The importance of data in cyber security governance

Advanced Data Collection and Risks

19/04/2016

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy

Agenda

- Relevant **future challenges** in cyber security
- The **strategy** at a glance
- **Why governance** in cyber security
- Examples for **data collection** in cyber security
- **Governance models** in cyber security
- **MONARC**
- **Outlook**

Relevant future challenges

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Fast moving target
- Lack of skilled people
- Need of intense collaboration
- Threat has professionalised since 2007
- Regulatory framework will increase in complexity

Go beyond compliance, towards security

Photo: François Thill

Relevant future challenges

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Strong governmental commitment to digitisation
  - IPCEI – HPC and big data
    - IoT – infrastructure mode in autonomous driving
    - FinTECH
    - SpaceTECH
- Increase of targeted attacks
- Need of medium and high security

Photo: Lena Thill

Relevant future challenges

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Stop struggling alone – it's a societal challenge!

- We need skills and human resources
- We have to reduce costs and complexity
- We have to create governance structures

Rootology: Rowboat with oars and two passengers.

Strategy of the governement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Cyber security is a factor of attractiveness
- Cyber security is a competitive advantage
- Cyber security is an opportunity
- Cyber security concerns everybody

"**Digital security risk should be treated like an economic rather than a technical issue, and should be part of an organisation's overall risk management and decision-making**", OECD – 2015

Strategy of the governement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Democratisation of security
- Security for all - together
  - Reduce costs and complexity for everybody
  - Agree upon a taxonomy and mutualise
  - **C**ollaborate, **C**ooperate, **C**oordinate: Competitive advantage

Why governance

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Tremendous potential of synergies

- Behaviour and skills
  - Awareness, training, education

- Organisational security
  - Diagnostic tools, towards best practice
  - Risk management: more objective with less individual effort
  - Information security policies and light weight ISMS

- Technical security
  - Risk treatment
  - incidents handling
  - Threat intelligence

Gather intel

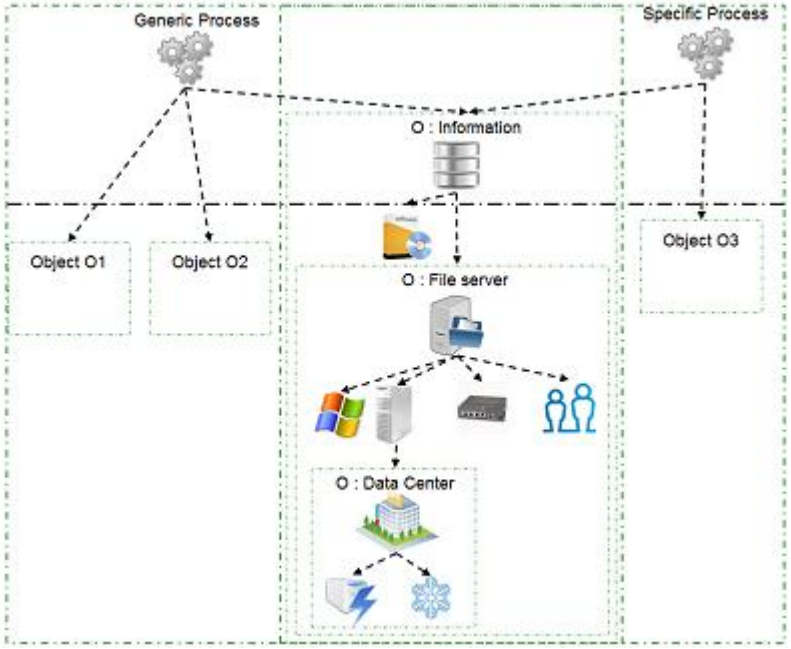
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

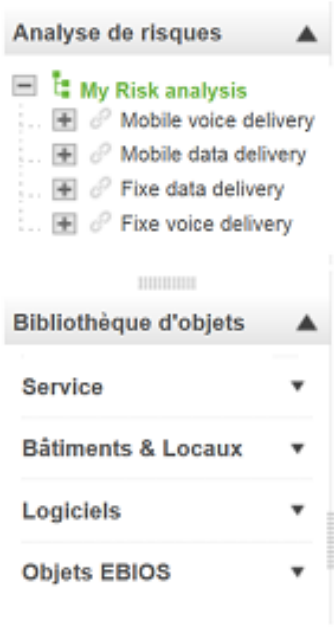
Gather intel in order to act intelligently and legally

