Détection d’intrusion

M1 RSI

Objectifs pédagogiques

- Identifier les objectifs de la supervision du SI
- Réaliser un test d'intrusion
- Analyser des logs
- Mettre en place un système de détection d'intrusion (Snort)
- Proposer des scénarios d'attaque adaptés.

Qu’est ce qu’une intrusion ?

- Toute action ayant pour but de compromettre, un système informatique (machine, système d’exploitation, réseau) les objectifs de la sécurité.
- Cette action peut : avoir réussi, avoir échoué, être en cours, ou être une simple phase préparatoire [20].

Qu’est ce que la détection d’intrusion ?

- Analyser les informations collectées par les mécanismes d’audit de sécurité, à la recherche d’éventuelles attaques.
- Fait partie d'un système de protection total, et non pas une mesure de protection autonome

Qu’est ce qu’un système de détection d’intrusion

- IDS Intrusion Detection System
- Tout outil, méthode et ressource qui nous aident à prévoir ou identifier toute activité non autorisée dans un réseau.
- Détecte les activités (évènements) qui peuvent être une intrusion.

Les IDS, pourquoi ?

Pourquoi chercher des signes d'intrusion si nous somme protégés ?

- Les mécanismes de sécurité ne peuvent pas assurer une sécurité complète
- Déployer des systèmes sans failles est impossible
- Impossible de trouver et réparer toutes les failles de sécurité

- **Quelle confiance peut on avoir en un système de protection ?**
  - ➢ problèmes de configuration
  - ➢ matériel inadapté
  - ➢ erreur humaine
  - ➢ backdoor

Utilisation des IDS : objectifs divers

- **Rôle global dans une architecture de sécurité :**
  - Support pour les défenses
  - contrôle des politiques de sécurité
  - prévention quand son déploiement est connu (intimidation ?

- **Favoriser la mise en place de défenses adaptées**
  ➢ détection d'attaques inconnues
  ➢ détection de phases préliminaires d'attaques

- **Assainir un système**
  ➢ l'IDS peut mettre en avant certains comportements «polluants» du système : aide à l'administration classique

- **Rôle statistique**
  ➢ source d'informations pour la hi érarchie
  ➢ vision des menaces courantes

Comment détecter une intrusion ?

- **La détection d'intrusion consiste à mettre en œuvre les moyens permettant de mettre en évidence d' éventuelles intrusions :**
  - en surveillant l'activité du système (réseau, machine ou application) afin d'en recueillir les différents événements
  - en analysant ces événements à la recherche de signes suspects

- **Les IDS ont pour but d'automatiser ces phases de collecte d'information et d'analyse.**

Audit de sécurité

- Un événement c'est toute activité système produite suite à un ensemble d'action effectué à un moment donné par un utilisateur, processus ou application.

- Le journal d'audit de sécurité c'est le fichier qui enregistre par ordre chronologique tout ou une partie des événements produits dans un système donné

- journal d'audit permet de connaitre l'opération faite, l'utilisateur qui la fait, quand il la fait, les ressources système affectés par cette opération, l'utilisateur a pu terminer l'opération sinon pourquoi l'opération a échoué [4].

Les activités auditables du système

- D'après la politique de sécurité et le niveau de sécurité souhaité, l'administrateur peut définir des événements auditables correspondants à certaines informations qui peuvent être [4] :
- **Un accès au système:** qui a accédé au système? Quand? Où ? et comment?
- **Un usage des ressources système**: les informations relatives à l'utilisation des ressources système: commandes système, CPU, RAM, les entrées/sorties.
- **Un usage des fichiers** : comprend toutes les informations concernant l'accès aux fichiers comme l'horodatage de l'accès, type d'accès, source d'accès…etc.
- **Des événements liés aux applications**: événements engendrés par des applications comme le lancement et l'arrêt des applications, les entrées utilisés et les sorties produites…etc.
- **Les violations éventuelles de la sécurité**: tentatives d'accès non autorisé à des ressources système comme l'exécution d'une application ou d'une commande en mode privilégie, changement des droits d'accès …etc.
- **Les statistiques du système**: informations de nature statistique qui peuvent nous aider à repérer toute activité anormale comme les statistiques sur le nombre de tentatives d'accès refusés.

