



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



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 
- ◆ L'innovation, accélérateur de la transformation



Cloud Computing

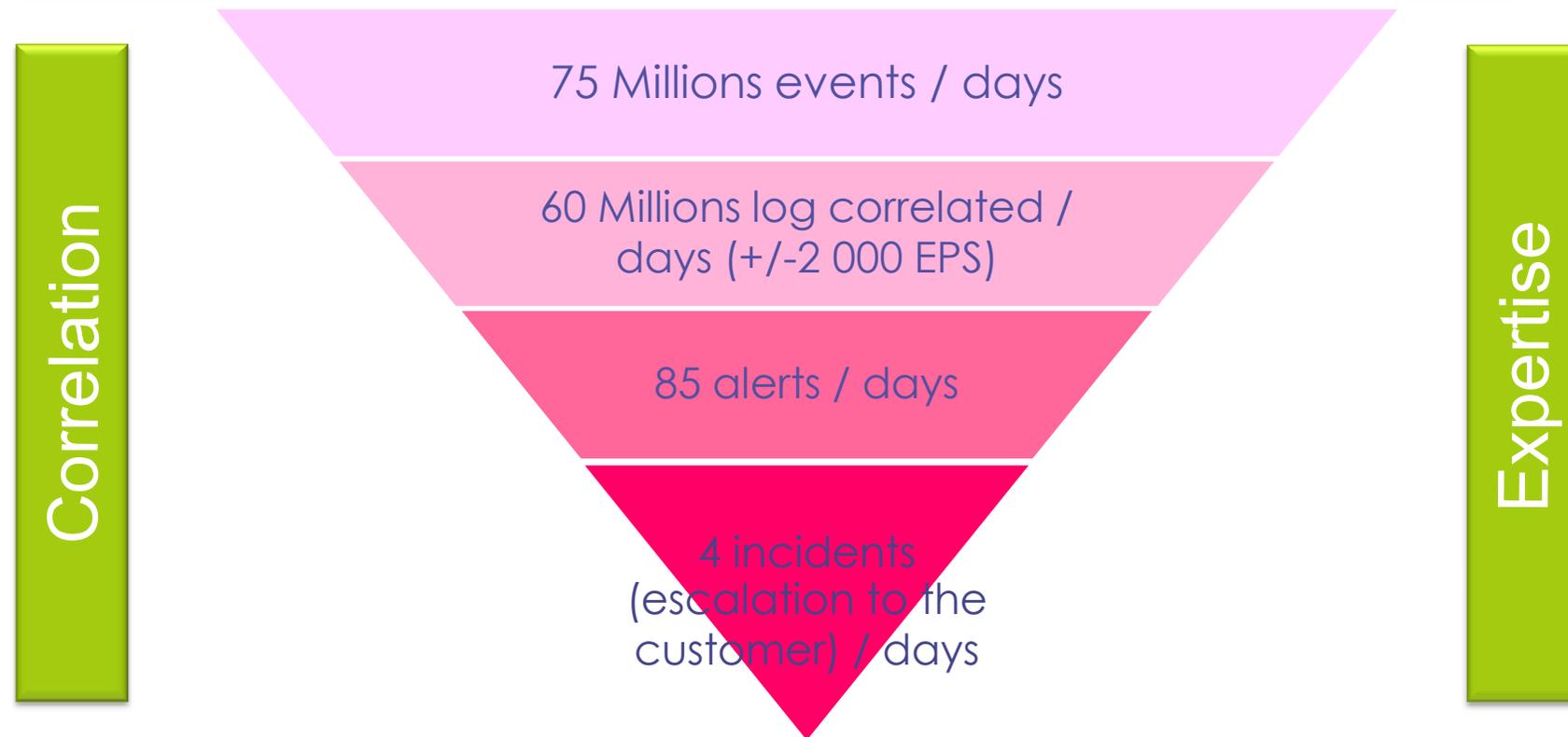
Un marché émergent qui nécessite des solutions sûres et résilientes



