DGA/DET/CELAR
laurent.roger@dga.defense.gouv.fr

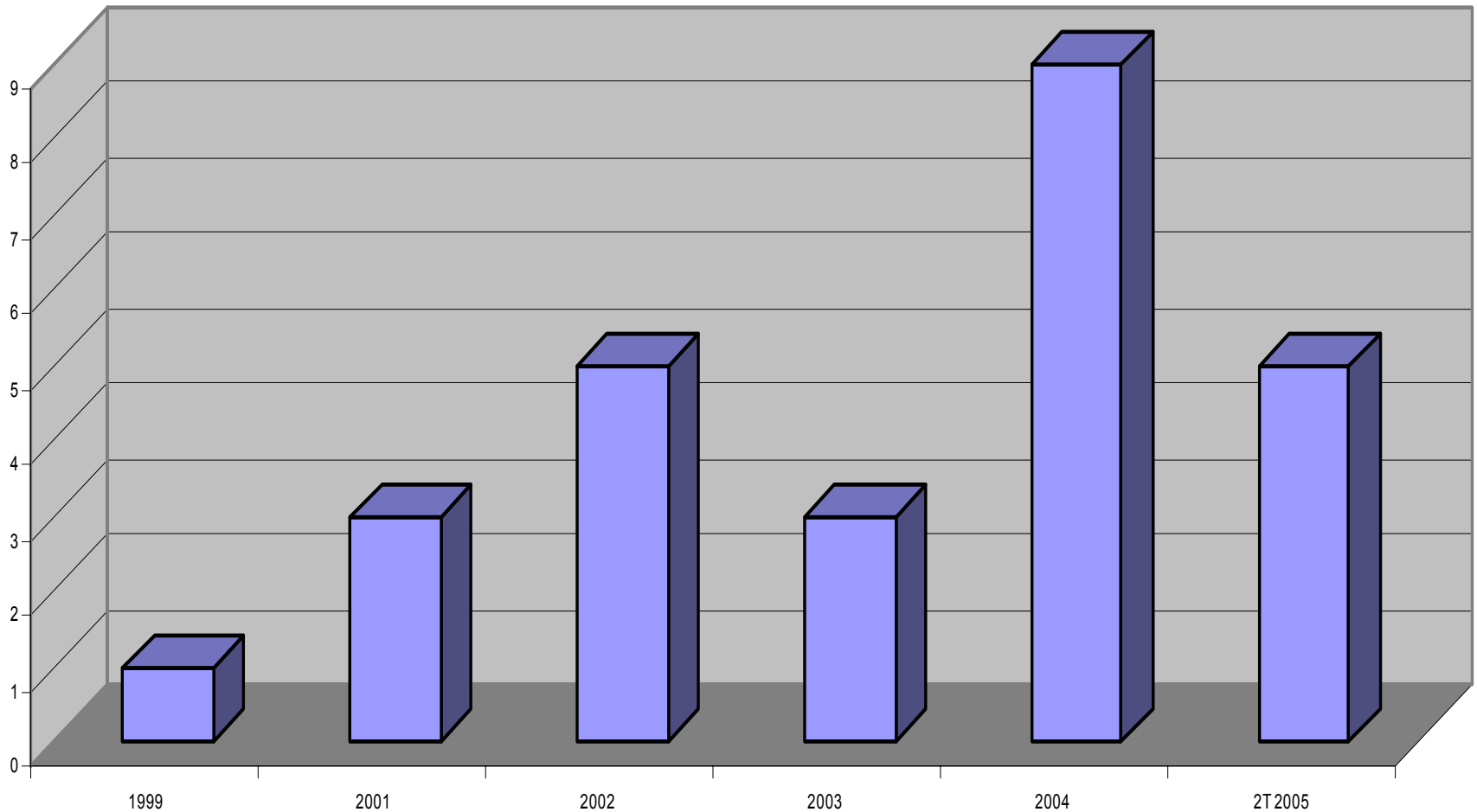
Anti-forensic

- Définition
- Historique
- Processus
- Modélisation
- Conclusion

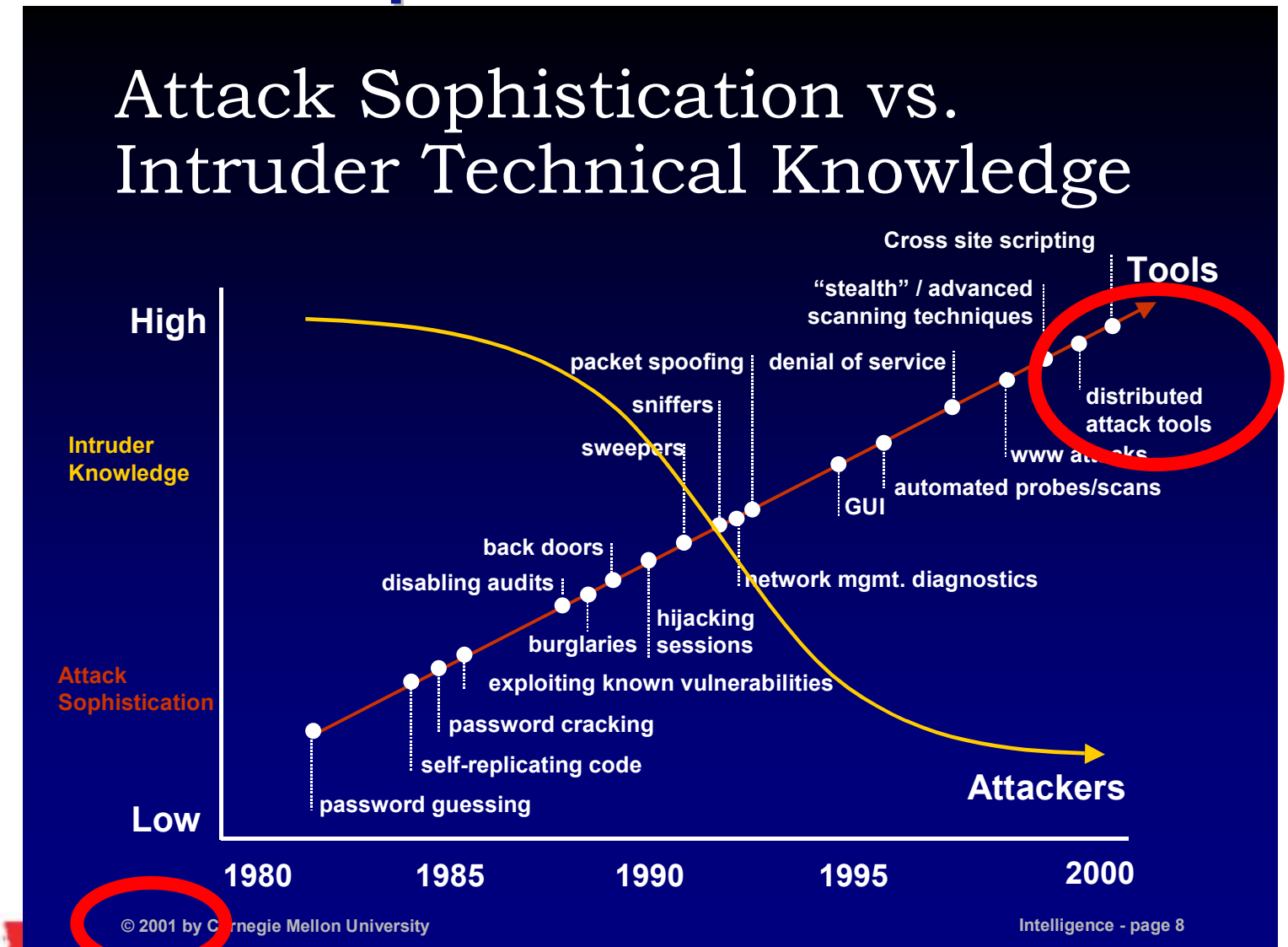
Définition

- Anti-forensic :
  - procédures et techniques ayant pour objectif de limiter les moyens d ’enquête ou d ’examen d ’un système
  - moyens : détruire, camoufler, modifier des traces , prévenir la création de traces

