Méthodes de détection intrusion

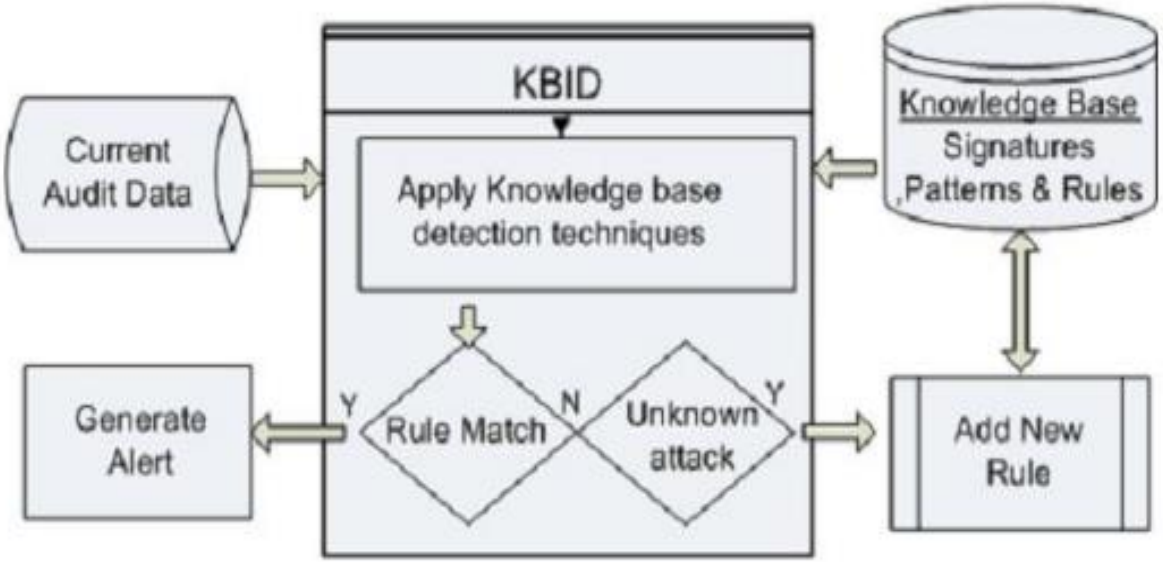
Détection par signature (par scénario)

- Rechercher dans l'activité du système surveillé les empreintes d'attaques connues.
- Des règles qui:
  - décrivent les usages non désirés;
  - s'appuient sur des intrusions passées ou des faiblesses théoriques connues;
  - faites pour reconnaître un seul événement ou une séquence d'événements représentant un scénario d'intrusion;
- L'efficacité de cette détection repose sur l'acuité et la couverture de toutes les intrusions possibles par les règles.

Détection par signature (par scénario)

- Repose sur une base de signatures d'intrusion
- Recherche ces signatures dans le journal d'audits.
- Si un événement correspond à une signature de la base, l'alerte correspondante est levée
- Faible taux de faux positifs pour une signature pertinente,
- cependant l'attaque doit être connue pour être détectée.

Détection par signature (par scénario)