La collecte des évènements

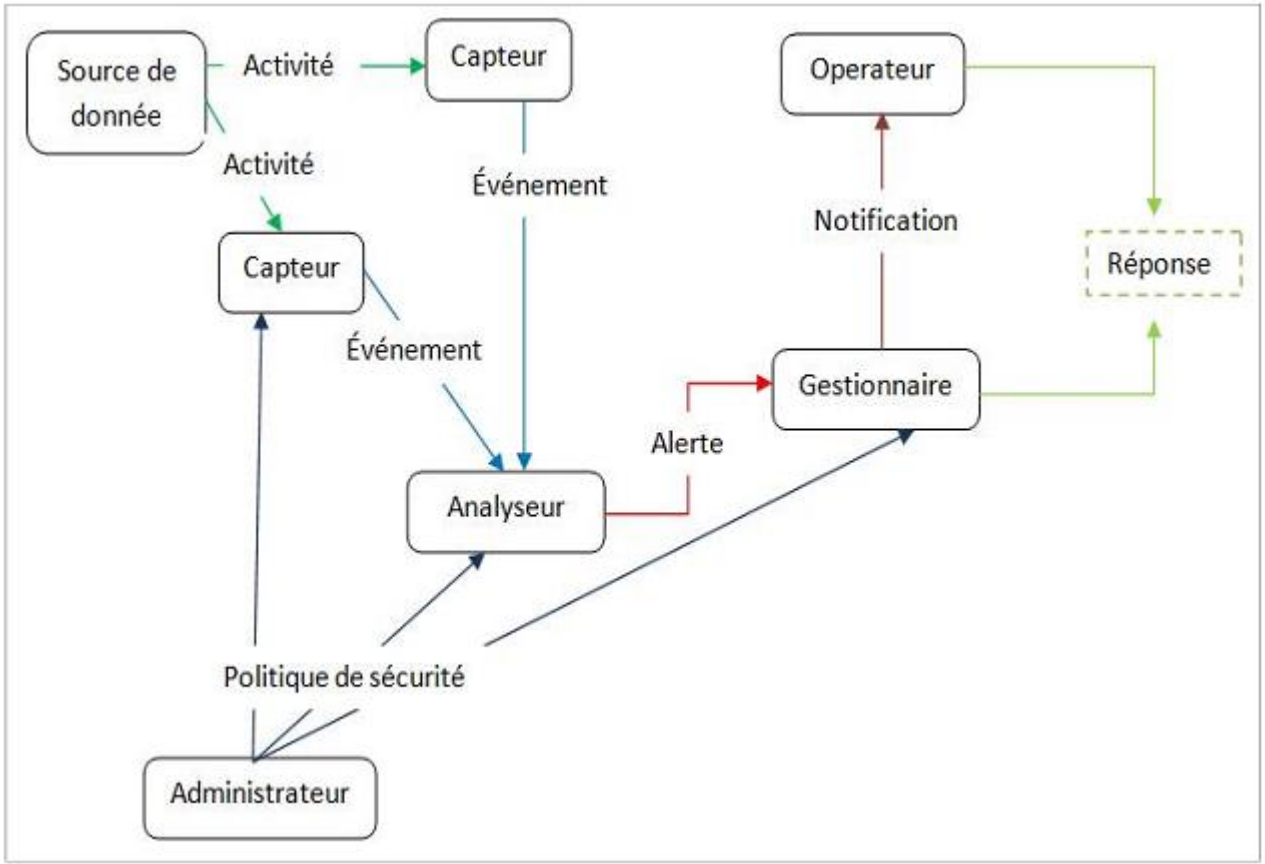
- Les systèmes d'exploitation actuels possèdent un mécanisme d'audit capable de générer certains types d'événement.
- le noyau garantit la génération et la collecte de ces événements.
- les applications, les développeurs doivent se munir d'un ensemble de primitives de génération et de collecte des événements [4].

L’analyse du journal d’audit

- L ’analyse des journaux d’audit peut être faite soit en temps réel ou en temps différé.
- Il est recommandé de surveiller le système en temps quasi réel.
- Dans le cas d’un réseau, il faut créer un fichier d’audit global qui regroupe les différents audits collectés des différentes machines du réseau [4].
- Certains types d’attaques tentent de modifier le journal d’audit afin d’effacer toute trace qui peut révéler cette attaque.
- Pour traiter ce problème, il est nécessaire de protéger le journal d’audit contre toute tentative de modification par des utilisateurs non autorisés.
- Dans le cas d'un réseau informatique, il faut protéger non seulement le fichier global d’audit, mais aussi le transfert des informations auditées [4].

Le modèle d'un IDS (IDWG)

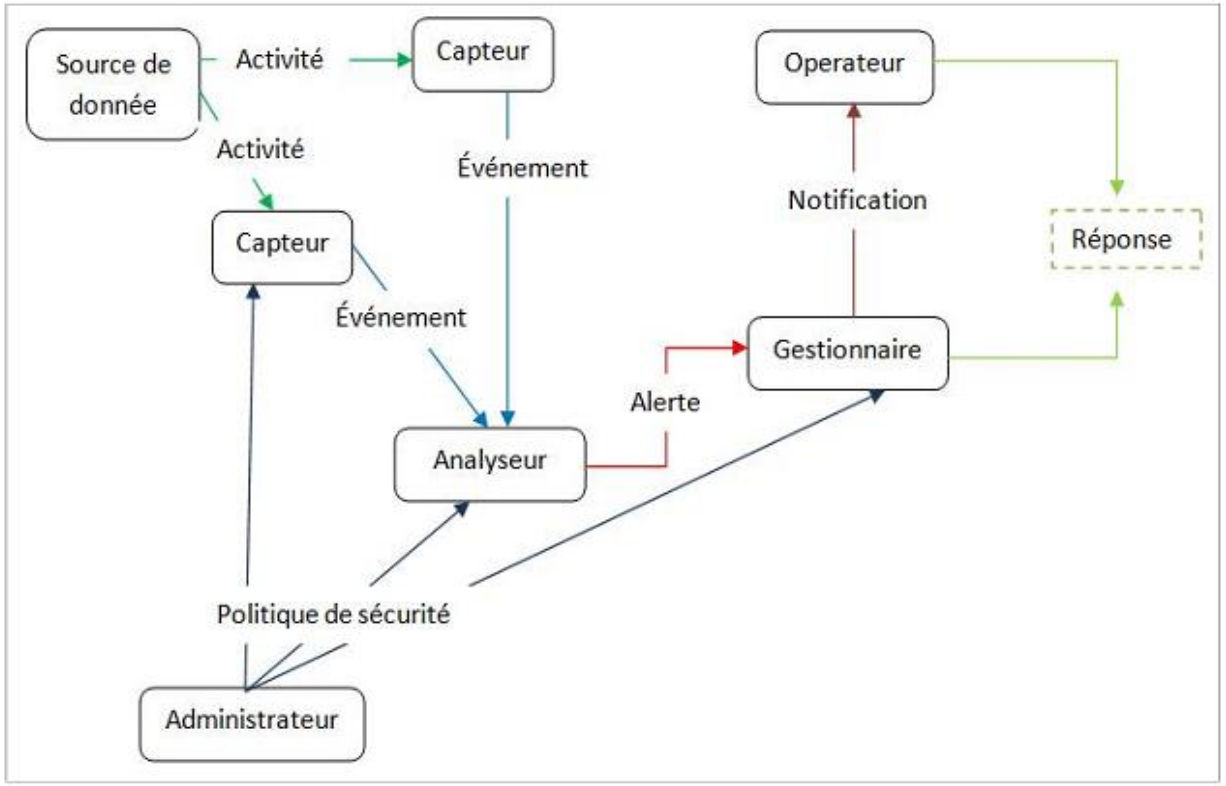
L'administrateur: c'est le responsable de l'établissement de la politique de sécurité de l'organisation, donc celui qui déploie et configure l'IDS. Cette personne peut ou peut ne pas être l'opérateur de l'IDS.



