Lutte Informatique Défensive

SOC, CERT et CTI

Georges Bossert - SEKOIA
Frédéric Guihéry - AMOSSYS

6 novembre 2018 - Université Rennes 1

SEKOIA

AMOSSYS
EXPERT IN CYBERSECURITY

Security Operation Center

Abréviation : SOC

Domaine : INFORMATIQUE - DÉFENSE

Définition : Unité organisationnelle qui assure la fonction de détection, de confinement et d'assainissement des menaces informatiques. Le cas échéant, elle coordonne la gestion d'incident.

Support de cours inspiré des supports de Guillaume Hiet (CentraleSupélec)

Contexte et besoin

Contexte

Les réseaux sont de plus en plus interconnectés

- un attaquant peut exploiter ces interconnexions pour mener à bien ses attaques

Détecter les attaques pour prévenir les intrusions

- Moyens techniques : parefeu, AV, NIDS, NIPS, HIDS, HIPS, diode…
- Moyens humains : équipe SSI, DSI, officier de sécurité…
- Moyens organisationnels : procédures, méthodologies, référentiels…

Besoin

Pourquoi mettre en œuvre une gestion des incidents de sécurité ?

- Mise en œuvre d'un plan sécurité avec un objectif de réduction du nombre et de l'impact des incidents
- Se conformer aux exigences réglementaires du secteur d'activité
- Mise en place d'un processus d'amélioration continue
- …

Terminologie

Terminologie

Intrusion

- Violation de la politique de sécurité

Attaque

- Tentative d'intrusion

Scénario

- Suite des étapes élémentaires d'une attaque ou d'une intrusion

Terminologie

Signature (règle)

- Selon le contexte:
  - symptôme(s) révélateur(s) d'une attaque ou d'une intrusion
  - motif caractéristique d'un comportement estimé « normal »

Vulnérabilité

- Défaut (bug) exploité par l'attaquant pour mettre en oeuvre son attaque
  - conception
  - réalisation (codage)
  - administration
  - utilisation…

Terminologie

Détection d'intrusions

- Ensemble de techniques permettant de surveiller un système informatique et d'identifier automatiquement les intrusions contre ce système en vue de prendre les contre-mesures adéquates pour ramener le système dans un état sain.
  - Détection d'intrusions vs. détection d'attaques
  - Importance de la qualité du diagnostic

Terminologie

Définition ANSSI

Événement de sécurité : occurrence identifiée de l'état d'un système indiquant

- une violation possible de la politique de sécurité
- un échec des mesures de sécurité
- une situation inconnue jusqu'alors et pouvant relever de la sécurité de l'information.

Terminologie

Définition ANSSI

Incident de sécurité : un incident de sécurité est indiqué par

- un ou plusieurs évènement(s) de sécurité de l'information indésirable(s) ou inattendu(s)
- présentant une probabilité de compromettre les opérations liées à l'activité de l'organisme
- et/ou de menacer la sécurité de l'information

Terminologie

Définition ANSSI

Notification

- action d'informer de l'occurrence d'un incident de sécurité portant atteinte au système d'information

Législation et cadre réglementaire

Cadre réglementaire

Cadre

- `RGS` – Référentiel Général de Sécurité
- `LPM` – Loi de Programmation Militaire

Qualification de prestataires par l'ANSSI

- `PASSI` – Prestataire d'Audit de la Sécurité des Systèmes d'Information
- `PDIS` – Prestataire de Détection d'Incidents de Sécurité
- `PRIS` – Prestataire de Réponse aux Incidents de Sécurité (sous-ensemble d'un CERT/CSIRT)

PDIS

en phase expérimentale

Le périmètre de la prestation

- Gestion des événements : recueil et stockage des éléments techniques permettant de détecter les incidents de sécurité
- Gestion des incidents : identification et qualification des incidents de sécurité sur la base des événements collectés
- Gestion des notifications : signalement au commanditaire des incidents de sécurité portant atteinte à son système d'information

PRIS

en phase expérimentale

Le périmètre de la prestation

- Propose une méthode de réponse aux incidents adaptée au contexte
- Collecte et analyse les traces issues du SI
- Identifie le mode opératoire de l'attaquant
- Qualifie l’étendue de la compromission
- Évalue les risques et les impacts associés
- Préconise des mesures de remédiation

Respect de la vie privée

Concerne les salariés (SI interne) et les clients (SI manipulant les données clients)

- Par exemple, dans une charte informatique

Qui doit contenir des informations précises sur

- Les catégories de personnes impactées
- La nature de l'analyse réalisée et l'objectif
- Les données conservées et la durée
- L'existence de dispositifs permettant une utilisation personnelle qui ne serait pas soumis à l'analyse des flux

Respect de la vie privée

D’un point de vue technique

- Nécessaire de mettre en œuvre une gestion stricte des droits d'accès des administrateurs

Respect de la vie privée

Besoin de minimiser les traces conservées

ATTENTION AUX TRACES !

- Exemples : fichiers malveillant, adresses IP/ports source et destination
- Mauvais exemples : identifiants et mots de passe

Protection des données d'alertes extraites de l'analyse

- Exemple : chiffrement, stockage en dehors de l'environnement de production
- Exemple : durée de conservation de 6 mois maximum

Les grandes étapes de la détection d'incidents

Les grandes étapes de la détection d'incidents

La capture et l'analyse de l'activité d'un SI

- Production d'événements de sécurité

La collecte et l'analyse des événements

- Production d'incidents de sécurité

L'analyse et la gestion des incidents

- Production de notifications de sécurité

Les grandes étapes de la détection d'incidents

Mise en place de contre-mesures techniques/organisationnelles en réponses aux incidents

CHAPITRE CERT

- Contre-mesures conjoncturelles
- Contre-mesures structurelles
- Amélioration continue
- …

Établir une stratégie de détection d'intrusions

Démarche

1) **Réalisation d'une analyse de risque**
   - Possibilité de s'appuyer sur les références suivantes
     - Annexe B de l'ISO27035
     - ETSI_ISG_ISI
   - On obtient
     - Une liste des incidents redoutés

Démarche

1) **Réalisation d'une analyse de risque**
   - On obtient
     - Une liste des incidents redoutés
       - Exploitation d'une vulnérabilité
       - Elévation de privilèges
       - Exfiltration de données
       - Propagation virale
       - Utilisation d'un mécanisme de persistance
       - Déni de service
       - Accès non autorisé à une ressource
       - Usurpation d'identité
       - Actions non conformes à la politique de sécurité

Démarche

1) **Réalisation d'une analyse de risque**
   - On obtient
     - Une liste des incidents redoutés
     - Un critère de vraisemblance pour chaque incident redouté, basé sur un échelle de vraisemblance
     - Un critère de gravité pour chaque incident redouté, basé sur un échelle de gravité

Démarche

1) **Réalisation d'une analyse de risque**
2) **Définition de la stratégie de détection**

Démarche

1) **Réalisation d'une analyse de risque**
2) **Définition de la stratégie de détection**
3) **Définition de la stratégie de collecte**

Démarche

1) Réalisation d'une analyse de risque
2) Définition de la stratégie de détection
3) Définition de la stratégie de collecte
4) Définition de la stratégie de notification

Démarche

1) Réalisation d'une analyse de risque
2) Définition de la stratégie de détection
3) Définition de la stratégie de collecte
4) Définition de la stratégie de notification
5) Mise en oeuvre / phase de build

Démarche

1) Réalisation d'une analyse de risque
2) Définition de la stratégie de détection
3) Définition de la stratégie de collecte
4) Définition de la stratégie de notification
5) Mise en oeuvre / phase de build
6) Exploitation / phase de run

Démarche

1) **Réalisation d'une analyse de risque**
2) **Définition de la stratégie de détection**
3) **Définition de la stratégie de collecte**
4) **Définition de la stratégie de notification**
5) **Mise en oeuvre / phase de build**
6) **Exploitation / phase de run**
7) **Amélioration continue**
    - Revue de l'analyse de risque
    - Changement du périmètre / etc.
    - Revue des stratégies d'analyse
    - Modifications de la mise en œuvre / nouvelle phase de Build
    - Changements sur l'exploitation

