



Network Security Monitoring

Julien Manteau

Plan

- Introduction, définition et but de NSM
- Types d'information
- Outils
 - IDS/IPS
 - Honey Pot

Introduction

Introduction : objectifs de la sécurité informatique

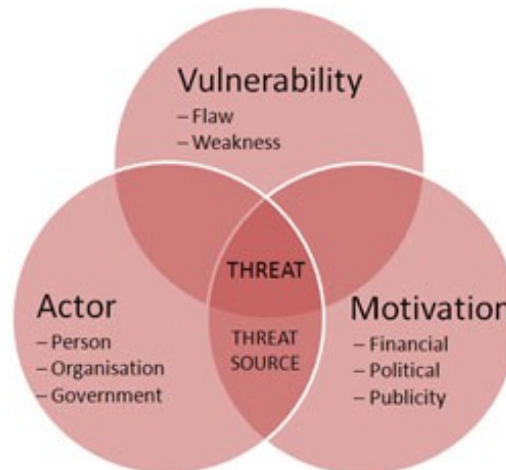
- **L'intégrité**, c'est-à-dire garantir que les données ne sont pas altérées
- **La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- **L'authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.
- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information.
- La non répudiation, permettant de garantir qu'une transaction ne peut être niée.

Introduction

- Vulnérabilité (Vulnerability)
 - ITSEC définition: L'existence d'une faiblesse, d'une conception ou d'une erreur d'implémentation qui peut mener à un événement imprévu, indésirable qui compromet la sécurité des ordinateurs, réseaux, applications ou protocoles impliquées

Introduction

- Menace (Threat)
- ENISA définition: Toute circonstance ou événement qui a le potentiel d'affecter négativement un bien au travers d'un accès non autorisé, d'une destruction, d'une divulgation, d'une modification des données, et/ou d'un déni de service.



Introduction

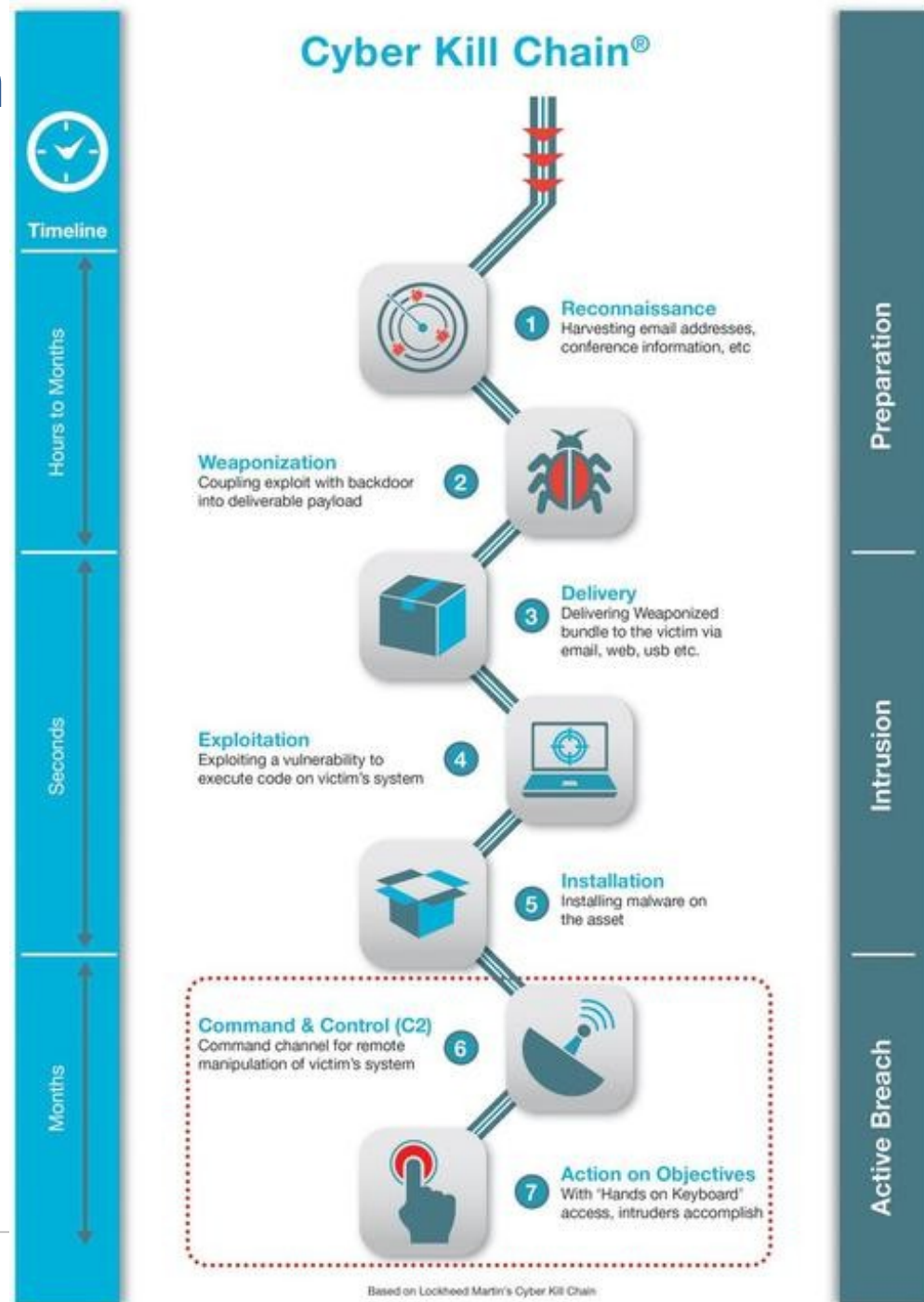
- Risque
 - Le potentiel qu'une menace donnée va exploiter une vulnérabilité d'un système d'information et par conséquent causera des dommages à l'organisation.

$$Risque = \frac{Menace \times Vulnérabilité \times Impact}{Contre - mesure}$$

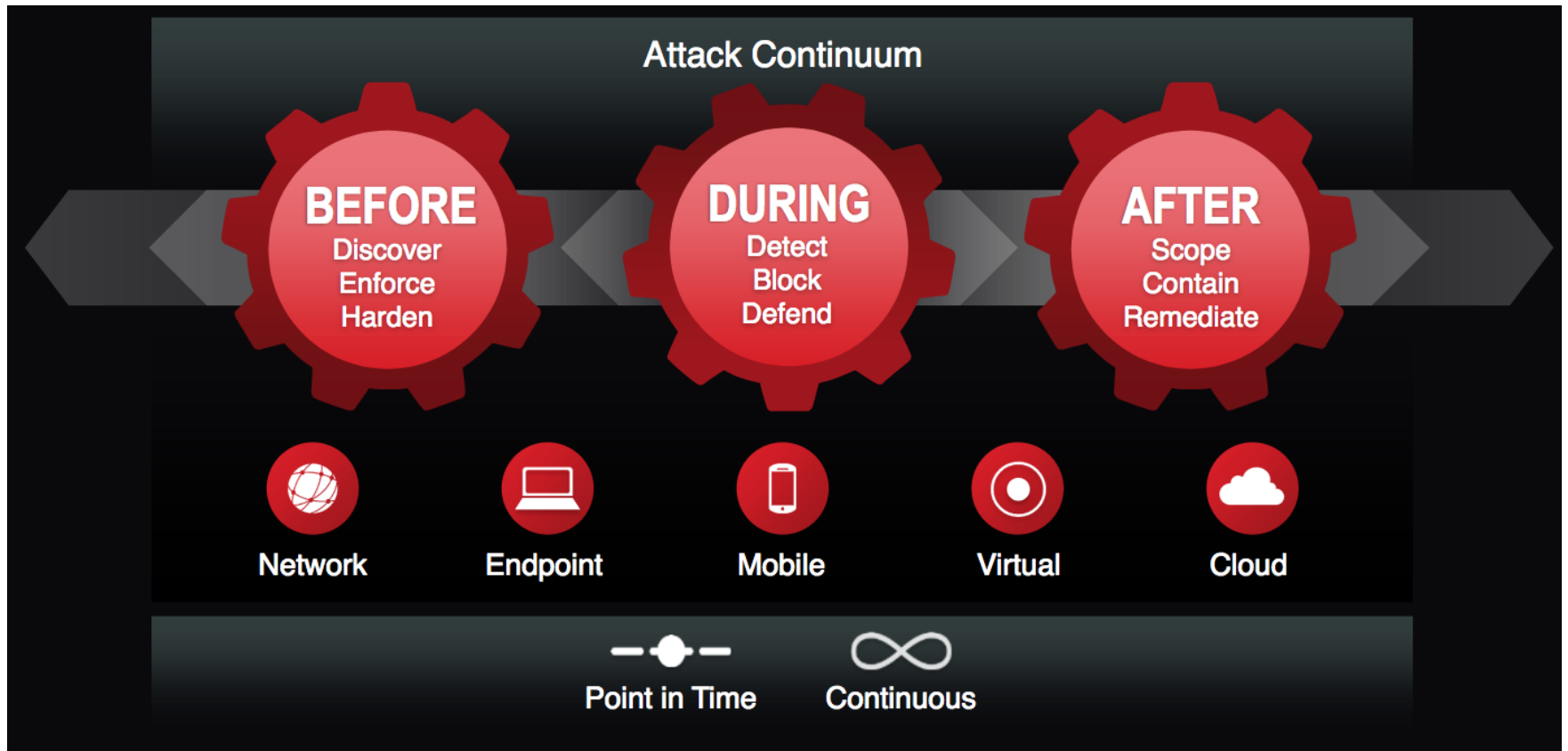
- Les contre-mesures
 - solutions techniques
 - des mesures de formation et de sensibilisation