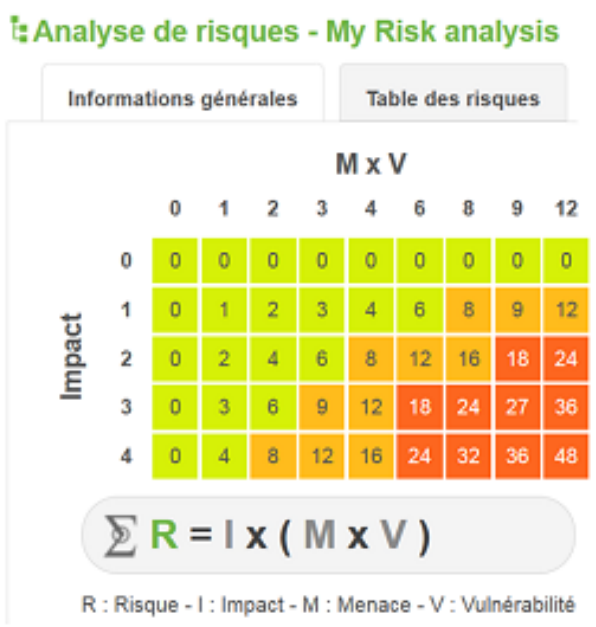
Example – CASES: *MONARC*

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Méthode Optimisée d'aNAlyse des Risques Cases - **MONARC**







- **Reduction** of individual effort by **80%**
- Towards a **common taxonomy**
- Towards **objectiveness** and **governance**

cases

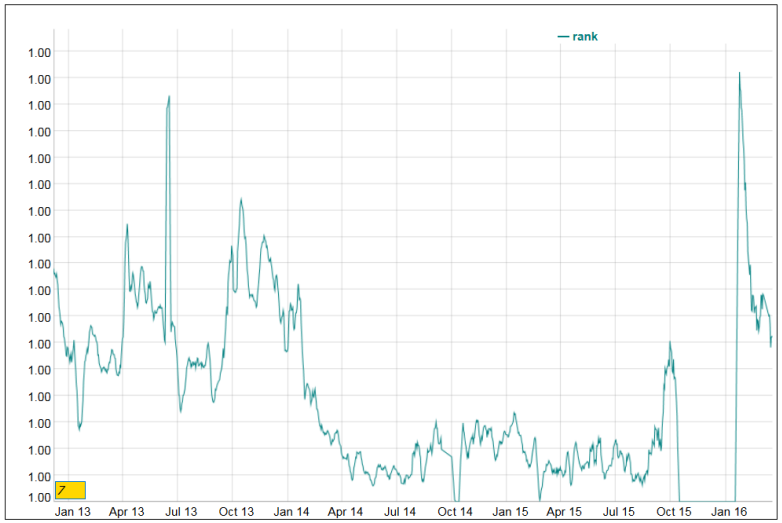
Example – BGPranking: *MISP*

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

BGPranking– ranking of AS

- Collect blacklists – link to AS
- Evaluate maliciousness of AS

We can calculate health and maliciousness indicator for AS



CIRCL
BGP Ranking

circl

Examples – CIRCL: *AIL*

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

AIL – Analysis of Information Leaks

- 20 sources
- 5-7 posts per second (in 2014: 27 GB data – 24 million pages)
- Analysis for breach indicators

We are able to **warning of victims**

CIRCL
AIL
Analysis of Information Leaks

circl

Example – CIRCL: *MISP*

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

MISP – Malware Information Sharing Platform

- 3040 events in the database
  - 336.000 attributes
  - 113.000 correlations

Not only **detect** and **block**, but also generate **intelligence** about **campaigns and attacks**

circl

Act intelligently and legally – principles of proportionality & necessity

Possible governance model

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Informed governance

- Governance based upon risk management facts and figures
  - Increase objectiveness

- Requirements formulated in RM jargon
  - Indicators (threats and vulnerabilities)
  - Risk acceptance matrix
  - Impact specifications