Capture et analyse de l'activité pour la détection d'intrusion

Objectif de la capture de l'activité d'un SI

Résultat : des événements représentant

- les états des composants surveillés
- des actions utilisateur/système
- des anomalies
- ...

dans divers formats

Sources de capture

Sondes réseau (inclus les NIDS/NIPS)

Sondes système (inclus les HIDS/HIPS)

Mécanismes de journalisation intégrés aux OS/applications

Autres produits de sécurité

- Pare-feu
- Proxy / Reverse proxy
- Antivirus locaux / réseau
- …

Les sondes réseau

Avantages

- Couverture large (dépend du mode de capture)
- Peu d'impact sur le SI car sondes dédiées (dépend du mode capture)
- Format standard de données
- Réaction possible (*Intrusion Prevention Systems*)

Inconvénients

- Réseau commuté → multiplication des sondes
- Montée en débit des réseaux
- Chiffrement des flux

Les sondes systèmes

Avantages

- Informations précises (utilisateurs, processus, fichiers…)
- Mécanisme de journalisation ou d'audit fourni par la plupart des OS (syslog, WMI, …)

Inconvénients

- Impact sur les performances de l'hôte (CPU, mémoire)
- Vulnérabilité de la sonde
- Hétérogénéité des formats de données à analyser
- Informations très bas niveau + vision locale

Les sondes applicatives

Avantages

- Moins de données à capturer, moins de formats à analyser, classes d'attaques à détecter plus restreinte → meilleurs performances de détection

Inconvénients

- Impact sur les performances de l'hôte (CPU, mémoire)
- Vulnérabilité de la sonde
- Multiplication des sondes

Approches de détection

Approches par scénarios ou signatures d'attaque (*misuse detection*)

- Modèle d'intrusions (base de signatures d'attaques)
  - Signature = symptômes d'attaque dans activités observées
- Alerte si présence de symptôme(s)
- Dans la pratique : *(multiple-)pattern matching*

Approches comportementales *(anomaly detection)*

- Modèle des comportements légaux
- Alerte si activité observée ≠ des comportements normaux
- Dans la pratique : *apprentissage et modèle statistique*
  - Légal → usuel

Propriétés attendues de la détection

Fiabilité (sensibilité)

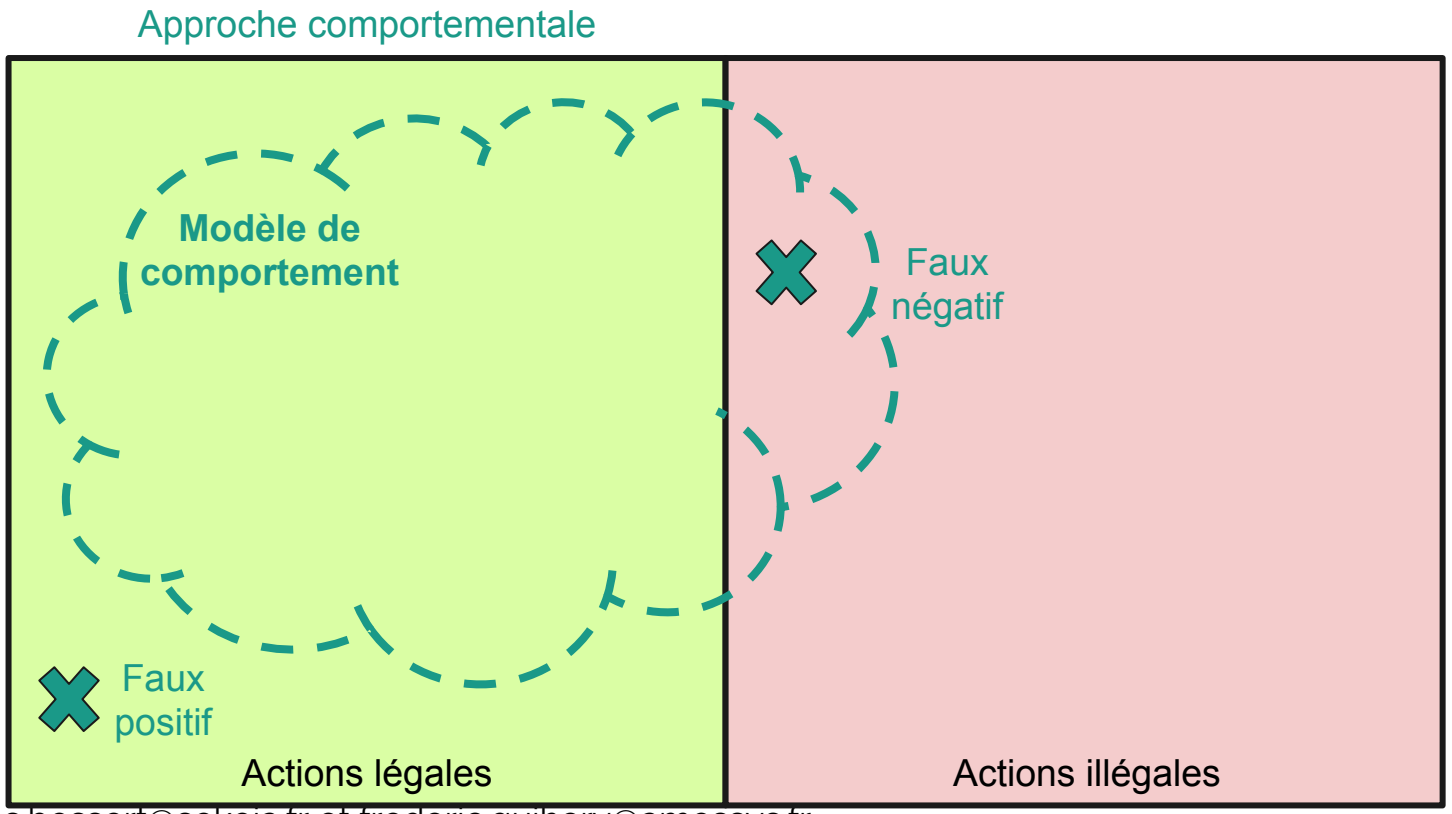
- Intrusion (pratique) → alerte
- Pas de faux négatif i.e. intrusion (attaque) non détectée

Pertinence (spécificité)

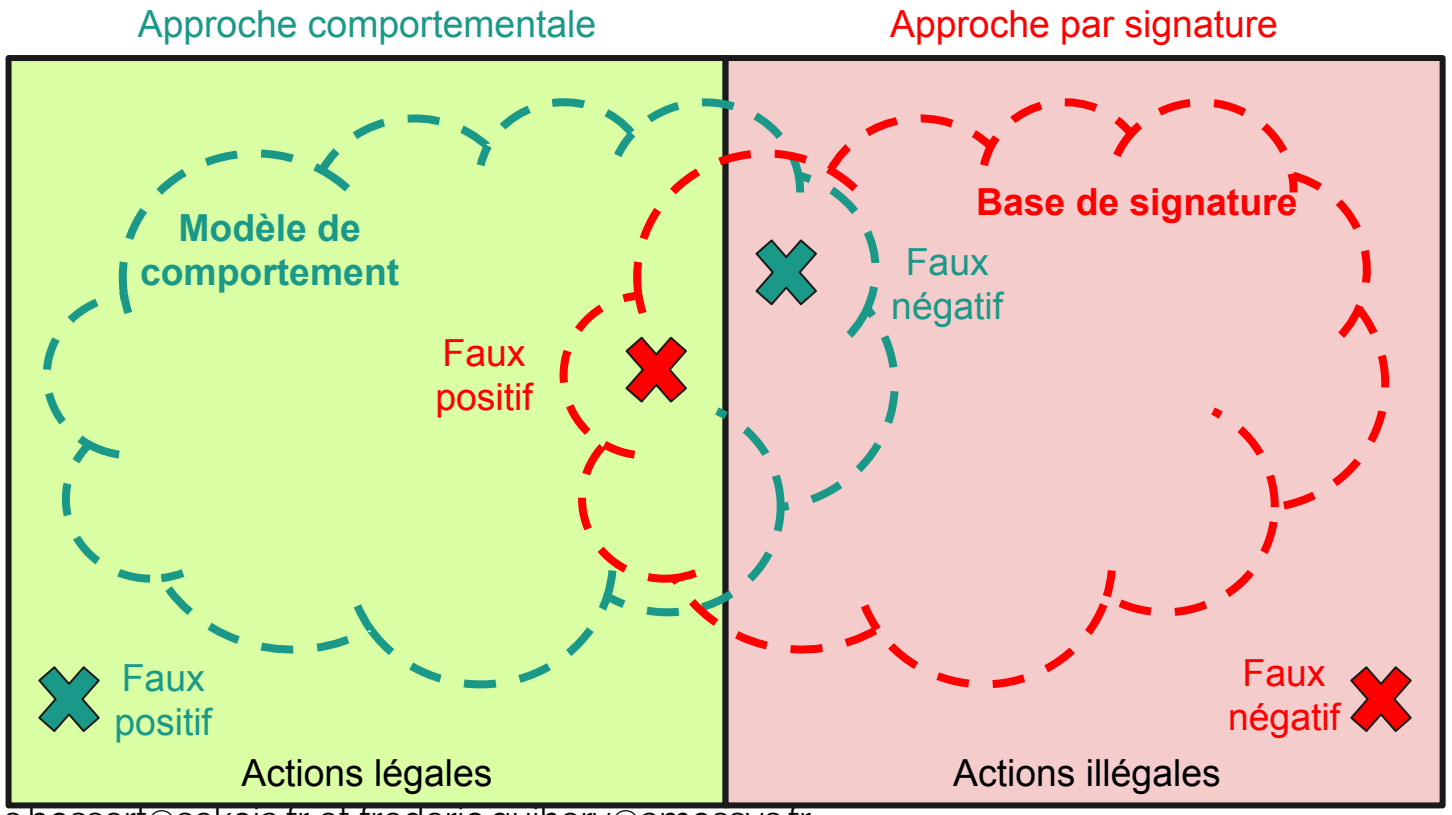
- Alert → intrusion (attaque)
- Pas de faux positif i.e. fausse alerte

