NATO OTAN

Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense

symposium SSTIC 09/06/2010

Philippe Lagadec
NATO C3 Agency
CAT2 – Cyber Defence and Assured Information Sharing

NATO C3 AGENCY

Au menu

- **Cyber-Défense**
- **Visualisation**
  - CIAP - Consolidated Information Assurance Picture
- **Analyse de Risque Dynamique**
  - DRA - Dynamic Risk Assessment

Cyber-Défense

- **Cyber-Défense (CND) / Lutte Informatique Défensive:**
  - Toutes les activités qui consistent à défendre en temps réel la sécurité des systèmes et réseaux.

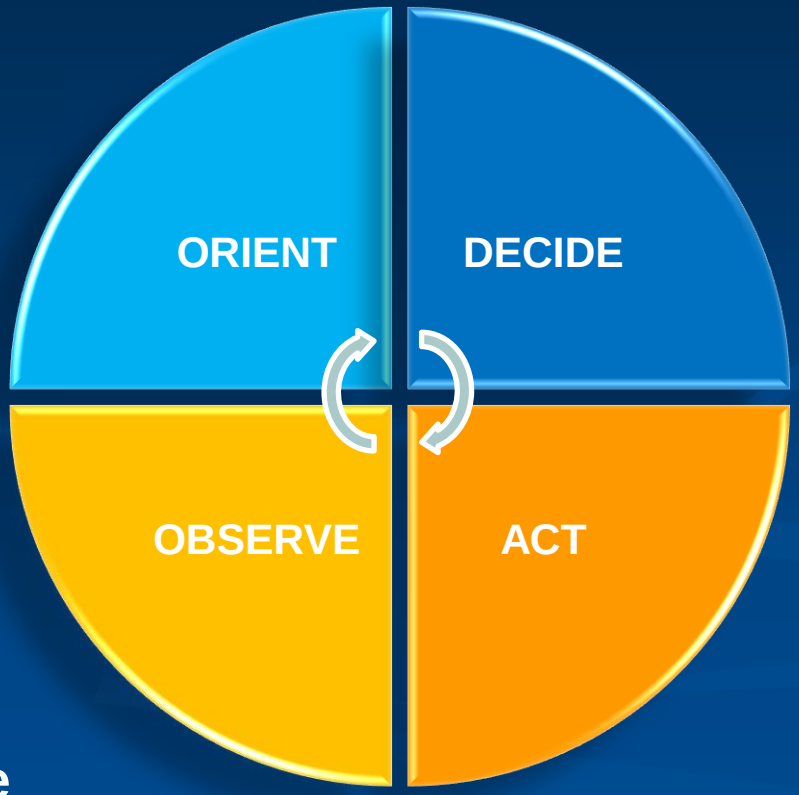
- **Couvre notamment:**
  - Détection d'intrusion
  - Antivirus
  - Corrélation d'événements, supervision
  - Analyse de malware
  - Forensics
  - Détection de vulnérabilités et gestion de patch
  - Gestion d'incidents

Cyber-Defence Operational Concept (R&D)

Cyber-Defence Operators

Corrélation
Analyse
Détection avancée
Visualisation

Recommandation de réponses
Simulation
Aide à la décision



IDS
Logs
Antivirus
Supervision réseau
Forensics
Analyse de Malware

Application de la réponse (automatisée ou non)
Reconfiguration dynamique du réseau