Modèle: Cyber Kill Chain

- Une “kill chain” est un terme militaire décrivant les étapes d'attaque d'un adversaire
- Des chercheurs de Lockheed Martin ont appliqués en 2011 ce principe à la cyber sécurité
- Ce modèle décrit les étapes typiques d'une intrusion.
- D'autres modèles existent (Mandiant attack chain)



Autre modèle (Cisco)

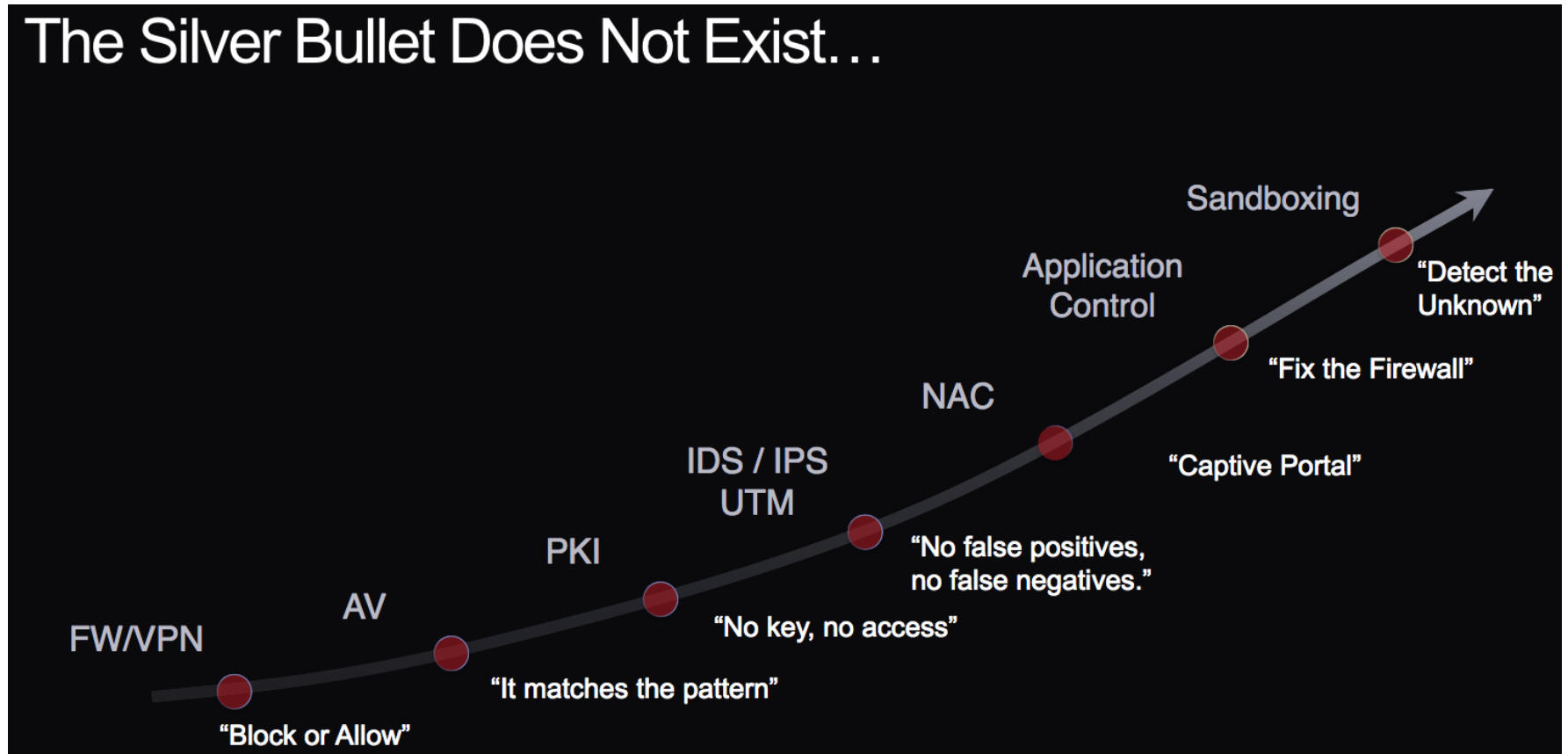


Actions de défenses possibles (non exhaustives)

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Web Analytics NBA FW/NIDS Logs Honeypot	Firewall ACL NIPS WAF				Firewall ACLs
Weaponization	NIDS	NIPS				NIPS
Delivery	Vigilant User	Proxy Filter NIPS File integrity App Whitelisting WAF	Inline AV	Queuing		App-Aware Firewall Firewall ACLs
Exploitation	HIDS Logs Monitoring	System Patching AV	DEP	Restricted user account		Inter-Zones NIPS
Installation	HIDS	jail	AV			
Command & Control	NIDS, Malware Sandbox	Firewall ACL	NIPS	Tarpit	DNS redirect	Trust Zones DNS Sinkholes
Actions on Targets	Audit logs DLP	Outbound ACL Encryption	DLP	Quality of Service	Honeypot	Trust Zones Incident Response

Sécurité préventive

The Silver Bullet Does Not Exist...



Network Security Monitoring

- Détection et réponse aux attaques informatiques via l'aspect réseau (opérations, outils et techniques)
- L'intérêt premier de NSM n'est pas de bloquer ou de filtrer mais de se concentrer sur la **visibilité**
- **Tout système de sécurité est faillible.** Le but de NSM n'est pas de reposer seulement sur la prévention mais également sur la détection et réponse à incidents.
- C'est un moyen de contremesure et de détection

Network Security Monitoring

- Collection, Détection, Analyse
- Collection: la partie I de ce cours va évoquer les différents types d'information obtainable via le réseau
- Détection: la partie II va se concentrer sur deux outils de détection: les IPS et les Honeypots
- Analyse: le TP va nous permettre de mettre en pratique ce cours via une analyse concrète.

Type d'informations

Exemple d'information utiles

- File
- URI - URL
- HTTP - GET
- HTTP - User Agent String
- URI - Domain Name
- Address - e-mail
- Address - ipv4-addr

- File - Path
- URI - URL

- File - Full Path
- File - Name
- File
- URI - URL
- HTTP - POST
- Email Header - Subject
- Email Header - X-Mailer
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - ipv4-addr

- Win Registry Key
- File - Name
- File
- URI - URL
- Streetname - McAfee
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - cidr
- Address - ipv4-addr

- Win Process
- Win Registry Key
- File - Full Path
- File - Name
- File
- File - Path
- URI - URL
- HTTP - GET
- HTTP - User Agent String
- Streetname - McAfee
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Hash - SSDEEP
- Address - e-mail
- Address - ipv4-addr

- Win Process
- Win Registry Key
- File
- URI - URL
- HTTP - GET
- HTTP - POST
- HTTP - User Agent String
- URI - Domain Name
- Hash - MD5
- Address - e-mail
- Address - ipv4-addr

