Pouvoirs locaux, développez votre stratégie de cybersécurité

Webinaire – 21 juin 2021

Union des Villes et Communes de Wallonie asbl

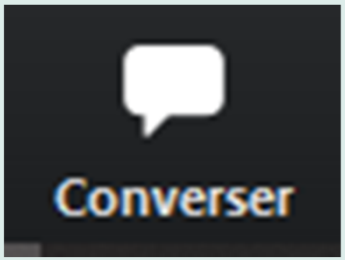
Wallonie

Quelques consignes pour débuter…

Converser/chat

01 Signaler un problème **technique**

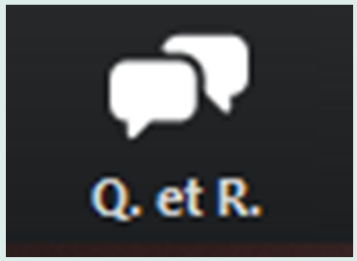
→ **Modérateur**



Q. Et R.

02 Poser une question liée aux **contenus**

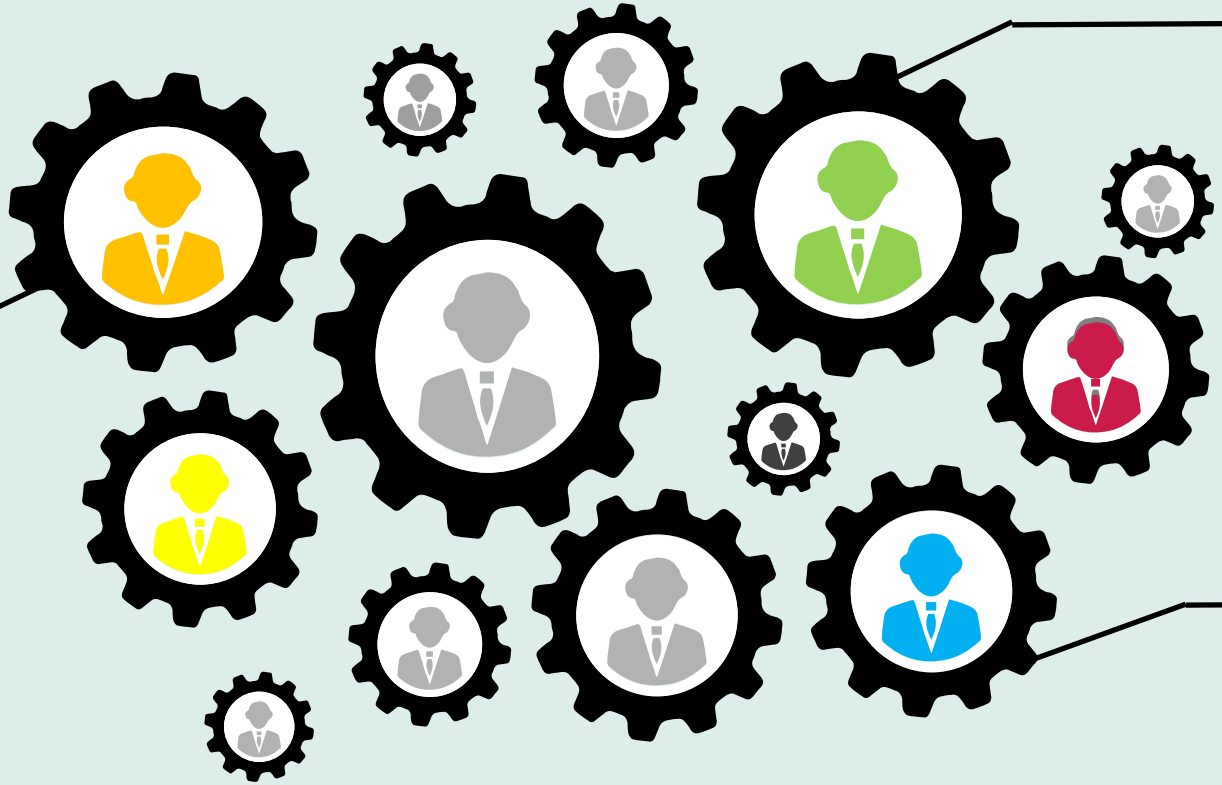
→ **Conférenciers**



Nos invités

Dominique GREGOIRE
Conseiller en sécurité de l'information - Président du Groupe de travail sur la sécurité de l'information (GTSI)

Olivier BOGAERT
CP
Computer Crime Unit, Police Fédérale



Christophe TOURMENT
Ingénieur système en infrastructure IT et responsable de la cellule de consultance - Imio

