Graphes d'attaques

Une exemple d'usage des graphes d'attaques pour l'évaluation dynamique des risques en Cyber Sécurité

Emmanuel MICONNET, Directeur Innovation

WISG 2013, UTT le 22/1/13

THALES

CyberSécurité, enjeux et positionnement de Thales

Cybersécurité : Un sujet stratégique pour de nombreux gouvernements et de grands comptes privés

- 1,5 million de victimes quotidiennement dans le monde / 556 Million de victimes par an (plus que le population Européenne)
- Coût global annuel du cibercrime : 110M$
- Evolution du cybercrime : Mobilité et réseaux sociaux
- Les vulnérabilités sur “mobile” ont doublé entre 2010 et 2011

Thalès, leader européen dans le domaine de la sécurité des systèmes d’information

- 80% des transactions financières dans le monde passe par un équipement Thales aujourd’hui
- Thales, opérateur de sécurité de Cloudwatt
- L’innovation, accélérateur de la transformation

THALES

2 exemples : les C4I au cœur des systèmes

Cloud Computing
Un marché émergent qui nécessite des solutions sûres et résilientes

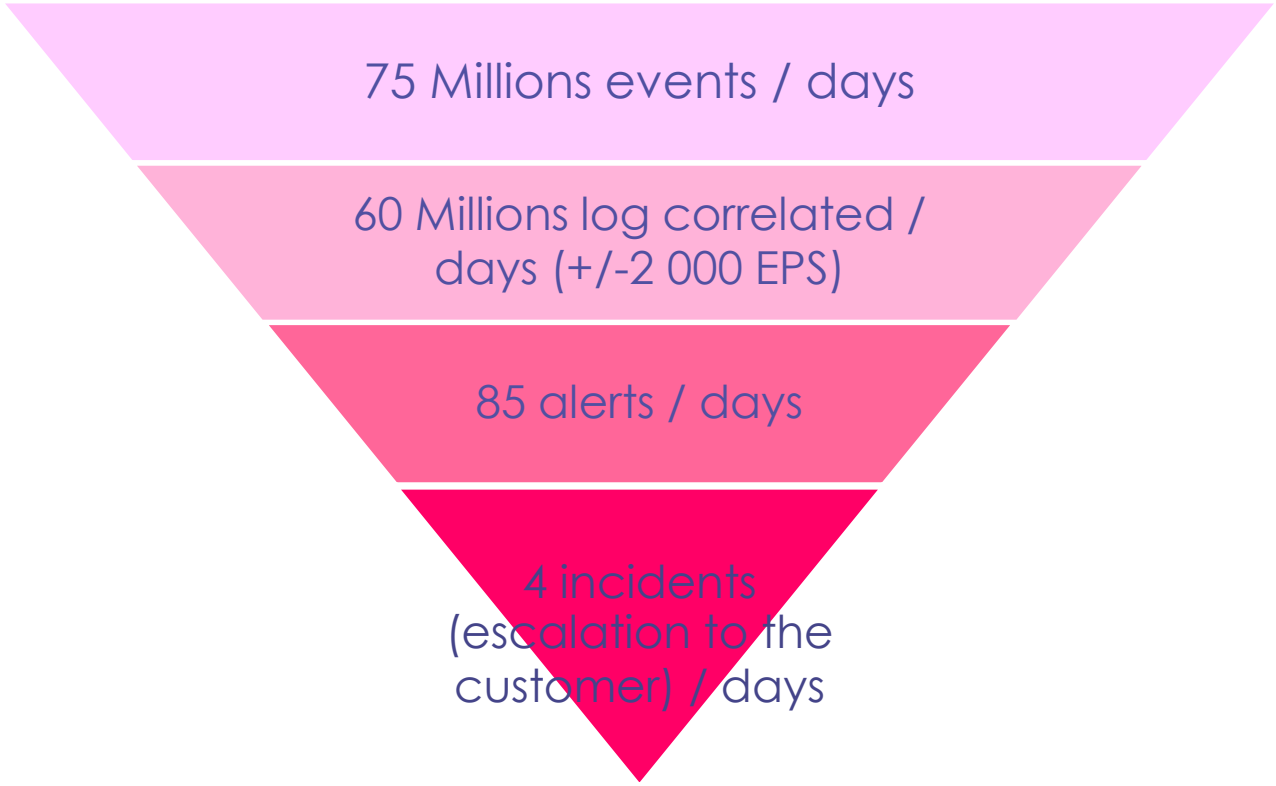
Cybersécurité
Un sujet stratégique pour de nombreux gouvernements et les grands comptes privés

THALES

Thales, opérateur de sécurité : métriques et problématiques ...