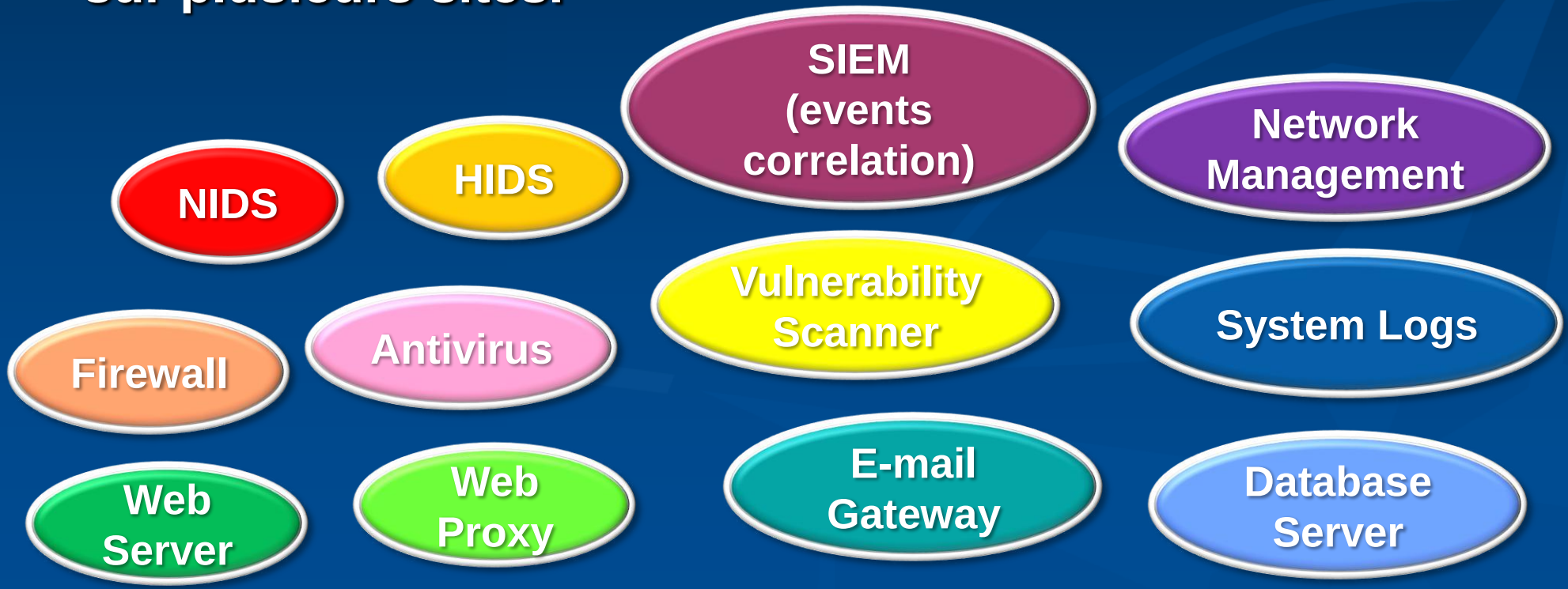
Existing Management Systems

Situation en Cyber-Défense

- **Comment définir la situation en cyber-défense:**
  - Topologie des systèmes et réseaux à défendre
  - Où sont les éléments / infrastructures critiques ?
  - Dépendances entre missions, services et ordinateurs, réseaux, applications ?
  - Quelles sont les vulnérabilités principales et leur impact ?
  - Y a-t-il des incidents ou attaques en cours ?
    - => impact, sources, cibles ?
  - Y a-t-il des activités de reconnaissance ?
  - Y a-t-il des machines compromises ?
  - Y a-t-il des changements dans l'architecture ?
  - Etc…

Difficultés actuelles

- Beaucoup d'outils génèrent une quantité astronomique d'information très technique.
- En particulier pour un système de grande taille réparti sur plusieurs sites.



Difficultés actuelles

- Chaque outil utilise ses propres formats, bases de données, sémantiques.
- Outils conçus pour générer des rapports pour les humains, mais pas pour partager l'information entre eux.
- Les SIEM permettent une certaine consolidation et corrélation, mais cela reste généralement limité aux événements / alertes. (par ex. pas de topologie réseau)
- Résultat: l'opérateur humain doit toujours **analyser et consolider mentalement** une grande quantité d'information.
- => Impossible à gérer pour de grands systèmes.
- **=> Difficile d'obtenir une vue globale de la situation.**

Difficultés actuelles

- En particulier, 2 lacunes dans les outils actuels sur le marché:
- Visualisation synthétique de la situation globale
- Comment déterminer l'impact réel d'une vulnérabilité ou d'une alerte IDS sur les missions et services critiques d'une organisation/entreprise ?

Visualisation

CIAP prototype:

Consolidated Information Assurance Picture

Visualisation en cyber-défense

- En cyber-défense, la visualisation peut servir à 2 choses différentes:
- **1) Analyse humaine / Détection:**
  - Présenter un très grand nombre de données techniques pour y déceler des tendances, anomalies, etc.
- **2) Supervision / Aide à la décision**
  - Montrer une vue d'ensemble de la situation pour identifier les priorités et guider les décisions.