Cybersécurité

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

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

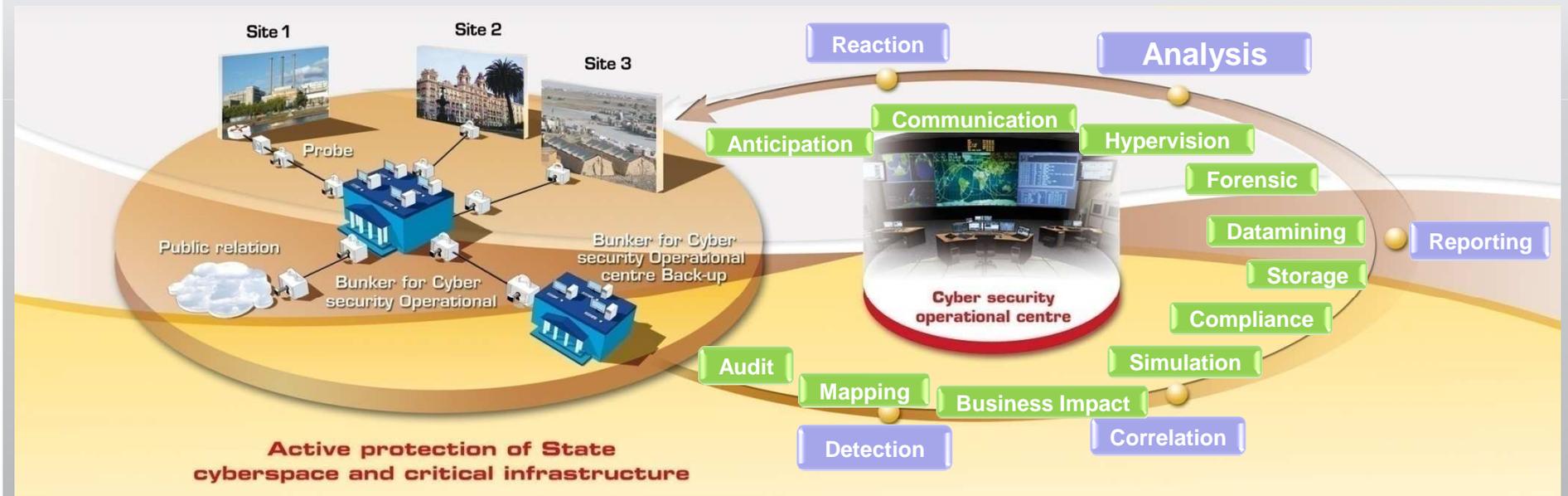


Délivrer une réponse opérationnelle

Quelle réponse : Cyber-security Operations Centre (CYBELS)



Key capabilities to ensure surveillance



Additional capabilities to help decision making process

Aide à l'analyse

Exemple d'axes de recherche :

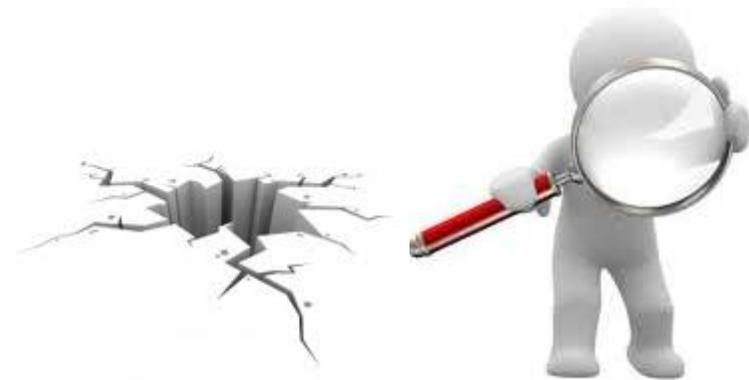
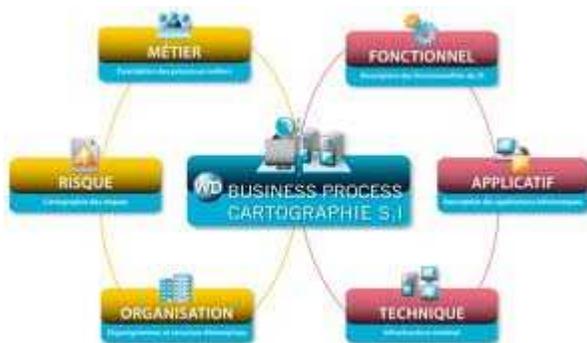
- **Topology Vulnerability analysis**