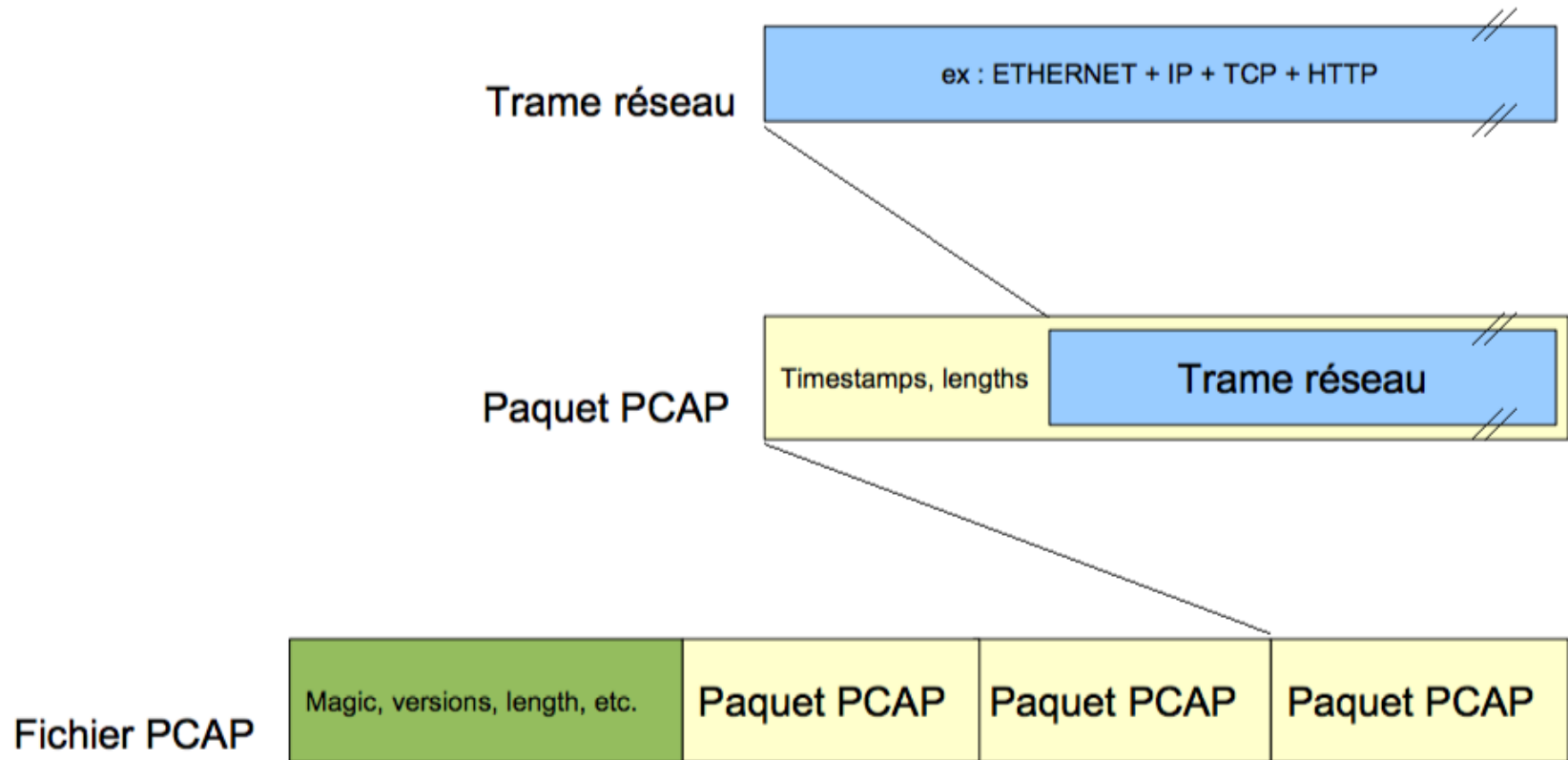
- Win Registry Key
- Win Service
- File - Full Path
- File - Name
- File
- File - Path
- URI - URL
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - ipv4-addr

Type d'information obtenues via NSM

- **Full content** : copie intégrale du trafic (PCAP)
- **Extracted content** : Information extraite depuis le trafic réseau comme des fichiers ou des pages web
- **Session data** : résumé des conversation réseaux se concentrent sur qui parle avec qui, quand et combien d'information on été échangées
- **Transaction data**: se concentre de façon plus granulaires sur les échanges et réponses dans les sessions réseaux.
- **Statistical data**: information calculée à partir des précédentes information et caractérise l'activité réseau
- **Metadata**: enrichissement des informations précédentes avec des informations tierces
- **Alert data**: remontée d'information par les outils

Full content

- Intégralité du trafic réseau stocké dans un PCAP (format de fichier contenant des paquets réseau capturés)



Full content

1679	1.176219	95.101.183.170	192.168.1.14	TCP	1506	80 → 50089 [ACK] Seq=1098721 Ack=1 Win=487 Len=1440 TSval=1690967221 TSecr=1001297270
1680	1.176249	192.168.1.14	95.101.183.170	TCP	78	[TCP Dup ACK 1676#2] 50089 → 80 [ACK] Seq=1 Ack=1095841 Win=4590 Len=0 TSval=1001297321 TSecr=1690967218 SLE=1097281 SRE=1100161
1681	1.177127	192.168.1.14	192.168.1.1	DNS	79	Standard query 0x067c A clients6.google.com
▼ Ethernet II, Src: Giga-Byt_52:c2:3e (90:2b:34:52:c2:3e), Dst: Sagemcom_81:32:ee (00:37:b7:81:32:ee)						
▶ Destination: Sagemcom_81:32:ee (00:37:b7:81:32:ee)						
▶ Source: Giga-Byt_52:c2:3e (90:2b:34:52:c2:3e)						
Type: IPv4 (0x0800)						
▼ Internet Protocol Version 4, Src: 192.168.1.14, Dst: 192.168.1.1						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes						
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 65						
Identification: 0x3869 (14441)						
▶ Flags: 0x00						
Fragment offset: 0						
Time to live: 64						
Protocol: UDP (17)						
▶ Header checksum: 0xbee3 [validation disabled]						
Source: 192.168.1.14						
Destination: 192.168.1.1						
[Source GeoIP: Unknown]						
[Destination GeoIP: Unknown]						
▼ User Datagram Protocol, Src Port: 49817 (49817), Dst Port: 53 (53)						
Source Port: 49817						
Destination Port: 53						
Length: 45						
▶ Checksum: 0x839e [validation disabled]						
[Stream index: 1]						
▼ Domain Name System (query)						
[Response In: 1735]						
Transaction ID: 0x067c						
▼ Flags: 0x0100 Standard query						
0... = Response: Message is a query						
.000 0... = Opcode: Standard query (0)						
.... ..0. = Truncated: Message is not truncated						
.... ..1. = Recursion desired: Do query recursively						
....0.. = Z: reserved (0)						
....0 = Non-authenticated data: Unacceptable						
Questions: 1						
0000	00 37 b7 81 32 ee 90 2b 34 52 c2 3e 08 00 45 00	.7..2..+ 4R.>..E.				
0010	00 41 38 69 00 00 40 11 be e3 c0 a8 01 0e c0 a8	.A8i..@.				
0020	01 01 c2 99 00 35 00 2d 83 9e 06 7c 01 00 00 015.-				
0030	00 00 00 00 00 00 08 63 6c 69 65 6e 74 73 36 06c lients6.				
0040	67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01	google.c om....				

Extracted content

- Flux de data de niveau applicatif (comme des fichiers)
- Applicatif au sens OSI. On ne parle plus d'adresses MAC ou IPs
- Information extraite depuis le trafic réseau comme des fichiers ou des pages web
- Outils: Bro extract_files,

Extracted content

```
GET /index.php HTTP/1.1
Host: wikipedia.fr
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Fri, 06 May 2016 20:12:41 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3334
Connection: close
Content-Type: text/html
```

```
.....Z.r...}.|....RE$uY;...H.TvE.....Hb8.@.....T.5....%.K...
2....lEek8...ht..@.o^?.p~.&*c.....c..a...q....B.|=|
{.v.m4.8.TQ.c..'.<.M.*..p6.....4.^..z..M..}.....x.N.0..X..K.....z.7.....
\....W'.N.....^.....nb.K..S,%).L....f..$.S.%&.l.:#
.3=.,#...~.D...BQK2!8..=....sI..}.....C.....V..E...,
$Q...S....j..g..M....."....f.....W.bH..?..$.0g..&.+.....~k.s....%.
.O...Hj}..
./..V[Z
..<.Fs[m-.,...$(<&.....?.\.....d.(#..$"..S....,lE..+.....r....1>.....`K...
1.....D.q.;.....0....l..8|.+)...4.c.|..z3...v.NgN2u..'.(.)..g.....f...y...uz.0n....
.D.8.....>3.K..u..~<.y.l<.@0..t.. ...Y.%t.(.2..(.....~:k.w=...E4.~..}....<.#...
```

Session Data

- Enregistrement de la conversation entre noeuds réseaux.
- Peut être généré depuis le full traffic ou généré à la volée et stocké en utilisant moins d'espace
- Exemple de protocol de Session Data: Netflow
- Netflow est à la full capture ce que la facture détaillée est à l'écoute téléphonique.