Objectifs : Une détection fiable et pertinente (un détecteur sensible et spécifique)

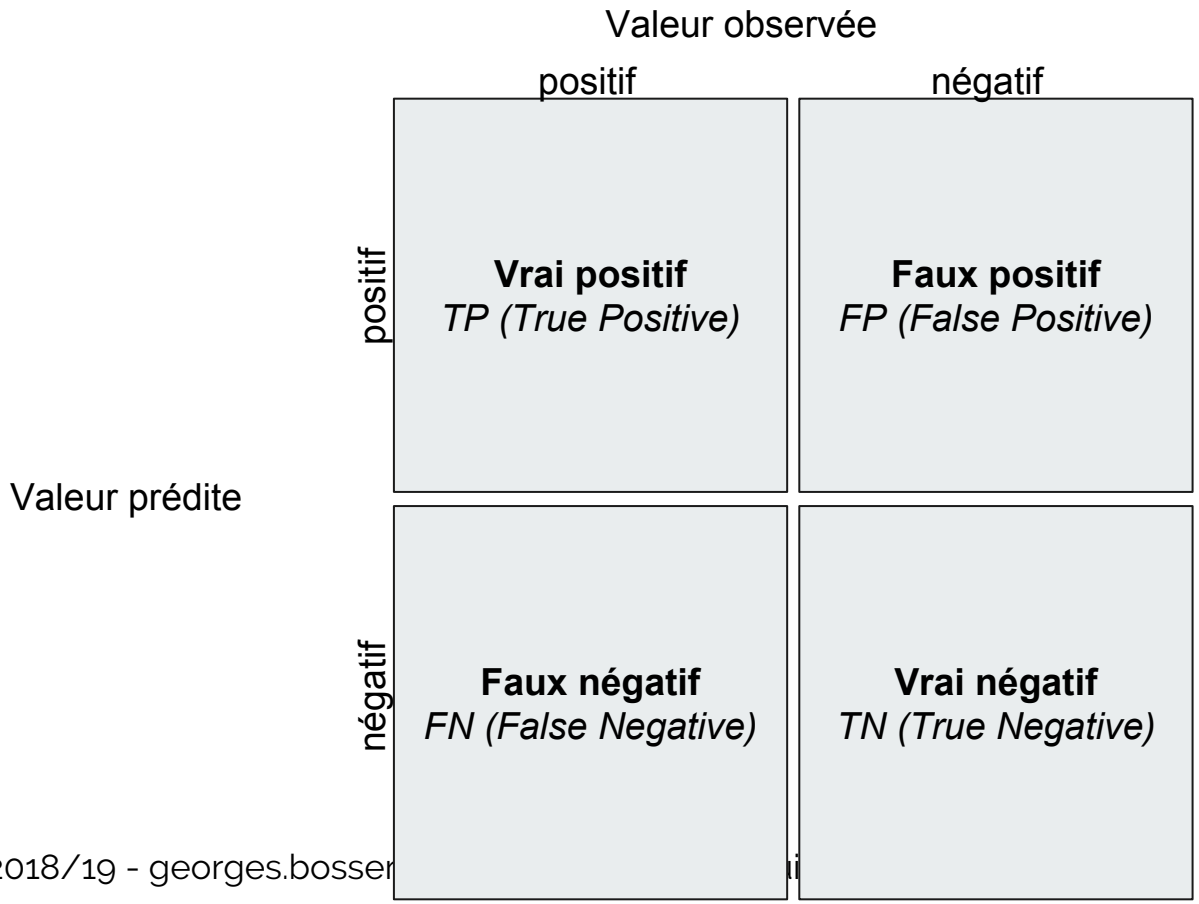
Propriétés attendues de la détection



Propriétés attendues de la détection



Fiabilité *vs* pertinence



Fiabilité : True Positive Rate
TPR = TP / (TP + FN)

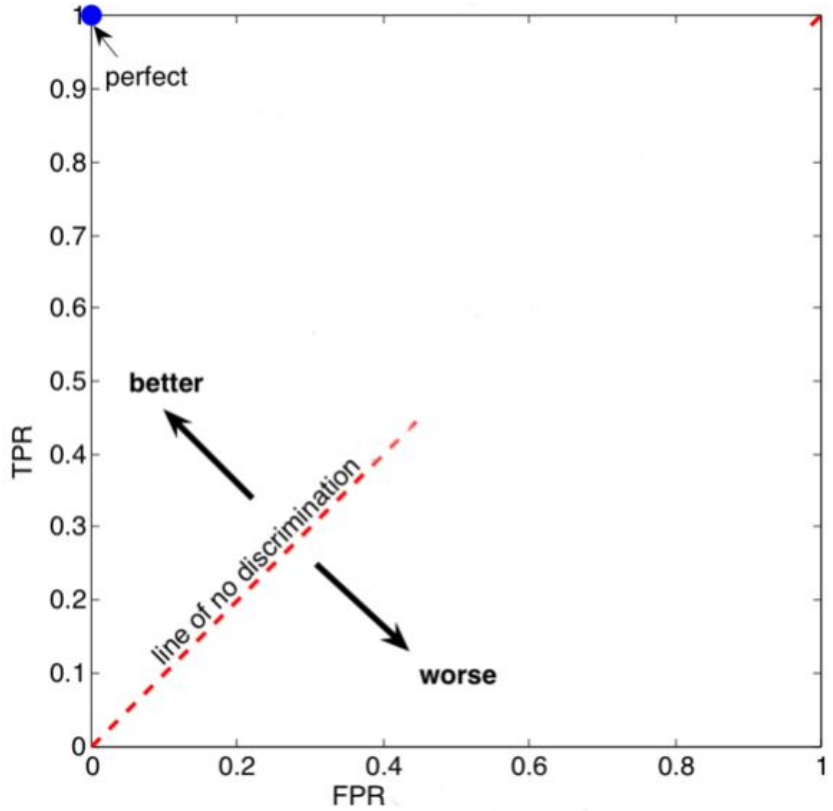
Pertinence : False Positive Rate
FPR = FP / (FP + TN)

