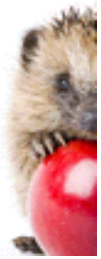


Threat Management
déploiement rapide de contre-mesures

J. Viinikka, E. Besson

13 décembre 2011

- notre métier : éditeur de **solutions de lutte intelligente contre les menaces informatiques**

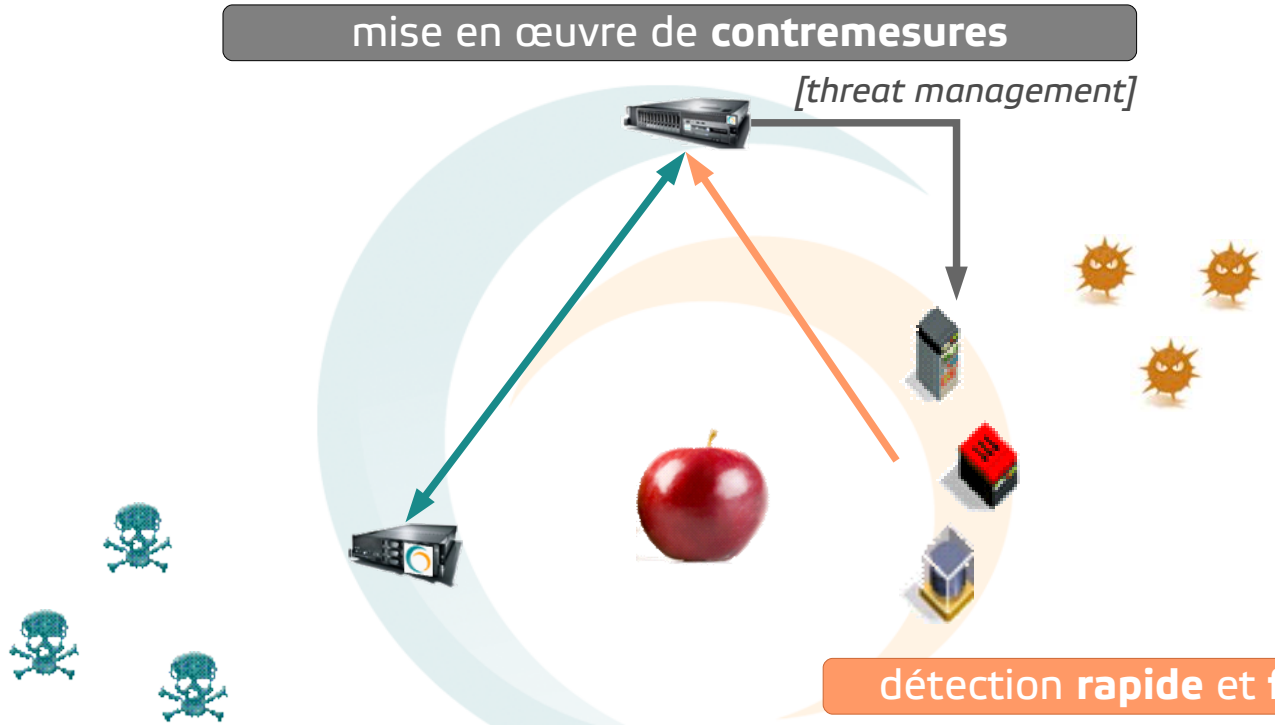
- partenaires
  - spin-off des Orange Labs
  - Ministère de la Recherche, OSEO

- nos pôles d'activité
  - apporter des **solutions** « clé en main » à nos clients
  - poursuivre et enrichir l'**innovation** (R&D)
  - fournir **expertise** et **conseil**

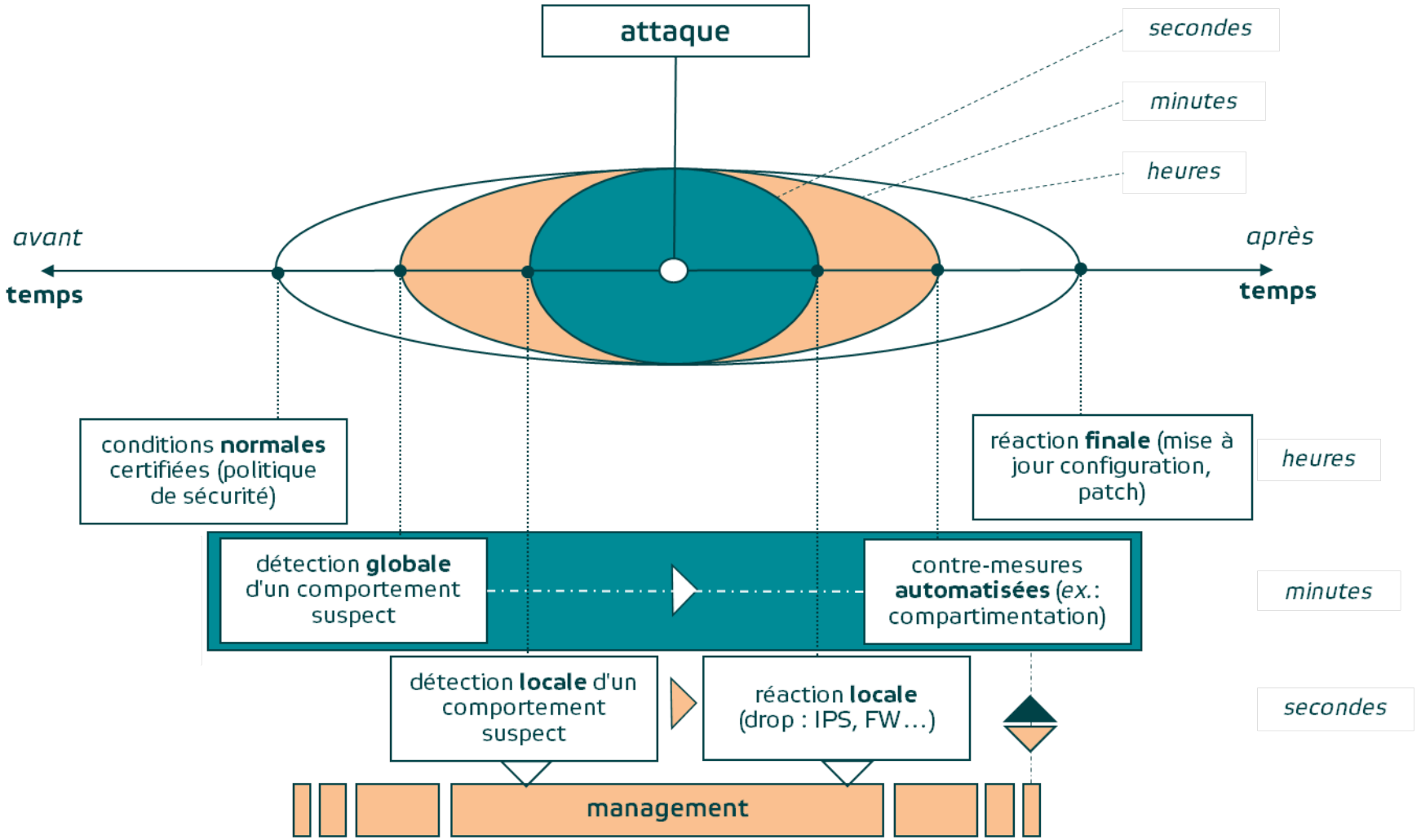
>MASSIF<

solutions innovantes de sécurité

- notre ambition : offrir une véritable solution de « **réaction managée** » aux attaques informatiques



approche par réaction



la problématique

- contexte : prévention, détection, réaction
- réaction intelligente
  - défis
    - énumération des contre-mesures possibles
    - estimation d'impact
  - notre proposition
    - en recherche
    - en produit

approche par prévention

- renforcement de la sécurité en phase de conception, avant le « run »
  - politiques de sécurité
  - contrôle d'accès, authentification, chiffrement
- limitations
  - notamment en « run »
  - plus ou moins statique, contrairement au SI supervisé
  - nouvelles menaces, erreurs humaines, etc.