- **(1) est déjà bien couvert par de nombreux outils (cf. www.secviz.org, DAVIX)**
- **(2) n'est pas encore très développé: besoin de R&D**

CIAP rationale

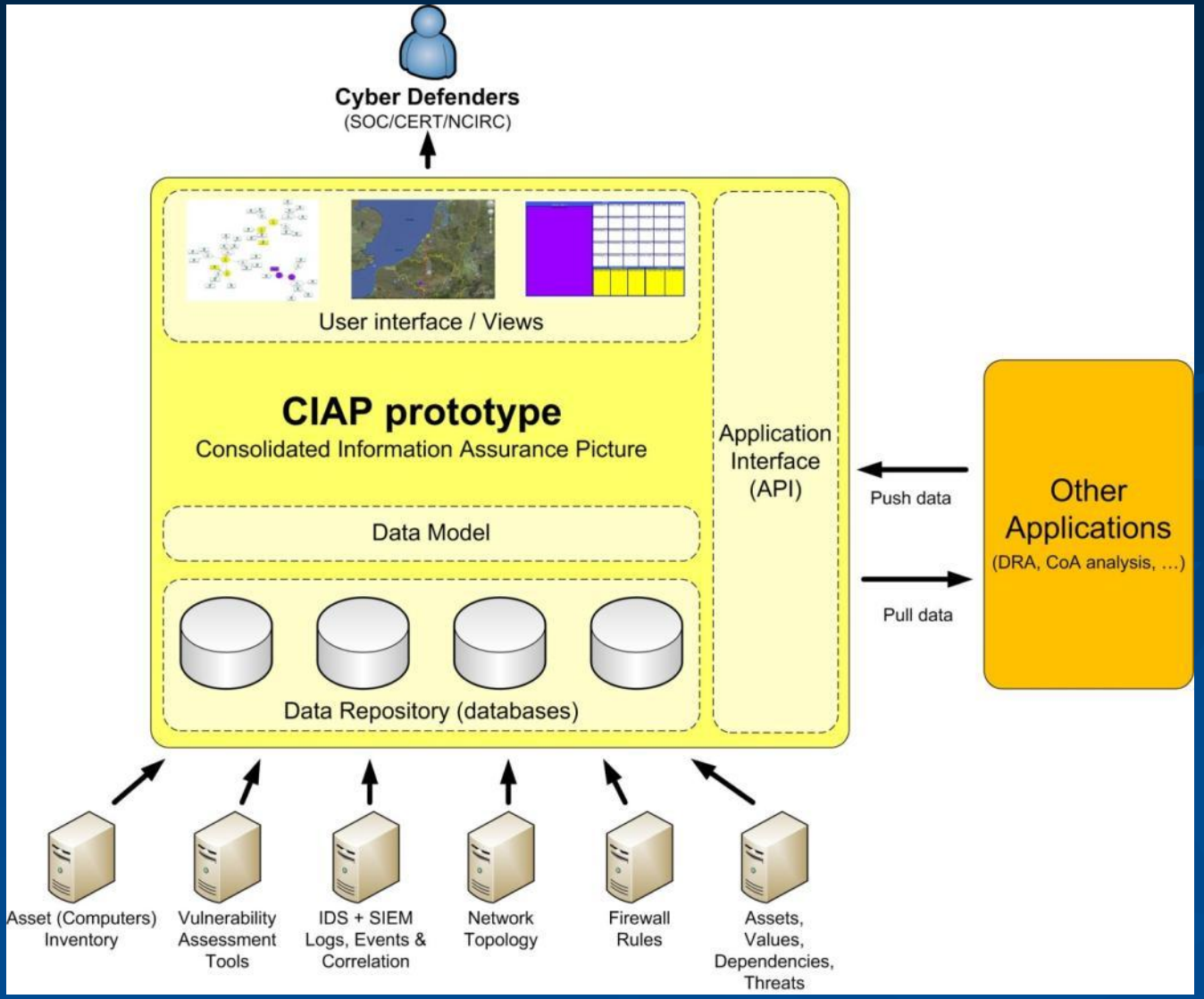
- **“A picture is worth a thousand log records.”**
  - *Raffy Marty, Applied Security Visualization*

- **For now, cyber defence is performed using a variety of tools and products:**
  - Each tool provides a piece of the puzzle.
    - Events, IDS alerts, vulnerabilities, network topology, …
  - Each tool has its own specific data model.
  - No tool provides a comprehensive picture of the situation.
  - Visualization for situational awareness is not really addressed.