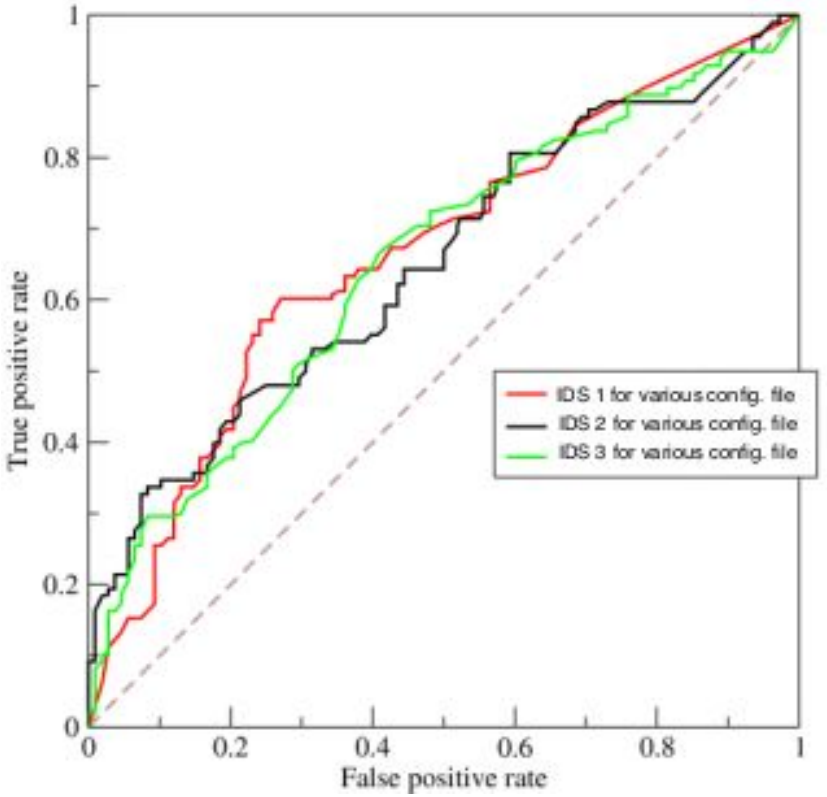
Précision : Accuracy
ACC = (TP + TN) / (P + N)

Taux de positifs prédits : Positive Predictive Value
PPV = TP / (TP + FP)

Taux de négatifs prédits : Negative Predictive Value
NPV = TN / (TN + FN)

Courbe ROC: Receiver Operating Characteristic





Fiabilité des approches de détection

Approches par scénarios ou signatures d'attaque (*misuse detection*)

- [+] Pas parfaitement fiable mais peu de faux positifs
- [+] Qualification des alertes aisée
- [–] Fiabilité décroît si base de signature mal maintenue
- [–] Mauvaise détection des nouvelles attaques (zero day)
- [–] Difficulté pour la spécification des signatures
  - Trop précises → facilement contournable (polymorphisme) + grand nombre de signatures (impact perf.)
  - Trop génériques → faible pertinence

Fiabilité des approches de détection

Approches comportementales *(anomaly detection)*

- [+] Pas toujours pertinent mais peu de faux négatifs
- [+] Capacité théorique à détecter de nouvelles attaques (zero-day)
- [–] Difficile prise en compte de l'évolution du comportement (ré-apprentissage)
- [–] Pas de diagnostic associé aux alertes (Cause de l'alerte)

NIDS : Network Intrusion Detection System

Les sondes réseau

Capture passive

- [+] furtivité, surveillance au sein d'une zone (via hub ou switch), non-intrusive
  - perturbation limitée au réseau surveillé
- [−] évasion, réaction moins facile

Capture *inline*

- [+] facilite la réaction (IPS), normalisation
- [−] non-furtif, impact les performances, trafic entre zones

Les sondes réseau

Network TAP

Capture passive

- Hub
  - uniquement pour petit réseau/faible débit
- Switch (port mirroir)
  - [+] pas de matériel supplémentaire, surveillance de zone
  - [–] limité en début, risque de perte, risque de mauvaise configuration
- TAP
  - [+] pas de problème de débit, pas de perte sur la transmission
  - [–] coût, utilisation sur un brin (surveillance inter-zone)
  - **Remarque: préférer des TAP sans fonction d'administration**

Les sondes réseau

Niveaux de captures

- Couche IP Flux : IP/ports sources/destinations
  - exemple format netflow
- Couche protocolaire non-applicative
- Toutes les couches : Full Packet Capture

Les sondes réseau

Sonde Netflow

- Interface réseau d'entrée
- Adresses IP source et destination
- Ports source et destination
- Type de service IP

```
Date flow start          Duration Proto Src IP Addr:Port Dst IP Addr:Port    Packets Bytes Flows
2010-09-01 00:00:00.459 0.000    UDP   127.0.0.1:24920 -> 192.168.0.1:22126 1       46    1
2010-09-01 00:00:00.363 0.000    UDP   192.168.0.1:22126 -> 127.0.0.1:24920 1       80    1
```

Architecture d'un NIDS

Fonctionnalités attendues

- Décodage protocolaire
- Gestion d'une base de signatures
- Moteur de comparaison du trafic au regard de la base de signatures
- Réalisation d'actions
  - Journalisation des événements
  - Blocage du trafic (IPS)
  - Réalisation d'actions sur la cible attaquée (désactiver un service, éditer une règle de pare feu)

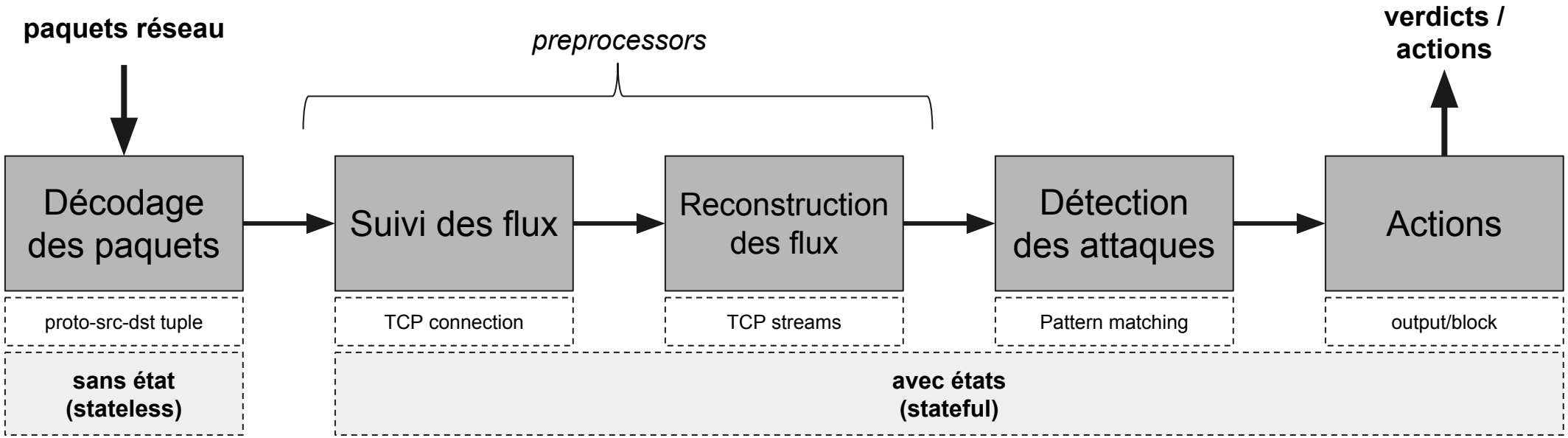
Architecture d'un NIDS

Exemple de SNORT

- Sonde NIDS/NIPS libre créée par Marty Roesch
- Développée par Sourcefire (rachetée par Cisco en 2013)
- Première version en 1998 (pour UNIX)
  - « Lightweight » intrusion detection
  - Simple pattern matching sur le paquets
  - Pas de défragmentation, pas de reconstruction de flux
- Aujourd'hui, logiciel complet utilisé dans des applications