A quoi devons nous faire face en terme de collecte d'informations ?

Correlation



Expertise

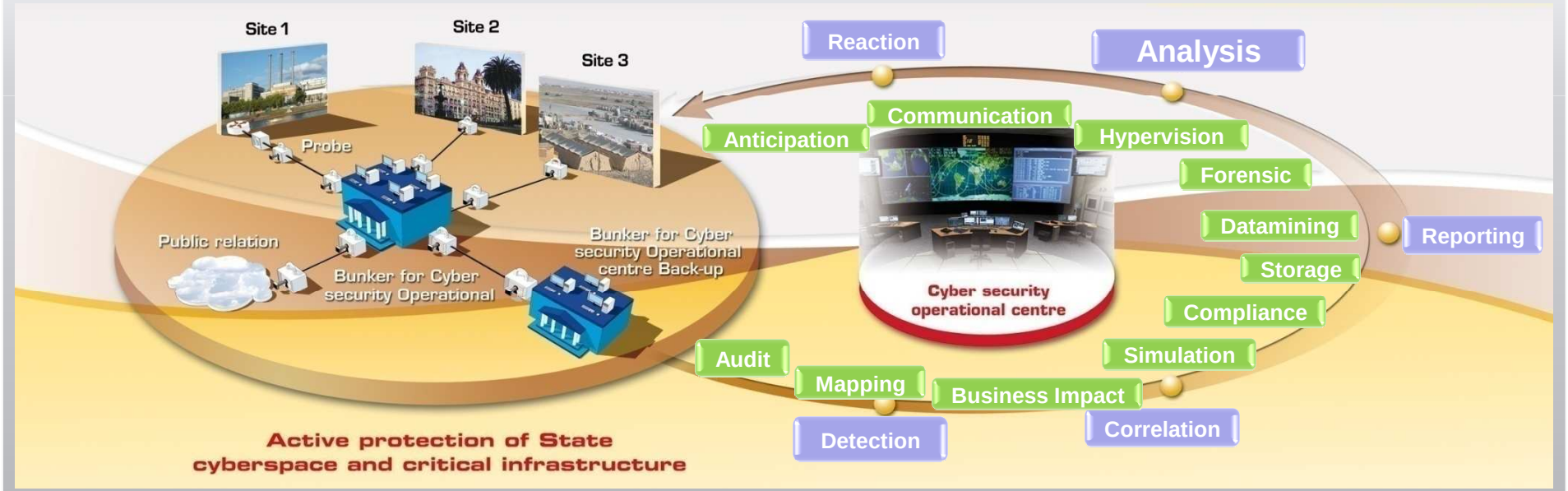
Délivrer une réponse opérationnelle

THALES

Quelle réponse : Cyber-security Operations Centre (CYBELS)



Key capabilities to ensure surveillance



Additional capabilities to help decision making process

THALES

Aide à l'analyse

Exemple d'axes de recherche :