- Aggregation should be possible
  - Identification of systemic risks

Governance – a taxonomy

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

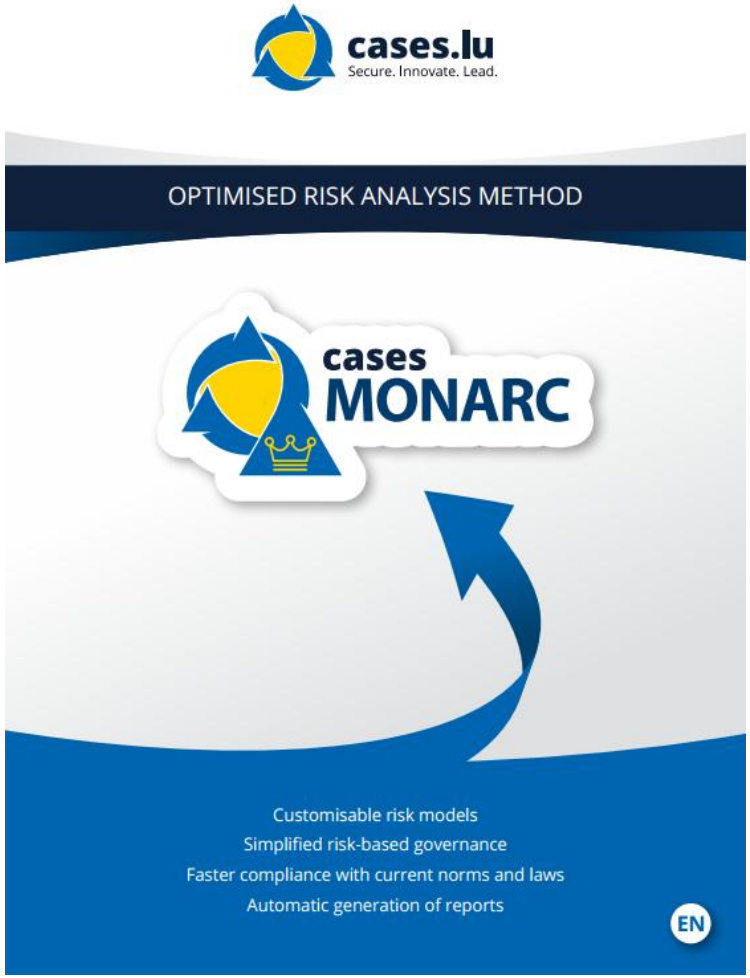
- Scope ?
- What granularity ?
- What primary and secondary assets ?

- What impacts?
- What risk appetite?

➢ What threats and probabilities of threats ?
➢ What vulnerabilities and ease of exploitation ?
➢ What risk treatments and what effectiveness?

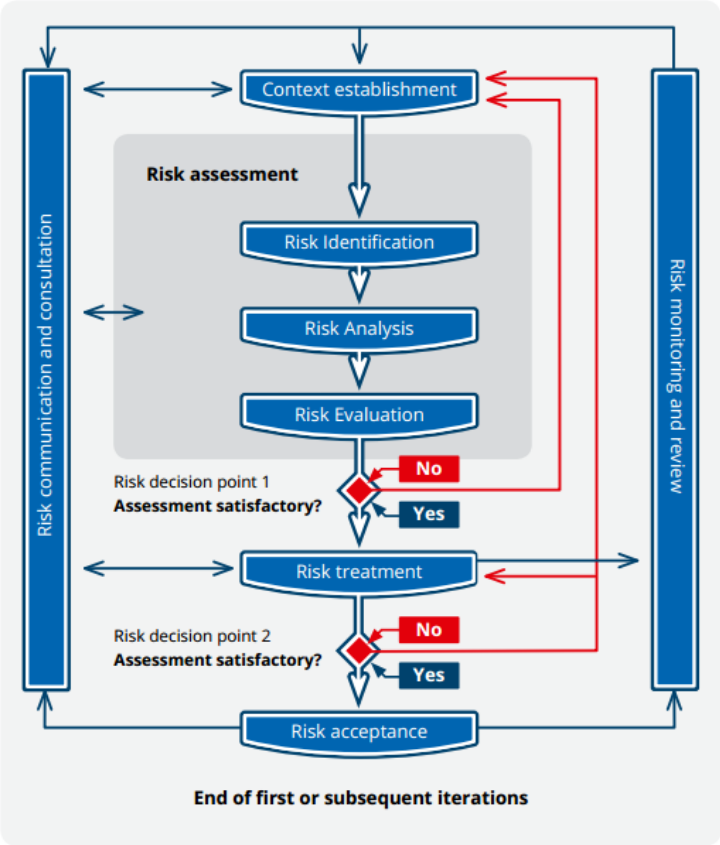
What is proportionate and necessary?