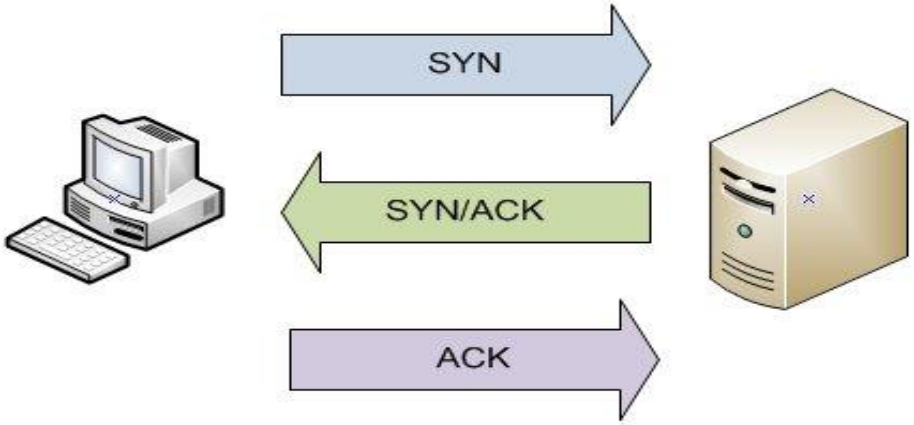


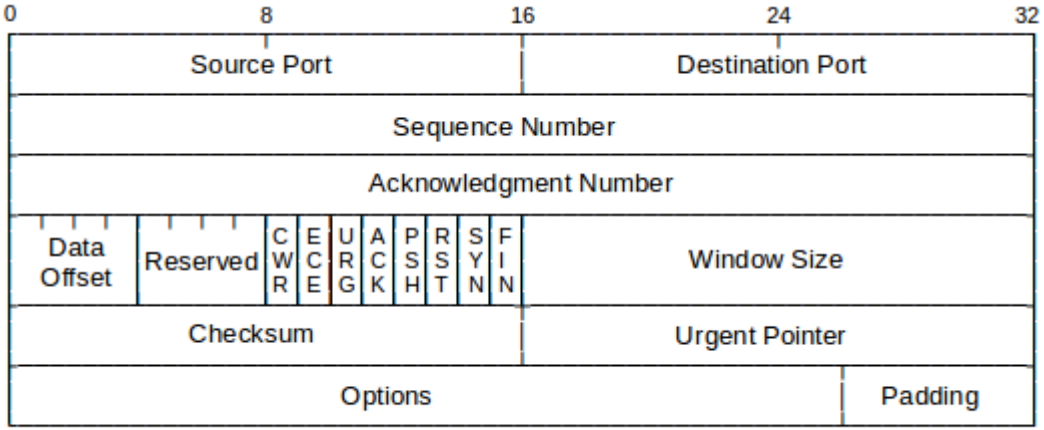
Techniques

- **Systèmes experts**
- Coder les signatures de malveillance avec des règles d'implication ***si . . .alors***.
- Les signatures décrivent un aspect d'une attaque ou d'une classe d'attaque.
- Nouvelles règles pour détecter de nouvelles attaques.
  - Les règles deviennent généralement très spécifiques au système cible et donc sont peu portables.
- **Analyse des transitions d'états**
- Consiste à créer un modèle tel qu'à l'état initial le système ne soit pas compromis.
- L'intrus accède au système. Il exécute une série d'actions qui provoquent des transitions sur les états du modèle, qui peuvent être des états ou l'on considère le système compromis.
- Cette approche de haut niveau peut reconnaître des variations d'attaques qui passeraient inaperçues avec des approches de plus bas niveau.

Exemple: TCP SYN Scan

Envoyer sur chaque port ciblé un paquet TCP SYN
En temps normal (si le port est ouvert), le serveur va renvoyer un SYN\ACK





Exemple: TCP SYN Scan

Attaque:

- Envoyer sur chaque port ciblé un paquet TCP SYN
- En temps normal (si le port est ouvert), le serveur va renvoyer un SYN\ACK

Exemple 1: TCP SYN Scan (Scenario 1)

Les paquets contenant cette attaque avaient les caractéristiques suivantes :

- Diverses adresses IP sources
- TCP port source 21, port destination 21 (réflexifs)
- Type of service 0
- Flags SYN et FIN positionnés
- Numéros de séquence divers
- Numéros d'acquittement divers
- La taille de la fenêtre est fixe (1028), alors qu'elle est normalement négociée
- Le flag d'acquittement n'est pas positionné, pourtant un numéro d'acquittement est défini
- le numéro d'identification du paquet est toujours le même (39426)

Exemple 1: TCP SYN Scan

- Ce paquet comporte donc de nombreuses caractéristiques qui peuvent être exploitées pour former une signature de détection de cette attaque.
- On va donc conserver ses caractéristiques les plus saillantes afin de limiter le temps d'analyse des paquets (en effet, plus il y a de paramètres à analyser, plus cette analyse va durer).
- On va prendre les trois paramètres les plus adaptés pour détecter cette attaque :
  - Uniquement les flags SYN and FIN positionnés
  - Numéro d'identification IP 39426
  - Taille de la fenêtre TCP 1028

Exemple 2: TCP SYN Scan (Scenario 2)