Le modèle d'un IDS (IDWG)

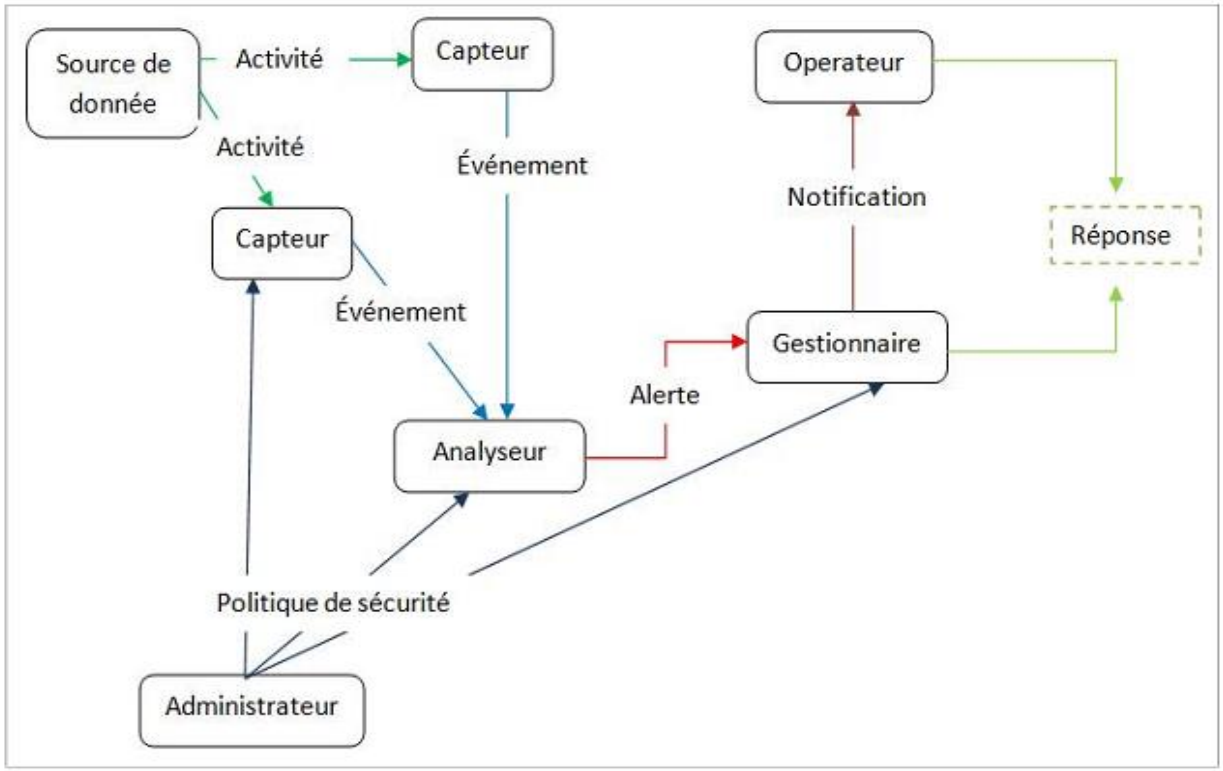
- **La source de données**: les paquets bruts du réseau, les journaux d'audit du système d'exploitation, les journaux d'audit d'applications et les données de contrôle générées par le système.

- **L'activité**: Par exemple, les entrées des fichiers journaux du système d'exploitation montrant un utilisateur qui tente d'accéder à des fichiers auxquels il n'est pas autorisé … etc.