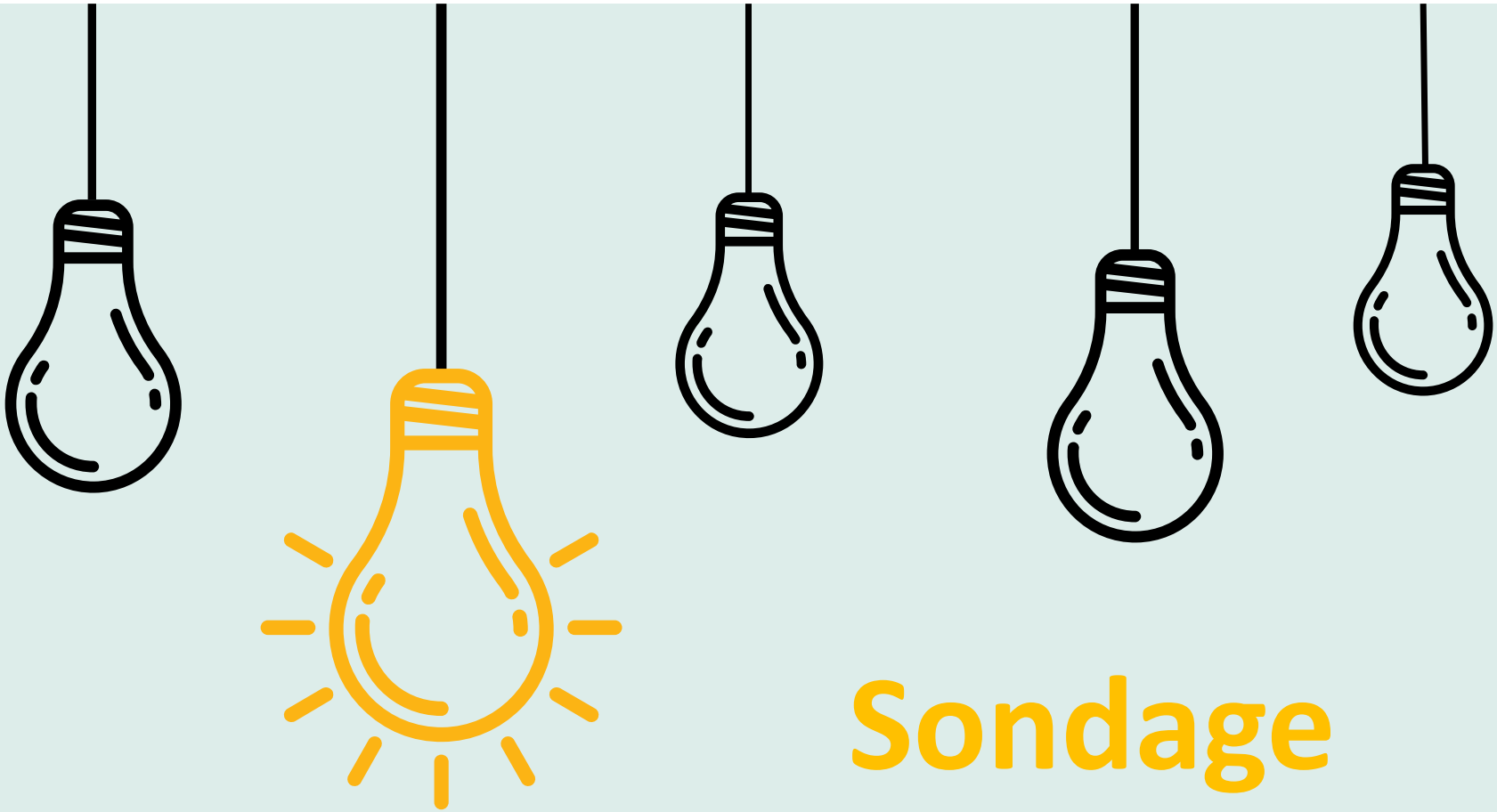
Menu de la séance

01 Cybercriminalité - constat et risques

02 Une institution cybersécurisée, le facteur humain

03 Réaliser son audit de sécurité : prévention et solution

04 Une cyberattaque, que faire ?



Sondage

1) Avez-vous déjà été victime d'une cyberattaque ?
2) Avez-vous une politique de cybersécurité dans votre institution ?