- **Attack graph**

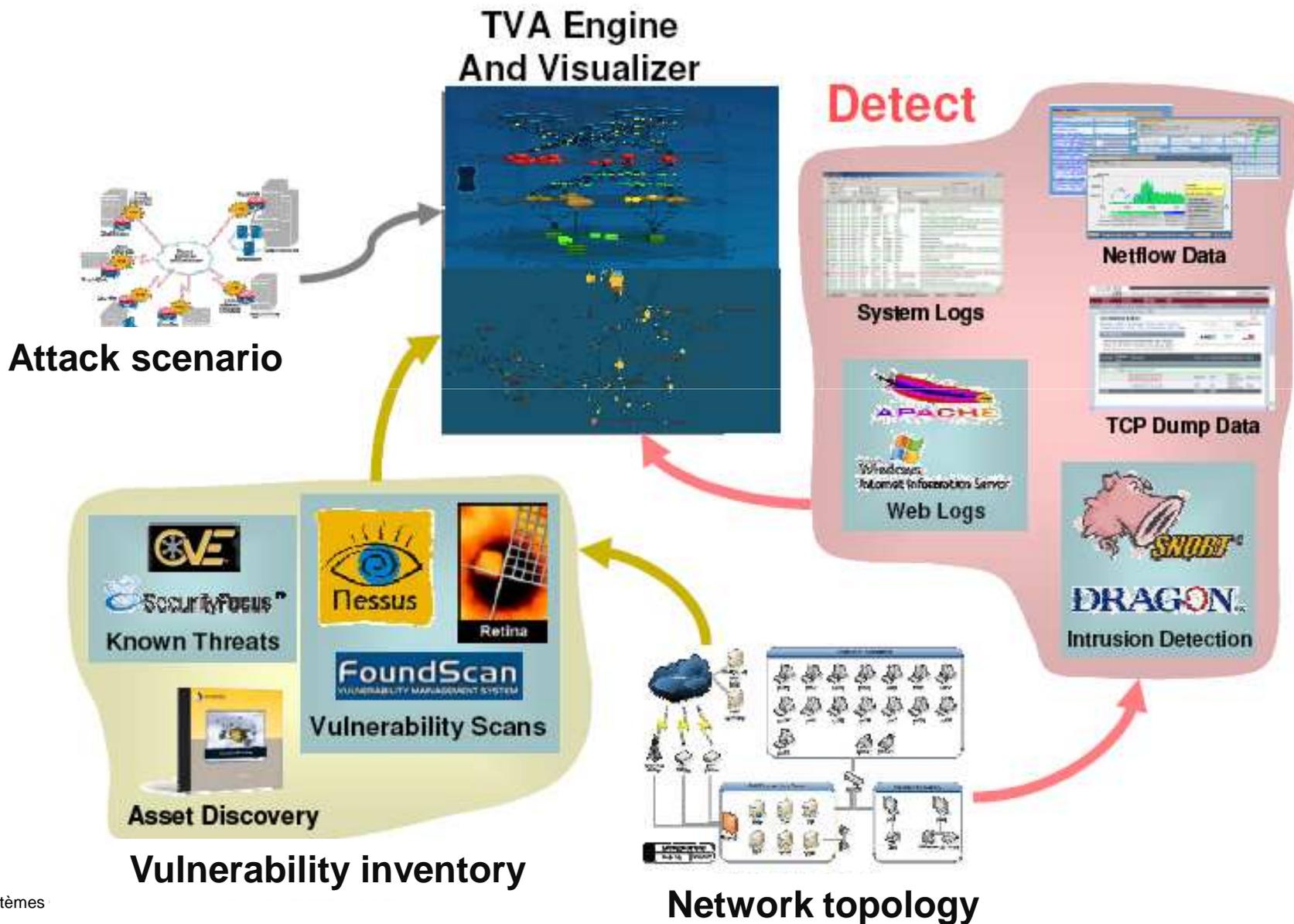


**Modélisation du Système
d'info sur les couches
Métier, Application &
Réseau**

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



Topological Vulnerability Analysis : building blocks (1/2)



CVE : Standard de Vulnérabilités

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2009-2446)

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2446

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 39200 CVE Vulnerabilities
- 128 Checklists
- 182 US-CERT Alerts
- 2347 US-CERT Vuln Notes
- 2517 OVAL Queries
- 17881 CPE Names

Last updated: Sun Oct 11 22:43:08 EDT 2009

CVE Publication rate: 14.23

Email List

NVD provides four mailing lists to the public

Done

National Cyber-Alert System

Vulnerability Summary for CVE-2009-2446

Original release date: 07/13/2009

Last revised: 08/07/2009

Source: US-CERT/NIST

Overview

Multiple format string vulnerabilities in MySQL 5.0.83 allow remote authenticated users to execute arbitrary code via a format string specifier in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request. NOTE: some of these details are obtained from third party information.