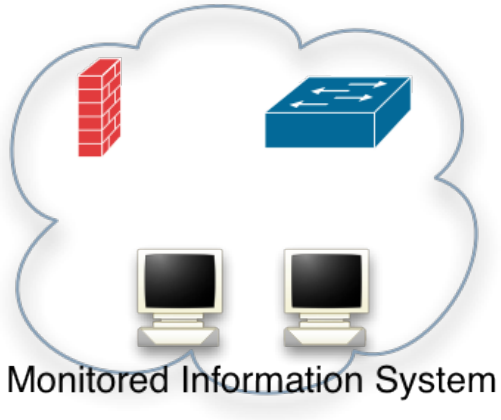
approche par détection

- observons si nos mesures de prévention sont efficaces...
  - analyse des logs équipements réseau, OS, applications, etc.
  - sondes dédiés : IDS, anti-virus, etc.
  - appels utilisateurs/clients
- faisons nous aider dans l'analyse...
  - log management systems
  - **S**ecurity **I**nformation & **E**vent **M**anagement
    - normalisation, enrichissement, corrélation, visualisation
- limitations
  - difficultés dans la détection et gestion des événements
  - dans le meilleur des cas, nous pouvons assister au massacre de notre SI en temps (quasi) réel

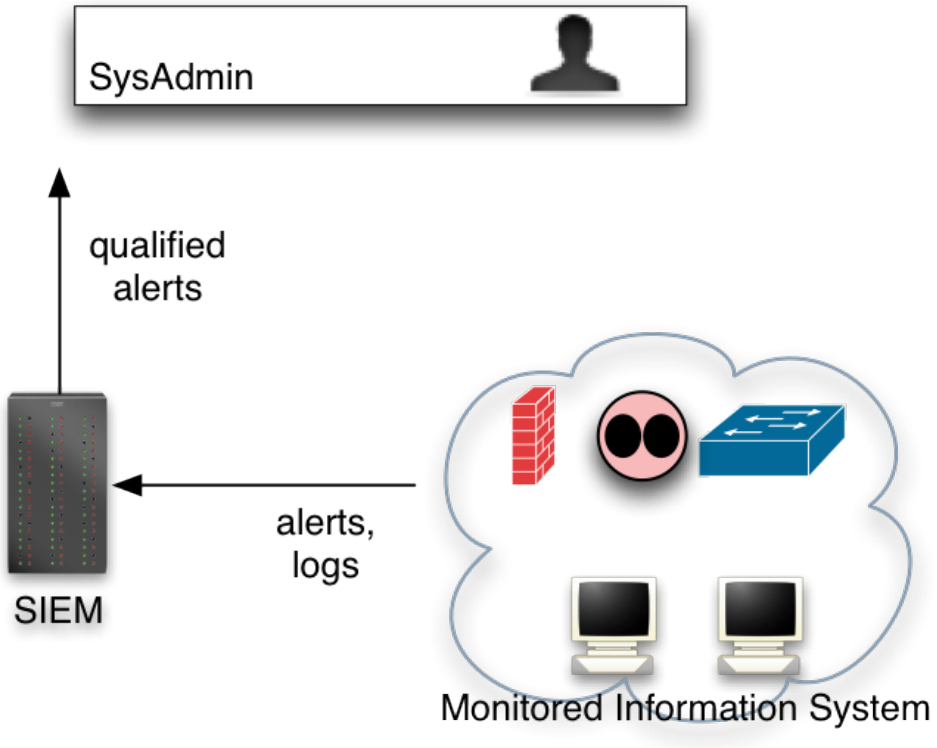
approche par réaction

- de l'observation au déploiement des contre-mesures
  - contre-mesure =! contre-attaque
  - des actions sur nos équipements
    - activation, reconfiguration, etc.
    - routeurs, switches, pare-feux, IDS, IPS, annuaires, applications...
- aujourd'hui réaction ± intervention manuelle
  - latence (réunion de crise, process, outils hétérogènes...)
  - risqué : erreurs de manipulation, estimation d'impact
- **objectif** : aider l'opérateur de sécurité
  - proposition des contre-mesures possibles
  - estimation de l'**impact** de l'attaque et des contre-mesures
  - automatisation de reconfiguration des équipements