01 02 03 04

Cybercriminalité - constat et risques

Olivier BOGAERT

Commissaire de Police

Computer Crime Unit

Police Fédérale

Le web 1.0

- ✓ L’internet de 1re génération
- ✓ Contenus (texte/image/vidéo/son) sont produits et hébergés par une entreprise, propriétaire du site
- ✓ L'utilisateur n'est que lecteur de l'information

Le web 2.0

- ✓ Web participatif ou web collaboratif
- ✓ Les contenus (texte/image/vidéo/son) sont produits et réalisés par les internautes
- ✓ Utilisation intense des réseaux sociaux
- ✓ Sans connaissance en informatique, l'utilisateur va déposer le contenu grâce à des solutions technologiques simplifiées
- ✓ Ce contenu est hébergé sur le serveur du propriétaire du site

JAN 2020

BELGIUM

THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND THE STATE OF MOBILE, INTERNET, AND SOCIAL MEDIA USE

TOTAL POPULATION	MOBILE PHONE CONNECTIONS	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS
11.56 MILLION	10.81 MILLION	10.41 MILLION	7.50 MILLION
URBANISATION: 98%	vs. POPULATION: 93%	PENETRATION: 90%	PENETRATION: 65%

17

SOURCES: POPULATION: UNITED NATIONS; MOBILE: GSMA INTELLIGENCE; INTERNET: ITU; GLOBALWEBINDEX; GSMA INTELLIGENCE; EUROSTAT; LOCAL TELECOMS REGULATORY AUTHORITIES AND GOVERNMENT BODIES; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; APJII; KEPIOS ANALYSIS; SOCIAL MEDIA: PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; COMPANY ANNOUNCEMENTS AND EARNINGS REPORTS; CAFEBAZAAR. ALL LATEST AVAILABLE DATA IN JANUARY 2020. ◈ COMPARABILITY ADVISORY: SOURCE AND BASE CHANGES.

we are social

Hootsuite

Que cherchent les criminels du net ?

- Faire de l'argent en jouant de :
  - la récolte d'informations
  - la force de la conviction
- L'argent ?
  - soit en revendant des données
  - soit via l'escroquerie ou l'extorsion

Leurs méthodes

- Utiliser une identité : faux profil ou profil volé
- Nuire à la réputation de la structure
- Fraudes & escroqueries :
  - ✓ Arnaque via l'interception de données
  - ✓ Arnaque via des logiciels malveillants

RECUPERATION DE DONNEES

- Les pirates accèdent aux bases de données
- Ils modifient le numéro de compte bénéficiaire
- Dans certains cas, ils vont modifier des coordonnées de l'émetteur de la facture
- Ils deviennent les interlocuteurs en cas de doute
- Exemple : si la structure visée est locataire de ses locaux, ils peuvent, par exemple, se présenter comme les nouveaux propriétaires et justifient ainsi un nouveau numéro de compte

Autre infection : le cheval de Troie

- Utilisation de la capacité du système
  → distribution de spam
- Installation de spyware (logiciels espions)
- Espionnage ⇒ données financières/mots de passe
  → keylogging
- Attaques massives sur les serveurs ou nœuds du réseau
- Objectifs : ralentir, bloquer ou récupérer des infos

Fraude au logiciel malveillant

- Ransomware ou rançongiciel
- L'escroc contacte un membre de l'entreprise par mail
- Le mail cible le destinataire tenant compte de sa fonction
- Objectif : susciter son intérêt et le faire cliquer sur une pièce jointe ou un lien
- Pièce ou lien qui vont installer le logiciel malveillant qui va crypter toutes les données
- Un compte à rebours et le chantage commence

- Le phishing, un de leurs outils favoris
- Un mail qui contient un lien qui pointe sur de faux sites dans lesquels les données d'identité sont demandées
- Les sites frauduleux peuvent aussi contenir et pousser les logiciels malveillants