Impact

CVSS Severity (version 2.0): HIGH

CVSS v2 Base Score: 8.5 (HIGH) (AV:N/AC:M/Au:S/C:C/I:A/S:A)

Impact Subscore: 10.0

Exploitability Subscore: 6.8

CVSS Version 2 Metrics:

- Access Vector:** Network exploitable
- Access Complexity:** Medium
- Authentication:** Required to exploit

Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

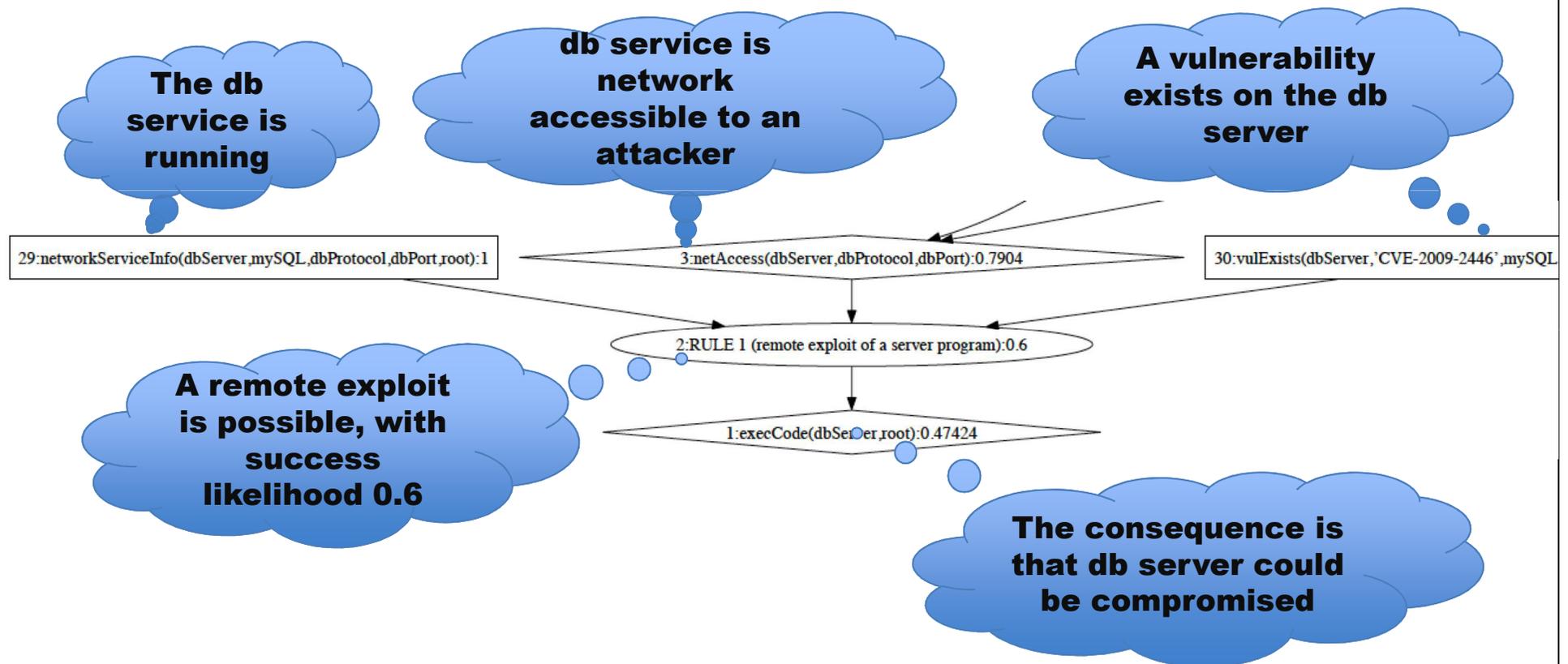