Session Data

StartTime	Flgs	Proto	SrcAddr	Sport	Dir	DstAddr	Dport	TotPkts	TotBytes	State
11:14:51.068922	e	udp	192.168.10.101	netbi*	->	192.168.10.255	netbi*	1	243	INT
11:14:53.758743	e	arp	192.168.10.127		who	192.168.10.101		2	120	CON
11:14:53.759078	e	icmp	192.168.10.127	0x0008	<->	192.168.10.101	0x0002	2	148	ECO
11:14:53.759659	e	tcp	192.168.10.127	1196	->	192.168.10.101	micro*	18	5178	CON
11:14:53.760213	e	icmp	192.168.10.127	0x0008	<->	192.168.10.101	0x0002	2	148	ECO
11:15:03.738050	e	udp	192.168.10.120	53533	->	255.255.255.255	2222	1	194	INT
11:15:05.126995	e	tcp	192.168.10.127	1196	->	192.168.10.101	micro*	7	560	FIN
11:15:13.287420	e	udp	192.168.10.128	1088	<->	192.168.10.101	domain	2	324	CON
11:15:13.287811	e	arp	192.168.10.101		who	192.168.10.100		2	120	CON
11:15:13.288346	e	udp	192.168.10.101	1036	<->	216.239.34.10	domain	2	324	CON
11:15:13.792503	e	arp	192.168.10.101		who	192.168.10.128		2	120	CON
11:15:13.794069	e	tcp	192.168.10.128	1295	->	74.125.45.100	http	7	1172	CON
11:15:14.082389	e	udp	192.168.10.128	1088	<->	192.168.10.101	domain	2	232	CON
11:15:14.082824	e	udp	192.168.10.101	1036	<->	72.14.235.9	domain	2	216	CON
11:15:14.391432	e	tcp	192.168.10.128	1296	->	74.125.19.103	http	27	15995	RST
11:15:14.917050	e	tcp	192.168.10.128	1297	->	74.125.19.103	http	13	6532	CON
11:15:15.525020	e	udp	192.168.10.128	1088	<->	192.168.10.101	domain	2	246	CON
11:15:15.525403	e	udp	192.168.10.101	1036	<->	216.239.34.10	domain	2	406	CON
11:15:15.589817	e	udp	192.168.10.101	1036	<->	74.125.77.9	domain	2	224	CON
11:15:15.652690	e	tcp	192.168.10.128	1298	->	74.125.19.113	http	23	4941	CON
11:15:16.603137	e	tcp	192.168.10.128	1299	->	74.125.19.113	http	20	4369	CON
11:15:18.742540	e	udp	192.168.10.100	2905	->	239.255.255.250	1900	1	329	INT

Transaction data

- Similaire à Session data mais se concentre sur les échanges entre deux hosts
- Moins détaillé que le full content mais également moins abstrait que session data
- Si le full content c'est l'écoute téléphonique et session data la facture détaillée alors transaction data donne un résumé succinct de chaque appel.

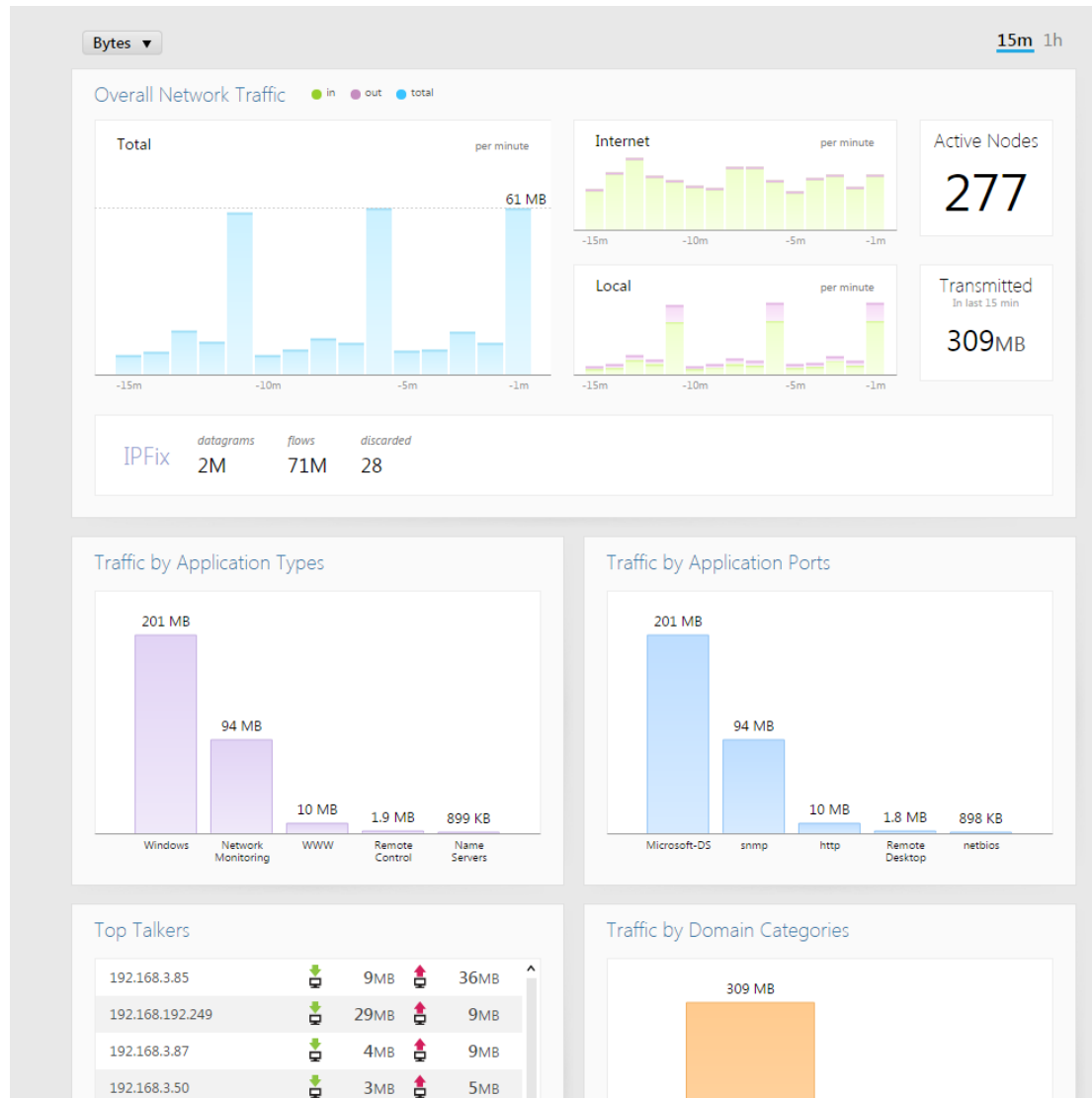
Transaction data

192.168.10.128	1295	74.125.45.100	80	1	GET	google.com	/	-	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219
192.168.10.128	1296	74.125.19.103	80	1	GET	www.google.com	/	-	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	6300
192.168.10.128	1296	74.125.19.103	80	2	GET	www.google.com	/intl/en_ALL/images/logo.gif	http://www.google.com/	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219
192.168.10.128	1297	74.125.19.103	80	1	GET	www.google.com	/extern_js/f/CgJlbhICdXMrMAo4DSwrMA44BCwrMBY4BCwrMBc4ASwrMBg4AywrMCU4yYgBLCswJzgALA/		Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	6300
192.168.10.128	1296	74.125.19.103	80	3	GET	www.google.com	/images/nav_logo3.png	http://www.google.com/	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219
192.168.10.128	1298	74.125.19.113	80	1	GET	clients1.google.com	/generate_204	http://www.google.com/	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219
192.168.10.128	1298	74.125.19.113	80	2	GET	clients1.google.com	/complete/search?hl=en&gl=us&q=bn	http://www.google.com/	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219
192.168.10.128	1299	74.125.19.113	80	1	GET	clients1.google.com	/complete/search?hl=en&gl=us&q=bni	http://www.google.com/	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219
192.168.10.128	1298	74.125.19.113	80	3	GET	clients1.google.com	/complete/search?hl=en&gl=us&q=b	http://www.google.com/	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219
192.168.10.128	1299	74.125.19.113	80	2	GET	clients1.google.com	/complete/search?hl=en&gl=us&q=bi	http://www.google.com/	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 0	219

Statistical data

- Calculé ou capturé sur une “longue période” (soit sur un mois ou alors sur la longueur du PCAP)
- Penser en terme d'évolution, de tendances
- Utilisation des compteurs de supervision réseau possible