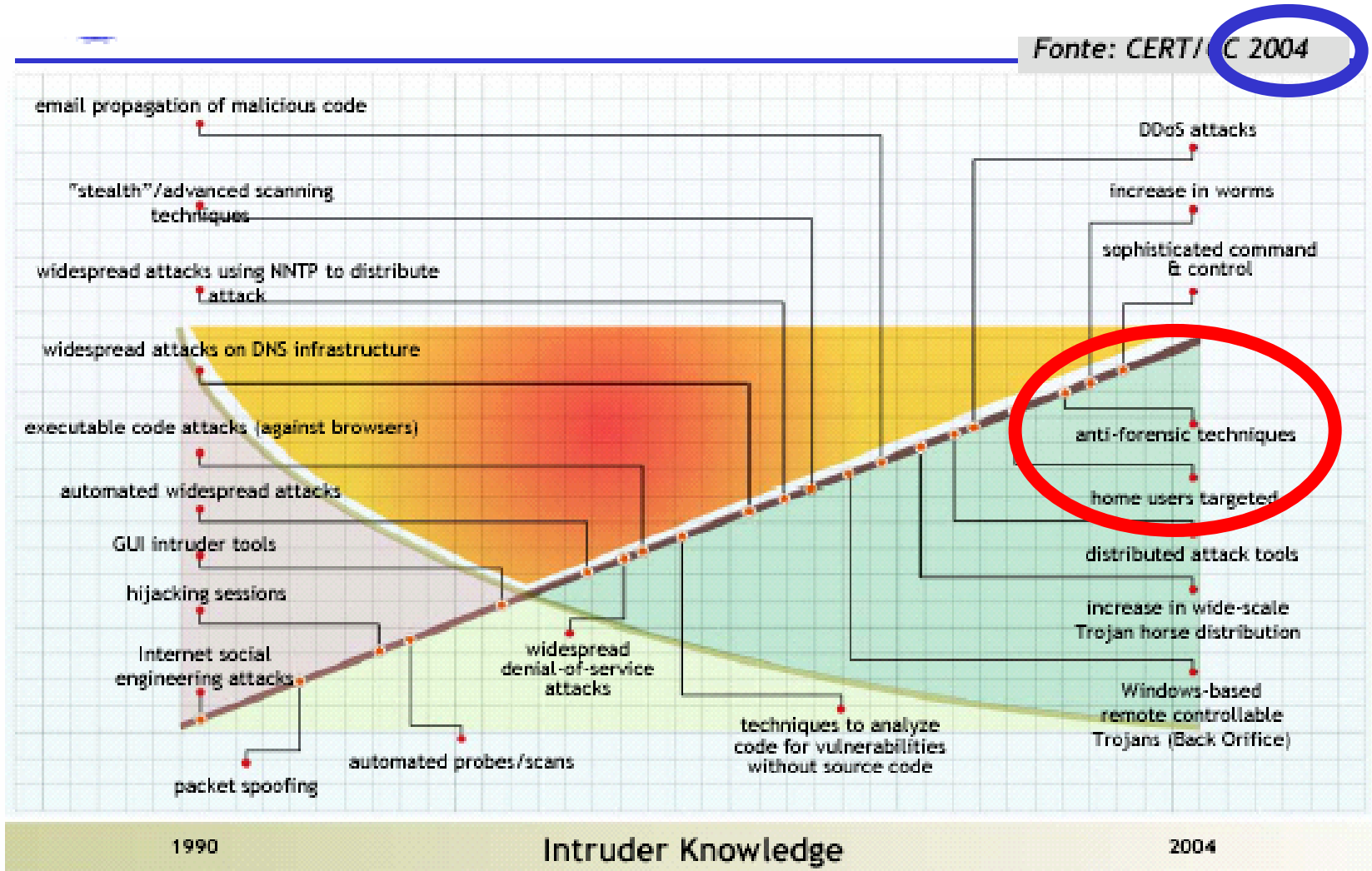
Nombre de publications



Historique



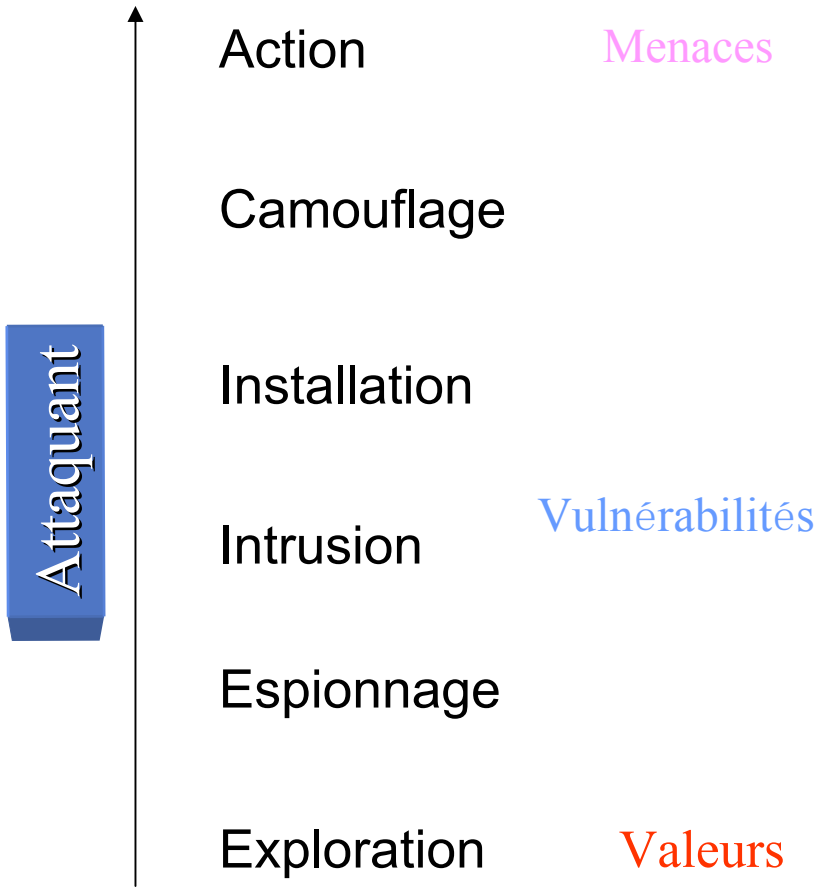
Historique


Fonte: CERT/ C 2004
email propagation of malicious code
"stealth"/advanced scanning techniques
widespread attacks using NNTP to distribute attack
widespread attacks on DNS infrastructure
executable code attacks (against browsers)
automated widespread attacks
GUI intruder tools
hijacking sessions
Internet social engineering attacks
packet spoofing
automated probes/scans
widespread denial-of-service attacks