- Une caractéristique commune (flag ACK non positionné et valeur d'acquittement non nulle)
- Flags SYN et FIN positionnés pour la première attaque
- Taille de fenêtre inférieure à un seuil (incluant 40 octets) pour la deuxième.
  - Valeur d'acquittement non nulle et flag ACK non positionné
  - Flags SYN et FIN positionnés
  - Taille de la fenêtre TCP en dessous d'une certaine valeur

Exemple 2: TCP SYN Scan (Scenario 2)

- Très semblables à la première attaque, mais suffisamment différente pour ne pas être détectée par la signature.
- Elaborer une nouvelle signature qui permettrait de détecter les deux attaques ainsi que les variantes qui pourraient survenir.
- Les différences entre la première et la deuxième attaque :
  - Seulement le flag SYN positionné
  - La taille de la fenêtre TCP fixée à 40
  - Port 53

Exemple: TCP SYN Scan (Scenario 2)

- les sites des vendeurs d'IDS proposent des mises à jour des signatures en fonction des nouvelles attaques identifiées.
- Néanmoins, plus il y a de signatures différentes à tester, plus le temps de traitement sera long, l'utilisation de signatures plus élaborées peut donc procurer un gain de temps appréciable.

Exemple: Autres TCP scan

- le **TCP XMAS scan** envoie des paquets TCP avec les **flags URG, PUSH et FIN à 1** dans le but de déjouer certains pare-feu ou mécanismes de filtrage.
- lors d'un envoi de paquet avec ces trois flags activés, un service actif derrière le port visé ne renverra aucun paquet.
- En revanche, si le port est fermé, nous recevrons un paquet **TCP RST/ACK**. On saura alors différencier le comportement d'un port ouvert et d'un port fermé pour lister les ports sur une machine :

Exemple: TCP Null scan

- À l'inverse du TCP XMAS scan, le **TCP Null scan** va envoyer des paquets TCP scan avec tous les flags à 0.
- Il s'agit là aussi d'un comportement que l'on ne trouvera jamais dans un échange normal entre des machines
- L'utilisation de ce scan peut, comme le TCP XMAS scan, perturber certains firewalls ou modules de filtrage et alors laisser passer les paquets :

Limites

- Ne peut détecter que les attaques dont il ne possède pas la signature. De ce fait, il nécessite des mises à jour fréquentes. De plus, l'efficacité de ce système de détection dépend fortement de la précision de sa base de signature
- Base de signatures difficiles à construire.
- Pas de détection d’attaques inconnues.

Détection comportementale

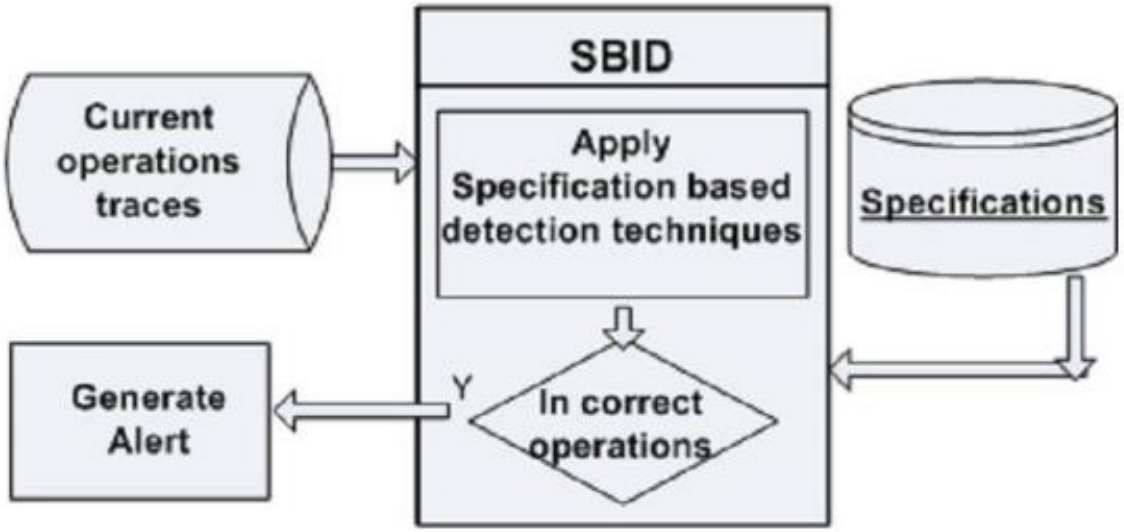
- le comportement actuel du système est-il cohérent avec son comportement habituel ?
- l'exploitation d'une faille du système nécessite une utilisation anormale de ce système, et donc un comportement inhabituel de l'utilisateur.
- Nécessite une phase d'apprentissage au cours de laquelle l'IDS apprendera le comportement normal.
- Il est ainsi en mesure de signaler les divergences par rapport au fonctionnement de référence.