Architecture d'un NIDS

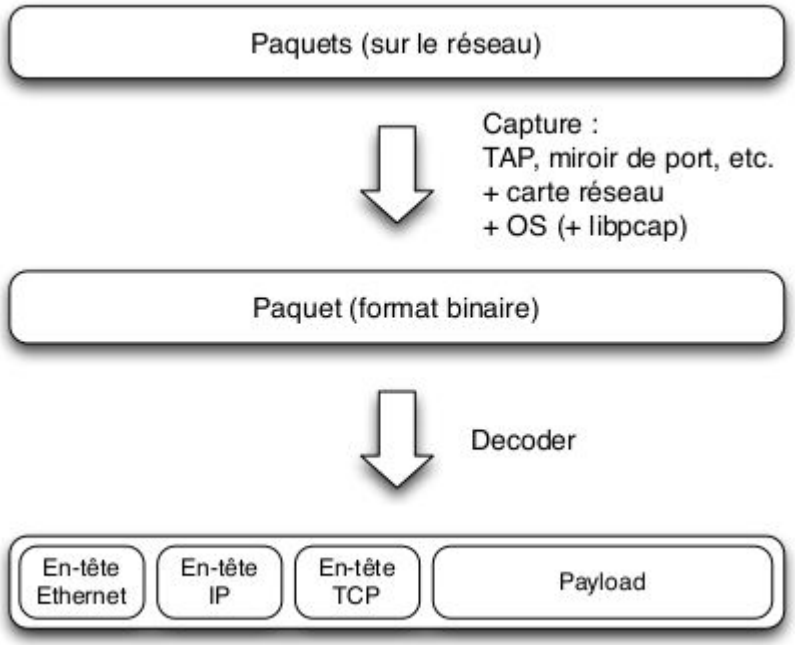
Exemple de SNORT



Architecture d'un NIDS

Exemple de SNORT - Module de capture

- Analyse de protocole sommaire
- Décodage des entêtes Ethernet, IP et TCP
- Quelques vérifications simples (tailles champs, en-têtes, …)



Architecture d'un NIDS

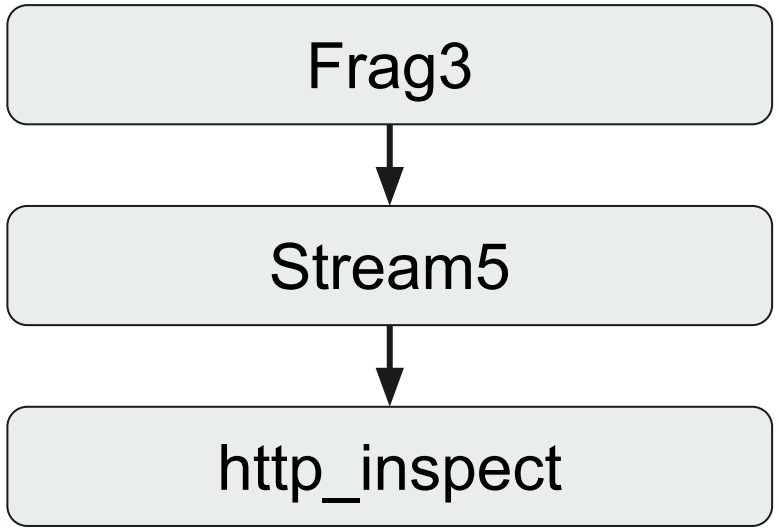
Exemple de SNORT - Preprocessors

- Défragmentation et reconstruction du flux
- Analyse des protocoles applicatifs
- Détection d'anomalie et normalisation
- …

Architecture d'un NIDS

Exemple de SNORT - Preprocessors

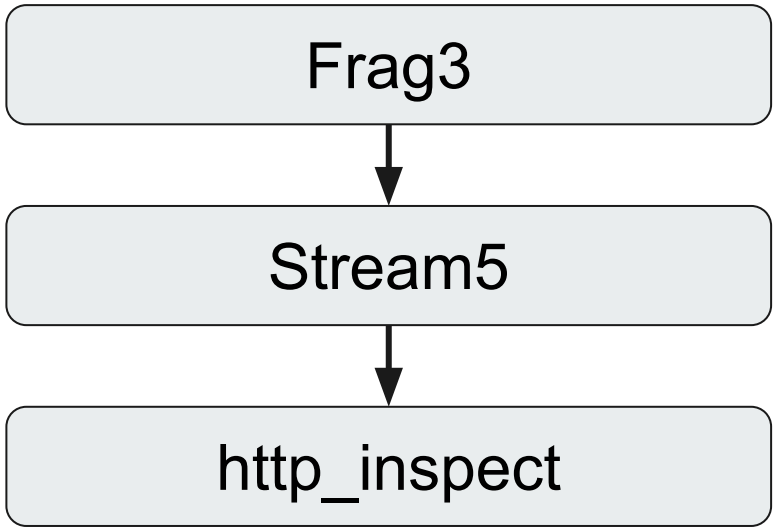
- Frag3
  - Défragmentation IP
  - Détection d'attaques liées à la fragmentation
  - Génération d'un pseudo paquet réinjecté
- Stream5
  - réassemblage des flux TCP, suivi des états
  - Détection attaques liées à la fragmentation TCP
  - Génération d'un pseudo paquet
  - Configuration par port



Architecture d'un NIDS

Exemple de SNORT - Preprocessors

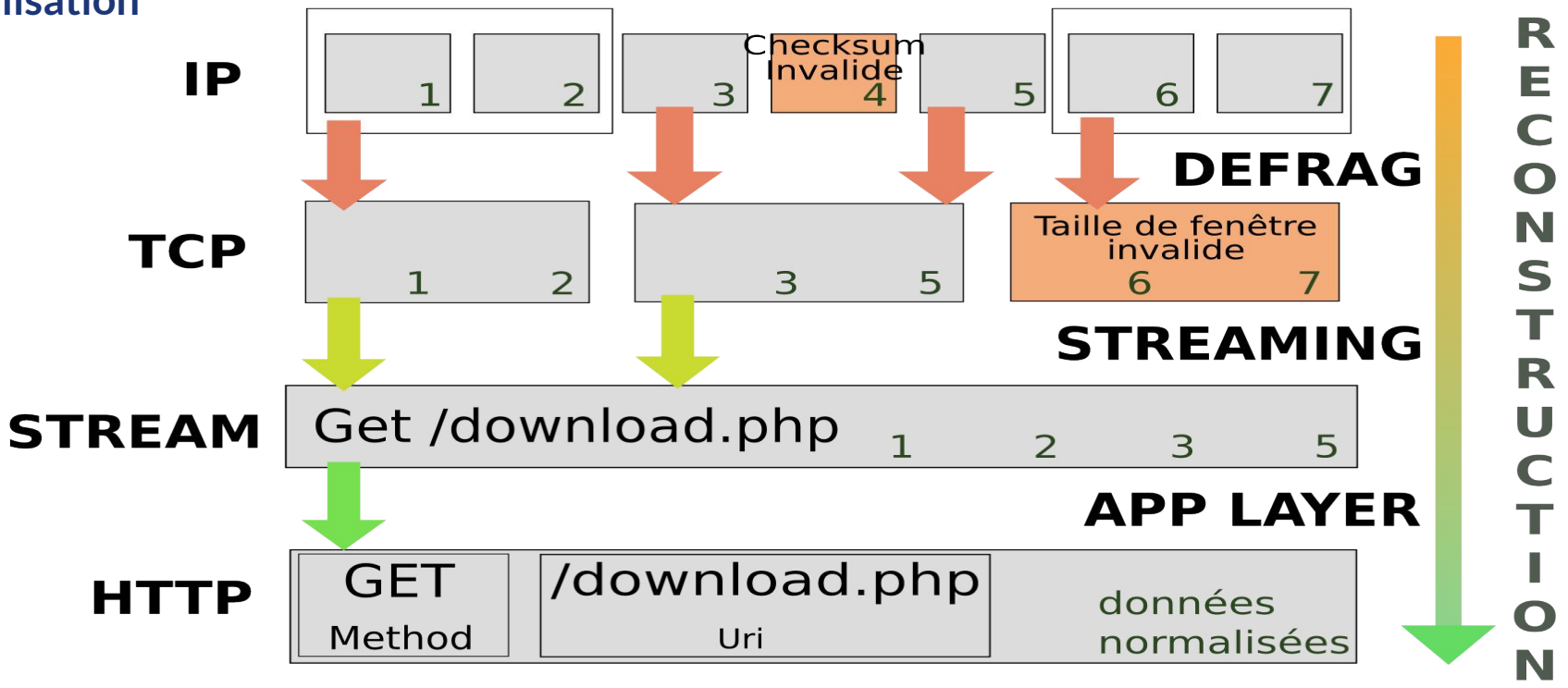
- http_inspect
  - Normalisation URI
  - Création d'un tampon URI
    - peut être inspecté dans les règles avec *uricontent*
  - Détection des tentatives d'évasion et des anomalies HTTP
  - Attention au paramétrage de *flow_depth*
    - faux négatifs *vs* consommation des ressources