CIAP prototype

- **Consolidated Information Assurance Picture**
  - Prototype developed by NC3A since 2007.
- Several components:
  - **Information Model:**
    - To model the whole CIS and networks to be protected.
    - Leveraging standards as much as possible.
  - **Data Repository:**
    - To store all data in one or several databases.
    - May leverage existing products and databases.
  - **User Interface:**
    - To visualize data with various views according to specific use cases.
  - **Application Interface:**
    - To allow other applications to push or pull data from/to CIAP, in order to build flexible and modular systems

CIAP overview



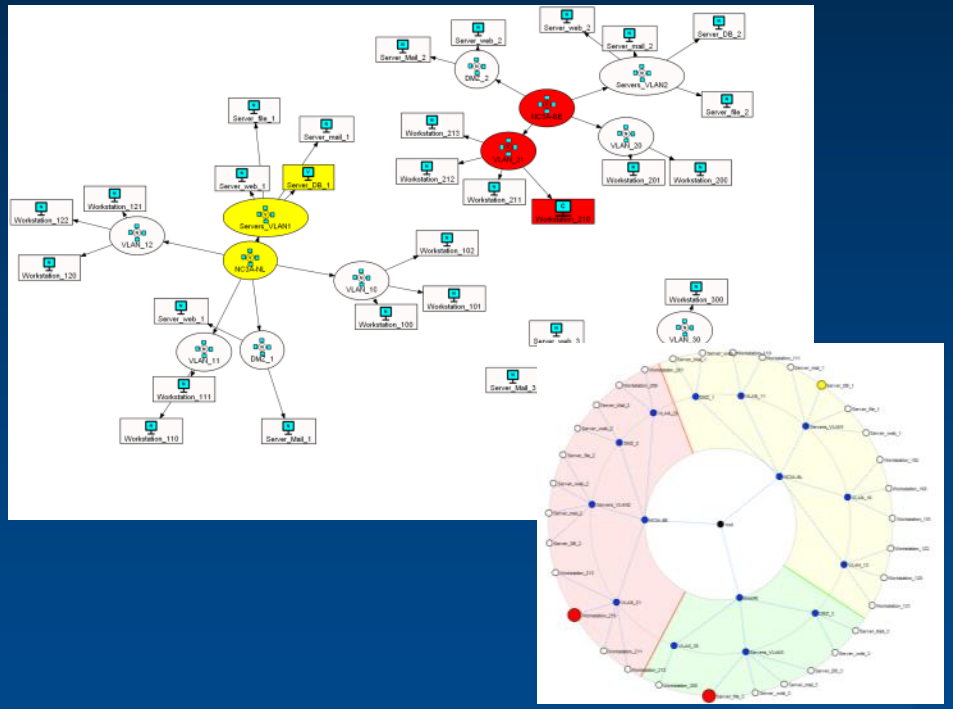
CIAP vs. SIEM

- **SIEM: Security Information and Event Manager**
  - A typical SIEM collects logs/events/alerts from many sources, and stores them in a central location.
  - Events can be normalized and correlated.
  - A SIEM may also leverage other information such as vulnerabilities and network topology, to improve correlation.

- **CIAP may be implemented using a SIEM.**
  - However, known products on the market do not cover all CIAP requirements yet. (data model, visualization)
  - In fact, a SIEM is an information source for the CIAP.

CIAP – New views for Situational Awareness

A few examples:



Network topology with vulnerable and compromised hosts

Geographical view with cyber layer

Treemaps to prioritize issues

CIAP demo

NATO

OTAN

Analyse de Risque Dynamique

DRA prototype

Dynamic Risk Assessment

NATO C3 AGENCY

Dynamic Risk Assessment (DRA)

- **Risk assessment that can be updated quickly and automatically as the system being assessed changes.**
- **These changes may be due to:**
  - The operational threat level, the mission type
  - The incremental system development and deployment (architecture)
  - New vulnerabilities
  - Alerts and actual attacks
- **Objectives of the DRA Prototype:**
  - To perform **real-time risk assessments** after an initial risk assessment has been conducted.
  - To be able to **recommend counter-measures** based on current level of risk.
  - To make the link between static risk assessment and the real security posture of the network and systems.