techniques to analyze code for vulnerabilities without source code
DDoS attacks
increase in worms
sophisticated command & control
anti-forensic techniques
home users targeted
distributed attack tools
increase in wide-scale Trojan horse distribution
Windows-based remote controllable Trojans (Back Orifice)
1990
Intruder Knowledge
2004
Attack Sophistication

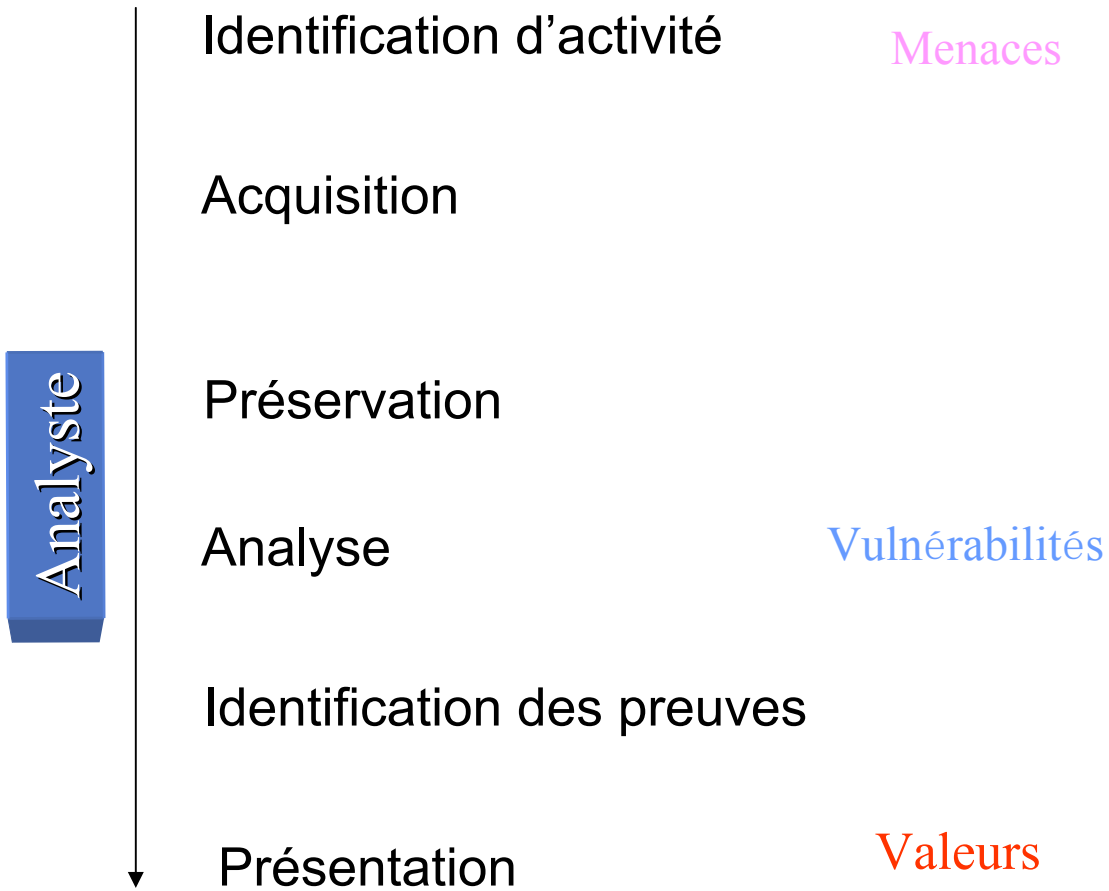
Historique

- Hit parade des moyens (nombre de citations dans les publications examinées)
  - Camouflage : 12
  - Destruction : 10
  - Modification : 10
  - Prévention des traces : 3