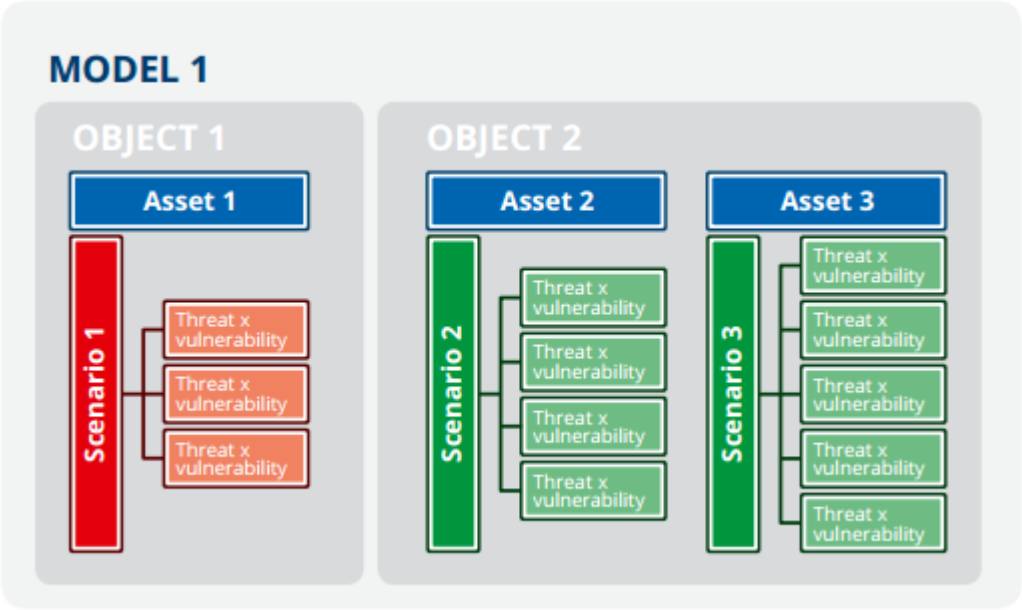
Reduce individual effort – increase objectivity