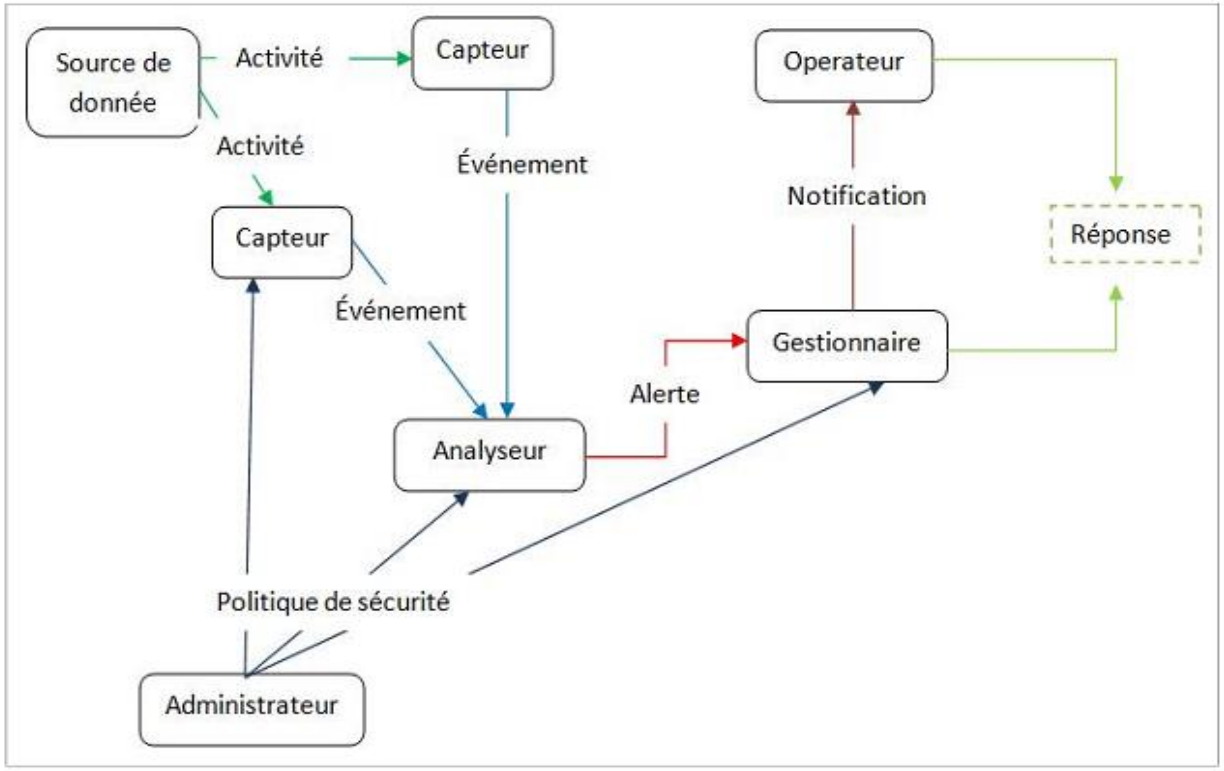


Le modèle d'un IDS (IDWG)

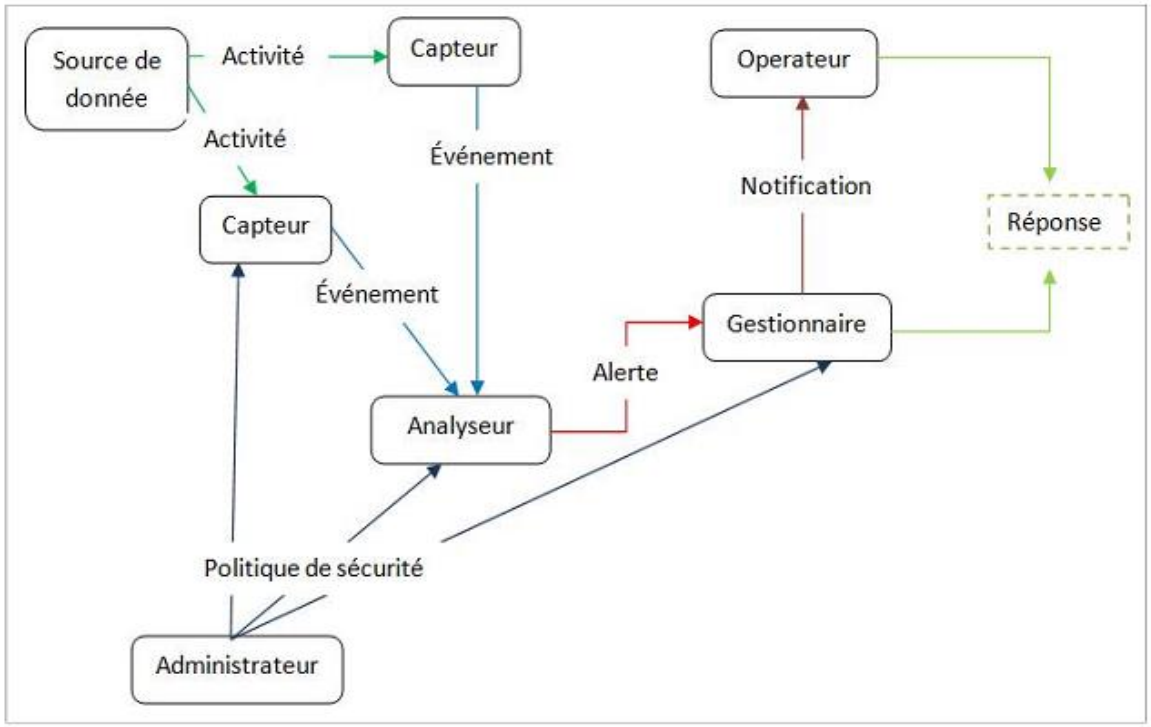
- **Le capteur**: le composant qui collecte des données à partir de la source de données. Le capteur (souvent simple hôte) est mis en place pour transférer des événements à l'analyseur.
- **L'événement**: toute occurrence détectée dans la source des données par un capteur et qui peut donner lieu à une alerte.