Scoring : impact potentiel

Exploit pre-condition

Exploit post-condition

Probabilité d'occurrence

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

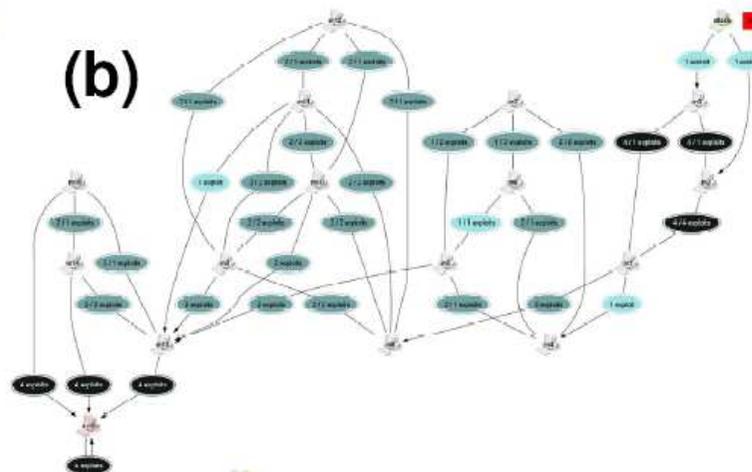
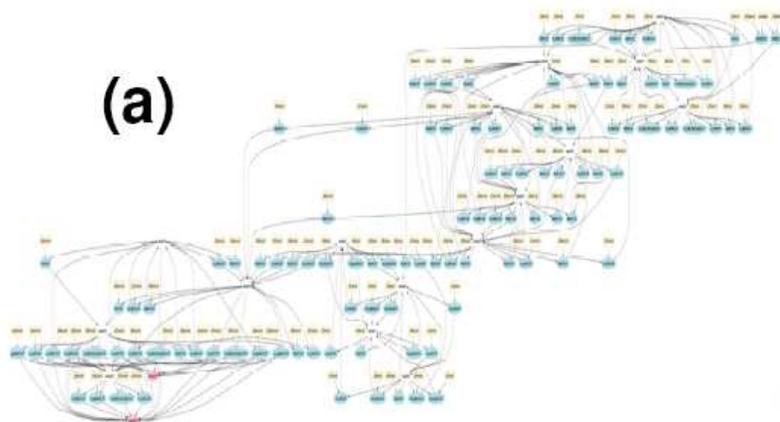
Planifier :

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

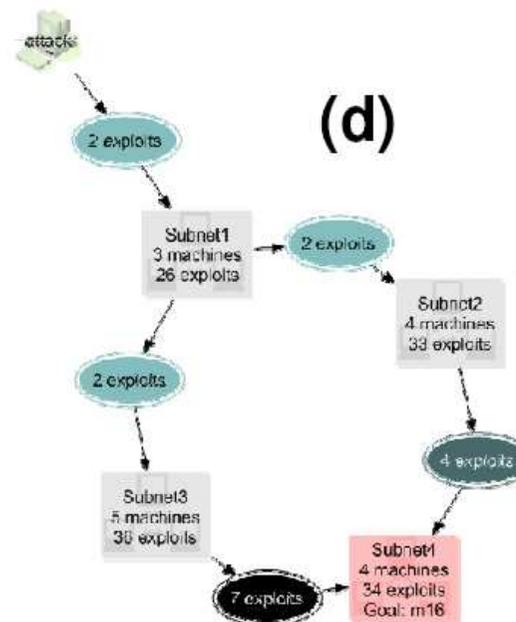
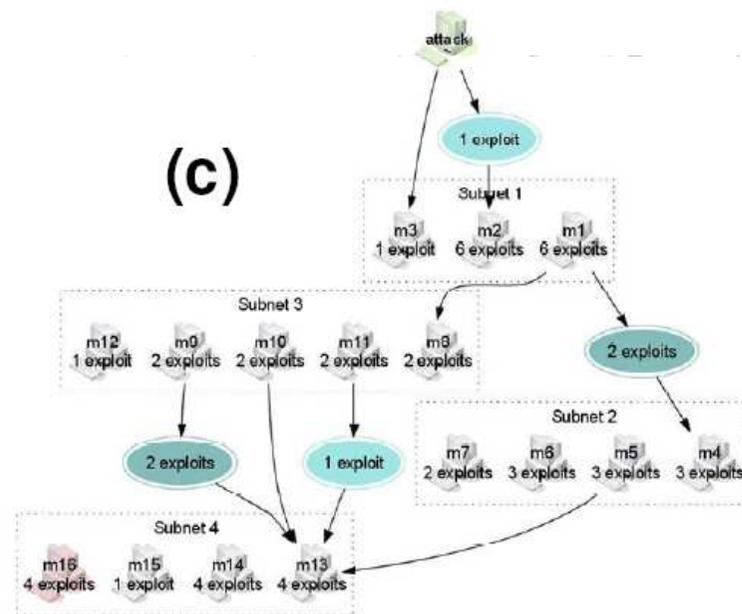
Réaction :