- Topology Vulnerability analysis

- Attack graph

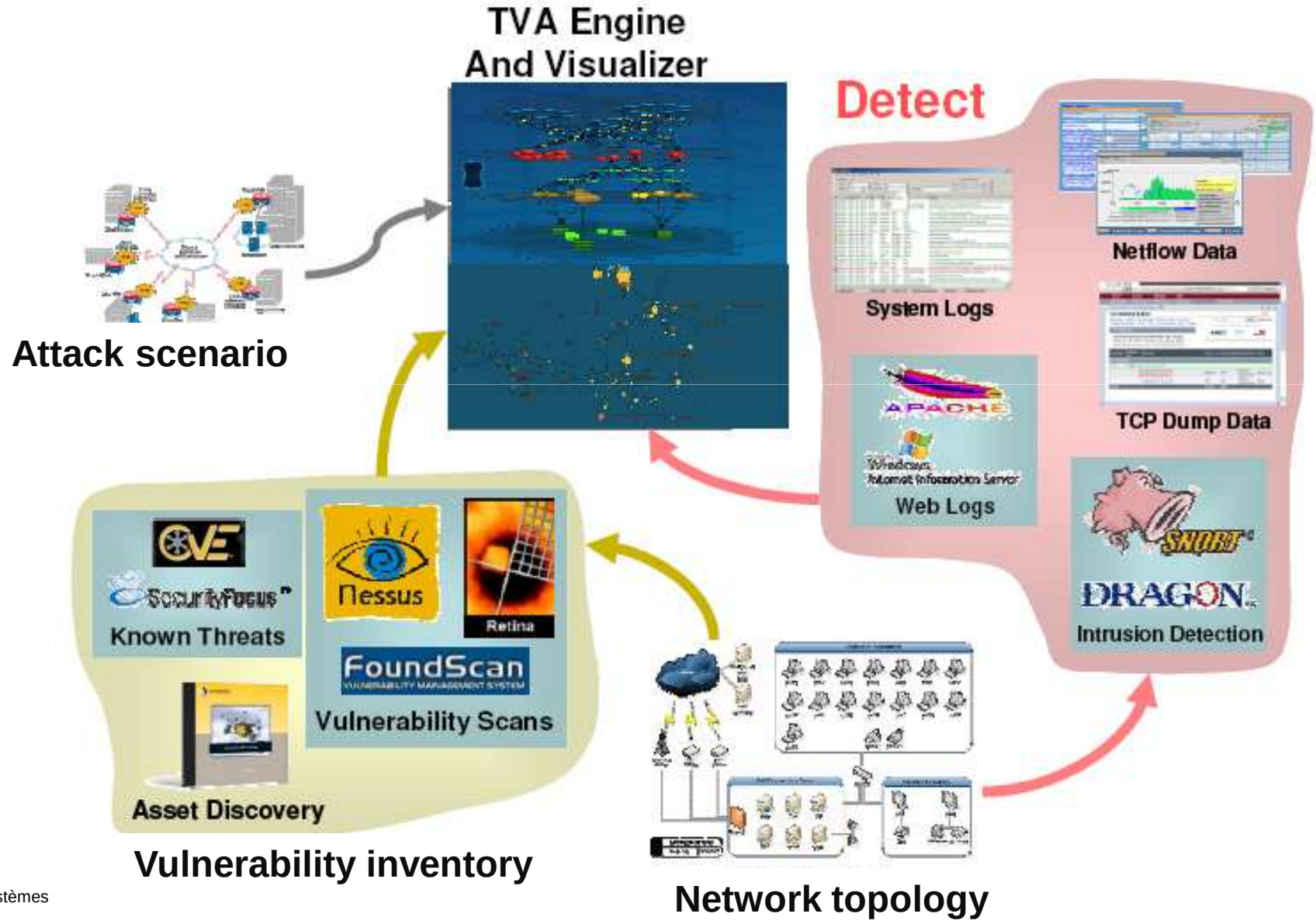
Topological Vulnerability Analysis

Modélisation du Système d'info sur les couches Métier, Application & Réseau

Graphe d'attaque: pour identifier les failles de sécurité et évaluer le risque encouru