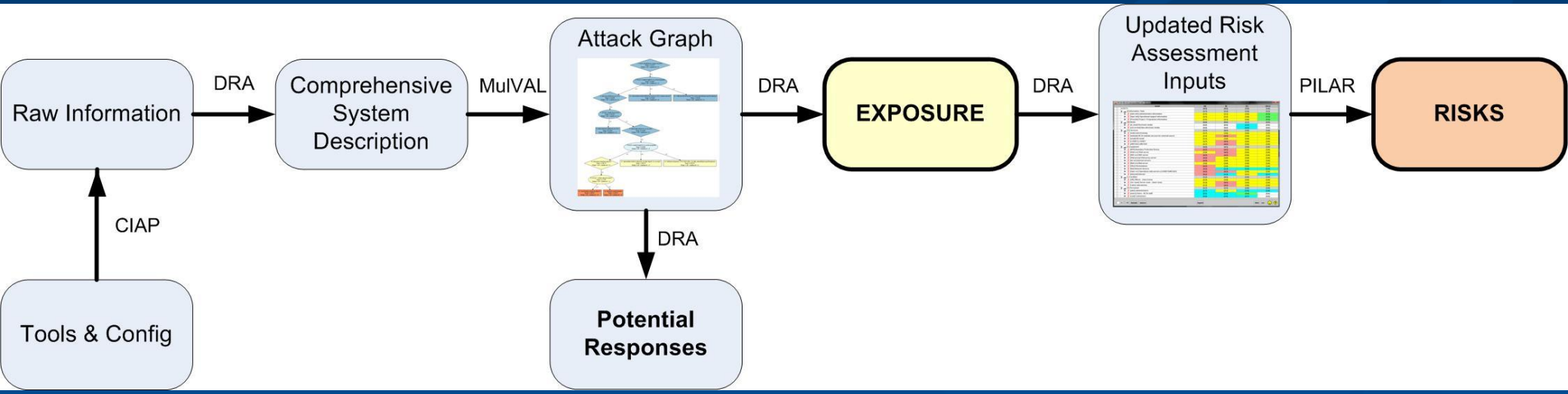
DRA – Dynamic Risk Assessment Prototype

- DRA Prototype developed by NC3A since 2007.
- In 2007 and 2008, several risk assessment methodologies were tested by NC3A on simple scenarios.
- **A new, innovative hybrid methodology has been developed**, combining attack graphs and "traditional" risk assessment (ISO27005).

- DRA prototype developed thanks to partnerships:
  - PILAR risk assessment tool provided by Spain.
  - MulVAL+AssetRank attack graph tool provided by Canada (DRDC).