Proposition des contre-mesures adaptées aux priorités

Graphes d'attaque : quelques exemples de complexité



TRAN

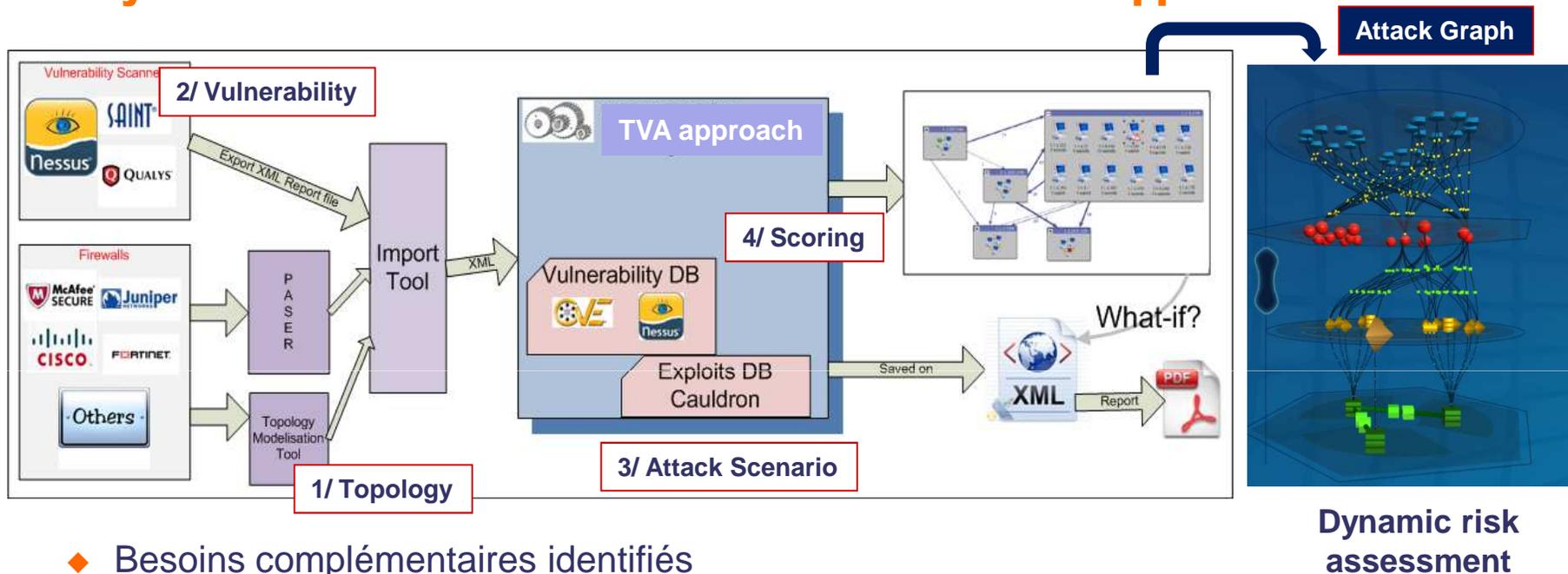


9

ITACK)