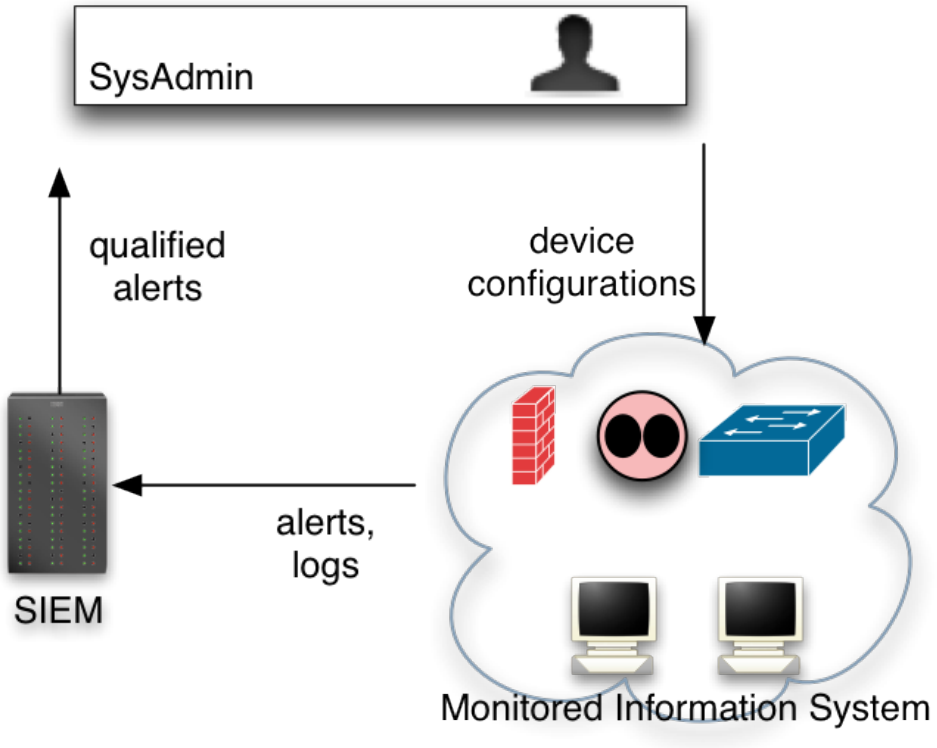
approche par prévention



approche par détection



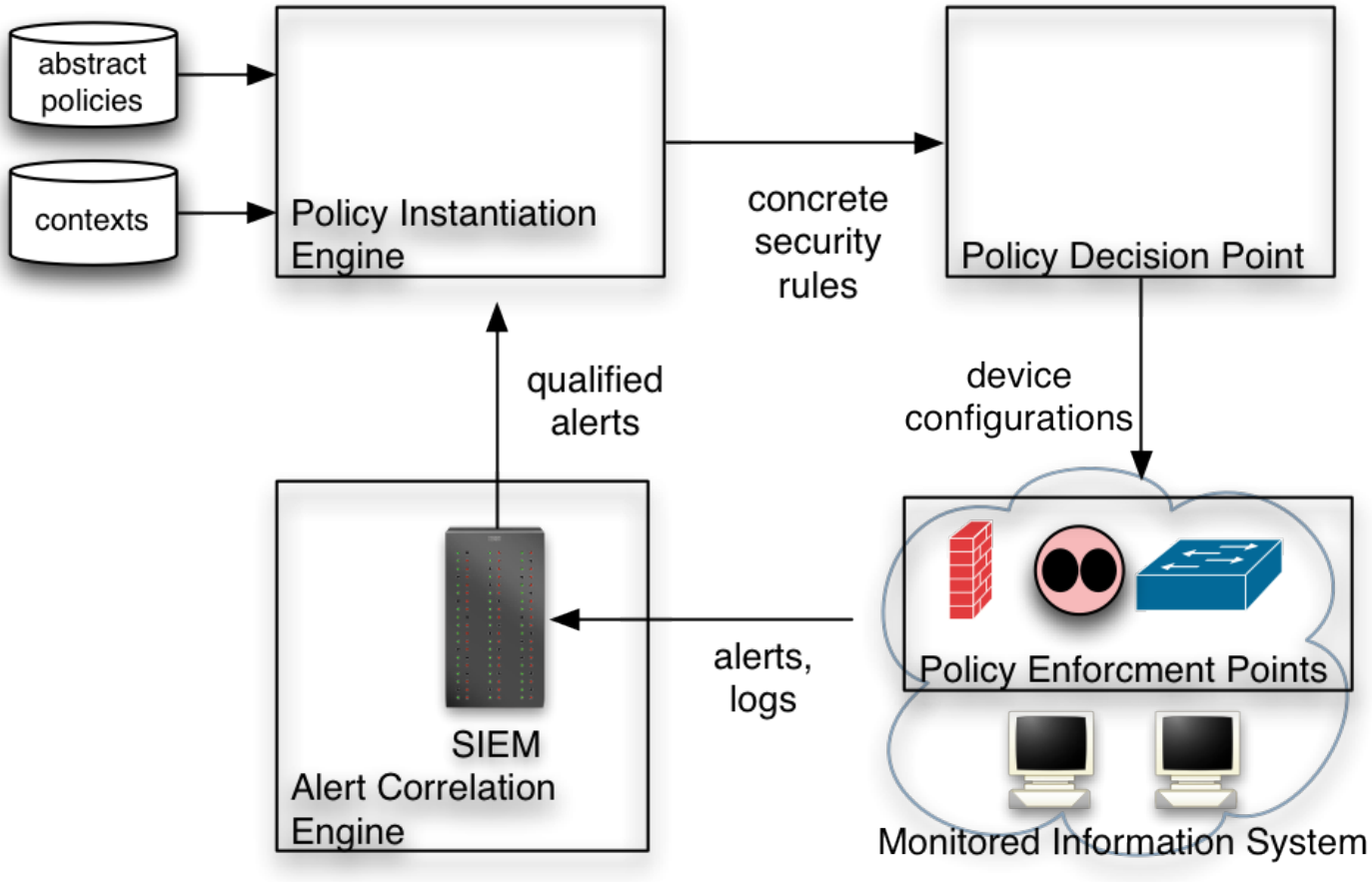
approche par réaction



réaction basée sur les politiques

- gestion dynamique des politiques de sécurité : un concept existant
  - e.g. [DTCCB2007] propose un système de pilotage de réaction basé sur formalisme Orbac
- politique contextuelle permet de déclencher des règles de sécurité en fonction de la menace portée par des alertes
- équilibrage entre sécurité et QoS
  - politique normale
  - politique de réaction
  - politique minimale
- résolution des conflits

réaction basée sur la politique



choix de la réaction optimale

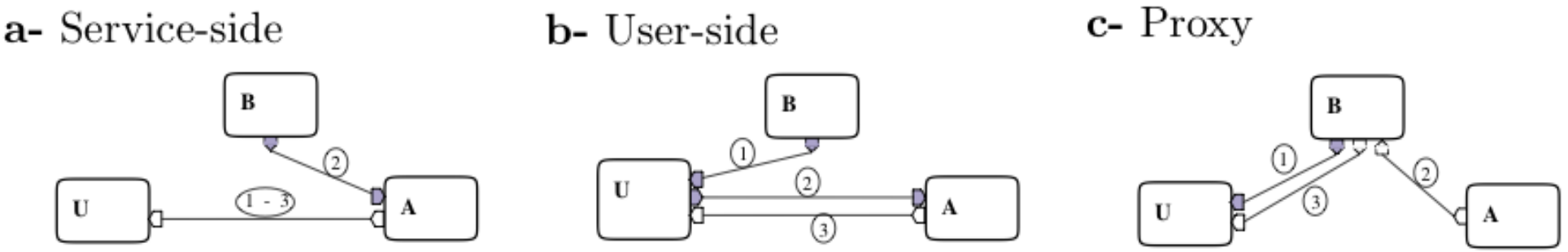
- le but : éviter que le remède ne soit pire que la maladie
- des défis :
  - énumération des contre-mesures possibles
  - évaluation d'impact de l'attaque et des contre-mesures
- une part de la solution :
  - modélisation des **dépendances** des services
  - propagation des **impacts**

dépendances de service

- un modèle « requires/provides » [KDCCV2009]
- un service fournit des informations, dont un autre peut avoir besoin pour fonctionner
- quelques caractéristiques d'un service :
  - *type* : données échangées et leurs chemins
  - *mode* : occurrence dans le cycle de vie de service
  - *impact* : effet de dégradation sur les services dépendants

dépendances de service

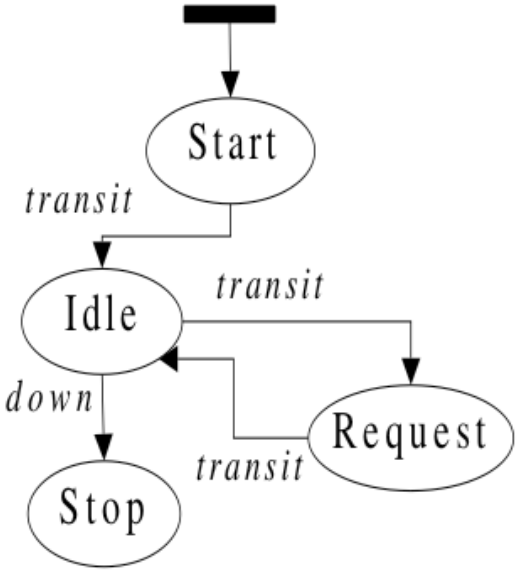
- type : données échangées et leurs chemins