ETUDE RECENTE

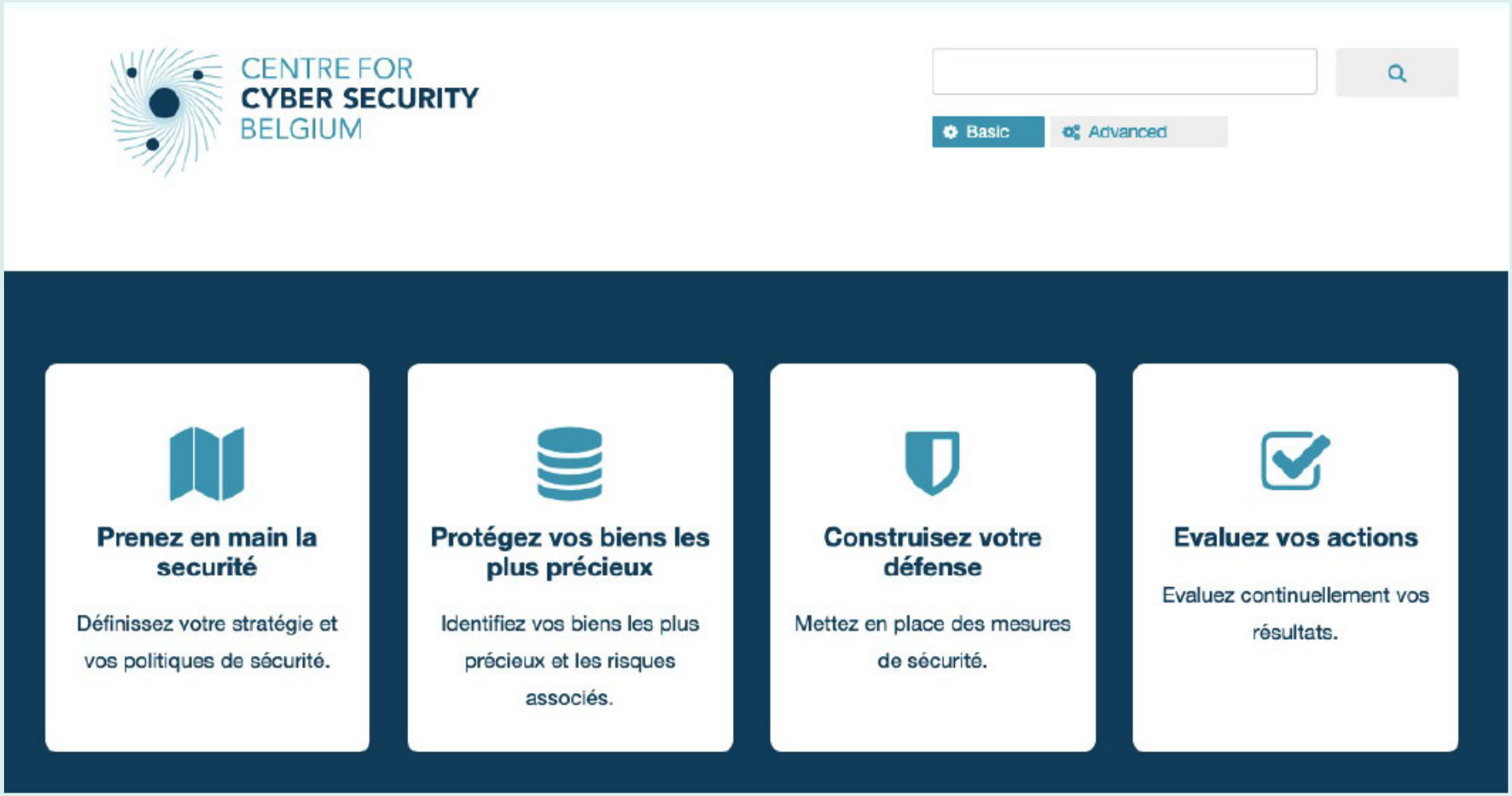
- 83 % des utilisateurs IT reconnaissent avoir passé plus de temps sur leur poste en 2020, mais seule la moitié d'entre eux a pris des mesures supplémentaires de protection
- 33 % admettent ne déployer les correctifs disponibles qu'au moins une semaine après en avoir eu connaissance
- 90 % des utilisateurs IT déclarent effectuer des sauvegardes, pourtant ils sont 73 % à déplorer au moins une perte irrémédiable de données, ce qui laisse penser qu'ils ne savent pas sauvegarder ou restaurer correctement

Bonnes pratiques

- Fixer et appliquer strictement des règles de sécurité et des procédures pour les paiements
- Sécurisation de l'environnement informatique : système et antivirus à jour, Wi-Fi bien protégé, ...
- Confidentialité quant à la structure de l'entreprise et son organisation

Bonnes pratiques

- Vérifier :
  - l'identité de l'interlocuteur,
  - l'origine des appels et des mails et, dans le doute, les adresses IP
- Contacter le donneur d'ordre via un autre moyen
- Idem pour un fournisseur si annonce de changement des coordonnées
- Prévoir un membre du personnel comme référent


CENTRE FOR
CYBER SECURITY
BELGIUM
Basic
Advanced
Prenez en main la securité
Définissez votre stratégie et vos politiques de sécurité.
Protégez vos biens les plus précieux
Identifiez vos biens les plus précieux et les risques associés.
Construisez votre défense
Mettez en place des mesures de sécurité.
Evaluez vos actions
Evaluez continuellement vos résultats.