GET /downloads/../cgi-bin/../pics\../downloads/./snort.tar.gz HTTP/1.0 → /downloads/snort.tar.gz

Architecture d'un NIDS

La normalisation



Signatures de détection

Les signatures

Exemple de SNORT

- Community Ruleset (gratuit - GPLv2)
  - Fréquence 1/jour
- Subscriber Ruleset (payant)
  - Fréquence : en temps réel
  - Ordre de grandeur : 400 $ / an / sonde
  - Disponible gratuitement 30 jours après leur mise à disposition
  - Règles « utilisateur »

Les signatures

Entête

- **action** : `log, alert, reject, drop`
- **protocole** : `IP, TCP, UDP, ICMP`
- **source :** un adresse IP + un port *(définition par plages, avec négations, …)*
- **Direction du flux :** `<-, ->, <>`
- **destination :** un adresse IP + un port *(définition par plages, avec négations, …)*

Options

- **general** : `msg, reference, sid, classtype, priority…`
- **payload** : `content, uricontent, isdataat, pcre…`
- **non-payload** : `flow, ttl, tos, id, fragbites, dsize, flags, flowbits…`
- **post-detection** : `resp, react, tag, activate, activate by, count, replace…`

Les signatures

Exemples des options

content: Recherche d'un contenu dans la payload d'un flux

```
content:[!]"<content string>";
```

pcre: Recherche d'un motif dans la payload d'un flux

```
pcre:[!]"/<regex>/";
```

protected: Recherche d'un contenu secret dans la payload d'un flux

```
protected_content:"293C9EA246FF9985DC6F62A650F78986"; hash:md5; offset:0; length:4;)
```

Les signatures

Exemples de règles simples

```
alert tcp any any -> any 21 (content:"user root";)
```

```
alert tcp any any -> any 21 (flow:to_server,established; \
                             content:"root";pcre:"/user\s+root/i";)
```

```
alert ip any any -> any any (content:"a"; content:"b";within:5;)
```