Détection comportementale

- Les modèles comportementaux peuvent être élaborés à partir d'analyses statistiques.
- Ils présentent l'avantage de détecter des nouveaux types d'attaques.
- fréquents ajustements sont nécessaires afin de faire évoluer le modèle de référence de sorte qu'il reflète l'activité normale des utilisateurs et réduire le nombre de fausses alertes

Détection basée sur la spécification

- Dans cette approche, un ensemble de règles et contraintes de fonctionnement du système sont spécifiés,
- les intrusions sont détectées comme des violations de ces règles de fonctionnement.



Exemple 1 : Détection à base de spécification

- Le diagramme états-transitions suivant représente la spécification du protocole DHCP, il modélise le comportement normal du protocole.
- Tout état ou transition non spécificité dans le diagramme est considér

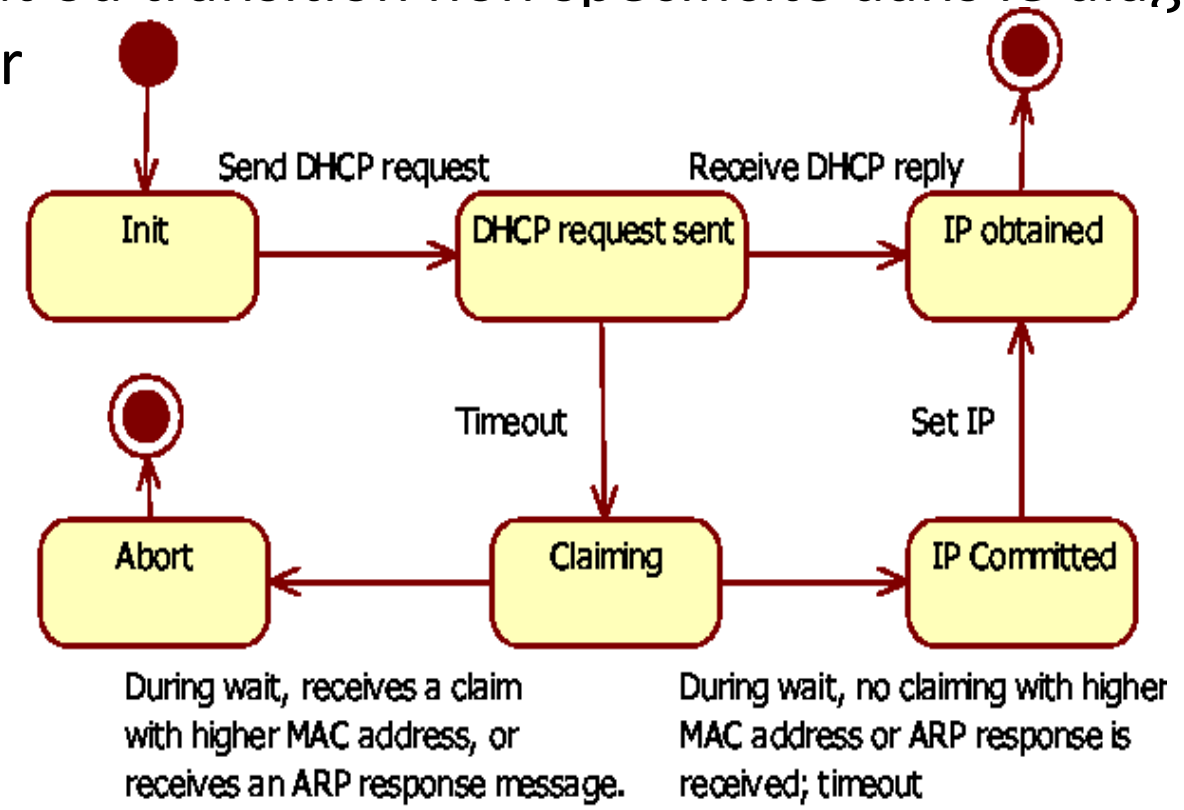
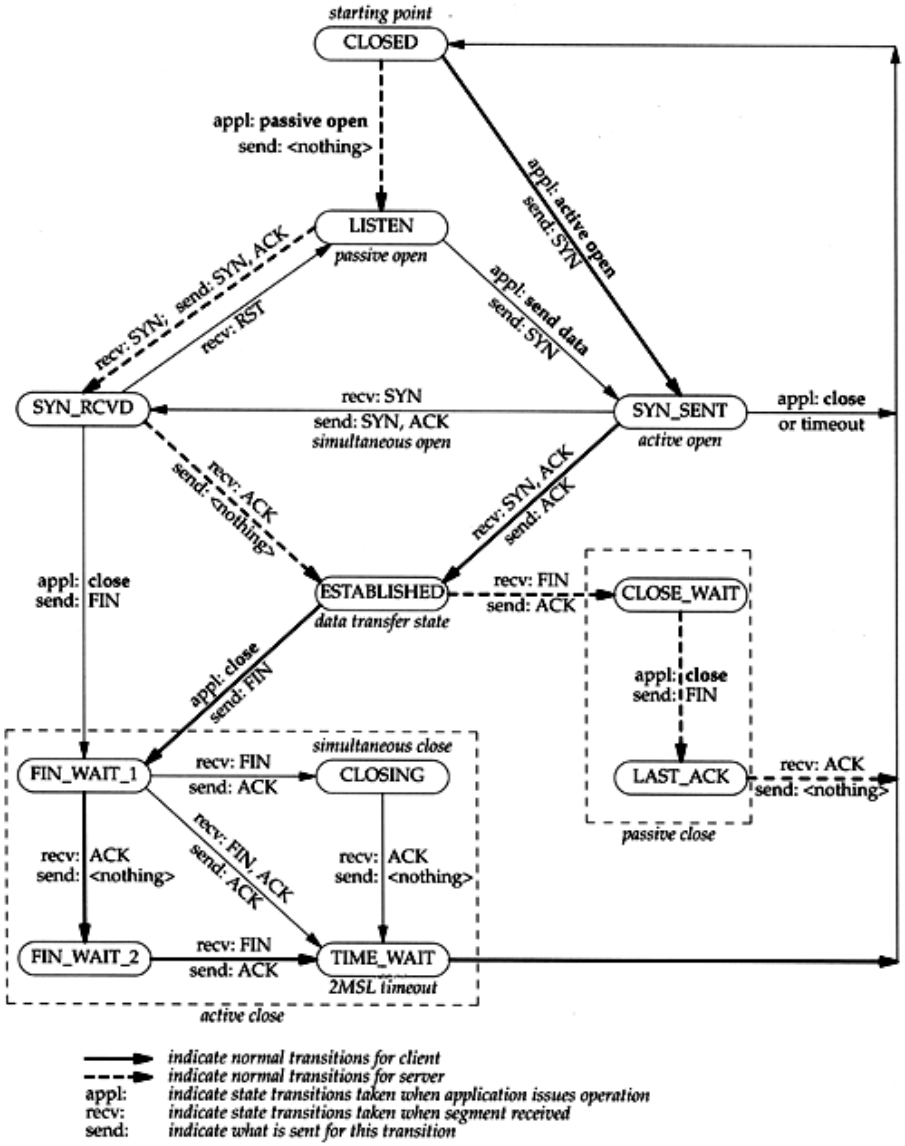


Diagramme transition d'états TCP



Détection basée sur la classification

- Algorithmes de classification afin de modéliser le comportement normal du système.
- Classer les évènements comme étant normaux ou anormaux (anomalie)
- Techniques : le plus proche voisin, réseaux de neurones, machines à vecteurs de support (SVM), et les méthodes statiques.
- Définir le comportement normal n'est pas une tâche facile,
- le système de détection d'intrusion doit mettre à jour périodiquement le comportement normal du système.