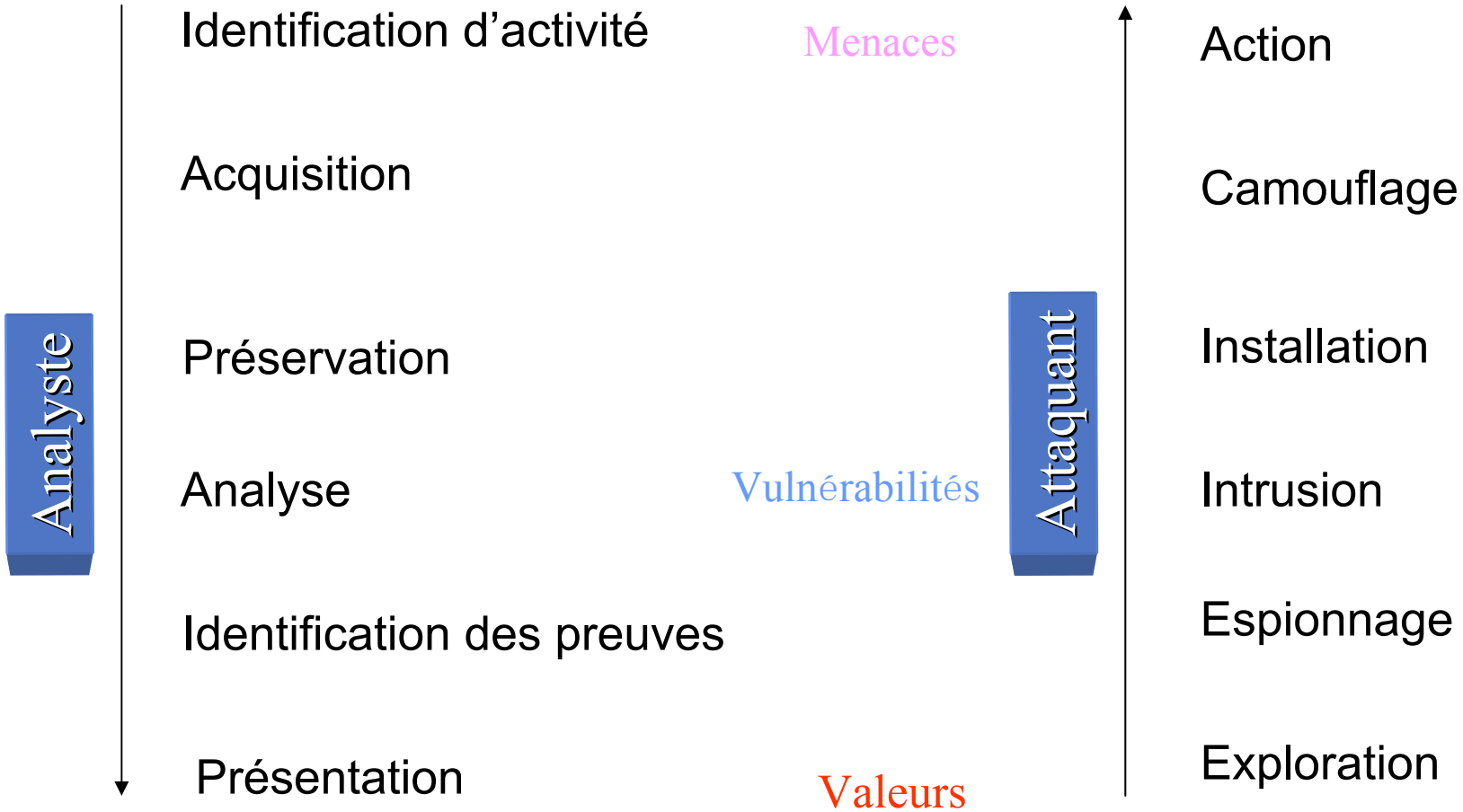
Activités de l'attaquant



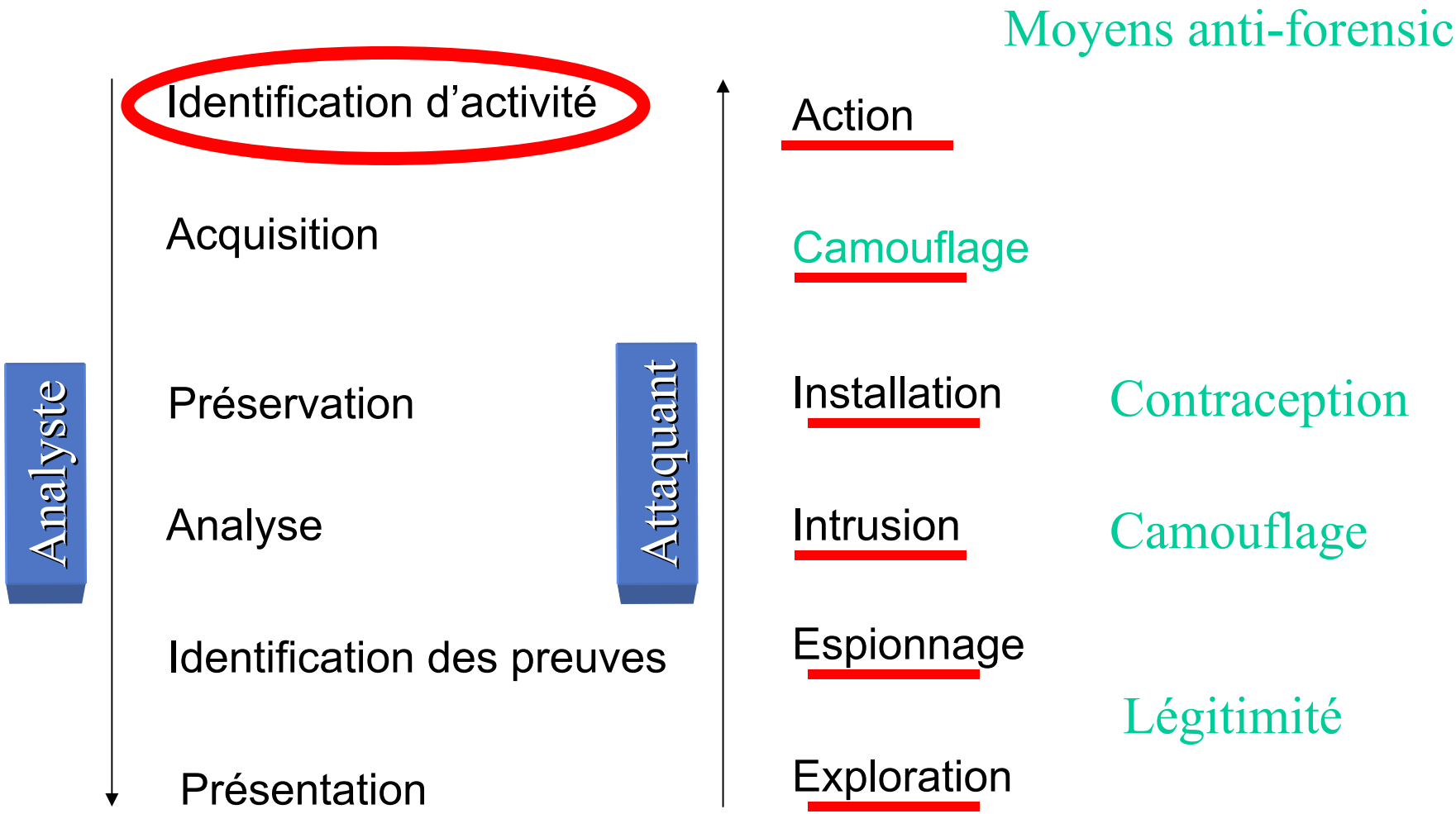
Processus forensique



Mise en parallèle



Etape 1 - identification d'activité