- A : service dépendant, B : service antécédent, U : utilisateur du service dépendant

dépendances de service

- mode : occurrence dans le cycle de vie du service



a- Stateless sequencing

b- Statefull sequencing

c- Alternative sequencing

quelques références

- [DTCCB2007] Hervé Debar, Yohann Thomas, Frédéric Cuppens, and Nora Cuppens-Boulahia. *Enabling automated threat response through the use of a dynamic security policy*. Journal in Computer Virology (JCV), 3:195–210, August 2007
- [KDCCV2009] Kheir, N., Debar, H., Cuppens, F., Cuppens-Boulahia, N., Viinikka, J.: *A service dependency modeling framework for policy-based response enforcement*. In: Flegel, U., Bruschi, D. (eds.) DIMVA 2009. LNCS, vol. 5587, pp. 174–193. Springer, Heidelberg (2009)

de la R&D au(x) produit(s)...

- en **théorie**, inputs nécessaires (liste non exhaustive...)
  - topologie réseau, cartographie applicative
  - dépendances des services
  - équipements et capacités de réaction (et canaux de contrôle)
  - politiques de sécurité formelles
- en **pratique**, possible (et obligé...) de travailler avec moins
  - visualisation des configurations proposées
  - automatisation de certaines manipulations
    - ordre BGP, trap SNMP, manipulation de switch bypass
  - gestion des réactions en cours (workflow)
  - lien entre SIEM et réaction

threat management – principes (1/2)

- visualisation temps réel des attaques (alertes)
  - **cartographie** de l'attaque (topologie)
  - sources, destinations, relais… (niveaux réseau, service, utilisateur)
- aide à la décision (optimisation sous contrainte)
  - **cartographie** des **éléments actifs**
  - corrélation événement / actions (/ politiques)
- **évaluation** de la stratégie de réponse :
  (objectif) ratio efficacité / impact

taux de flux/clients malveillants éliminés

taux de flux/clients "innocents" impactés

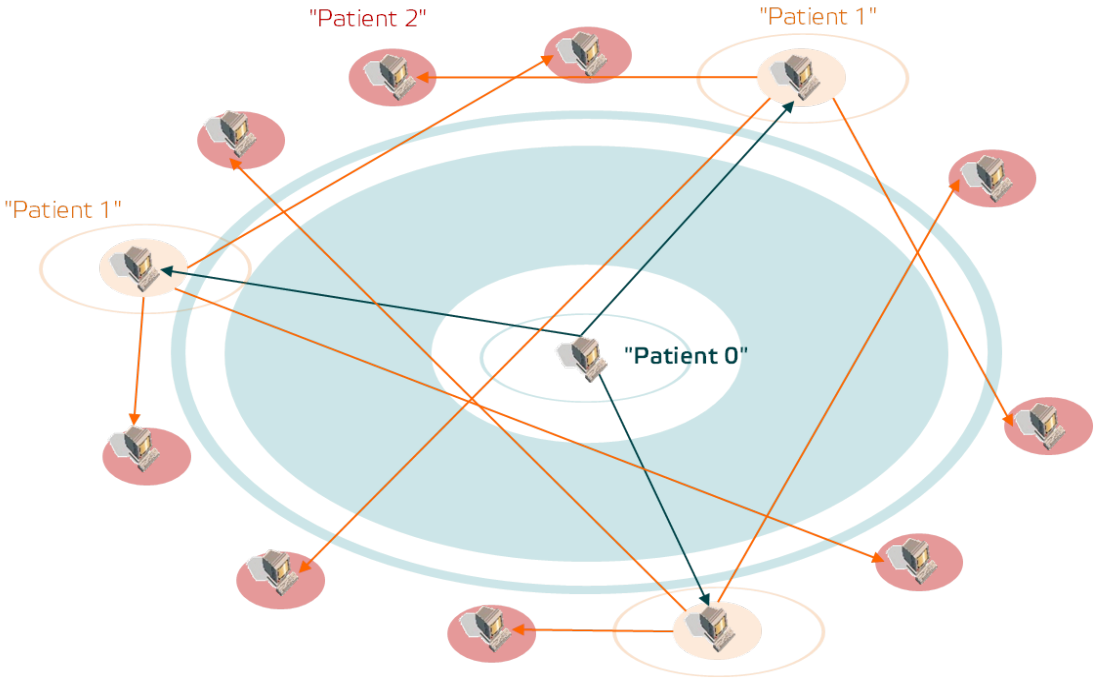
threat management – principes (2/2)

- pilotage de contremesures (**compatibilité**)
  - redirection de flux
    - poubellisation (ex.: black/sink holing)
    - compartimentation (ex.: redirection VLAN de quarantaine)
    - (… ou première réaction avant…)
  - filtrage
    - contrôle d'accès (ex. : ACL, désactivation compte LDAP)
    - poubellisation (ex. : drop IPS)
  - nettoyage

- **interopérabilité**
  - alertes (SIEM, IDS, logs)
  - cartographie (NMS, inventaires, annuaires)