Techniques

- **Observation des seuils** : par la donnée de seuils à certaines mesures (par exemple, le nombre maximum de mots de passe erronés). On a ainsi une définition claire et simple des comportements non acceptés. Il est cependant difficile de caractériser un comportement intrusif en termes de seuils, et on risque beaucoup de fausses alarmes ou beaucoup d'intrusions non détectées sur une population d'usagers non uniforme.
- **Profilage d'utilisateurs** : on crée et on maintient des profils individuels du travail des usagers, auxquels ils sont censés adhérer ensuite. Au fur et à mesure que l'utilisateur change ses activités, son profil de travail attendu se met à jour. Il reste cependant difficile de profiler un utilisateur irrégulier ou très dynamique.

Techniques

- **Profilage de groupes** : on place chaque utilisateur dans un groupe de travail qui montre une façon de travailler commune. Un profil de groupe est calculé en fonction de l'historique des activités du groupe entier. On vérifie que les individus du groupe travaillent de la manière que le groupe entier a définit par son profil. Cette méthode réduit drastiquement le nombre de profils à maintenir.

- **Profilage d'utilisation des ressources** : on observe l'utilisation de certains ressources comme les comptes, les applications, les mémoires de masse, la mémoire vive, les processeurs, les ports de communication sur de longues périodes, et on s'attend à ce qu'une utilisation normale n'induise pas de changement sur cette utilisation par rapport à ce qui a été observé par le passé.

Limites

- Définir le comportement ou profil normal est un défi majeur. Le profil normal peut changer avec le temps et le système de détection d'intrusion doit être mis à jour périodiquement.
- Génère un taux élevé de faux positifs c.-à-d. les activités normales détectées par l'IDS comme anomalies.

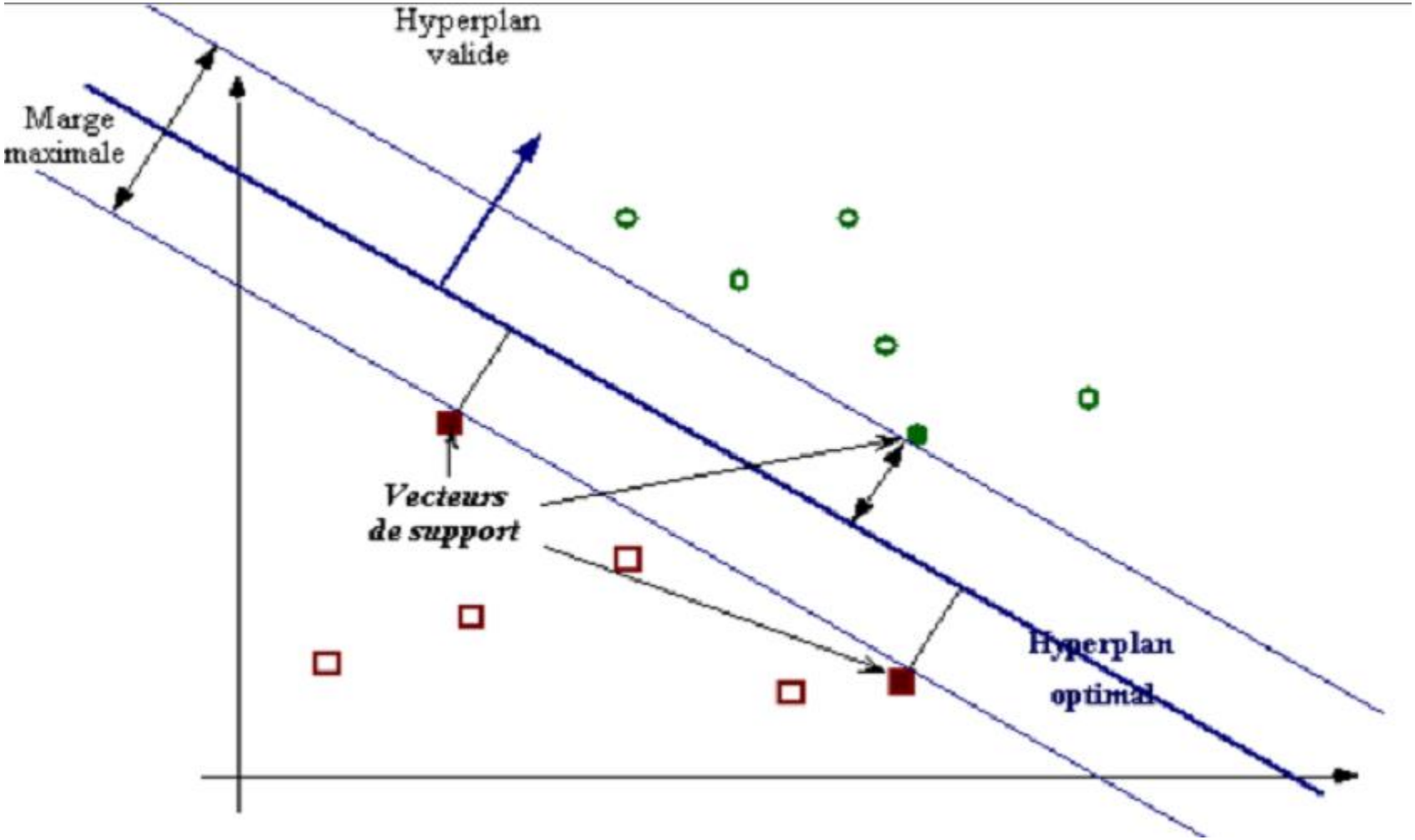
Exemple 2 : Détection d'anomalie basée sur la classification