Etape 1 - identification d'activité

Légitimité

-Ingénierie sociale
-Requêtes du système

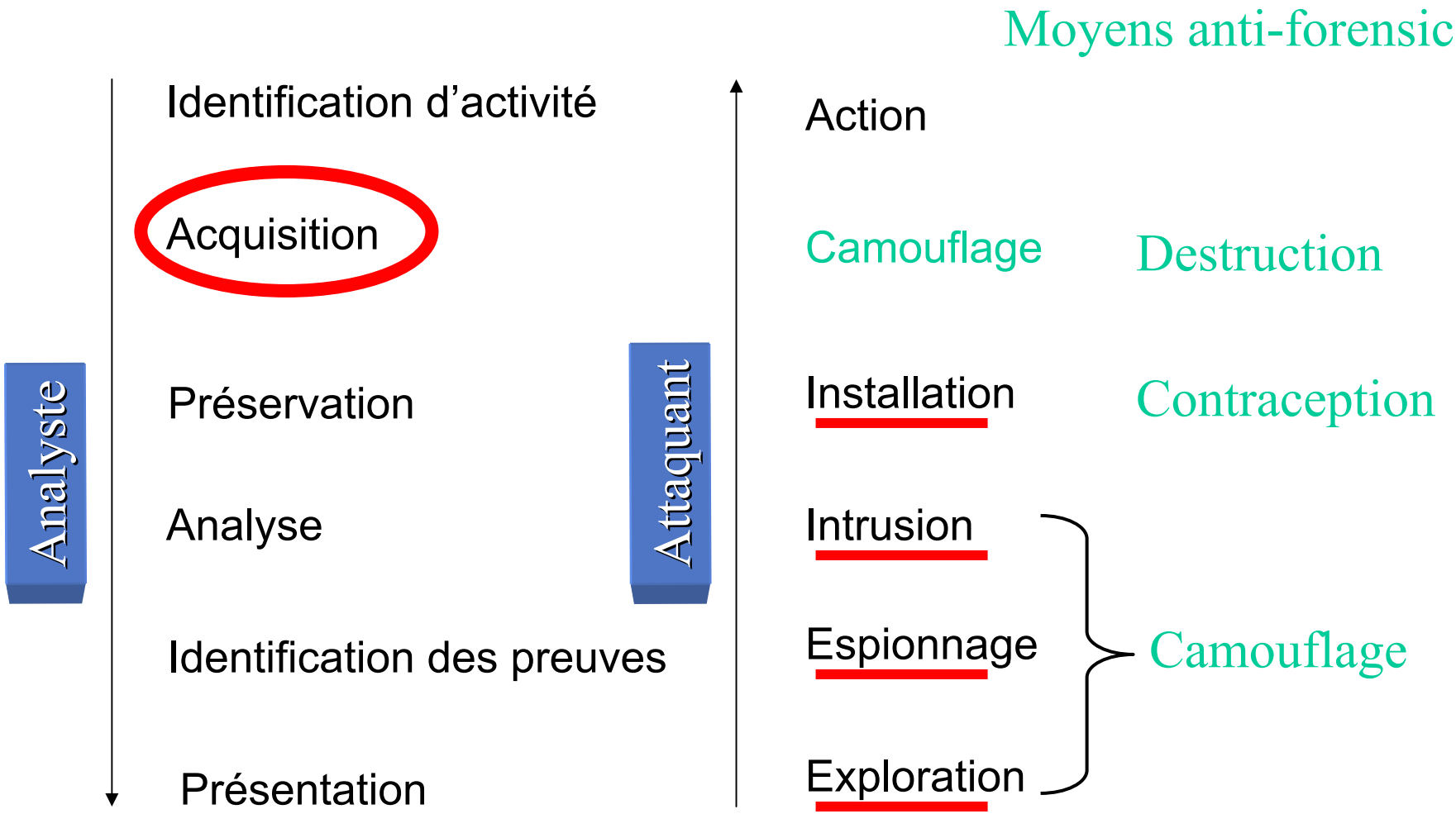
Camouflage

- Obfuscation ou suppression des traces d'activité système ou réseaux -> demo evt