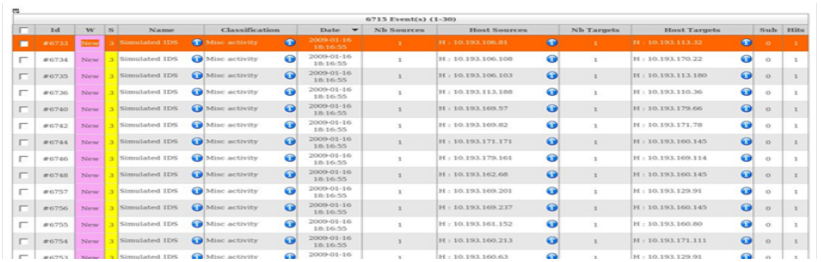
application : propagation virale

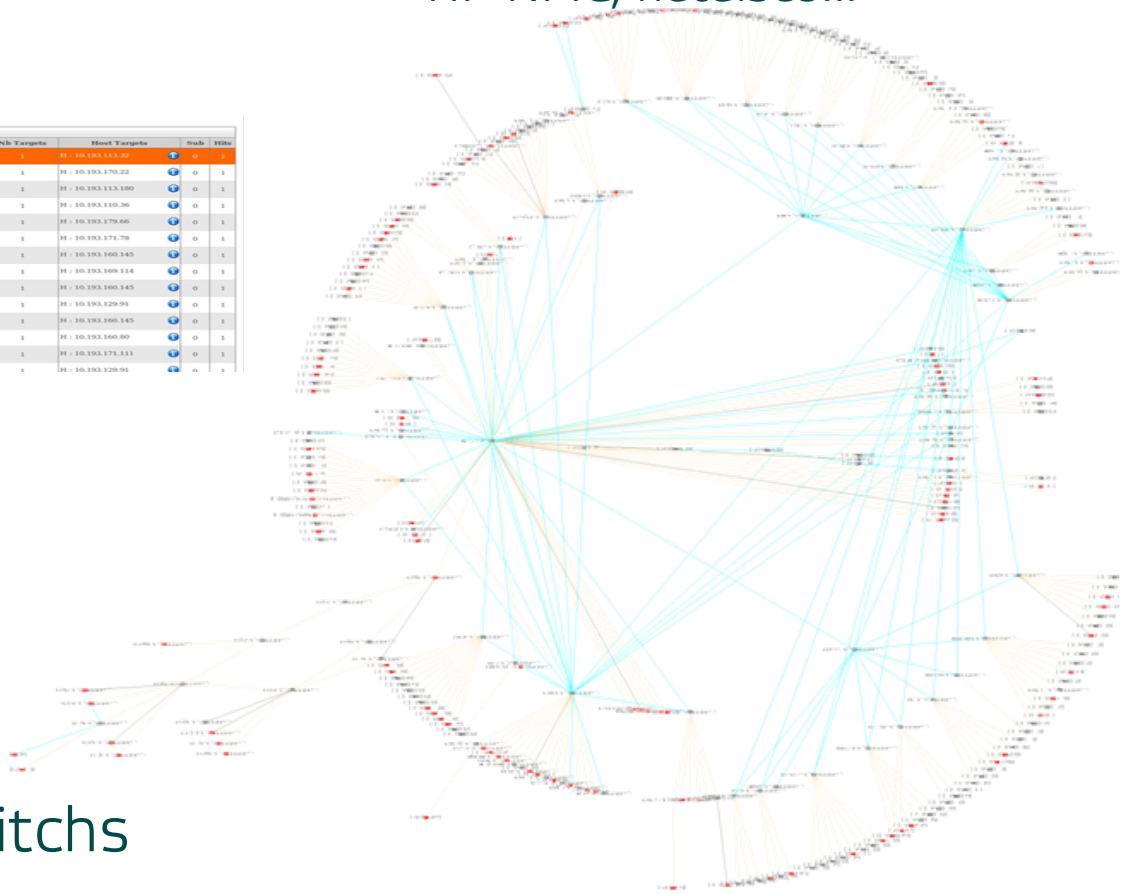
- modèle "source-centric"
- alertes
  - analyse de logs (IDS, anti-virus)
  - corrélation d'anomalies réseau (arbre de propagation)
- réaction
  - confiner la propagation
  - *patch management* (hors scope)



application : propagation virale

- moteur d'aide à la décision
  - données d'événements SIEM
    sources / destinations
  - bases de cartographie NMS
    HP NMC, netdisco...





- éléments actifs : switchs

application : propagation virale

- réaction : compartimentation des hôtes infectés
  - désactivation de port
  - bascule VLAN

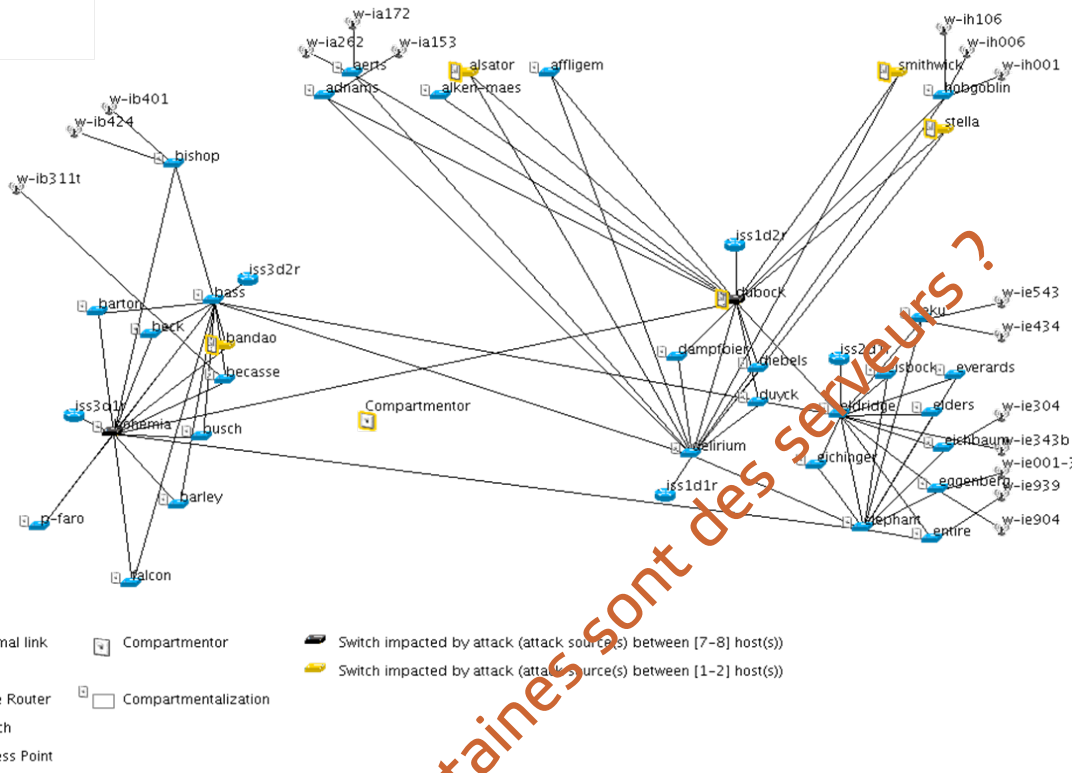
Reaction #2

Perimeter	Type	Description	Events	Date	State	Operation
ftrd	Compartmentalization	Compartmentalization	#6209 #6253 #6259 #6262 #6358	Sat Jan 17 19:36:39 CET 2009	New	

List redirection operations

Id	Parameter	Value	State	Operation
	Type	Compartmentalization		
	Equipment	Compartmentor		
#2	Commands	Id / Switch / Port / Community / Command / Action	New	

Id	Switch	Port	Community	Command	Action
1	172.26.48.123	4.19	unknown	Deactivate	
2	172.26.48.77	2.15	unknown	Deactivate	
3	172.26.48.74	3.9	unknown	Deactivate	
4	172.26.48.89	4.45	unknown	Deactivate	
5	172.26.48.89	4.25	unknown	Deactivate	
6	10.193.165.27	fastethernet0/1	unknown	Deactivate	
7	172.26.48.123	4.21	unknown	Deactivate	
8	172.26.48.114	2.27	unknown	Deactivate	
9	10.193.165.27	fastethernet0/2	unknown	Deactivate	
10	172.26.48.123	4.36	unknown	Deactivate	
11	172.26.48.123	4.26	unknown	Deactivate	
12	172.26.48.123	4.11	unknown	Deactivate	
13	172.26.48.78	2.42	unknown	Deactivate	
14	172.26.48.123	4.23	unknown	Deactivate	