Topological Vulnerability Analysis : Chaîne développée

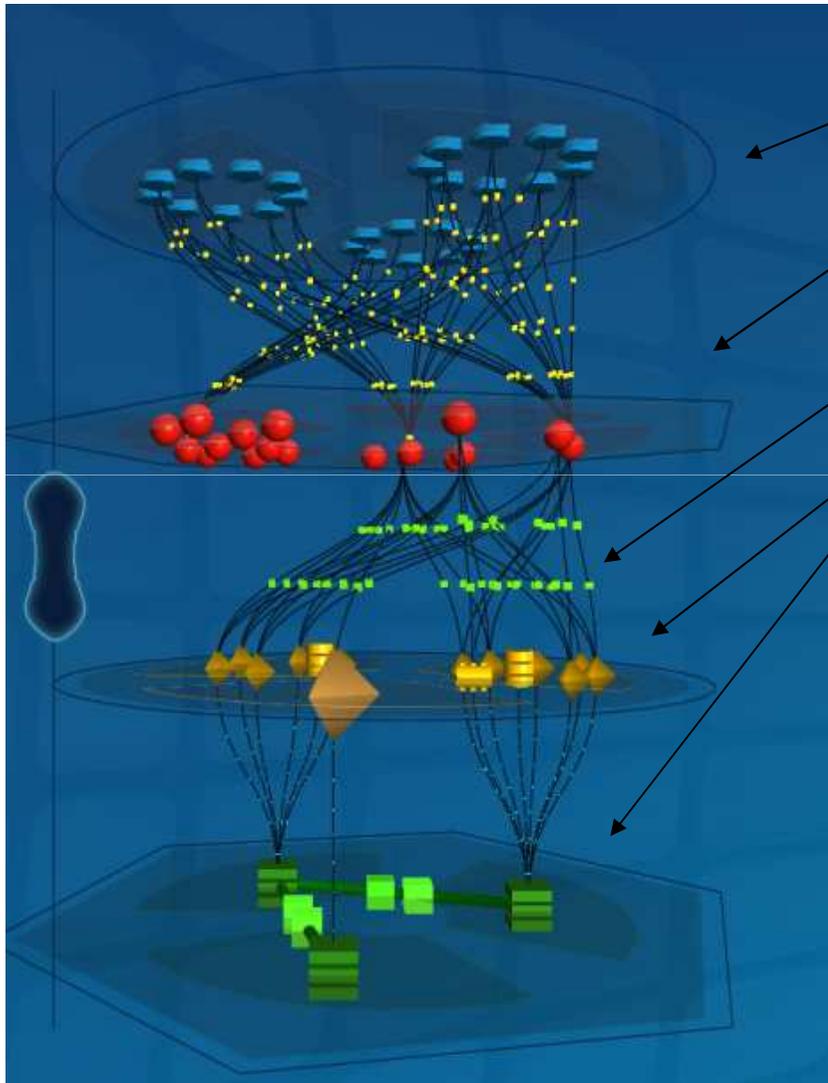
Dynamic risk assessment : Chaîne de valeur développée