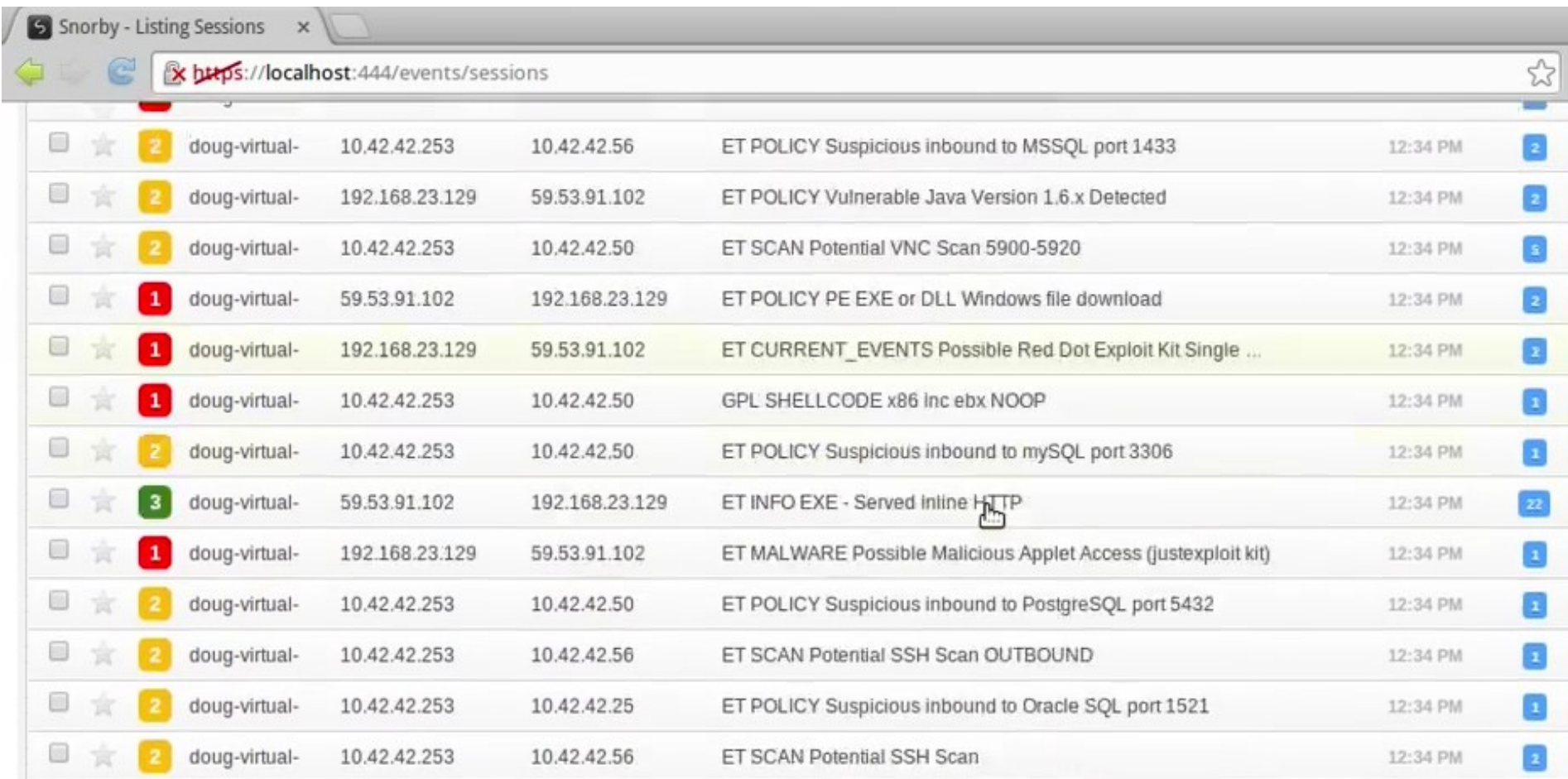
Statistical data



Alert data

- Information obtenue via l'analyse d'un outil
- Provient essentiellement d'un IPS (mais peut venir d'un SIEM également)

Alert data



<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	10.42.42.253	10.42.42.56	ET POLICY Suspicious inbound to MSSQL port 1433	12:34 PM	2
<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	192.168.23.129	59.53.91.102	ET POLICY Vulnerable Java Version 1.6.x Detected	12:34 PM	2
<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	10.42.42.253	10.42.42.50	ET SCAN Potential VNC Scan 5900-5920	12:34 PM	5
<input type="checkbox"/>	<input type="checkbox"/>	1	doug-virtual-	59.53.91.102	192.168.23.129	ET POLICY PE EXE or DLL Windows file download	12:34 PM	2
<input type="checkbox"/>	<input type="checkbox"/>	1	doug-virtual-	192.168.23.129	59.53.91.102	ET CURRENT_EVENTS Possible Red Dot Exploit Kit Single ...	12:34 PM	2
<input type="checkbox"/>	<input type="checkbox"/>	1	doug-virtual-	10.42.42.253	10.42.42.50	GPL SHELLCODE x86 Inc ebx NOOP	12:34 PM	1
<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	10.42.42.253	10.42.42.50	ET POLICY Suspicious inbound to mySQL port 3306	12:34 PM	1
<input type="checkbox"/>	<input type="checkbox"/>	3	doug-virtual-	59.53.91.102	192.168.23.129	ET INFO EXE - Served Inline HTTP	12:34 PM	22
<input type="checkbox"/>	<input type="checkbox"/>	1	doug-virtual-	192.168.23.129	59.53.91.102	ET MALWARE Possible Malicious Applet Access (justexploit kit)	12:34 PM	1
<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	10.42.42.253	10.42.42.50	ET POLICY Suspicious inbound to PostgreSQL port 5432	12:34 PM	1
<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	10.42.42.253	10.42.42.56	ET SCAN Potential SSH Scan OUTBOUND	12:34 PM	1
<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	10.42.42.253	10.42.42.25	ET POLICY Suspicious inbound to Oracle SQL port 1521	12:34 PM	1
<input type="checkbox"/>	<input type="checkbox"/>	2	doug-virtual-	10.42.42.253	10.42.42.56	ET SCAN Potential SSH Scan	12:34 PM	2

Beaucoup d'information ?

- L'idée n'est pas de seulement attendre l'alerte d'un outil
- L'important est de pouvoir extraire ce type d'information avant une éventuelle attaque.
- Le but de ces collectes est d'accroître la visibilité sur son réseau pour détecter des potentielles attaques mais également des problèmes de configuration, anomalies, etc.
- Correctement analysé dans un tableau de bord, cela peut donner des pistes même si rien n'est détecté par les outils (l'oeil humain reste l'outil le plus efficace pour des corrélations de sources diverses).

IDS / IPS

IDS / IPS

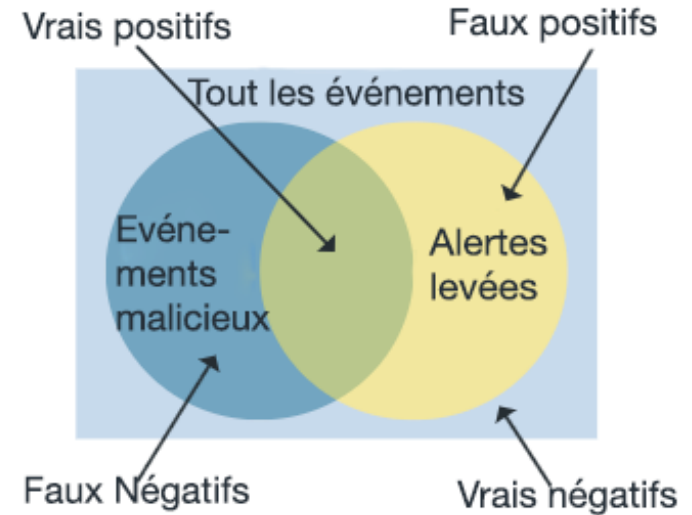
- L'IDS (Intrusion Detection System)
 - Surveiller
 - Contrôler
 - Détecter
- Permet de détecter des activités suspectes
- Composant important dans la surveillance du réseau.
- N'est pas infallible

Pourquoi un IDS / IPS ?

- Outils pour pirates amateurs facilement disponibles
- Anticiper des erreurs de configurations
- Principe de la sécurité de l'oignon
 - On ajoute des composants de sécurité par couches
 - Si on ne peut pas arrêter l'attaquant, on essaye de le ralentir le plus longtemps possible.