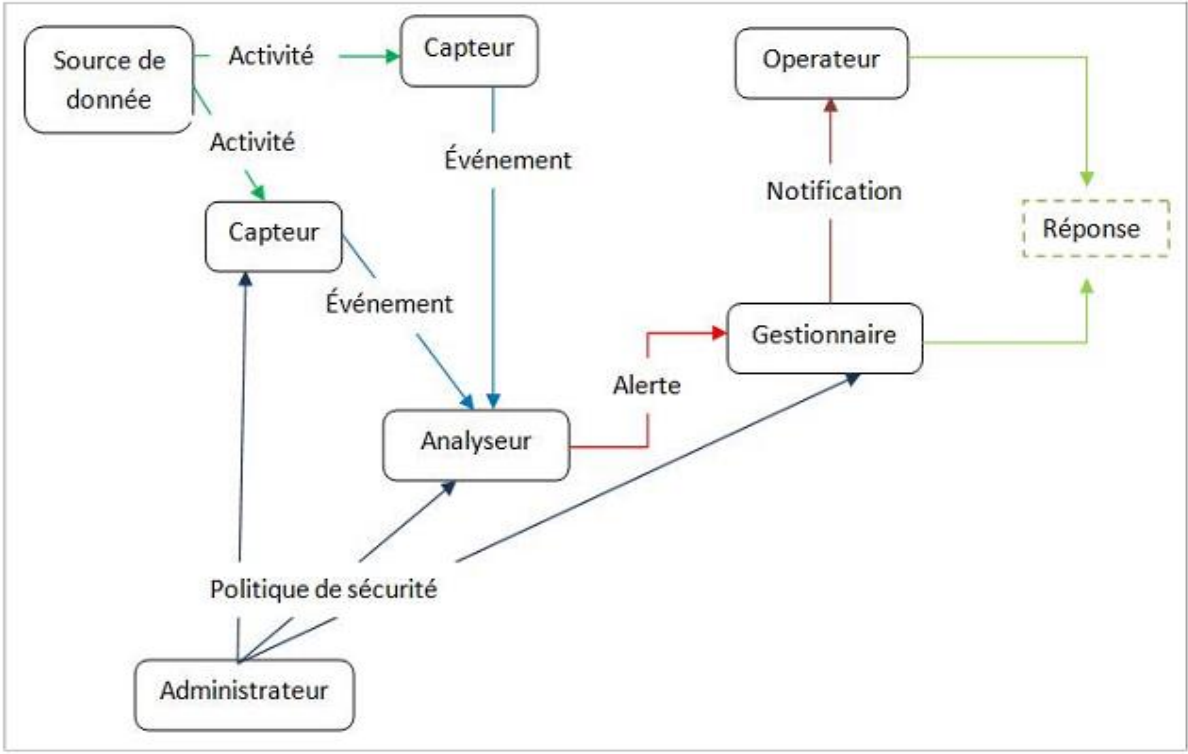
- **L'analyseur** : composant clé, il analyse les données collectées par le capteur pour signaler les activités non autorisées,
- **L'alerte** : c'est un message qui passe de l'analyseur au gestionnaire pour lui informer qu'un événement d'intérêt a été détecté.
- **Sonde** : un ou des capteurs couplés avec un analyseur forment une sonde.



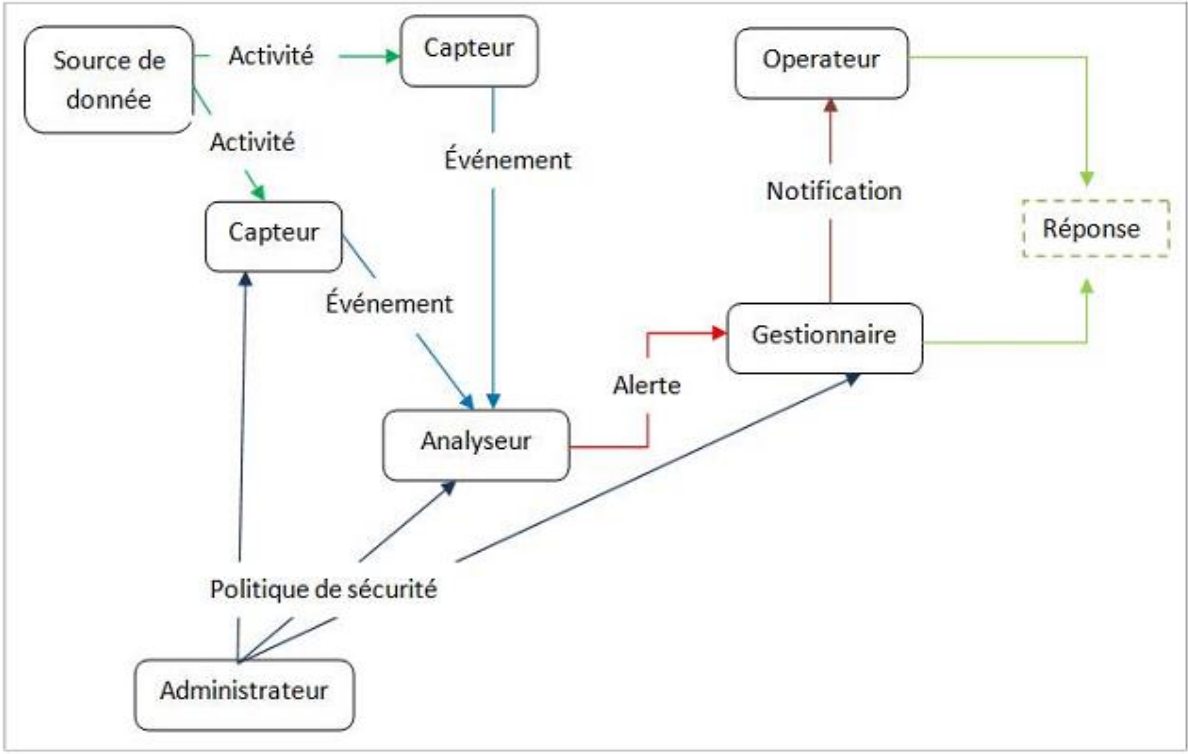
- **Le gestionnaire**: le processus à partir duquel l'opérateur gère les différents composants du système. Les fonctions du gestionnaire comprennent généralement:
  - la configuration du capteur,
  - la configuration de l'analyseur
  - la gestion de la notification d'événements, gestion des rapports.