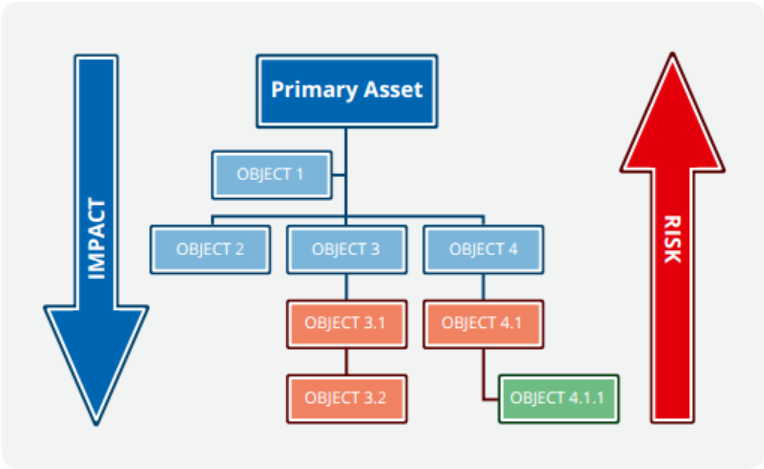


MONARC

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

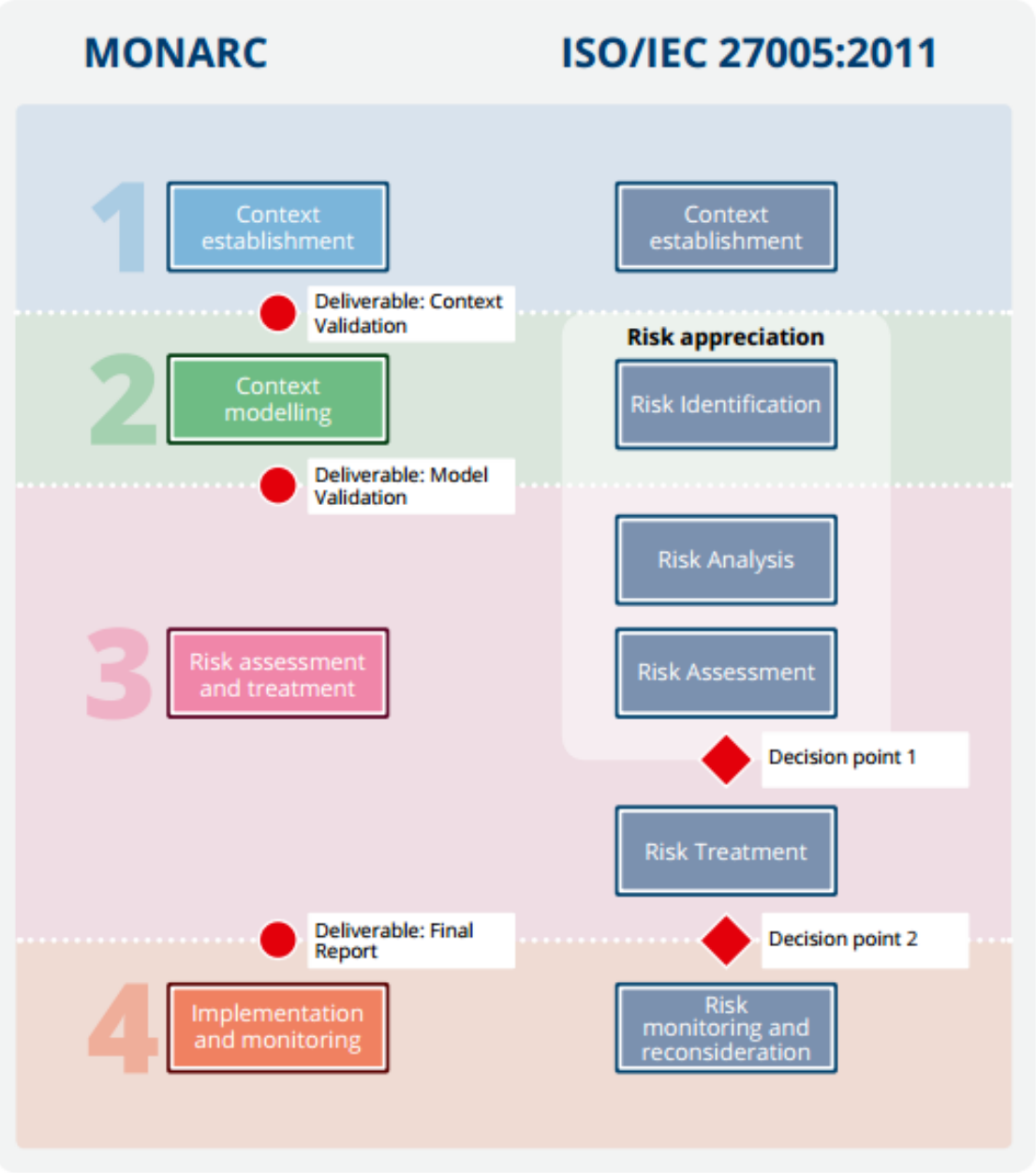






MONARC

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



MONARC

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Méthode Optimisée d'Analyse des Risques CASES

0%

1. Établissement du contexte

- [ ] Contexte de l'analyse des risques
- [ ] Évalution des tendances
  Évaluation des menaces
  Synthèse de l'évaluation des tendances et des menaces
- [ ] Contexte de la gestion des risques
- [ ] Définition des critères d'évaluation, d'acceptation et d'impact

Livrable : validation du contexte

0%

2. Modélisation du contexte

- [ ] Identification des actifs, des vulnérabilités et appréciation des impacts
- [ ] Synthèse des actifs / impacts