Vocabulaire

- Vrai positif: un incident est survenu et le système l'a détecté
 - Vrai négatif: Une activité bénigne est survenu et aucune alerte a été générée
 - Faux positif: Le système a alerté mais l'activité n'était pas malicieuse
 - Faux négatifs: un incident est survenu et le système ne l'a pas détecté
-
- Evasion: Technique utilisée pour dissimuler une attaque et faire en sorte qu'elle ne soit pas décelée par l'IDS
 - Obfuscation (encodage, encryption, polymorphisme)
 - Insertion et évasion (fragmentation, TCP segments, protocol ambiguities, low-bandwidth attacks)
 - Denial of Service (CPU or memory exhaustion, noise generation)



Vocabulaire

- IDS : surveillance
 - NIDS: Network IDS
 - HIDS: Host IDS
- IPS: analyse et réaction
 - NIPS: Network IPS
 - HIPS: Host IPS
- NBA
 - Network Behaviour analysis

IDS

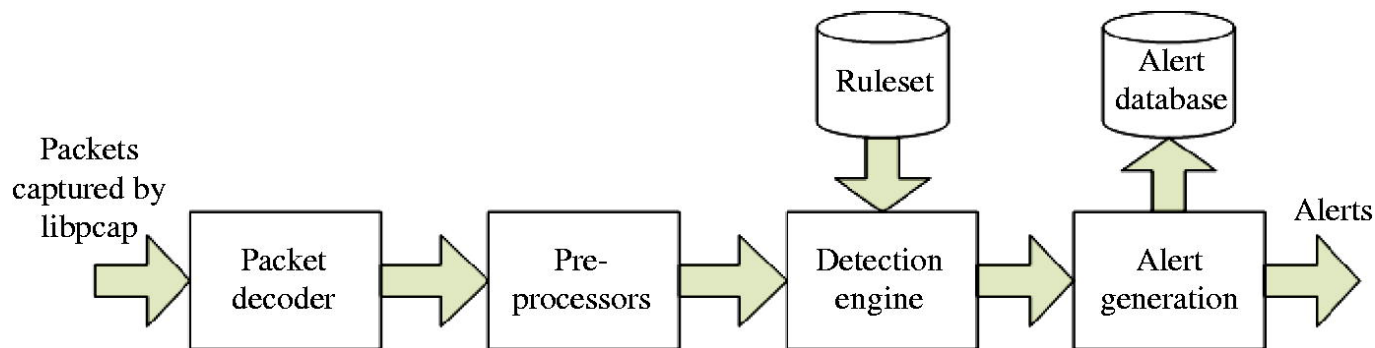
- Un IDS :
 - Analyse, surveillance
 - En cas de détection:
 - Journalise la tentative (données brutes et/ou log succinct)
 - Remonte l'alerte vers un système central (SNMP) ou vers une action humaine (Mail, SMS, etc...)
 - Capable de corrélations simples

HIDS

- S'installe sur un ordinateur comme un logiciel
- Surveille le système et les applications
 - Journaux système
 - Intégrité des fichiers
 - Appels systèmes
 - Connexions réseaux
- HIDS accède à des composants non-réseau
 - ex: Base de registre
- Ne surveille que l'ordinateur sur lequel il est installé

NIDS

- Un NIDS est essentiellement un sniffer réseau couplé avec un moteur qui analyse le trafic selon des règles
- Ces règles décrivent un trafic à signaler
- L'IDS peut analyser
 - Couche Réseau (IP, ICMP)
 - Couche Transport (TCP, UDP)
 - Couche Application (HTTP, Telnet)



Méthodes de détections

- 3 approches principales pour les IDS
 - A base de signatures: surveille le réseau ou les fichiers et les comparent à une base de données de menaces connues
 - Approche comportementale (Recherches d'anomalies): On prend un profil du système en état normal et on alerte lorsque l'état observé s'écarte trop de l'état normal.
 - Par intégrité: utilisé surtout sur les HIDS

Par signatures

- Basé sur la reconnaissance de schémas déjà connus
- Efficace sur les menaces connues mais inefficace pour menaces inconnues ou sur tentative d'évasion.
- Utilisation d'expressions régulières
- Les signatures d'attaques connues sont stockées dans une base; et chaque événement est comparé au contenu de cette base. Si correspondance l'alerte est levée
- L'attaque doit être connue pour être détectée
- Peu de faux-positifs
- L'efficacité est alors liée à la gestion de la base de signatures
 - MAJ
 - Nombre de règles
 - Signatures suffisamment précises
- Mécanisme à base de réputation est un sous-ensemble de reconnaissance par signatures

Par signatures

- **Avantage**
 - Simplicité de mise en œuvre
 - Rapidité de diagnostic
 - Précision (en fonction des règles)
 - Identification du procédé d'attaque (Procédé, Cibles, Sources, Outils)
- **Inconvénients**
 - Ne détecte que les attaques connues
 - Maintenance de la base
 - Techniques d'évasion possibles dès lors que les signatures sont connues

Par anomalies

- Basée sur le comportement « normal » du système
 - Phase d'apprentissage
 - Détecter une intrusion consiste à détecter un écart
 - Exemple de profil : Volumes des échanges réseau, Appels systèmes d'une application, Commandes usuelles d'un utilisateur
- Une déviation par rapport à ce comportement est considérée suspecte
- Le comportement doit être modélisé : on définit alors un profil
- Une attaque peut être détectée sans être préalablement connue
- Repose sur des outils de complexité diverses (Seuils, Statistiques, Méthodes probabilistes, Réseaux de neurones, Etc)
- Complexité de l'implémentation et du déploiement

Par anomalies

- Autre détection par anomalies: stateful protocol analysis
- Au lieu d'apprentissage, on compare contre le comportement protocolaire attendu
- Pour chaque type de protocole connu (DNS, FTP, HTTP), une machine d'état “normale” est définie
- L'IDS peut alors identifier une commande ou un état normalement non prévu
- Difficulté d'implémentation des “machines d'états”

Par anomalies

- Avantages
 - Permet la détection d'attaque inconnue
 - Facilite la création de règles adaptées à ces attaques
 - Difficile à tromper
- Inconvénients
 - Les faux-positifs sont nombreux
 - Générer un profil est complexe
 - Durée de la phase d'apprentissage
 - Activité saine du système durant cette phase ?
 - Stateful protocol analysis: nécessite une interprétation des standards. Consommateur de ressources.
 - Diagnostics longs et minutieux en cas d'alerte

Par intégrité

- Vérification d'intégrité
 - Génération d'une somme de contrôle sur des fichiers d'un système
 - Une comparaison est alors effectuée avec une somme de contrôle de référence
- Exemple : une page web
- Méthode couramment employée par les HIDS

IPS

- IPS = Intrusion Prevention System – Mieux vaut prévenir que guérir
- Constat :
 - On suppose pouvoir détecter une intrusion
 - Pourquoi alors, ne pas la bloquer, l'éliminer ?
- IDS vers IPS
 - Terme à la base plutôt marketing
 - Techniquement
 - Un IPS est un IDS qui ajoute des fonctionnalités de blocage pour une anomalie trouvée
 - IDS devient actif => IPS

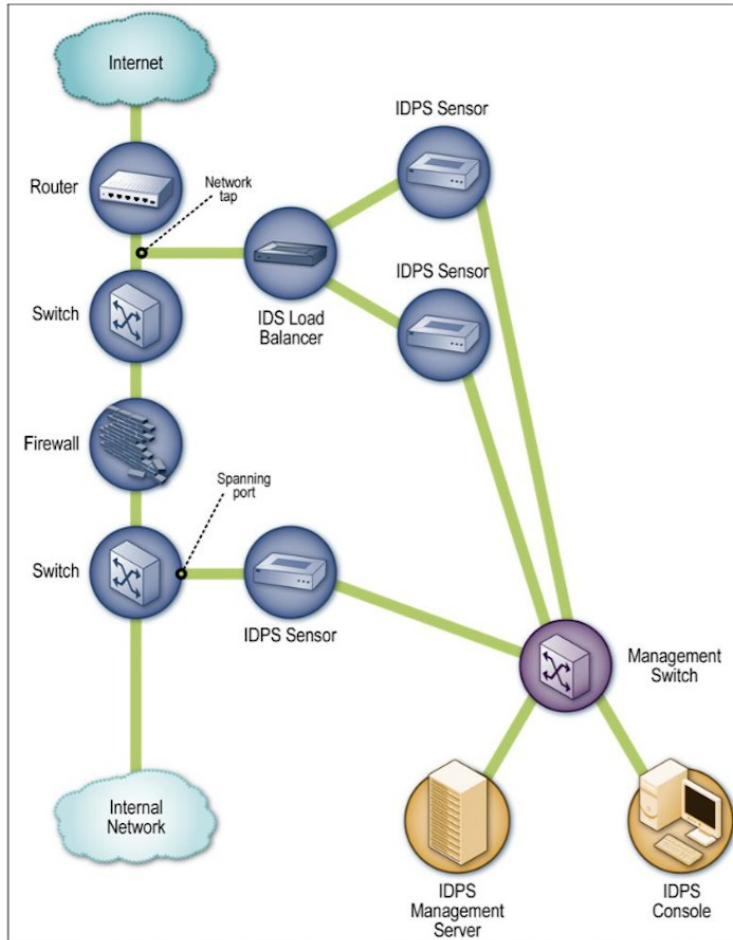
IPS

- Objectifs :
 - Interrompre une connexion
 - Ralentir la connexion
 - Blacklister les sources
- Moyens :
 - Règle Firewall (inline ou reconfigurer un autre équipement)
 - QoS
 - Intervention applicative (Proxy)
 - Blackholing (Routage)
 - Script
 - Sanitization (suppression pièce jointe malveillante)