- **La notification**: méthode avec laquelle le gestionnaire de l'IDS informe l'opérateur de la survenance d'une alerte.
- Par exemple: l'affichage d'une icône colorée sur l'écran du gestionnaire de l'IDS, l'envoi d'e-mail, ou la transmission d'un Simple Network Management Protocol (SNMP) trap…etc.

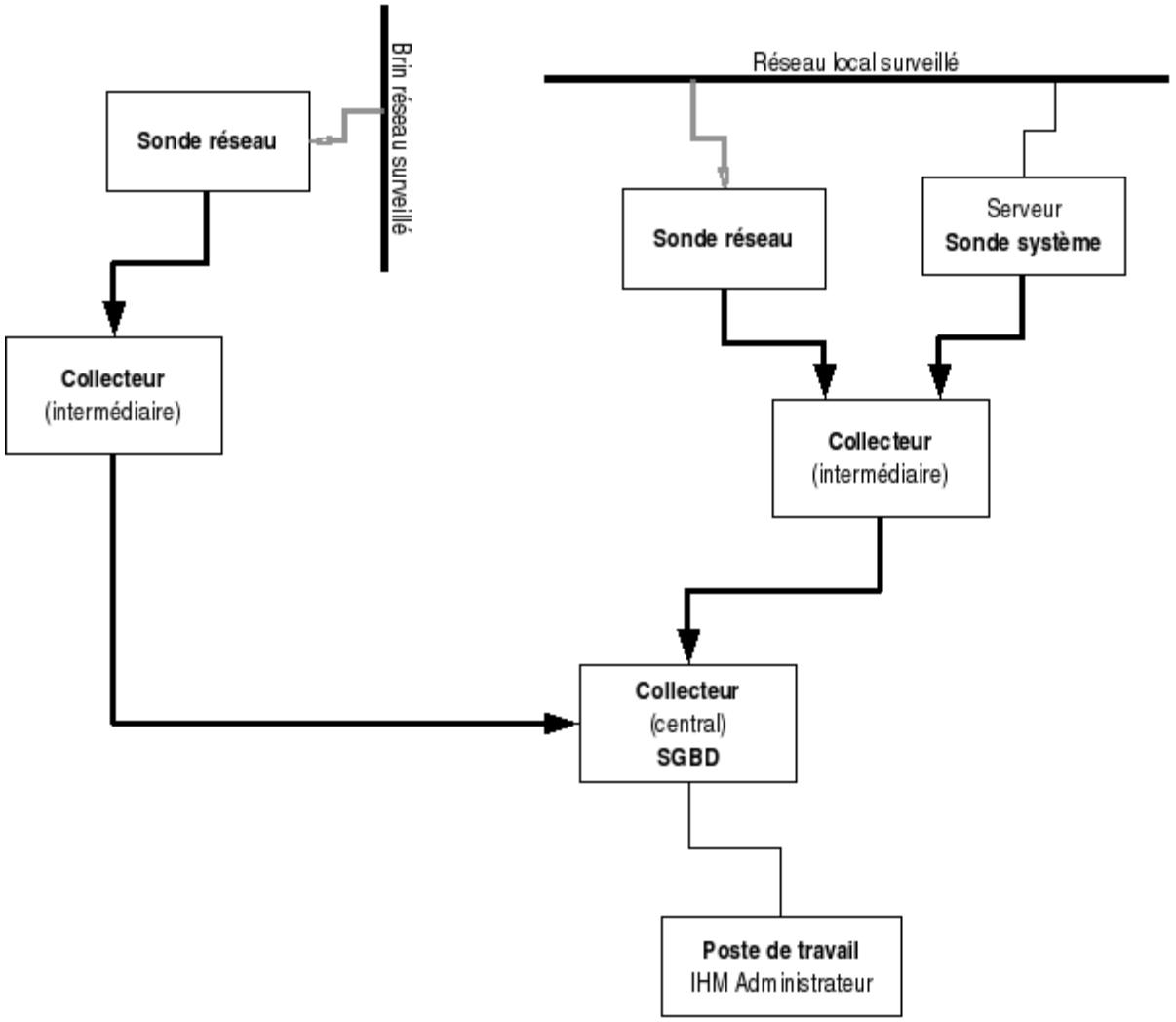


- **L’opérateur**: c’est l'utilisateur principal du gestionnaire de l’IDS.
- Surveille souvent la sortie du système de détection d’intrusion et déclenche ou recommande d’autres actions.



- **La réponse** : c’est les mesures prises comme réponse à un événement.
- Les réponses peuvent être effectuées automatiquement par une entité dans l'architecture de l’IDS ou peuvent être initiées par un humain.
  - L'envoi d'une notification à l'opérateur
  - la journalisation de l'activité, l'enregistrement des données qui ont caractérisé l'événement,
  - l’arrêt du réseau ou de l'utilisateur ou la session de l’application,
  - la modification des contrôles d'accès réseau ou système.