Livrable : validation du modèle

0%

3. Évaluation et traitement des risques

- [ ] Estimation, évaluation et traitement des risques
- [ ] Gestion du plan de traitement des risques

Livrable : rapport final

0%

4. Implémentation et surveillance

- [ ] Gestion de l'implémentation du plan de traitement des risques

MONARC

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Analyse de risques - Start-up (year 1)

Informations générales | Table des risques | Table des risques OP | Base de connaissances | Outils

Calcul du risque / Seuils - Risques de l'Information

Impact \ M x V	0	1	2	3	4	5	6	8	9	10	12	15	16	20
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	8	9	10	12	15	16	20
2	0	2	4	6	8	10	12	16	18	20	24	30	32	40
3	0	3	6	9	12	15	18	24	27	30	36	45	48	60
4	0	4	8	12	16	20	24	32	36	40	48	60	64	80

$\sum R = I \times (M \times V)$

R : Risque - I : Impact - M : Menace - V : Vulnérabilité

Mettre à jour les échelles

Calcul du risque / Seuils - Risques Opérationnels

Impact \ Probabilité	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	6	8
3	0	3	6	9	12
4	0	4	8	12	16

$\sum R = I \times P$

R : Risque - I : Impact - P : Probabilité

Mettre à jour les échelles

Actions pour l'analyse de risques

Instancier un fils | Modifier | Supprimer

START-UP – DEVELOP THE IDEA

Gemeinde Heagschroa

Analyse de risques

Recherchez une instance

Tout déplier / Tout plier

- Gemeinde Heagschroa
  - AP07: Gestion des salles des fêtes
  - AP25: Gestion des demandes diverses d'autorisation
  - AP32: Gestion des permis de pêche et chasse
  - AP16: Gestion de l'état civil
  - AP04: Gestion des repas sur roues

Bibliothèque d'objets

Recherchez un objet

Ajouter un objet à la bibliothèque

- Test
- Coffres
- Conteneurs
- Personnel
- Logiciels
- Processus
- Services
- Informations