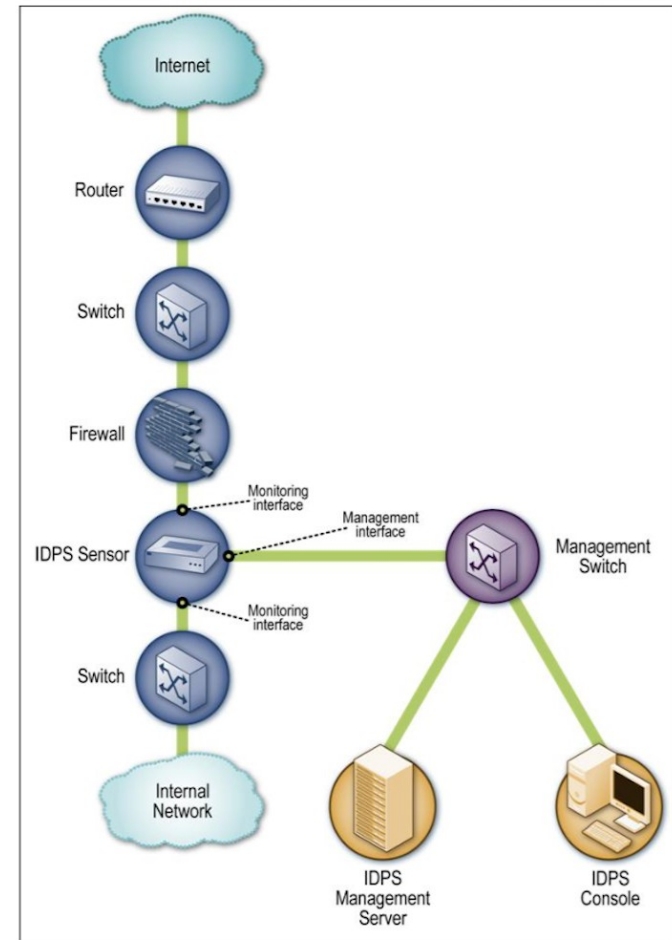
IDS / IPS positionnement

- IDS : inline, outband (TAP ou miroir de port)
- IPS: inline
- Positionnement
 - Entrée Internet: bruit
 - DMZ
 - LAN

IDS / IPS positionnement



Passive (outband) Network-Based IDPS



Inline Network-Based IDPS

IDS / IPS : le marché

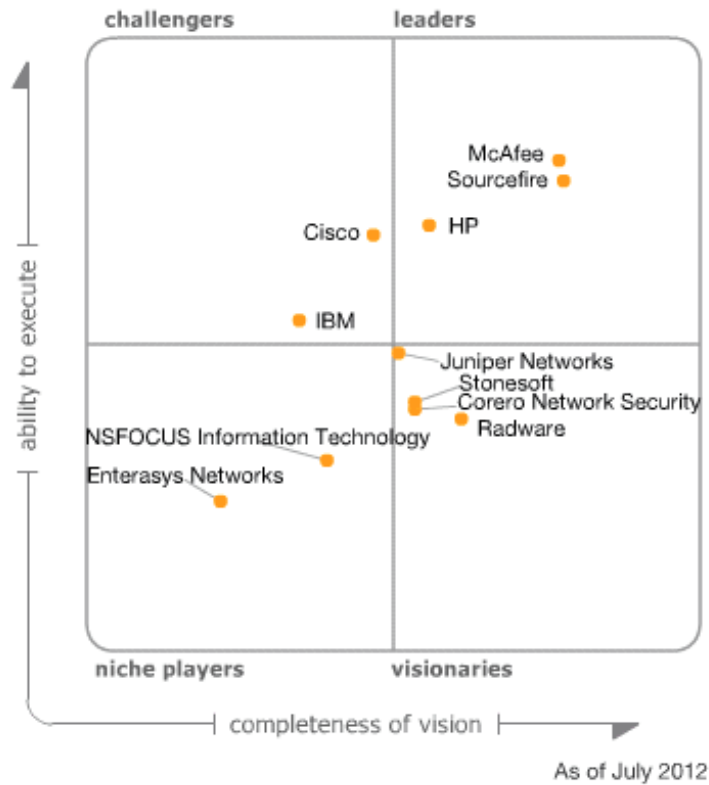
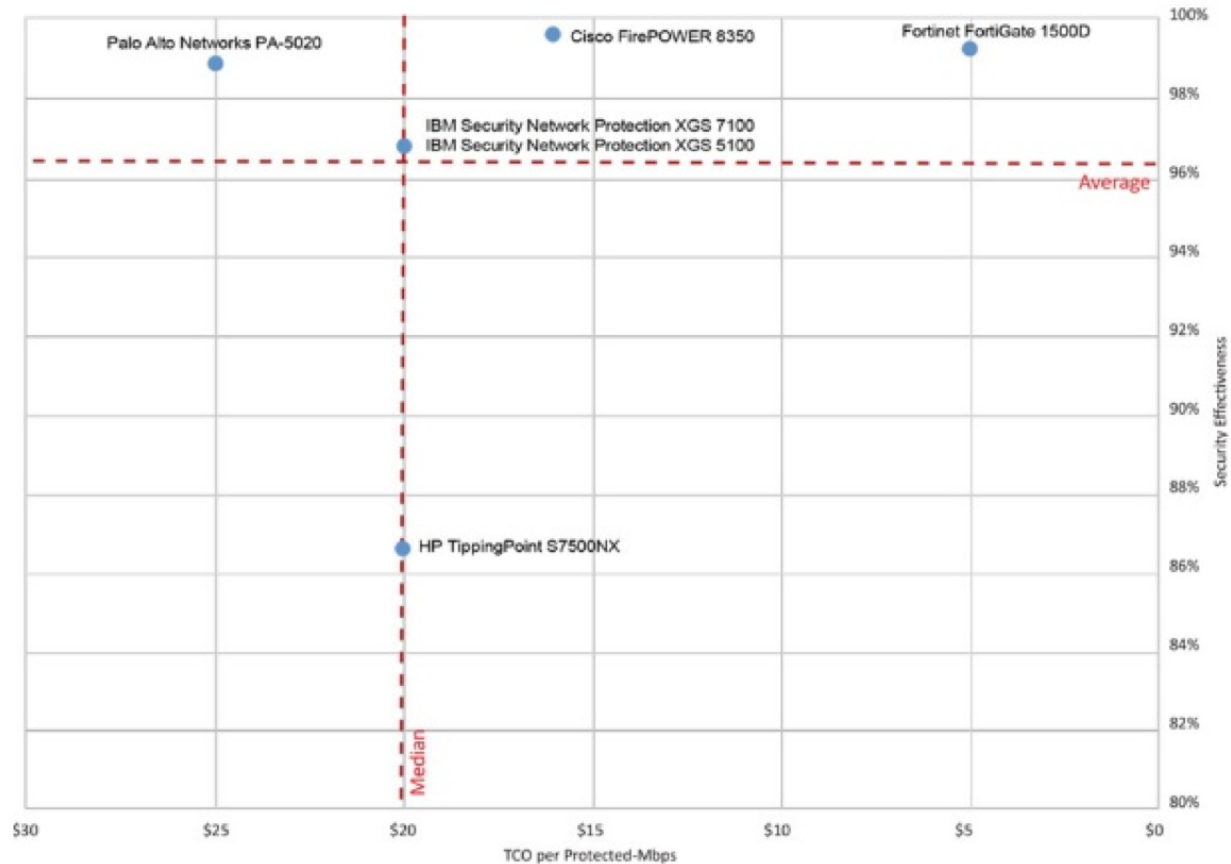


Figure 1. Magic Quadrant for Intrusion Prevention Systems



IDS / IPS : le marché



IDS / IPS : le marché

- NIDPS
 - Snort
 - Bro
 - Suricata
- HIDS
 - OSSEC
 - Tripwire
 - AIDE
 - Samhain
- Hybride
 - Prelude