- Machines à vecteurs de support est une méthode de classification, qui repose sur la construction d'un hyperplan qui sépare les données (comportement normal et anormal) en deux classes.

- Une multitude d'hyperplan peut être définie, le principe de la SVM est de déterminer une marge maximale entre les données d'apprentissage et l'hyperplan séparateur.

- On note que, la marge est la distance entre l'hyperplan et les données les plus proches. Cet hyperplan est défini comme étant la solution optimale, comme le montre la Figure .

Exemple 2 : Détection d'anomalie basée sur la classification



Systèmes hybrides

- Pour tenter de compenser quelques inconvénients de la détection par signature et de la détection comportementale,
- certains systèmes utilisent une combinaison de la détection d'anomalies et de la détection par signature.

Réponse aux intrusions (contre-mesures)

- Les contre-mesures donnent au système la capacité à réagir aux tentatives d'intrusions. Cette approche tente de remédier à la limitation des mécanismes qui reposent sur l'attention continue de personnel humain. Il est en effet très difficile d'avoir du personnel dévoué 24h/24h à la réponse aux intrusions. De plus il ne pourra pas grand-chose face à des attaques automatisées. Un système ayant été équipé pour le faire aura de plus grande chances de stopper l'intrusion.
- Il existe deux types de réponses, suivant les IDS utilisés. La réponse passive est disponible pour tous les IDS, la réponse active est plus ou moins implémentée.

Réponse passive

- La réponse passive d'un IDS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable sécurité.
- Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire.

Réponse active

- La réponse active au contraire a pour but de stopper l'intrusion au moment de sa détection. Les deux techniques les plus communes sont :
  - la reconfiguration du firewall
  - et l'interruption de la connexion TCP.
- D'autres réactions peuvent être envisagées, telles que:
  - Accroître la collection d'audits
  - Ré-authentifier l'utilisateur ou le système distant pour remédier aux attaques profitant d'une session ouverte et oubliée ou de paquets forgés utilisant une connexion authentifiée
  - Bloquer l'accès ; bloquer le compte local ; annuler les paquets concernés ; bloquer l'hôte totalement, le déconnecter du réseau
- On doit éviter le cas où un usager fait quelque chose d'inhabituel ou de suspect pour des raisons légitimes et se retrouve attaqué par un système de contremesures. De plus, il devient aisé pour un cyber-pirate de créer un déni de service pour un utilisateur donné en usurpant son identité et en effectuant en son nom des opérations qui déclencheraient les contre-mesures.