Contraception

- Minimisation des traces d'activité système ou réseaux
- Utilisation des supports les plus volatiles

Etape 2 - acquisition



Etape 2 – acquisition

Camouflage

- **Supports de stockage inhabituels**
  - **Téléphones portables (SIM, flash, SD)**
  - **Disques durs enfouis (magnétoscope, console de jeux …)**
  - **Montres, autoradios**
  - **Clés USB**
  - **Balladeurs**

- **ATA : Device Configuration Overlay**

  T5K80_spv2.1.pdf

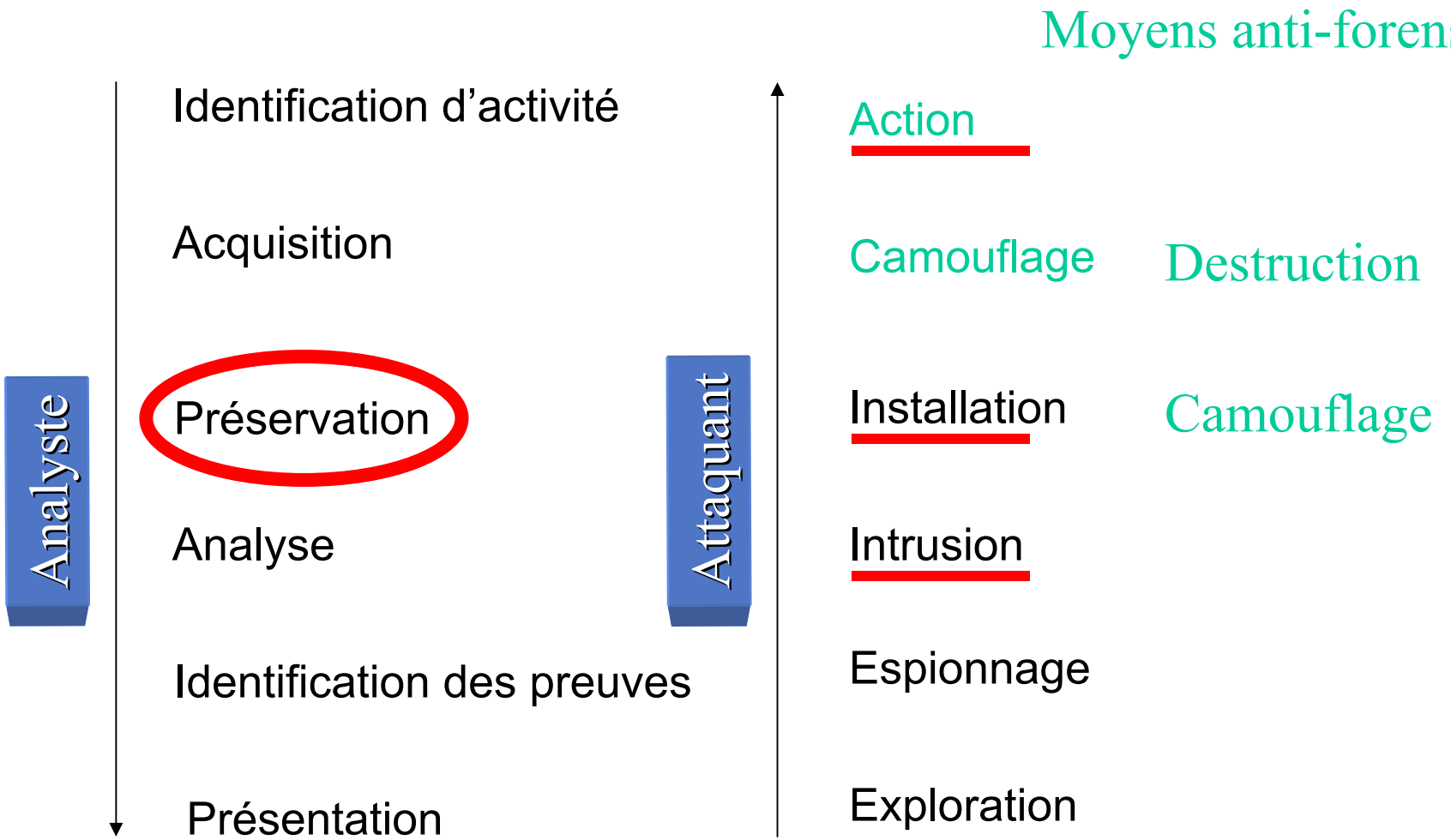
Image courtesy of www.scit.wlv.ac.uk

Etape 2 - acquisition

Destruction

Courtesy of PC911- Alex -

Etape 3 - préservation



Etape 3 – préservation

Camouflage

- **Collision de hash -> démo stripwire**
  - **fire.bin = vec1 + AES [charge, sha1(vec1)]**
  - **ice.bin = vec2 + AES [charge, sha1(vec1)]**
  - **MD5(fire.bin) = MD5(ice.bin)**