01 02 03 04

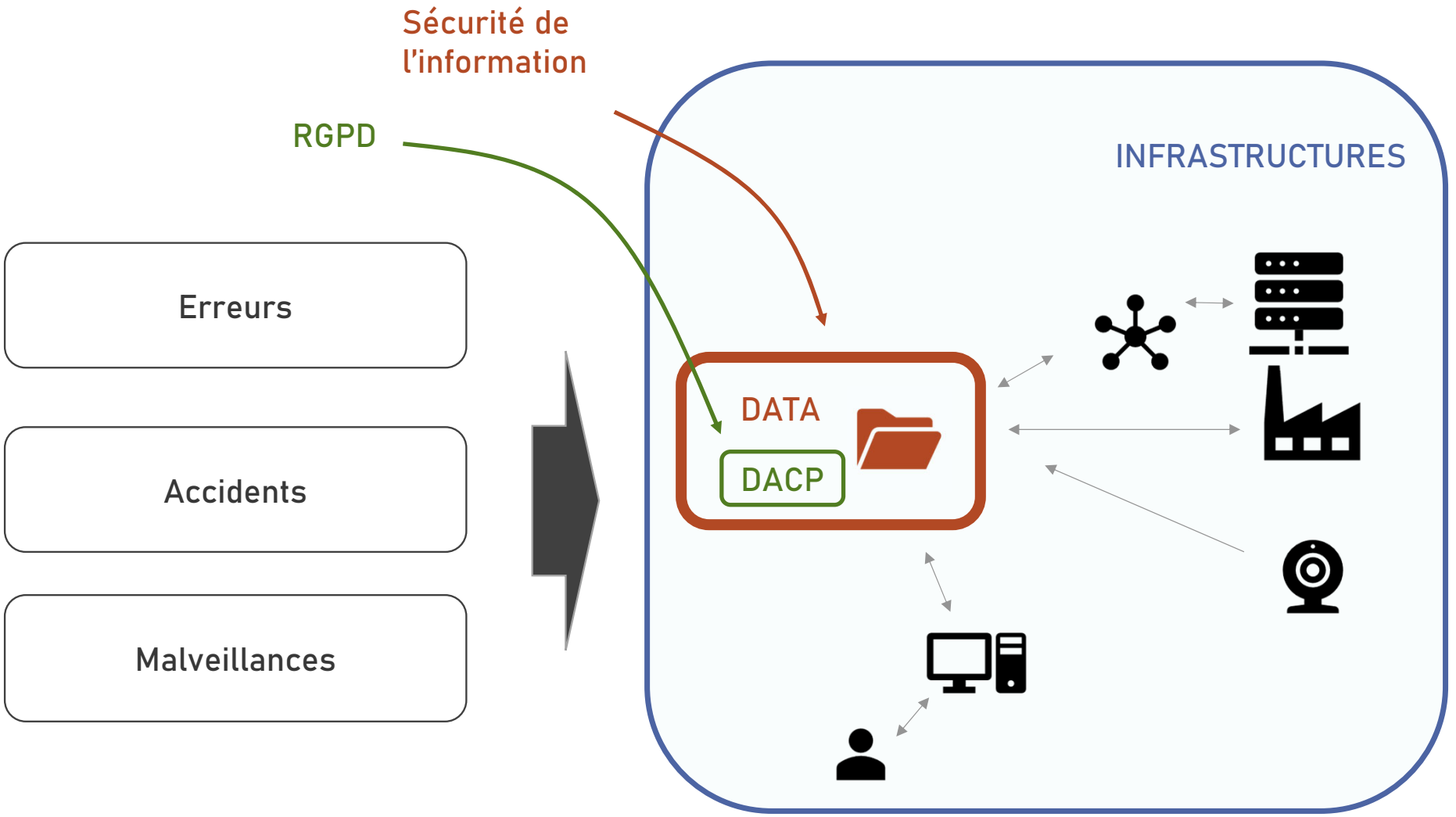
Une institution cybersécurisée, le facteur humain