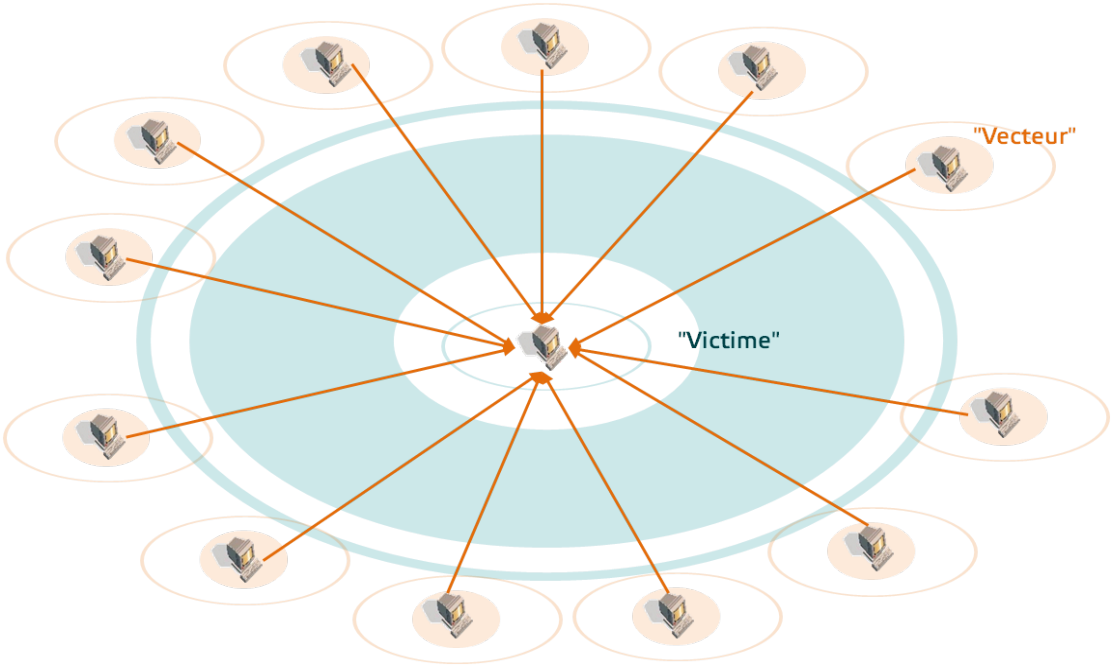


et si certaines sont des serveurs ?

- impact (source-centric) :
  machines non infectées "compartimentées"

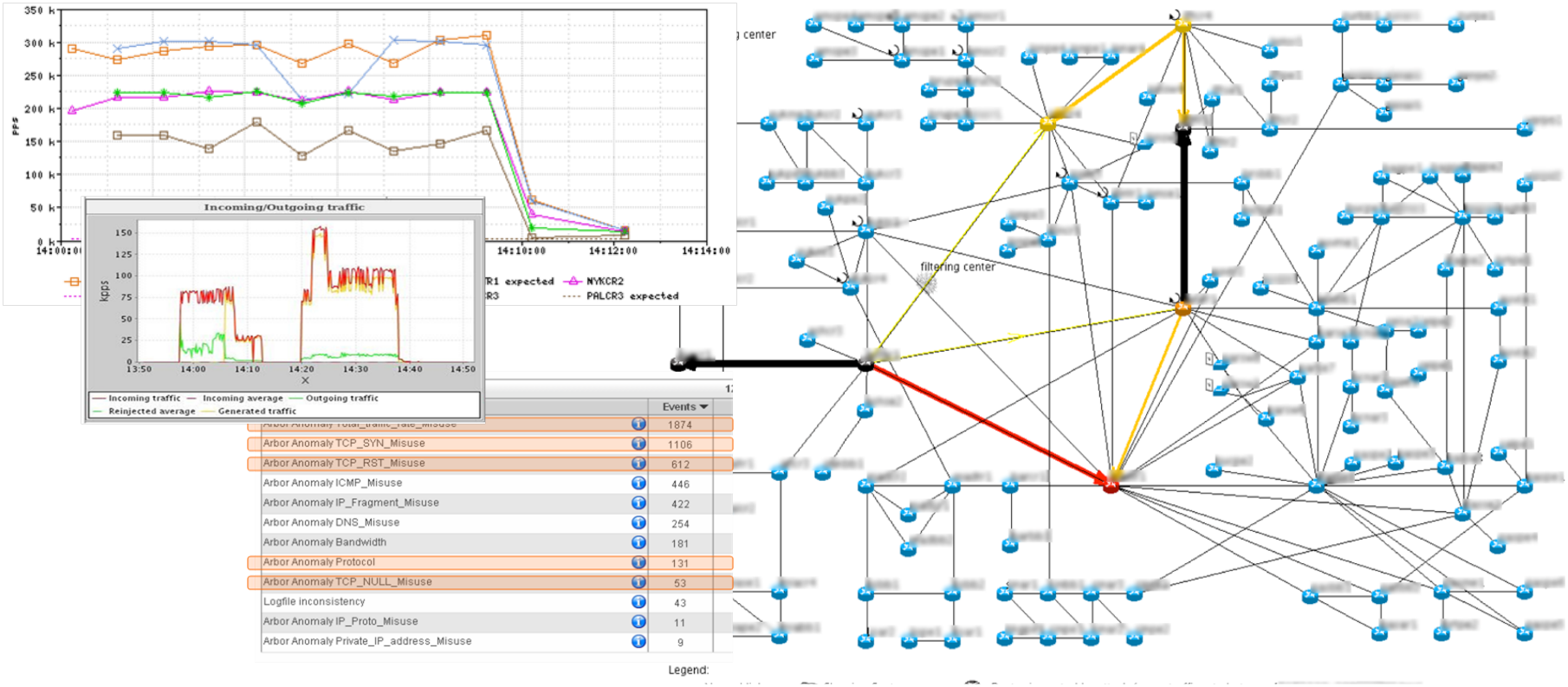
application : DDoS

- modèle "target-centric"
- alertes
  - analyse de flux (IPFIX) (ex. : Arbor Networks)
  - sondes spécifiques (ex. : 6cure TP)
  - téléphone
- réaction
  - « holing »
  - nettoyage