Exemple d'architecture



Exemple d’architecture

- Un IDS avec trois sondes: deux sondes réseau et une sonde système. Les deux sondes réseaux sont déployées à des endroits différents, l'une au niveau du réseau interne, l'autre dans un point réseau intéressant.
- La sonde système peut être associée à un serveur de centralisation de traces mis en place sur le réseau local.
- Les collecteurs intermédiaires ont été ajoutés à proximité de deux groupes de sondes : la sonde réseau surveillant le brin réseau distant, et les deux sondes réseau et système s'intéressant au réseau interne.
- Ces deux collecteurs intermédiaires propagent ensuite les traces vers un collecteur central associé à un SGBD sur lequel les administrateurs de sécurité peuvent consulter et traiter les alertes [14].
- Dans la pratique, ces collecteurs intermédiaires n'apparaissent généralement pas explicitement. Ils correspondent plus ou moins aux capacités de stockage temporaire et de transmission en différée

Alerte et fausse alerte

- les vrais négatifs et vrais positifs correspondent aux comportements souhaités.
- faux négatif correspond à une attaque non détectée,
- faux positif à l'émission d'une fausse alerte.

	Pas d'alerte	Alerte
Pas d'attaque	Vrai négatif	Faux positif
Attaque en cours	Faux négatif	Vrai positif

HIDS: IDS basé sur l'hôte

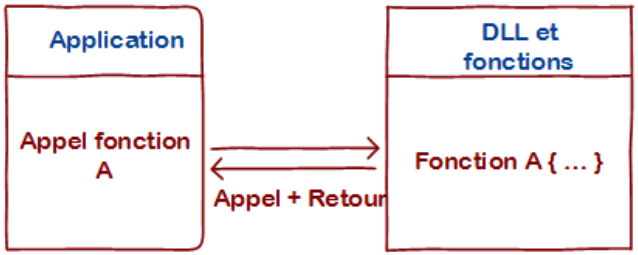
- HIDS (Host-based IDS)
- surveille le système sur lequel il est installé
- contrôle et analyse les activités et les informations concernant l'hôte
- Type d'attaques (locales):
  - élévation de privilèges (privilege escalation)
  - débordements de tampon (buffer overflows)
- Données d'audit
  - Système d'exploitation: appels système, informations sur des fichiers, et des logs,…
    - fiable parce qu'elles représentent des évènements de bas niveau
    - **Exemple**: Syslog est un service d'audit et de journalisation standard sur les systèmes Unix et Linux
  - Applications

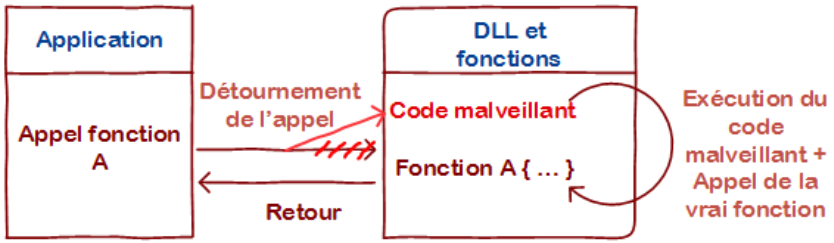
HIDS : mécanismes / types

- Les HIDS possèdent tout ou partie des mécanismes suivants :
  - **Surveillance des fichiers journaux (log analysis).**
    - Exemple : logcheck, logwatch, swatch, OSSEC...
  - **Contrôles d'intégrité des fichiers (file integrity checks)**
    - Exemple : tripwire, samhain, AIDE, mtree, OSSEC...
  - **Détection de rootkits (system integrity checks)**
    - Exemple : OSSEC, chrootkit, rootkithunter...
  - **Détection de comportements douteux (scans, étude des syscalls...)**
    - Exemple : portsentry, scanlogd, lids, systrace...

RootKit

- un “*kit*” permettant de devenir “*root*“, c’est à dire d’avoir les privilèges les plus élevés sur la machine.
- Un **rootkit** s’apparente en effet plus à une technique et un principe de dissimulation afin de passer inaperçu qu’à un logiciel à part entière.
  - Exemple: cheval de Troie
- Hooking





- Modes
  - **Utilisateur**: utilisent les applications et leurs privilèges pour s’exécuter
  - **Noyau** : couches basses du traitement de données

Surveillance des Logs

- Logcheck, par défaut, s'exécute toutes les heures et après chaque redémarrage.
  - Il analyse les logs (exemple : syslog et auth.log) à la recherche de patterns (motifs d'intrusion).
- Le moteur d'OSSEC se base sur un fonctionnement par patterns.
  - Dans les règles décrites, il est possible de spécifier de ne lever une alerte que si un pattern a déjà été repéré précédemment, dans un espace-temps défini.
- **Exemple**

```
<rule id="1608" level="13" timeframe="120">
<regex>^sshd[\d+]: fatal: Local: crc32 compensation attack</regex>
<if_matched_regex>^sshd[\d+]: \.+Corrupted check by bytes on</if_matched_regex>
<comment>SSH CRC-32 Compensation attack</comment>
<info>http://www.securityfocus.com/bid/2347/info/</info>
</rule>
```

Contrôle d'intégrité: *Comparaison avec des copies*

- Conserver des copies des fichiers critiques,
- périodiquement comparer le fichier sur le système et la copie.
- la méthode la plus apte à détecter s'il y a eu modification, et quelle modification.
- Limites:
  - requiert de l'espace de stockage pour conserver les copies et des ressources système pour effectuer les comparaisons.
  - Il est primordial que les copies ne puissent être altérées

Contrôle d’intégrité: Comparaison d'attributs du fichier

relever des champs caractéristiques des fichiers à contrôler:

- propriétaire, droits, taille, dates de création, de dernière modification.