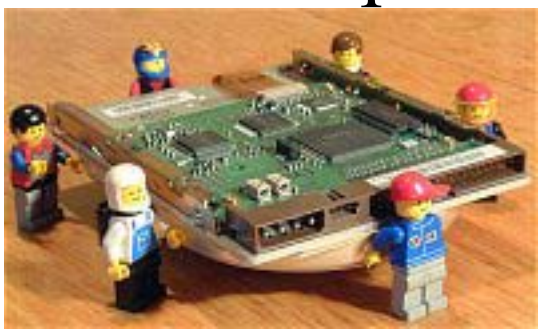
Action

Dan Kaminsky - MD5 to be considered harmful someday

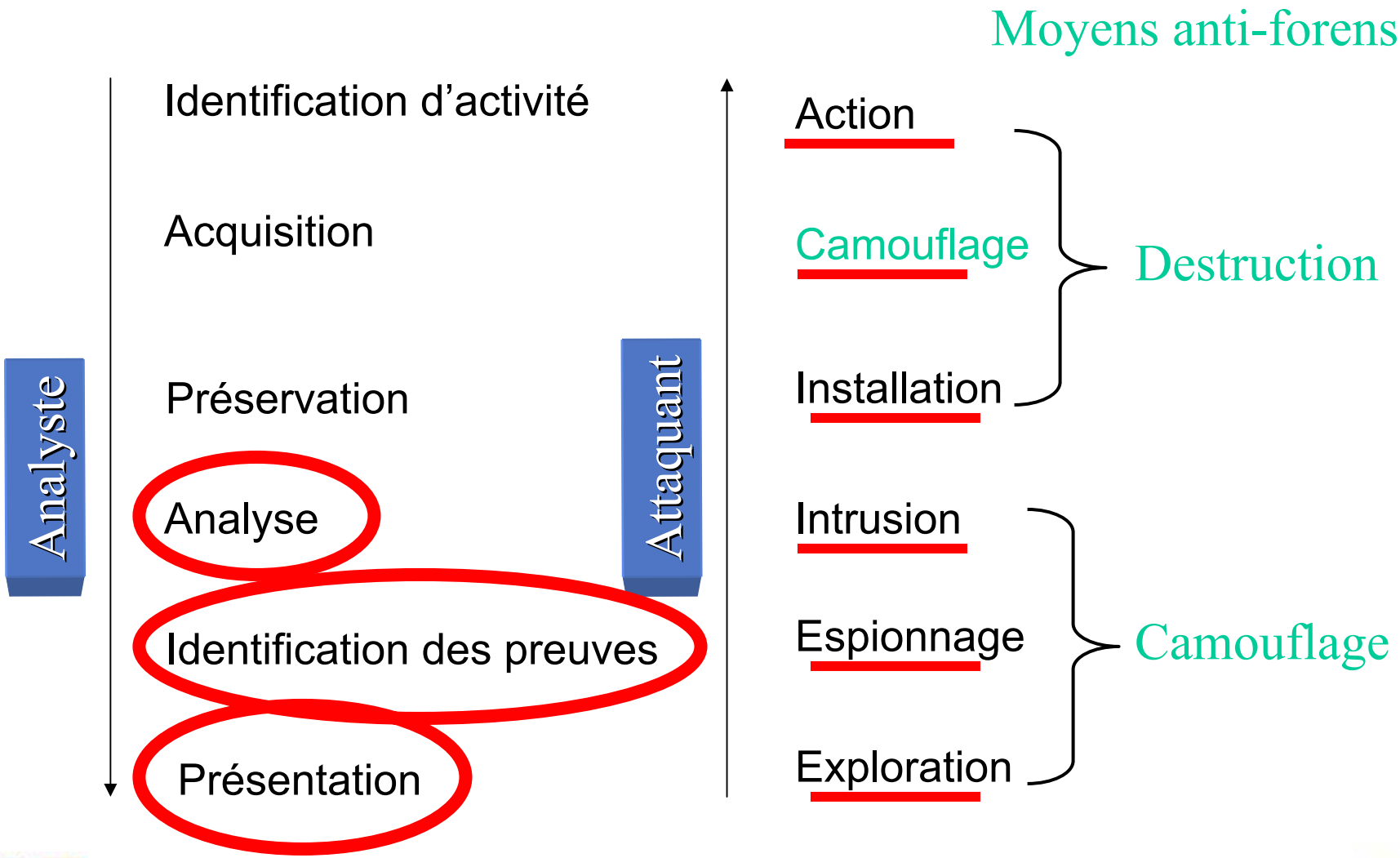
- **Attaques spécifiques sur les produits**

Etape 3 - préservation

Destruction



Etape 4 – 5 - 6


Moyens anti-forensic
Identification d'activité
Acquisition
Préservation
Analyste
Attaquant
Analyse
Identification des preuves
Présentation
Action
Camouflage
Installation
Destruction
Intrusion
Espionnage
Exploration
Camouflage

Etape 4 – analyse
Etape 5 – identification des preuves

Camouflage

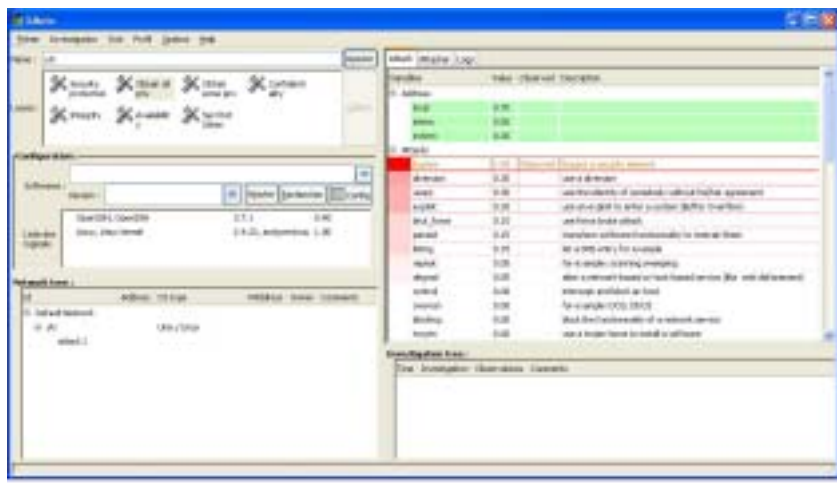
- **Modification de l'intégrité du système sans modification de fichier :**
  - **Ajout d'un seul fichier au démarrage**
  - **Fichier non existant au démarrage**
- **Obfuscation, chiffrement, polymorphisme**
- **Brouillage de la limite entre code et données**

Forensic Discovery - Dan Farmer et Wietse Venema

Etape 6 – présentation

Comment expliquer à des personnes non techniques les moyens utilisés par l'attaquant ?