DRA process overview

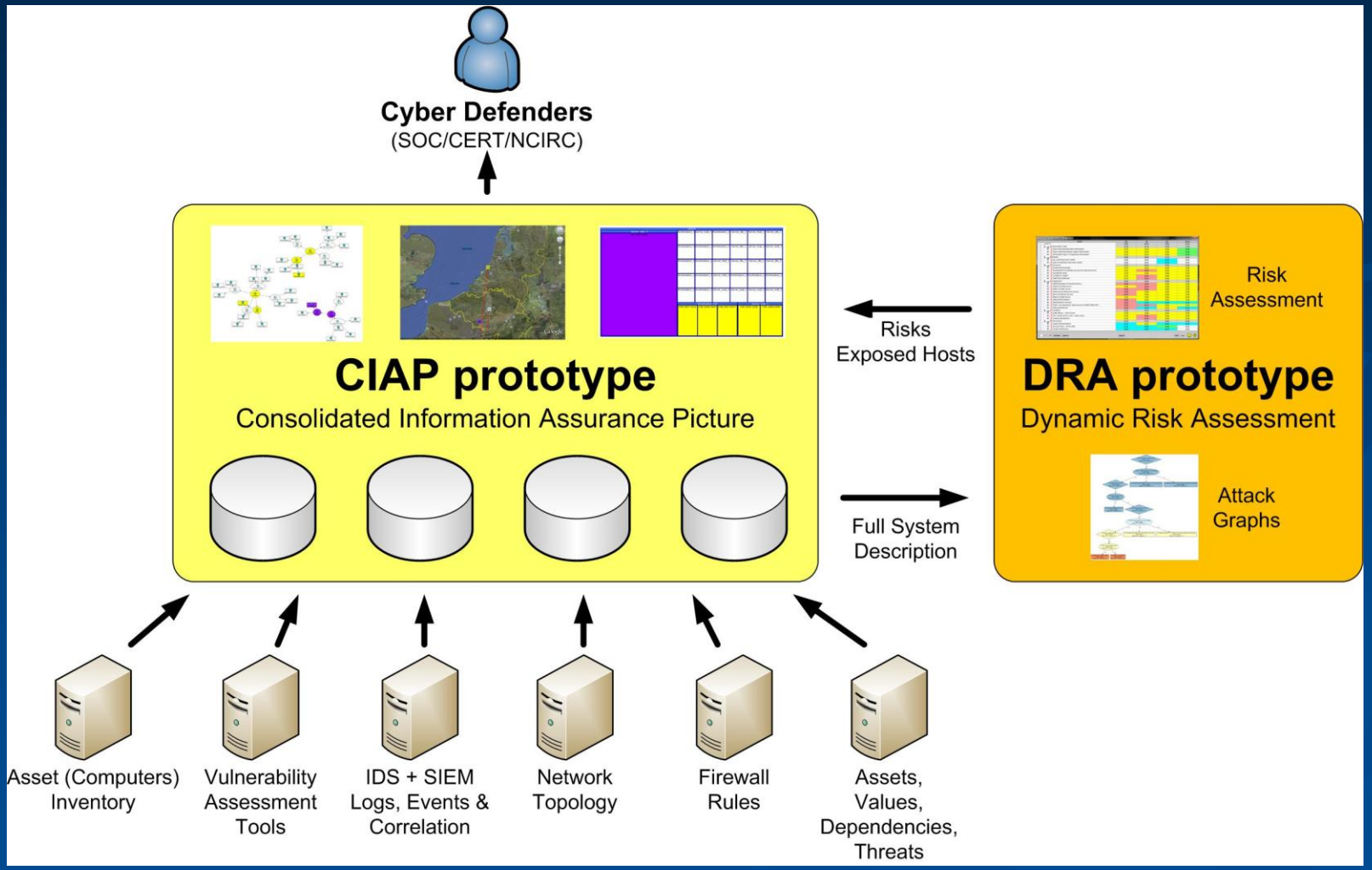
- **Main steps:**
  - 1) Build comprehensive system description from CIAP
  - 2) Generate attack graph => Exposure
  - 3) Update risk assessment => Risks



Host security status / Threat level

Host state	Description	Threat level (likelihood)
Normal	No known vulnerability, no alert.	**Normal**
Vulnerable	Known vulnerabilities, but no known attack path from outside.	**Low** (>Normal)
Exposed	Known attack path from outside (exploitable vulnerabilities wrt network topology & policy).	**Medium**
Compromised	IDS or SIEM Alert(s) indicating a potential compromise.	**High**

CIAP and DRA prototypes overview



DRA demo

Conclusion about CIAP and DRA prototypes

- **CIAP prototype:**
  - A comprehensive data model to merge information from various security tools, network management and asset inventory.
  - New views to improve situational awareness
  - Cyber defence data feeds for other applications.

- **DRA prototype:**
  - Attack graphs to determine which vulnerable hosts are really exposed to attackers.
  - Risk assessment methodology to analyze the actual risks on high-level assets (missions, business services).
  - Basic recommendation engine.
  - Provides new indicators to prioritize responses for incident handling.

CONCLUSION

- **La cyber-défense est une priorité pour l'OTAN**
- **Encore beaucoup de R&D nécessaire pour couvrir tous les besoins, entre autres:**
  - Consolidation des infos produites par tous les outils
  - Visualisation de la situation
  - Analyse de risque dynamique
  - Recommandation de réponse et aide à la décision
  - Réponse rapide et automatisée
- **CIAP et DRA sont des prototypes développés par la NC3A pour étudier les solutions techniques, et guider une implémentation opérationnelle avec l'industrie.**
- **Implémentation opérationnelle en cours pour 2011-2012.**

Contacting NC3A

NC3A Brussels

Visiting address:

Bâtiment Z
Avenue du Bourget 140
B-1110 Brussels
Telephone +32 (0)2 7074111
Fax +32 (0)2 7078770

Postal address:

NATO C3 Agency
Boulevard Leopold III
B-1110 Brussels - Belgium

NC3A The Hague

Visiting address:

Oude Waalsdorperweg 61
2597 AK The Hague

Telephone +31 (0)70 3743000
Fax +31 (0)70 3743239

Postal address:

NATO C3 Agency
P.O. Box 174
2501 CD The Hague
The Netherlands