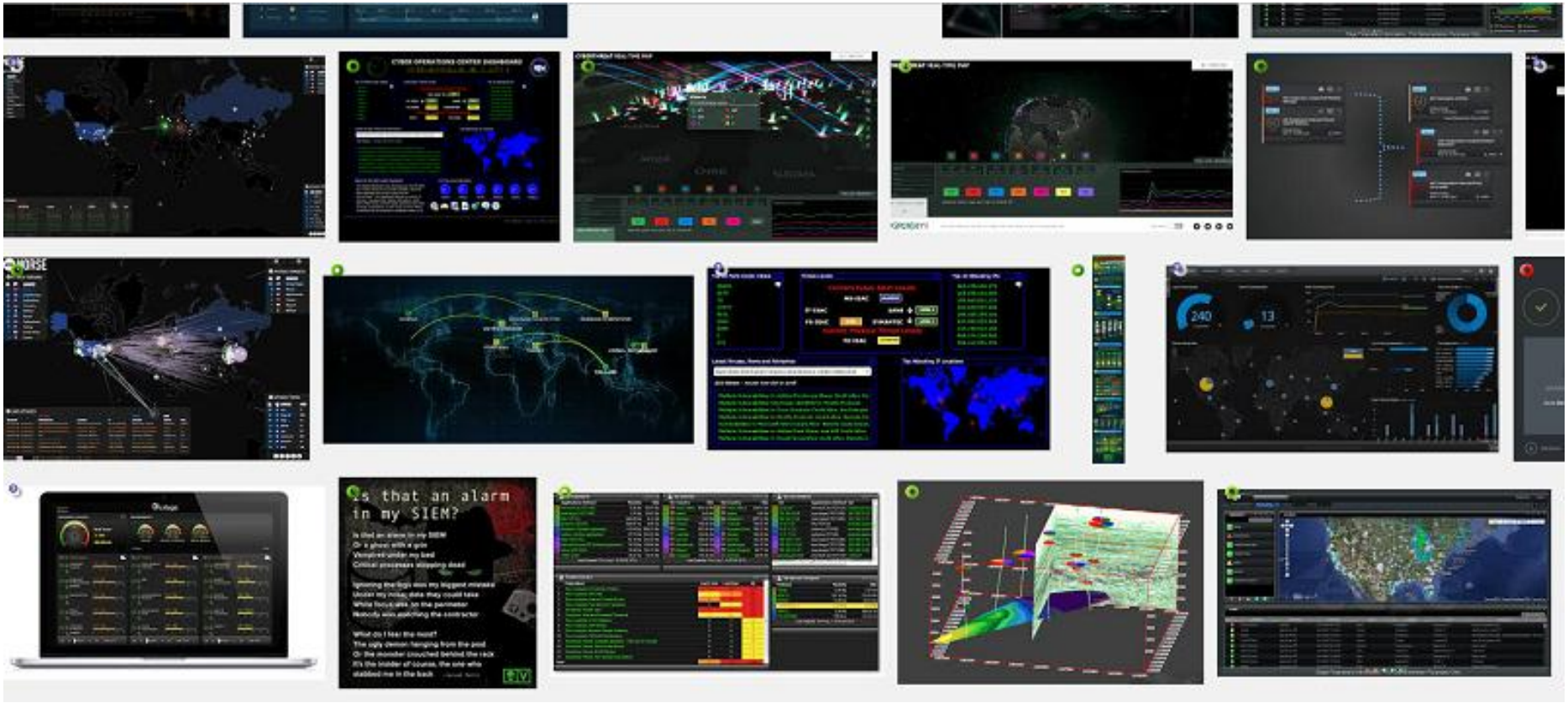
Instance	Impact C	Impact I	Impact D	Menace	Prob.	Vulnérabilité	Qualif.	Risque C	Risque I	Risque D	Constatation	T	Risque visé	Actions
Laptop dans Information Idea...	2	1	2	Infection par un malware	4	Absence de système de détection des logiciels malveillants	5	40	20	40	No antivirus		40	
Laptop dans Information Idea...	2	1	2	Vol ou destruction de supports, de documents ou de matériel	2	Présence d'information sur un support non soumis au backup	5	20		20	No backups		20	
Office dans Information Idea...	2	1	2	Vol ou destruction de supports, de documents ou de matériel	2	Failles dans les périmètres d'accès physiques	3	12		12	No Alarm		4	
Laptop dans Information Idea...	2	1	2	Ecoute passive	1	Utilisation d'un moyen de communication non sécurisé	5	10			Use mail to send confidential information		2	
Office dans Information Idea...	2	1	2	Sinistre environnemental (Incendie, eau, poussière, saleté, etc.)	2	Les locaux ne sont pas sécurisés ou peuvent être compromis par des éléments externes	1		2	4	No computer room		4	

Risk treatment

Instance	Impact C	Impact I	Impact D	Menace	Prob.	Vulnérabilité	Qualif.	Risque C	Risque I	Risque D	Constatation	T	Risque visé	Actions
Laptop dans Information Idea...	2	1	2	Infection par un malware	4	Absence de système de détection des logiciels malveillants	2	16	8	16	No antivirus	●	-	
Laptop dans Information Idea...	2	1	2	Vol ou destruction de supports, de documents ou de matériel	2	Présence d'information sur un support non soumis au backup	2	8		8	No backups	●	-	
Office dans Information Idea...	2	1	2	Vol ou destruction de supports, de documents ou de matériel	2	Failles dans les périmètres d'accès physiques	3	12		12	No Alarm	●	4	
Laptop dans Information Idea...	2	1	2	Ecoute passive	1	Utilisation d'un moyen de communication non sécurisé	5	10			Use mail to send confidential information	●	2	
Office dans Information Idea...	2	1	2	Sinistre environnemental (Incendie, eau, poussière, saleté, etc.)	2	Les locaux ne sont pas sécurisés ou peuvent être compromis par des éléments externes	1		2	4	No computer room		4	

Outlook

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



Outlook

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Dashboards

- Risk based formulation of requirements
- National metrics for threats, vulnerabilities and effectiveness of risk treatment measures
- Benchmarks

The End

Thank you for your attention

François Thill

LE GOUVERNEMENT

CESSEZ D'ÊTRE UNE PROIE SUR INTERNET. **PROTÉGEZ VOS DONNÉES.**

www.securitymadein.lu

bigi SYVICOL LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

SECURITY MADEIN.LU

aware.lu circl.lu cases.lu