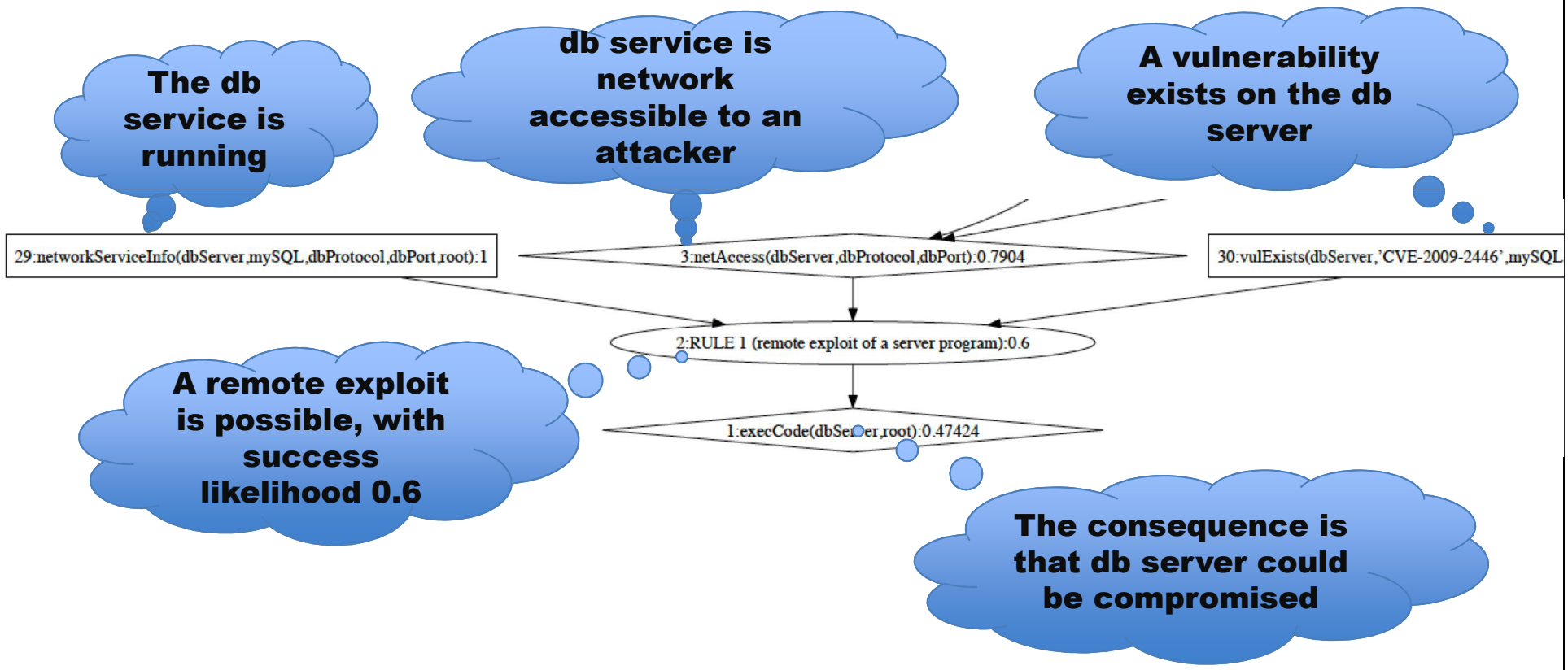
THALES

Topological Vulnerability Analysis : building blocks (1/2)