application : DDoS

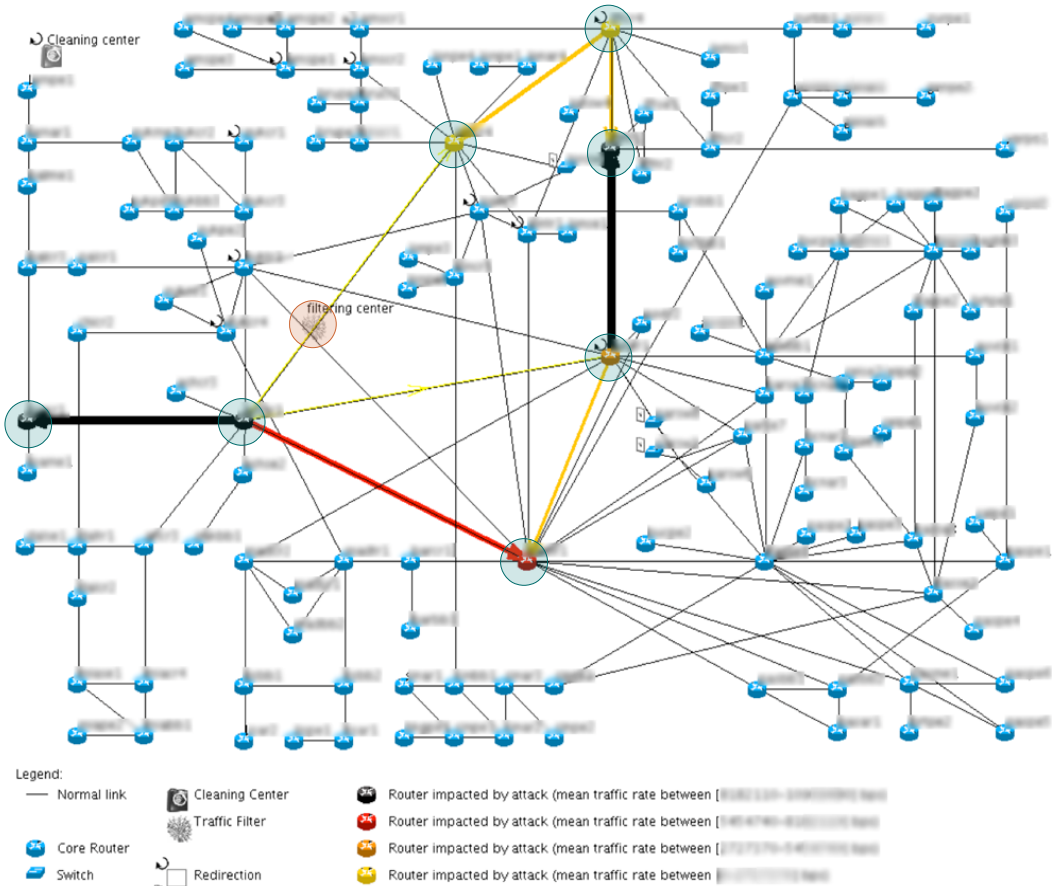
- moteur d'aide à la décision
  - données d'événements
    sources / destination(s)
  - cartographie
    Netflow, parc routeurs...



- éléments actifs : routeurs, solutions anti-DDoS

application : DDoS

- évaluation de réaction
  - black/sink holing global/sélectif
  - redirection vers centre de traitement
    - ACL routeurs
    - drop IPS
    - cleaning



- impact (target-centric) : joignabilité de la cible

application : DDoS

- ex. : black holing

Blackhole-based reactions					
Proposition id	Description	Efficiency	Impact	Operation id	Operation details
#1	Blackhole on all the crossed nodes of the attack for event #755957	28% Solved events: #755957	LOW	#1	• Type: Localized traffic redirection to the blackhole • Virtual router: Cleaning center • Network Address: [redacted] • Endpoint routers: o [redacted] o [redacted]
#2	General blackhole	100%	HIGH	#1	• Type: Generalized traffic redirection to the blackhole • Virtual router: Cleaning center • Network Address: [redacted] • Endpoint routers: o [redacted]

- réaction fortement impactante :
  - modification plan de routage
  - DDoS… réussi ?

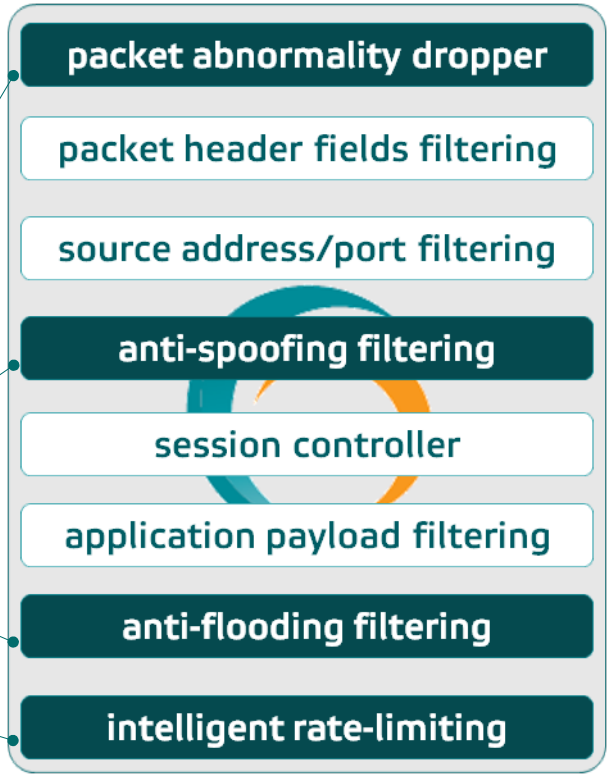
application : DDoS

- ex. : redirection vers centre de traitement

Cleaning-center-based reactions

Proposition id	Description	Efficiency	Impact	Operation id	Operation details
				#1	• Type: Generalized traffic redirection to a special destination • Virtual router: Cleaning center • Network Address: [redacted] • IP Next-Hop: unknown • Endpoint routers: ○ [redacted]

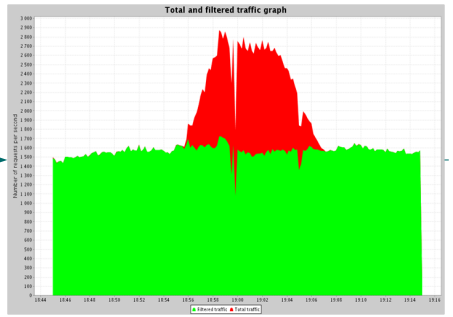
					• Type: Traffic cleaning
					• Equipment name: Cleaning center
					• Service #1
					  ○ Service definition
					  ▪ Name: TCP 22
					  ▪ Interface [In]: (Index:1 - Vlan:*)
					  ▪ Interface [Out]: (Index:2 - Vlan:no)
					  ▪ Network Addresses:
					  ▪ [redacted]
					  ▪ Protocol: TCP
					  ▪ Ports: 22
					  ▪ Complementary: false
					  ○ Service filtering modules configuration
					  ▪ IP Bogon and packet abnormalities filtering
					  ▪ IP bogon dropper
					  ▪ Logs
					  ▪ Heavy hitters list size: 20
					  ▪ Sampling rate: 1000
					  ▪ Sanity check
					  ▪ Logs
					  ▪ Heavy hitters list size: 20
					  ▪ Sampling rate: 1000
					  ▪ Anti-spoof filtering
					  ▪ Logs
					  ▪ Heavy hitters list size: 20
					  ▪ Sampling rate: 1000
					  ▪ Duplicated requests filtering
					  ▪ Default redundancies filtering
					  ▪ Parameters
					  ▪ Average Factor: 0.1
					  ▪ Tolerance: 0.05
					  ▪ Redefinition Time: 1000
					  ▪ Static Alerting Threshold: 7
					  ▪ Static Filtering Threshold: 10

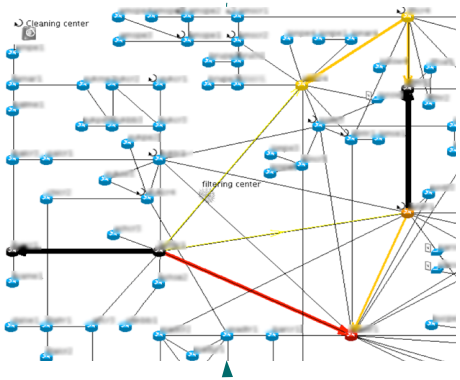


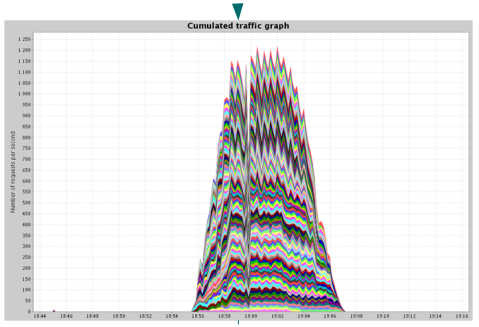
- réaction moyennement impactante
  - modification plan de routage
  - DDoS en échec ? ...

une chaîne vertueuse ?

