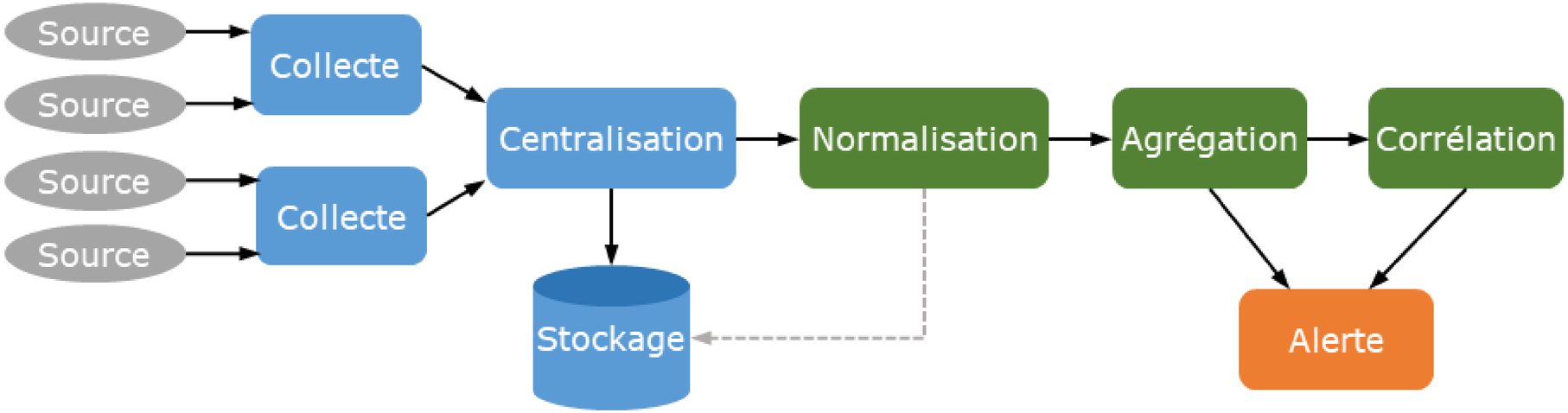
Le cas des SIEM

Il s'agit d'une solution utilisée pour la centralisation et la corrélation d'événements de sécurité présents dans les journaux d'audit des systèmes, applications et solutions de sécurité.

C'est la fusion de deux technologies :

- Les **SIM** (*Security Information Management*), qui centralisent et agrègent les événements de sécurité ;
- Les **SEM** (*Security Event Management*), qui réalisent des opérations de corrélation entre les événements pour détecter les intrusions.

SIEM, fonctionnement



La collecte

Ils prennent en entrée les événements du SI, les journaux système des équipements : pare-feux, serveurs, bases de données… sous différents formats (syslog, Traps SNMP, fichiers plats, etc.) ou nativement le format **IDMEF** (*Intrusion Detection Message Exchange Format*), spécialement conçu pour partager l'information qui intéresse un système de détection et protection aux intrusions.

Elle peut être **passive**, en mode écoute, ou **active** en mettant en place des agents directement sur les équipements ou à distance.

La synchronisation des horloges est essentielle pour la suite

Normalisation et agrégation

- Les traces sont normalisées sous un format plus lisible afin de permettre de faire des recherches multi-critères. Ce sont ces évènements qui seront éventuellement enrichis avec d'autres données puis envoyés vers le moteur de corrélation.
- Plusieurs événements normalisés peuvent être agrégés avant d'être transmis au moteur de corrélation. Ils peuvent aussi être à l'origine du déclenchement d'une alerte à ce stade (cas du SIM).

Corrélation et alerte

- C’est à ce niveau qu’interviennent les SEM.
- Les règles de corrélation permettent d'identifier un événement qui a causé la génération de plusieurs autres au niveau de points variés du système d’information.
- Elles permettent aussi de remonter une alerte via un trap, un e-mail, SMS ou ouvrir un ticket si la solution SIEM est interfacée avec un outil de gestion de tickets.

Stockage / Archivage

- Les traces brutes sont stockées sans modification pour garder leur valeur juridique ;
- Le stockage s'effectue généralement sur une période plus longue que pour les événements conservés « en ligne » ;
  - ↳ Permet de ressortir les données en cas de besoin (juridique notamment) ;
  - ↳ Permet de relancer une analyse a posteriori (fourniture de nouveaux indicateurs de compromission *IoC*) .

Produits

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (December 2017)

Produits Libres / Gratuits

- Prelude ;
- OSSIM ;
- ELK (Elasticsearch, Logstash, Kibana).

SOC / PDIS

Un SOC désigne une entité qui assure la sécurité de l'organisation. Il s'appuie sur la collecte des informations du système informatique grâce aux composants de sécurité mise en place, les analyser pour ensuite détecter d'éventuel anomalies. En cas d'incident détecté, le SOC va alerter l'entreprise (SOC externe) pour qu'elle déclenche son processus de gestion des incidents de sécurité ; ce processus peut-être directement initié par le SOC s'il est interne à l'organisation.

L'ANSSI a publié un référentiel d'exigences applicable aux prestataires de détection des incidents de sécurité (PDIS). Il s'agit d'un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir une qualification de leurs services dans ce domaine.

acceis

Merci de votre attention