CVE : Standard de Vulnérabilités

CVE : Pré- et Post-conditions pour construire le graphe d'attaque



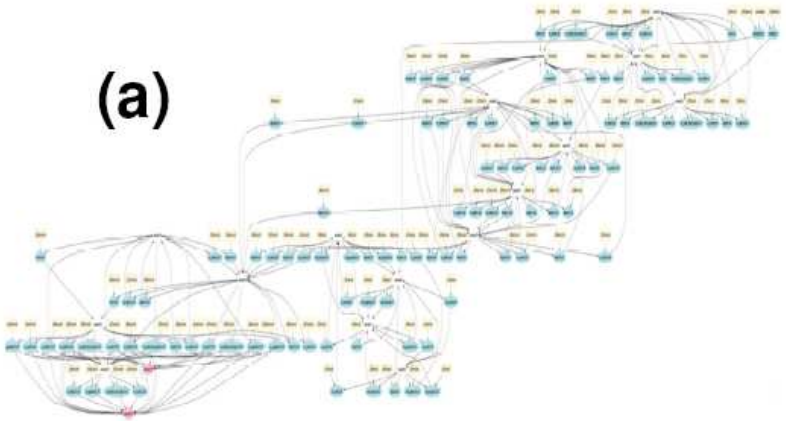
TVA & Attack Graphs

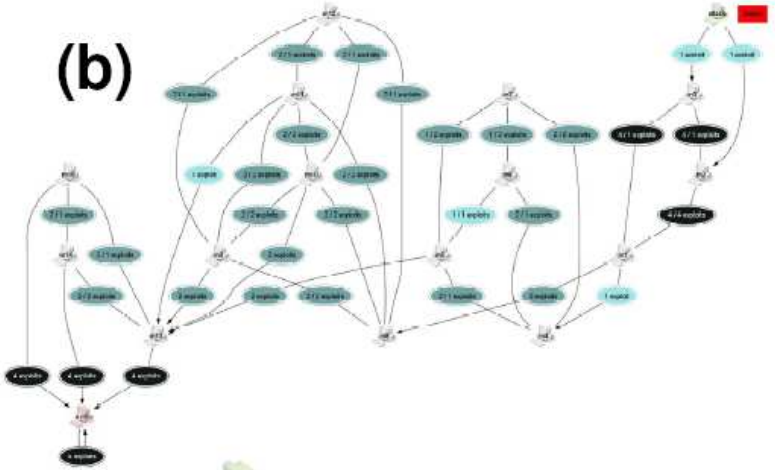
Anticiper :
Connaissance des chemins d'attaque visant les assets critiques pour le développement de Systèmes Cyber-résilients

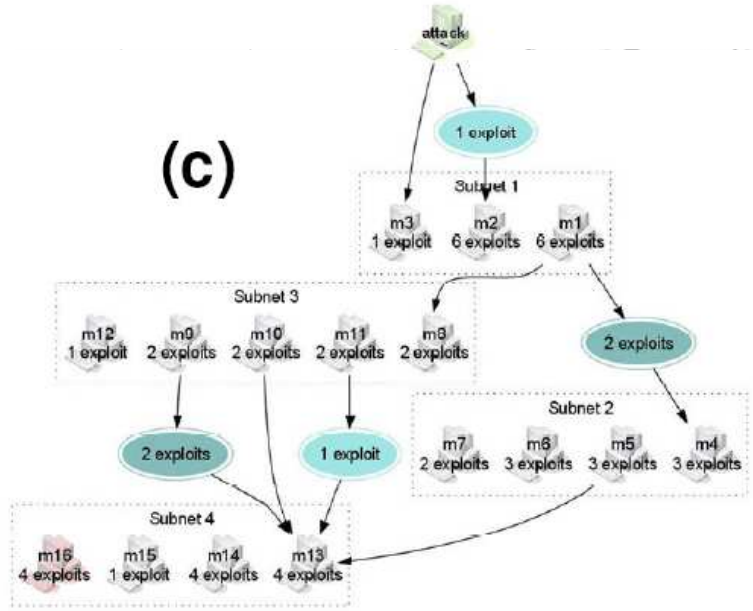
Planifier :
Evaluer le niveau de risque d'une architecture avant son déploiement

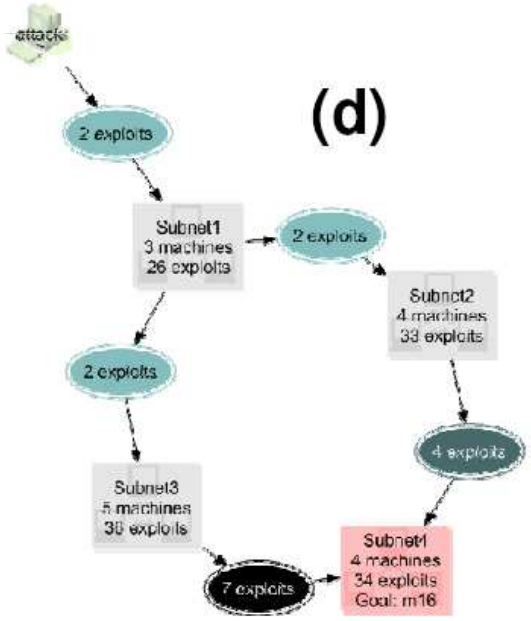
Réaction :
Proposition des contre-mesures adaptées aux priorités