- comparer ces champs aux valeurs originales, et éventuellement relever les modifications anormales.
- Détecter des modifications autres que celles du contenu du ficher.
- **Limites:**
  - ne permet pas de voir quelles ont été les modifications apportées aux fichiers.
  - Là encore, les données de référence doivent être fiables

Contrôle d'intégrité: *Comparaison de signatures*

- calculer une signature de chaque fichier à protéger, avec une fonction de hachage (md5).
- comparer périodiquement le checksum courant du fichier avec la valeur originale.
- permet la détection de modifications du contenu d'un fichier, pas de ses attributs.
- plusieurs algorithmes de hachage (notamment CRC32, SHA-1 et MD5).
- la base de données contenant les hashs doit être stockée sur un support amovible et de préférence non altérable.

Avantages et inconvénients

- Avantages :
  - l'impact d'une attaque peut être constaté et permet une meilleure réaction,
  - des attaques dans un trafic chiffré peuvent être détectées (impossible avec un IDS réseau),
  - les activités sur l'hôte peuvent être observées avec précision, etc.
- Inconvénients
  - les scans sont détectés avec moins de facilité ;
  - ils sont plus vulnérables aux attaques de type DoS

Les systèmes de détection réseau NIDS

- NIDS Network-based Intrusion Detection System
- Rôle: l'analyse et l'interprétation des paquets circulant sur le réseau.
- Les NIDSs sont installés dans des points stratégiques du réseau tels:
  - les périphériques réseau (pour contrôler les flux échangés avec l'extérieur).
  - au cœur du réseau afin de permettre le contrôle du comportement des utilisateurs internes et rechercher d'éventuelles intrusions
- Il est capable de détecter des paquets malveillants conçus pour outrepasser un pare-feu, et de chercher des signes d'attaque à différents endroits sur le réseau.

NIDS: données d'audit

- **Les informations SNMP :** protocole permettant de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
  - MIB (Management Information Base) contient les informations de configuration ainsi que les informations liées à la performance du réseau.
  - La MIB représente une intéressante source d'audit pour les systèmes de détection d'intrusion
- **Les paquets réseau :** les sniffeurs réseau représentent aussi une source de données
- **Les fichiers logs des applications** : les fichiers logs des applications sont devenus une source d'information pour les systèmes de détection d'intrusion.

NIDS: Surveillance du réseau

- Des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque.
- Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traite éventuellement.
- Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console
- Les capteurs sont placés sur le réseau en mode furtif, de façon à être invisibles aux autres machines.
- Un capteur possède en général deux cartes réseaux:
  - une placée en mode "promiscuous",
  - l'autre permettant de le connecter à la console de sécurité.

Placement des capteurs

- **Derrière le pare-feu** : permettent de détecter les intrusions qui n'ont pas été arrêtées par le pare-feu.
- **Avant le pare-feu** :
  - servent à détecter toutes les attaques en direction du réseau,
  - contrôlent le fonctionnement et la configuration du pare-feu
- **Zone sensible** : à l'entrée de zones du réseau particulièrement sensibles (parcs de serveurs, données confidentielles…), de façon à surveiller tout trafic en direction de cette zone

Analyse des paquets

- L'analyse considère différentes couches, chacune étant en mesure de fournir des informations pertinentes.
- L’analyse protocolaire :
  - anomalies au niveau de l'entête d'un paquet : combinaisons exotiques des flags TCP
  - incohérences des numéros de séquence et d'acquittement TCP
  - mauvais checksum, mauvaise taille de paquet, adresse incohérente

Analyse des paquets

- **L'analyse des données** : Il s'agit ici de rechercher dans les données (payload) des chaînes de caractères suspectes, correspondant à des attaques connues.
- D'abord un premier tri selon le protocole et les ports impliqués est effectué (protocole applicatif).
- Ensuite, mener une investigation concernant les attaques connues propres au protocole applicatif en question.
- Exemple:
  - si le protocole de couche 4 est TCP et le port est 80, alors le protocole applicatif est http.
  - Si de plus la requête, dans l'url, contient la chaîne *cmd.exe*, alors il s'agit vraisemblablement d'une attaque.
  - Une alerte sera alors levée au vu d'une requête type : *http://www.serveur.net/chemin/vers/cmd.exe*.

L'analyse de flux

- Il s'agit d'une approche comportementale, qui permet de déterminer quelle activité est normale sur le réseau, quelle activité est suspecte.
- L'objet de l'analyse devient le flux : connexion TCP, échange UDP, etc.
- L'IDS dans ce cas surveille :
  - qui communique avec qui ?
  - avec quels protocoles ?
  - la quantité des données échangées ?
  - y a-t-il des spécificités temporelles ?

NIDS Avantages et inconvénients

- Avantages :
  - les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic et permettent donc une surveillance discrète du réseau
  - les attaques de type scans sont facilement détectées,
  - il est possible de filtrer le trafic.
- Inconvénients:
  - conserver toujours une bande passante suffisante pour l'écoute de l'ensemble des paquets,
  - bien positionner l'IDS pour qu'il soit efficace.
  - la probabilité de faux négatifs est élevée et il est difficile de contrôler le réseau entier.
  - Difficile de voir l'impact d'une attaque.