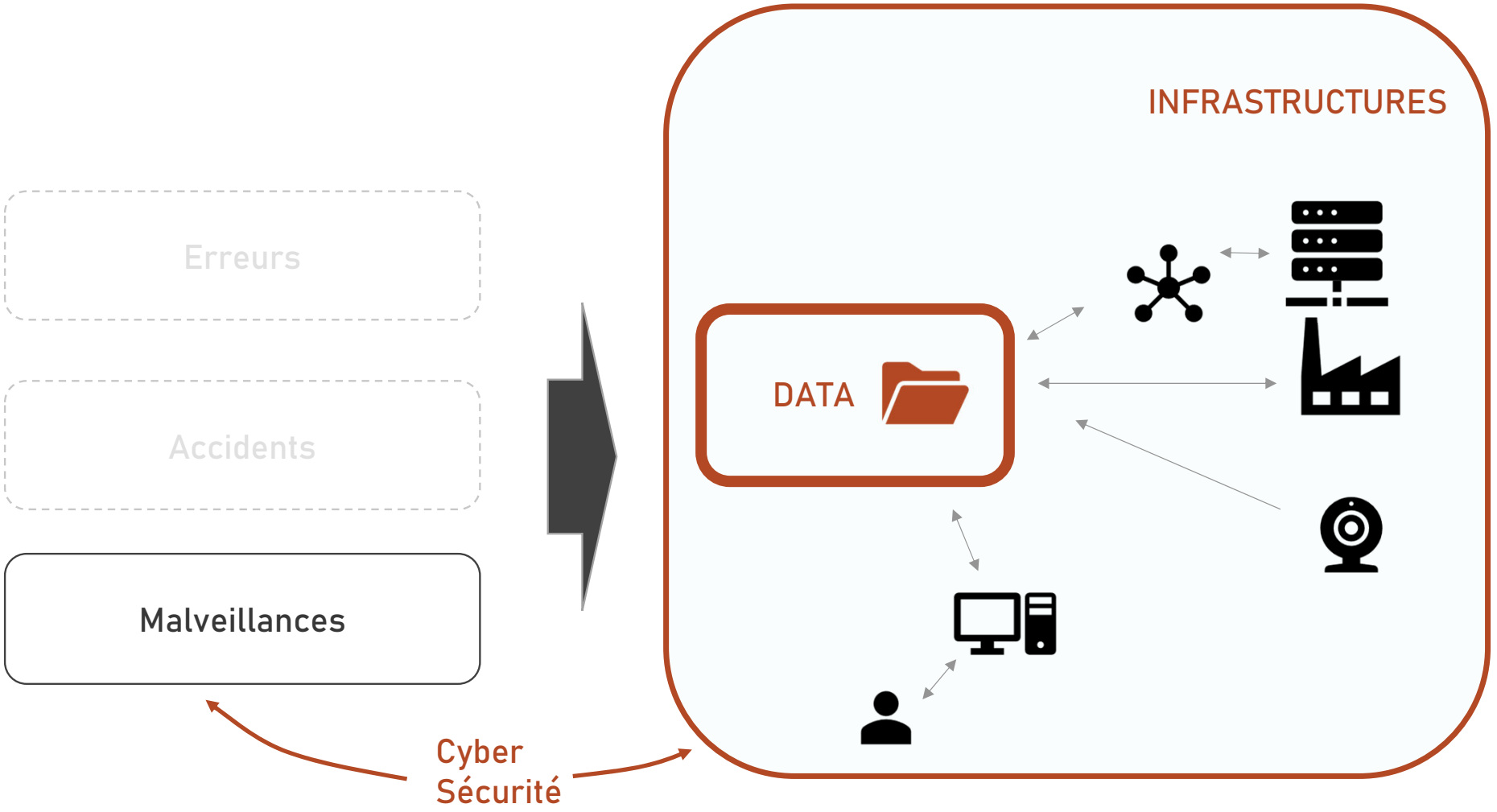
Dominique GREGOIRE

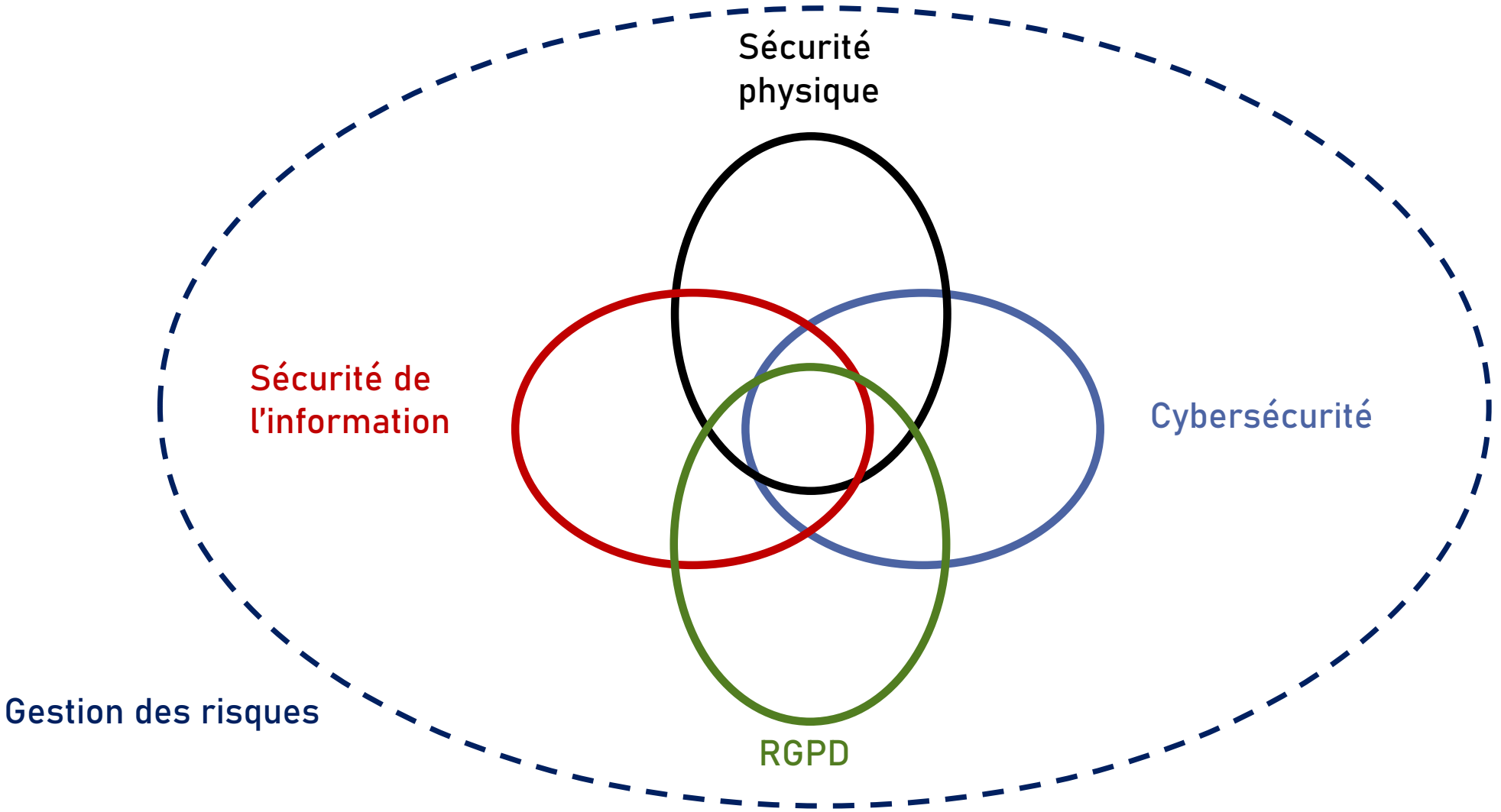
Conseiller en sécurité de l'information

Président du Groupe de travail sur la sécurité de l'information (GTSI)

Sécurité de l'information, Protection des données RGPD ou Cybersécurité ?


Sécurité de
l'information
RGPD
Erreurs
Accidents
Malveillances
INFRASTRUCTURES
DATA
DACP