Graphes d'attaque : quelques exemples de complexité





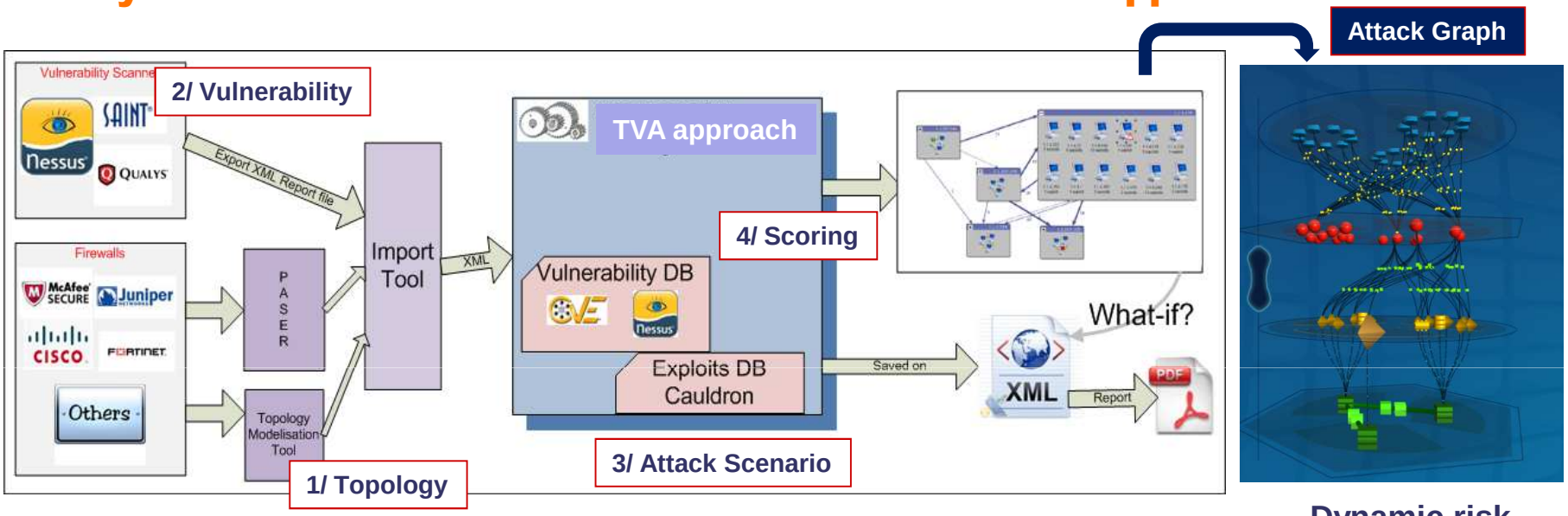




THALES

Topological Vulnerability Analysis : Chaine développée

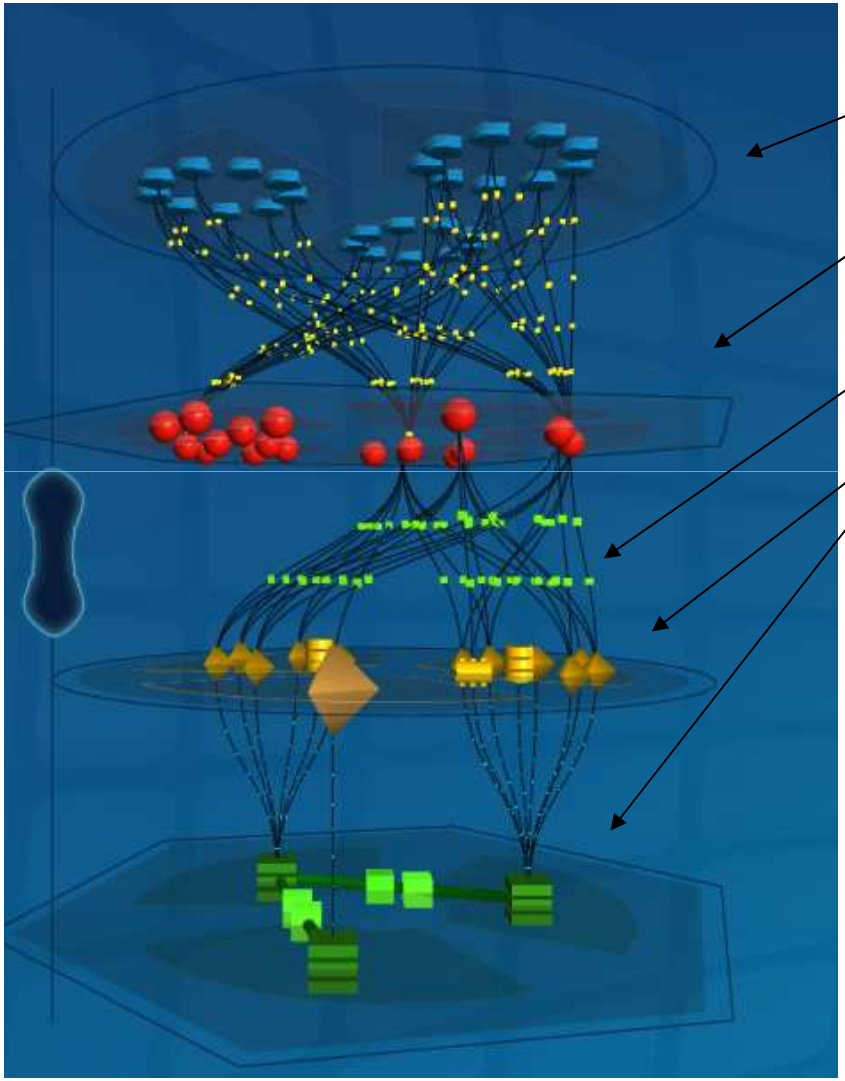
Dynamic risk assessment : Chaîne de valeur développée



Dynamic risk assessment

- Besoins complémentaires identifiés
  - *Paramétrer les sources de menaces retenues pour dessiner les arbres à partir de celle ci*
  - *Développer un lien entre analyse de risque « statique » (arbres d'attaques) et navigation dynamique au sein du SI fonction des vulnérabilités exploitées (graphes d'attaques)*
  - *Prendre en compte la virtualisation*
  - *Possibilité de paramétrer la fonction de scoring de gravité de l'attaque*