IDS / IPS

- Avantages

Sécurité = Visibilité + Contrôle

- IDS/IPS augmente ces facteurs
- Anticipation du trafic anormal
- Attaque bloquée immédiatement (IPS)
- Inspection applicative
- Journalisation du trafic

IDS / IPS

- Inconvénients
 - Les faux-positifs (temps, énergie)
 - Peut paralyser le réseau (IPS)
 - Technologie complexe
 - Nécessite un degré d'expertise élevé
 - Long à optimiser
 - Réputer pour générer de fausses alertes
 - Capacité à soutenir la charge
 - Trafic encrypté échappe à l'analyse
 - Evasion
 - Les UTM intégrant ces fonctionnalités, l'IDS/IPS seul se fait plus rare

Honeypot

Définition

- Logiciel dont le seul but est d'être sondé, attaqué, compromis, utilisé ou accédé d'une manière illégitime
- Peut être un service, une application, un système ou juste un fichier ou une information
- Point clé: toute entité se connectant ou essayant d'utiliser la ressource est par définition suspecte
- Reproduit fidèlement la ressource simulée.
- Buts différents: surveillance des vers/scans, détection de client compromis, capture de malware, étude des hackers, anticipation d'attaque

Classification

- Type de ressources attaquées
 - Server-side honeypot
 - Client-side honeypot
 - Honeytokens
- Type d'interaction
 - High-interaction
 - Low-interaction
 - Hybrid

Server-side Honeypot

- Agit comme un serveur
 - Écoute des ports, simule des services
 - Attend les connexions
- Détecte souvent les scans ou bots
- Sert aussi à détecter les attaques “manuelles”
- Considéré comme le honeypot “traditionnel”

Client-side Honeypot

- Honeyclients
- Détecte les attaques sur les applications clients
- Plus populaire et plus attaqué: Navigateur web
- Différents des server-side
 - Etablit activement des connexions aux services
 - Tente de détecter un comportement malicieux du serveur et/ou du contenu

Honeytokens

- Honeytrap qui est tout sauf un logiciel. Une donnée
- Nécessité de faire “vrai”
- Minimiser les faux positifs: unicité
- Exemples
 - Fichier sur FTP ou SMB (ex: confidential data)
 - Web
 - Fausse URL (listée dans robots.txt)
 - Cookie facilement modifiable
 - URL mis en commentaire dans code source HTML
 - Email
 - Financier
 - Enregistrement DNS

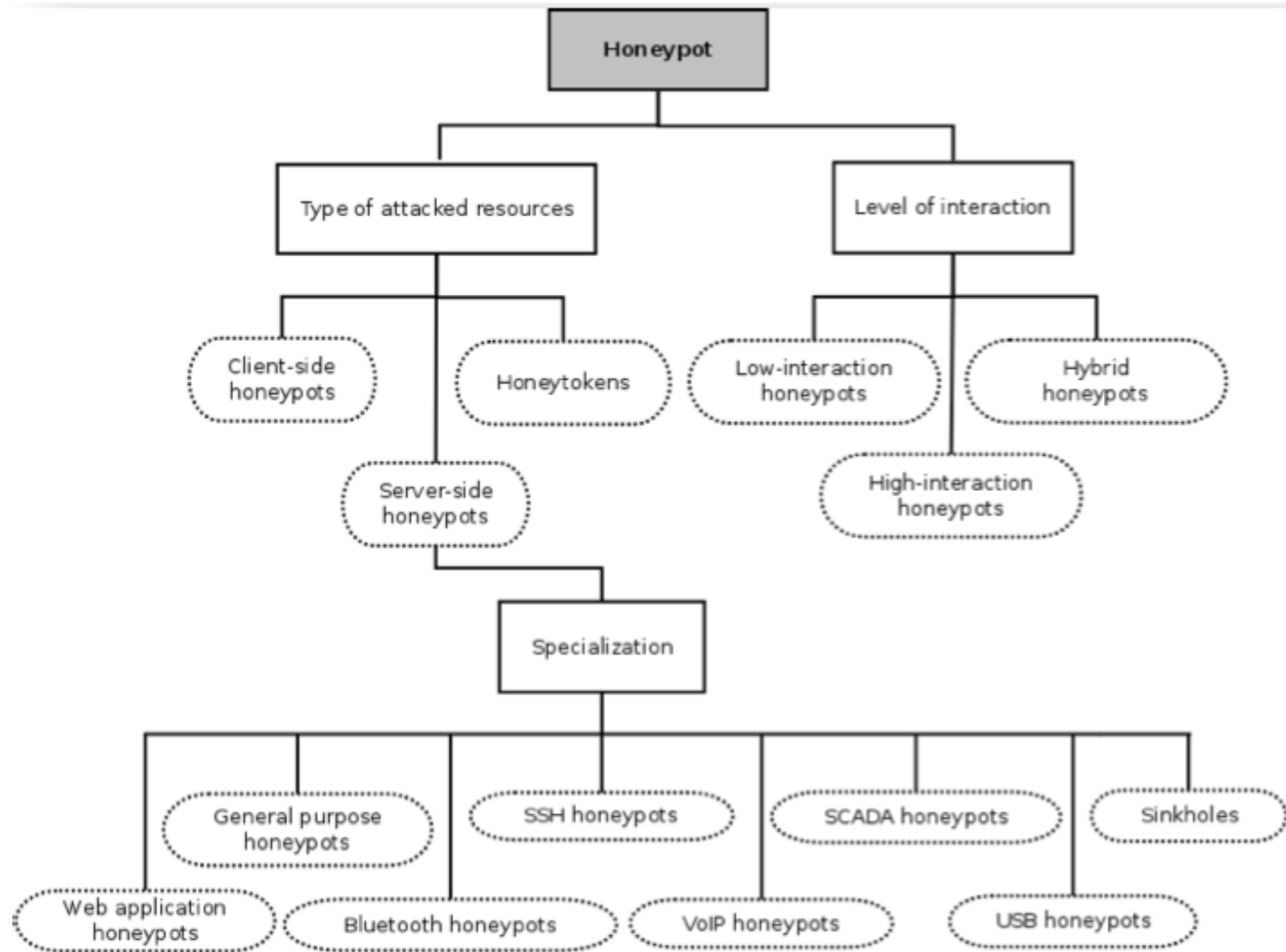
Low-interaction Honeypot

- Emule les ressources : limitées en fonctionnalités par rapport aux réelles
 - Service (server-side)
 - Application client (honeyclients)
- Interaction limitée. Degré de fidélité joue dans la qualité du honeypot.
- Facile à déployer et à maintenir. Emulation limite les risques de compromission réelle.
- Difficile à reproduire des 0-days

High-interaction Honeypot

- Fournit les vrais ressources. Non émulé.
 - Utilisation de la virtualisation
- Reproduction fidèle offre plus de possibilité: détection de 0-day par exemple.
- Limité aux applications et à la version de l'OS installé
- Complexité
 - Beaucoup de données
 - Différencier les données bénignes des comportements malicieux.
- Difficile à utiliser et déployer:
 - Nécessite plus de ressources
 - Risque de perte de l'honeytrap

Résumé



Honeypot et IDS/IPS

- Honeypot
 - Fait pour être accéder par le trafic malicieux
 - Moins de faux positifs
 - Ne détecte pas les attaques dirigées vers les ressources de production
- IDS / IPS
 - Plus de couverture
 - Plus de faux positifs
- Complémentaire
 - Honeypot peut détecter des attaques passant les IDS
 - IDS/IPS peuvent rediriger les attaques vers les honeypots

Positionnement

- Frontal d'internet
 - Le plus courant
- Interne
 - Détection d'APT
 - Attention aux faux positifs
- Réseau de honeypot

Software

Server-Side Low interaction

Port	Service	Honeypot
21/TCP	FTP	Dionaea
22/TCP	SSH	Kippo
42/TCP	WINS	Dionaea
69/UDP	TFTP	Dionaea
80/TCP	HTTP	Glastopf
135/TCP	MS Windows RPC	Dionaea
445/TCP	SMB	Dionaea
443/TCP	HTTPS	Dionaea
1433/TCP	MSSQL	Dionaea
3306/TCP	MySQL	Dionaea
5060/UDP	VoIP (SIP+SDP)	Dionaea
8080/TCP	HTTP	Glastopf
Other	Others at a basic level	Honeyd

Client-Side

- Thug (LI)
- Capture-HPC (HI)
- HoneySpider (framework)

Résumé

- Outil puissant et complexe.
 - Avantage
 - Faiblesse
- Implications légales (rebond)
- Peu de percée constructeurs (à part Juniper), essentiellement Open Source
- Utilisation de honeytokens à recommander

Bilan

Bilan

- “La sécurité n'est pas un produit, c'est un processus.”
Bruce Schneier