Les signatures

Une vraie règle

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS \
    (msg:"COMMUNITY WEB-ATTACKS Hydra Activity Detected";
     flow:to_server,established;
     content:"User-Agent|3A|"; nocase; content:"Hydra"; nocase;
     distance:0;
     pcre:"/^User-Agent\s*\x3A\s*Mozilla\x2f4\.0 (Hydra)/smi"; nocase;
     reference:url,www.thc.org/releases.php; classtype:misc-attack;
     sid:100000168; rev:1;)
```

Attaque d'un NIDS

Contournement d'un NIDS

Quelles techniques envisageables ?

Contournement d'un NIDS

Nombreuses attaques

- **Insertion:** exploiter des paquets invalides pour obscurcir une information
- **Evasion:** contourner l'analyse de paquets valides
- **Denial of Service (DoS):** exploiter la saturation des ressources (CPU/RAM/Buffers)
- **Pattern-matching weaknesses:** attaques en complexité algorithmique
- **Encryption and tunneling:** SSL, SSH, IPSec, etc.
- **Protocol violation:** exploitation de la complexité de certains protocoles (e.g. SMB)

Insertions et évasions protocolaires

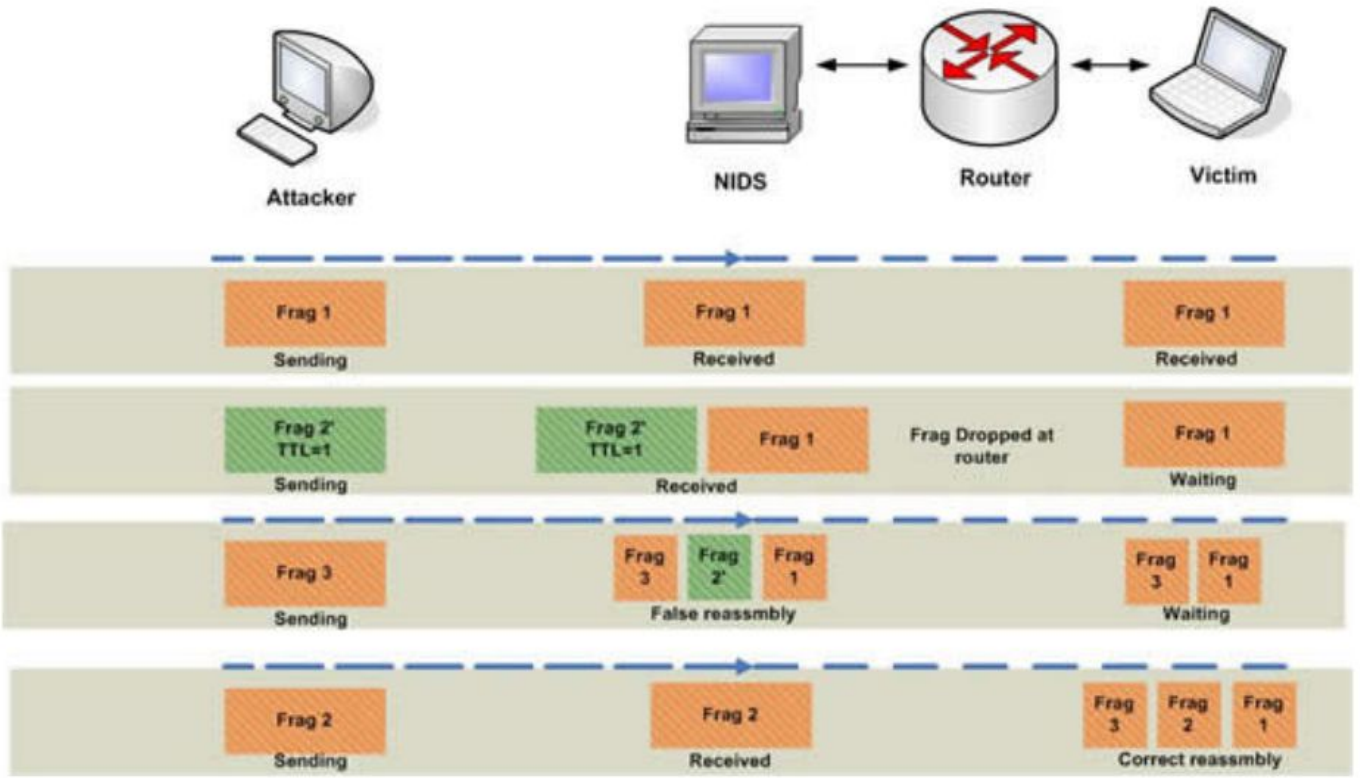
Principes

- Le paquet observé sera-t-il reçu ? Comment sera-t-il interprété ?
- Un NIDS doit interpréter les paquets **exactement** de la même manière que chaque cible
- En pratique, impossible car :
  - il n'est pas placé au même endroit dans le réseau
  - interprétations différentes des paquets suivant les implémentations des piles réseau (ambiguïtés des spécifications)
  - la sonde ne dispose (généralement) pas des informations de contexte concernant les cibles
  - la simulation de toutes les possibilités est impossible (ressources limitées)
- Souvent, vérifications « lâches » pour limiter la consommation des ressources (CPU, mémoire)
- Objectif de l'attaque : exploiter les incohérences entre l'interprétation de l'IDS et celle de la cible
  - injecter des paquets que l'IDS rejettera mais pas la cible
  - injecter des paquets que l'IDS acceptera mais pas la cible (insertion)

Insertions et évasions protocolaires

Exemple - évasion en jouant sur le TTL

- Exploiter la connaissance partielle de la topologie réseau par l'IDS.



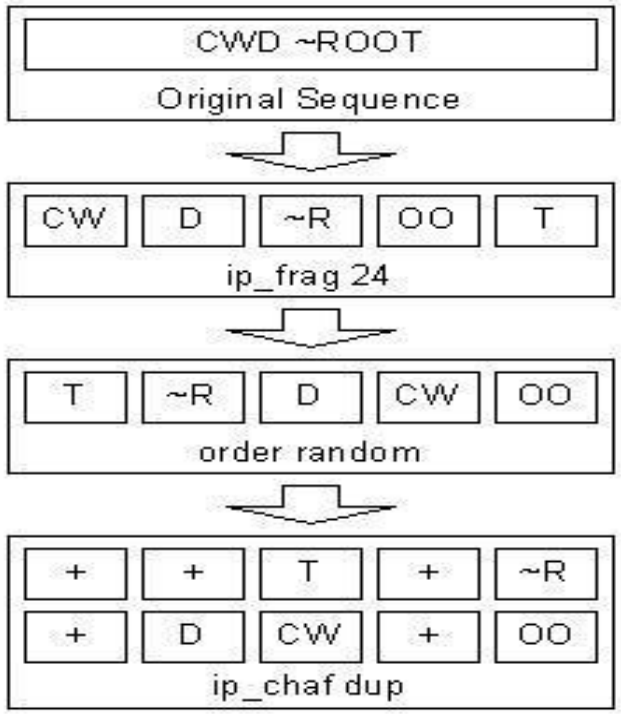
Insertions et évasions protocolaires

Exemples d'ambiguités (*cf.* Ptacek & Newsham 98)

Info Needed	Ambiguity
Network Topology	IP TTL field may not be large enough for the number of hops to the destination
Network Topology	Packet may be too large for a downstream link to handle without fragmentation
Target Config.	Destination may be configured to drop source-routed packets
Target OS	Destination may time partially received fragments out differently depending on its OS
Target OS	Destination may reassemble overlapping fragments differently depending on its OS
Target OS	Destination host may not accept TCP packets bearing certain options
Target OS	Destination may implement PAWS and silently drop packets with old timestamps
Target OS	Destination may resolve conflicting TCP segments differently depending on its OS
Target OS	Destination may not check sequence numbers on RST messages

Contournement d'un NIDS

Évasion protocolaire (outil Fragroute)