Aide à l'analyse : Visualisation avancée et TVA

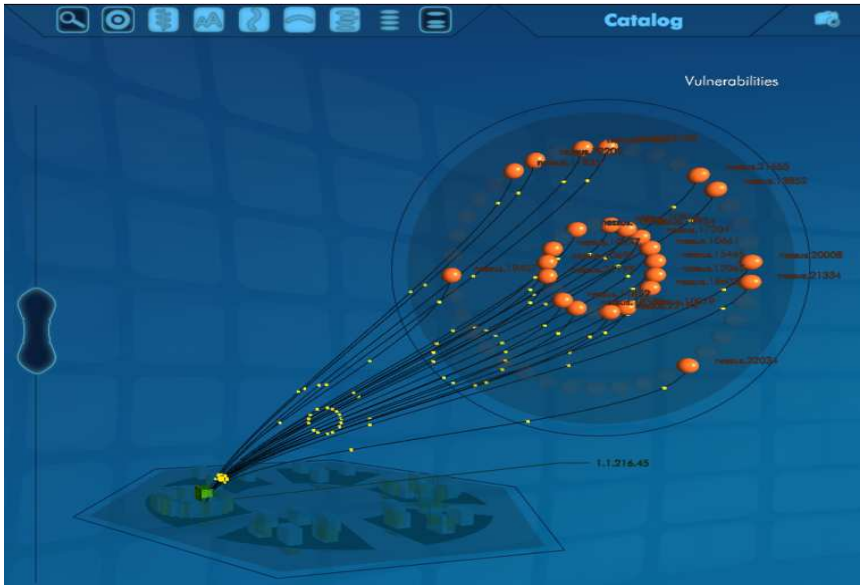


Processus métiers

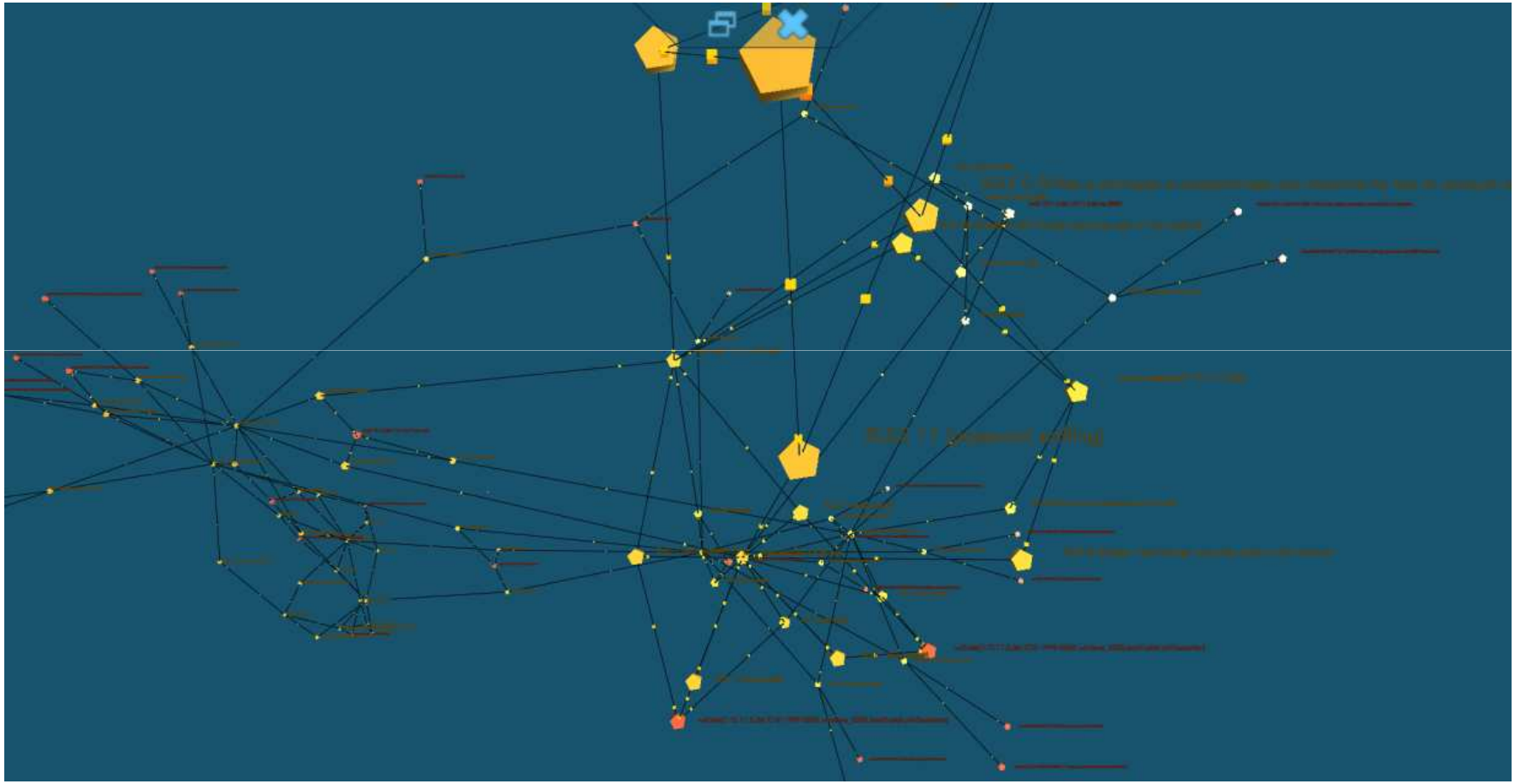
Applications

Liens de dépendances

Equipements



Aide à l'analyse : Visualisation avancée et TVA



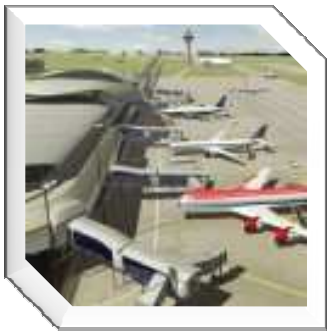
Exemple de graphe d'attaque

Plus d'intelligence pour plus de sécurité

www.thalesgroup.com

QUESTIONS / REPONSES





THALES