- alerte DDoS
- redirection sink hole
- extraction botnet
- push ACLs







IP	Contributor request counter (average) [req/s]
86.215.200.153	309.80 (460.39)
86.215.102.194	80.80 (109.59)
217.128.151.115	50.20 (45.25)
193.252.62.151	21.40 (20.94)
90.12.182.164	18.40 (20.31)
86.208.85.146	16.20 (19.93)
90.56.74.110	19.80 (19.83)
90.38.221.157	19.60 (20.20)
86.195.252.89	18.80 (19.37)
90.39.118.35	16.40 (19.00)
86.215.212.38	17.80 (19.08)
90.23.24.187	18.20 (18.64)
90.4.126.104	17.60 (18.91)
83.113.79.57	21.80 (21.70)
90.9.46.178	17.00 (18.56)
86.206.79.71	18.80 (17.95)
83.204.173.98	18.40 (17.62)
83.196.23.84	16.80 (17.53)
82.125.28.117	16.00 (17.73)
90.18.48.66	16.00 (17.25)
86.221.187.111	13.20 (18.83)
90.7.216.67	13.00 (16.76)
82.124.133.102	30.80 (31.51)
82.124.133.102	30.00 (31.51)
81.50.212.234	14.80 (16.80)

en résumé

- premier niveau d'évaluation d'efficacité/impact : **connectivité IP**

- choix de contremesures fortement dépendants...
  - … des choix (disponibilités) d'éléments actifs (ex. : routeurs?)
  - … des droits de contrôles sur les configurations (ex. : ACLs ?)
  - … des réticences humaines (« to click or not to click? »)

- un avenir possible et prometteur
  - résilience des réseaux / services
  - consolidation Network Management / Security Management et normalisation des échanges ?

quelque(s) conclusion(s)

- de l'intérêt (et de la confiance) dans une réaction rapide et coordonnée...

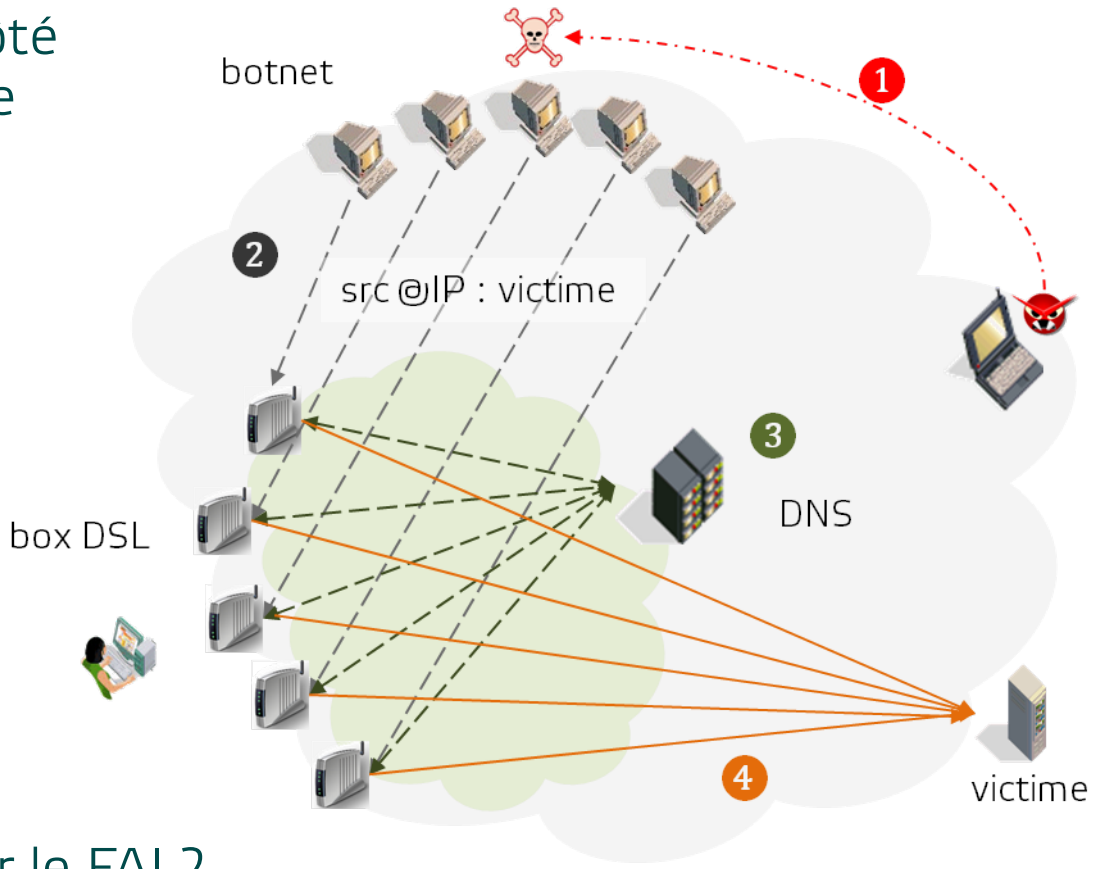
- un champ de R&D ouvert
  - **impact** flux / services / utilisateurs (privilégiés) et indicateurs
  - répartition optimale des (points de) réactions
  - pilotage par les politiques de sécurité (contraintes, politiques de réaction préévaluées)
  - évaluation des contremesures par simulation
  - liens NMS / SIEM ...

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

>MASSIF<

application : Dr(r)DoS

- un peu d'imagination...
  - ... et un DNS ouvert côté WAN sur une version de box...



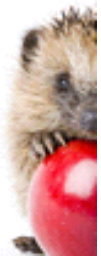
- un peu de réflexion...
  - quelle(s) réaction(s) pour le FAI ?

contacts

- 6cure SAS
  Campus Effiscience
  2 rue Jean Perrin – 14460 Colombelles
  (+33) 250 011 509
  contact@6cure.com

- vos interlocuteurs

  - Jouni Viinikka, Directeur R&D
    (+33) 250 011 539
    jvi@6cure.com
  - Emmanuel Besson, Directeur Technique
    (+33) 673 088 772
    emmanuel.besson@6cure.com



merci

plus d'info ? contact@6cure.com