◆ 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

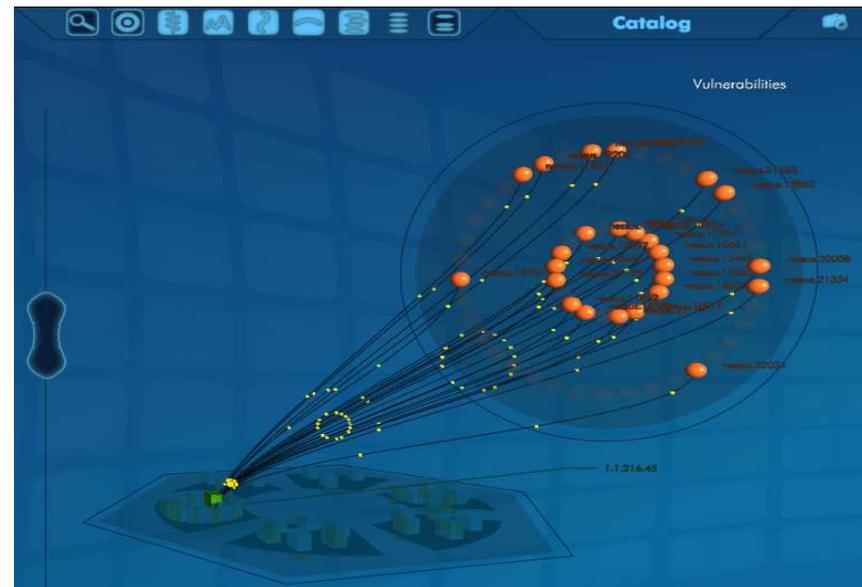


Processus métiers

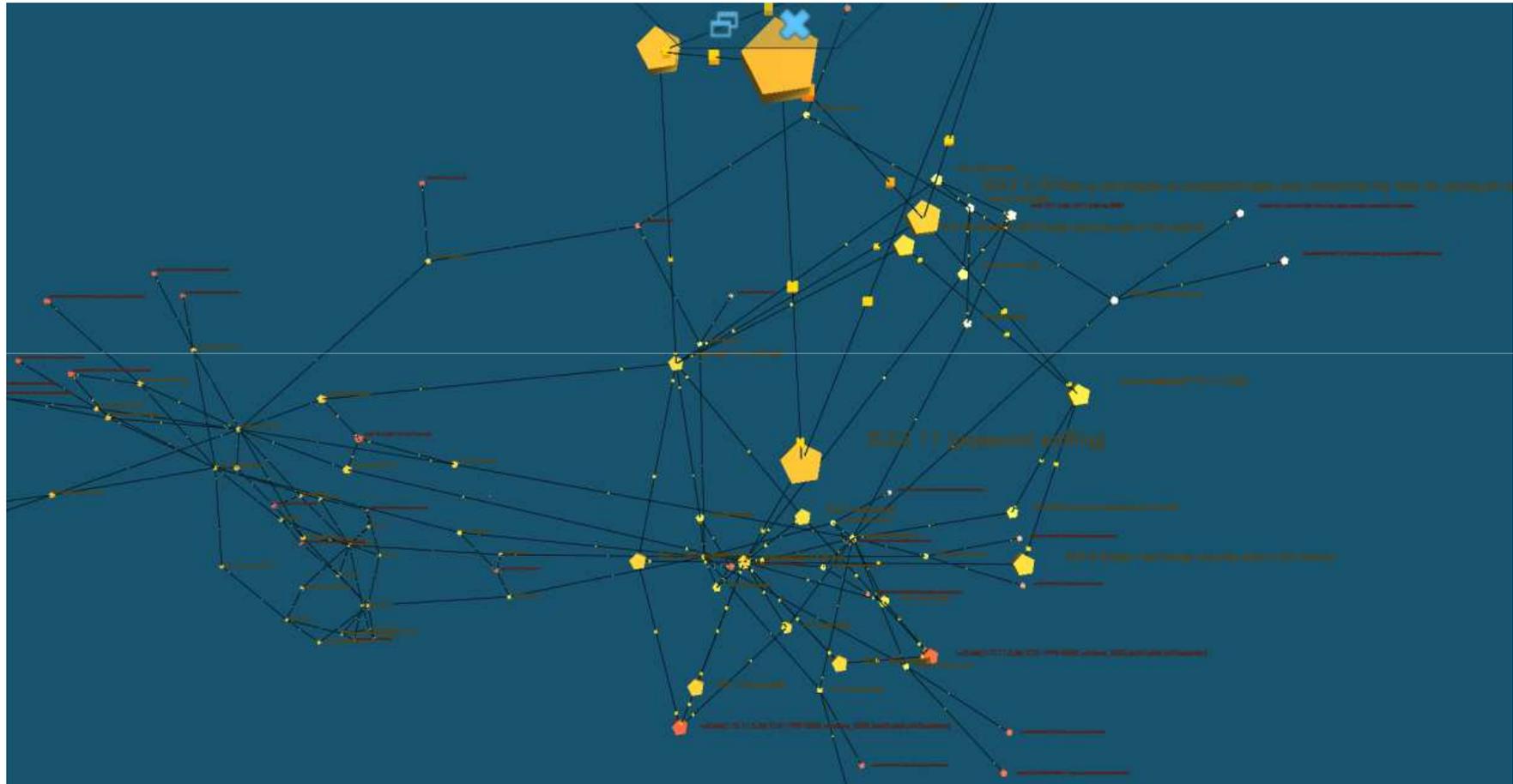
Applications

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