-> **projet SIRAGE** : simulateur de restitution de scénario d'agression



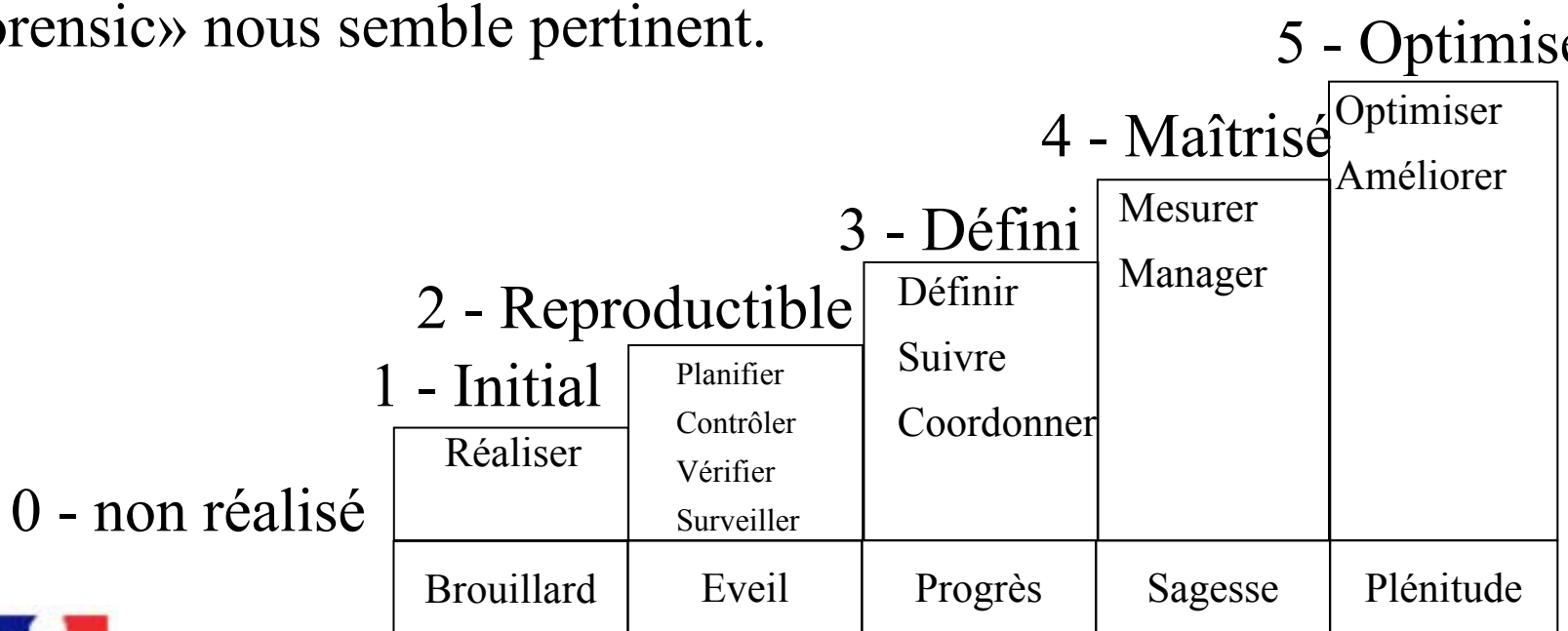
Comment être certain de l'identité de l'attaquant ? de sa volonté de nuire ou de ses motivations (« syndrome du troyen ») ?

-> **projet META** : méthodes d'analyse des traces – thèse Thomas Duval(Supélec)

La présence d'activités spécifiquement anti-forensic peut elle être un élément à charge ? ?

Modélisation (IRF-CMM)

Il est (encore ?) temps pour les organisations de prendre en compte l'antiforensic dans leur processus de réponse à incident !
Afin de mesurer cette prise en compte et sa dynamique de progrès, la déclinaison des modèles de maturité CMM (Capability Maturity Model) sur une thématique spécifique de « réponse à incident et forensic» nous semble pertinent.



Modélisation (IRF-CMM)

- Ingénierie de la réponse à incident et investigation
  - PA 01 : Administrer la réponse à incident
  - PA 02 : Evaluer les impacts
  - PA 03 : Evaluer les risques
  - PA 04 : Evaluer les menaces
  - PA 05 : Evaluer les vulnérabilités
  - PA 06 : Donner l 'assurance de la réponse à incident
  - PA 07 : Coordonner la réponse à incident
  - PA 08 : Contrôler la réponse à incident
  - PA 09 : Fournir des ressources
  - PA 10 : Spécifier les besoins de réponse à incident
  - PA 11 : Vérifier et valider la réponse à incident
- Projet et *organisation*
  - PA 12 : Assurance qualité
  - PA 13 : Gestion de configuration
  - PA 14 : Manager les risques projet
  - PA 15 : Contrôler et maîtriser l 'effort technique
  - PA 16 : Planifier l 'effort technique
  - *PA 17 : Définir les processus d 'ingénierie système de l 'organisation*
  - *PA 18 : Améliorer les processus d 'ingénierie système de l 'organisation*
  - *PA 19 : Manager l 'évolution des produits ou services*
  - *PA 20 : Manager l 'environnement support de l 'ingénierie des systèmes*
  - *PA 21 : Fournir en permanence des compétences et des connaissances*
  - *PA 22 :Coordonner les fournisseurs*

Avant dernier transparent

Can a Rootkit hide from RootkitRevealer?
It is theoretically possible for a rootkit to hide from RootkitRevealer. Doing so would require intercepting RootkitRevealer's reads of Registry hive data or file system data and changing the contents of the data such that the rootkit's Registry data or files are not present. However, this would require a level of sophistication not seen in rootkits to date. Changes to the data would require both an intimate knowledge of the NTFS, FAT and Registry hive formats, plus the ability to change data structures such that they hide the rootkit, but do not cause inconsistent or invalid structures or side-effect discrepancies that would be flagged by RootkitRevealer.

RootkitRevealer Help
Copyright (C) 2005 Bryce Cogswell and Mark Russinovich
Sysinternals - www.sysinternals.com

Conclusion

- La connaissance approfondie des techniques anti-forensiques permet :
  - de mettre en place des contre mesures spécifiques
  - visant à déclencher des actions de maîtrise de la sécurité du système
  - permettant de déceler au plus tôt des activités nuisibles au processus de réaction après incident

Merci de votre attention