Our original attack sequence fits within one packet.

Using the "ip_frag 24" option splits the sequence into packets with payloads of 24 bytes or less

Using the "order random" option puts the fragments in random order.

Using the "ip chaf dup" option inserts duplicate packets copying the header from a valid portion of the stream, but with invalid TCP options, garbage payloads, or invalid checksums.

Contournement d'un NIDS

Insertion attack

- Réalisable lorsque la fonction d'analyse des paquets de l'IDS est **moins stricte** que celle utilisée sur le réseau de la victime (le NIDS accepte des paquets considérés comme invalides par la victime)

Flux de données de l'attaquant

2	3	3	5	1	4	6
T	T	X	C	A	A	K

Flux de données analysé par le NIDS

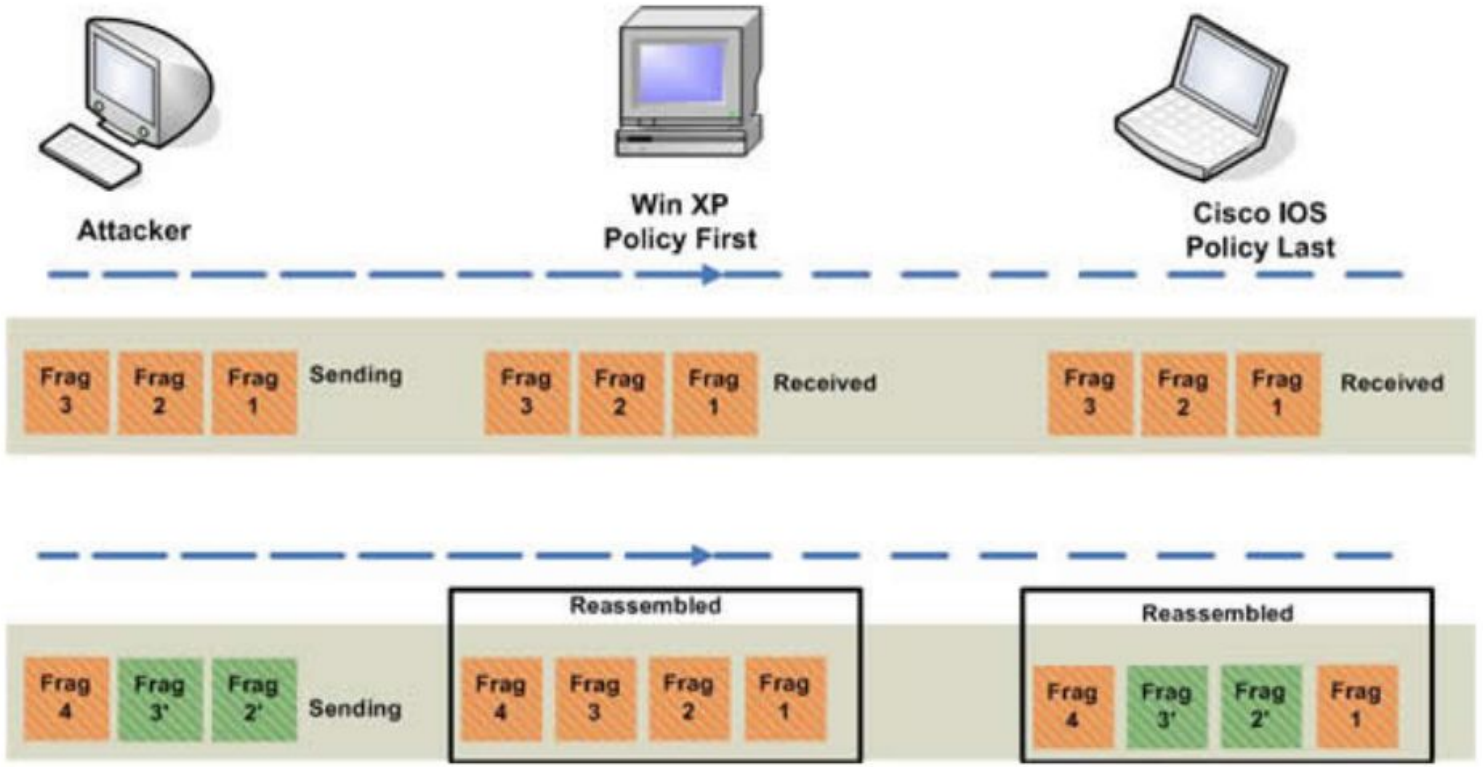
1	2	3	3	4	5	6
A	T	T	X	A	C	K

Flux de données reçu par la victime

1	2	3	4	5	6
A	T	T	A	C	K

Contournement d'un NIDS

Overlapping



Contournement d'un NIDS

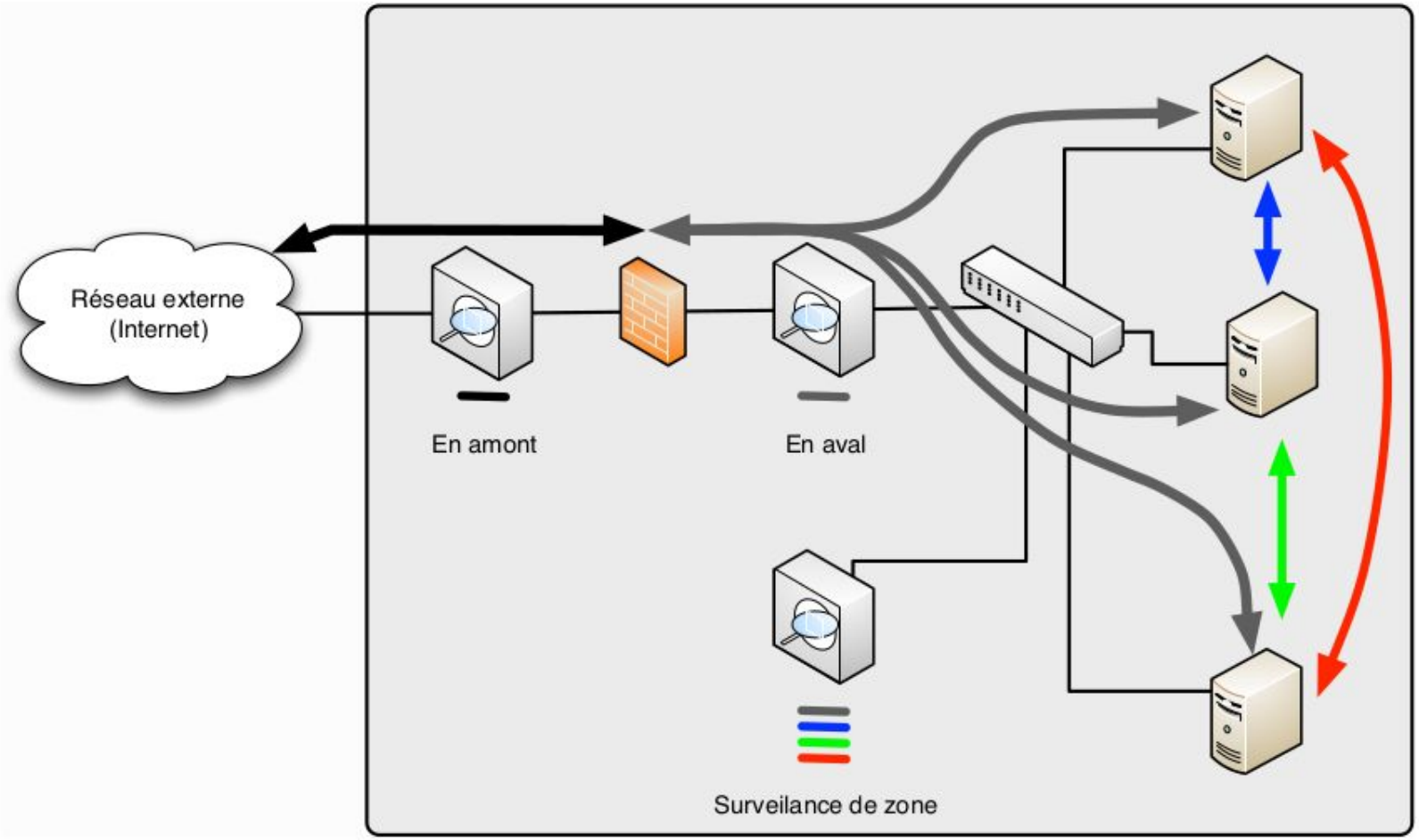
Retour d'expérience

- Tous les NIDS sont exposés à ces attaques
  - plusieurs outils : Frageroute, Wisker/Nikto, Scapy, Netzob
- Importance d'un pare-feu en amont pour la normalisation du trafic
  - exemple "paquet filter" (openbsd)

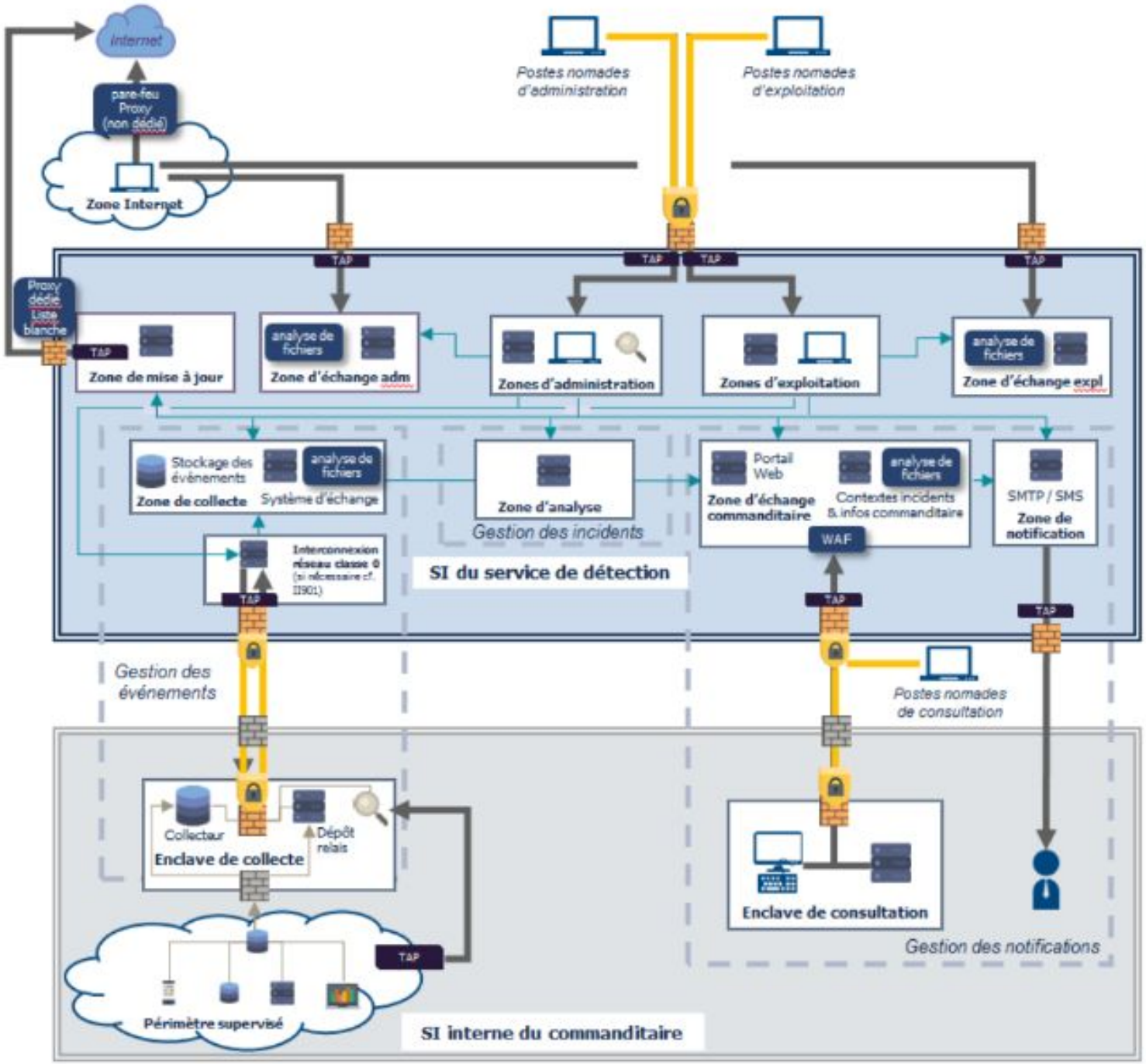
```
no-df                # Efface le bit don't fragment
random-id            # Remplace la valeur d'identification IP
min-ttl num          # Ecrase le TTL avec une valeur minimum
max-mss num          # Ecrase la MSS avec une valeur minimum
fragment reassemble  # Réassemble les paquets IP fragmentés
fragment crop        # Les fragments dupliqués sont droppés
fragment drop-ovl    # Idem pour les fragments qui se chevauchent
reassemble tcp       # Normalisation au niveau TCP
```

Exemples de déploiement

Exemple de déploiement



Exemple de déploiement (PDIS)



Chacun des flux représentés sur ce schéma doit faire l'objet de **chiffrement et d'authentification par des solutions IPSec** agréées par l'ANSSI dès lors qu'il circule sur un réseau non dédié au service de détection

LÉGENDE

- Zone de confiance
- *Activités du service de détection*
- Solution de filtrage qualifiée par l'ANSSI
- Solution de filtrage administrée par le Commanditaire
- TAP
- Sonde qualifiée par l'ANSSI
- Solution de chiffrement agréée par l'ANSSI
- Flux chiffré par une solution agréée par l'ANSSI

L'évaluation de NIDS

L'évaluation de NIDS

Quelles approches pour évaluer un NIDS ?

M2 Cyber 2018/19 - georges.bossert@sekoia.fr et frederic.guihery@amossys.fr

L'évaluation de NIDS

Exemple de démarche

- Fait partie des catégories de produit certifiés/qualifiés par l'ANSSI (Critères Communs et CSPN)
- Analyse des capacités du produit
  - Capture des flux réseau
  - Décodage des protocoles
    - Richesse des protocoles supportés
    - Richesse d'accès aux métadonnées
  - Gestion des signatures
    - Niveau de couverture
    - Niveau de mise à jour
  - Comparaison du trafic au regard des signatures
    - Efficacité du moteur avec / sans trafic de fond / trafic de stress
    - Niveau d'expressivité du langage
  - Journalisation des événements
    - Moteur fonctionnel même en cas de saturation disque ?