Erreurs
Accidents
Malveillances
INFRASTRUCTURES
DATA
Cyber
Sécurité

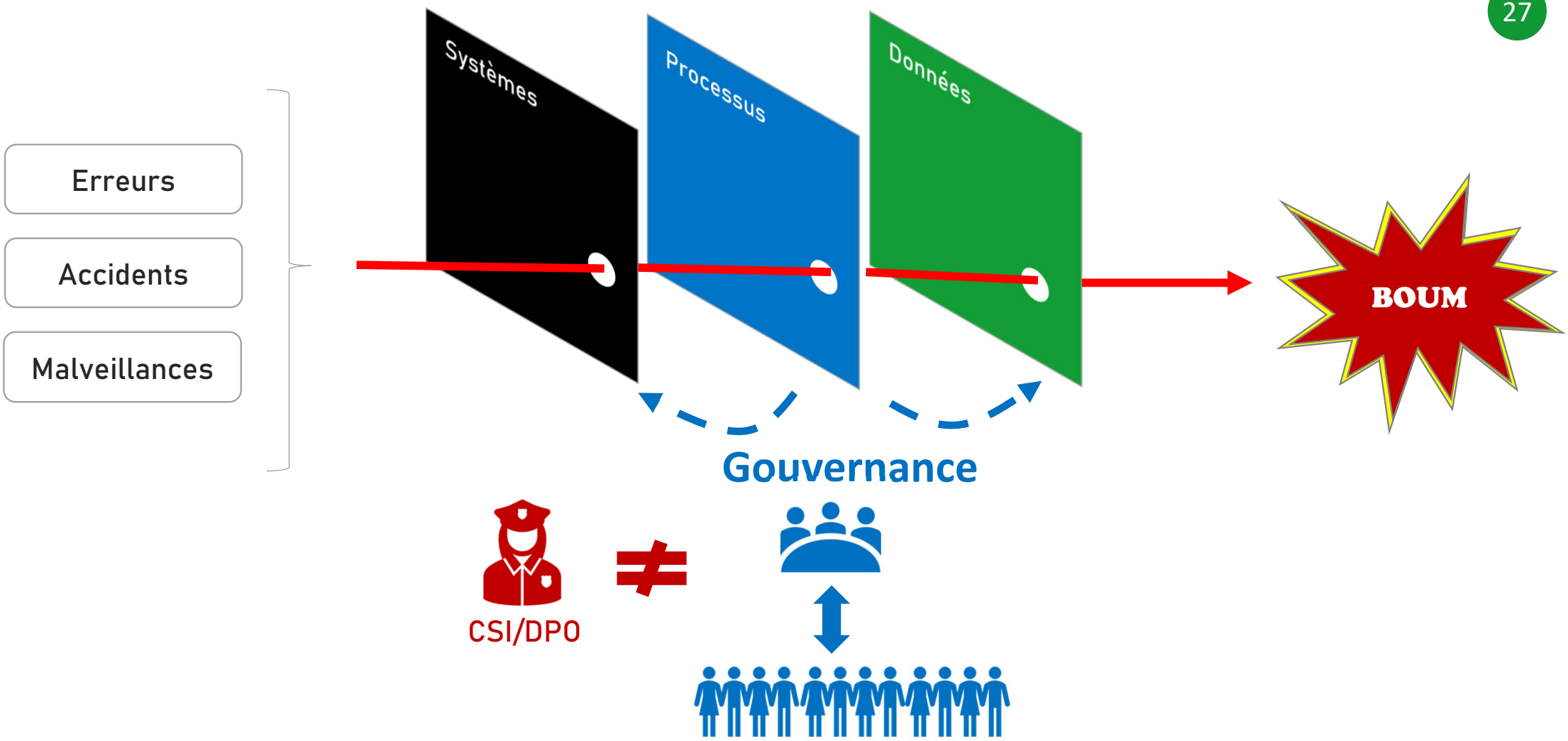

Sécurité
physique
Sécurité de
l'information
Cybersécurité
RGPD
Gestion des risques

L'objectif : ça ?

©blog.airbagsolutions.com

… ou ça ?

©Huyndai


Erreurs
Accidents
Malveillances
Systèmes
Processus
Données
BOUM
Gouvernance
CSI/DPO

Niveau à atteindre ?

La théorie…

…le challenge…

…la pratique…

…le pragmatisme ?

Maturité de l'organisation

1
Niveau initial

2
Reproductible

3
Défini

4
Géré

5
Optimisé

(Niveaux CMMI)

Quelques constats

“On ne me donne aucune ressource !”

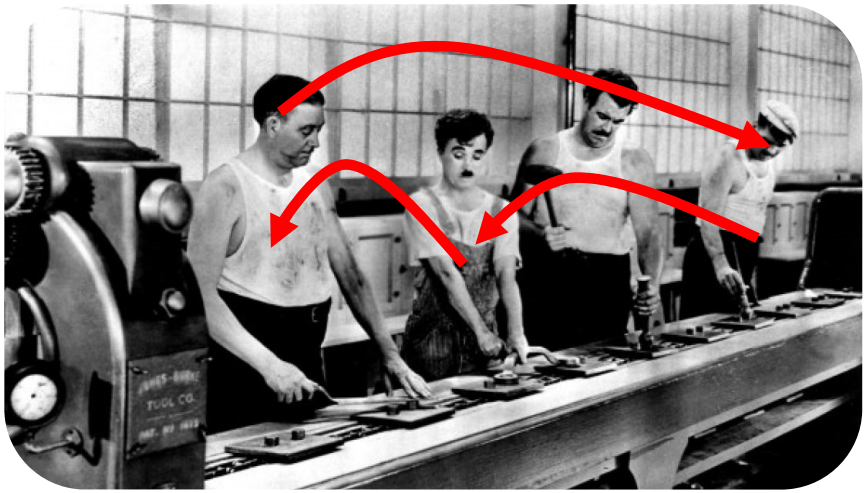
“ La cybersécurité est un boulet ! ”

“Personne ne m’écoute !”

“Tout le monde s’en f... !”

“Je fais tout le temps face à des oppositions !”

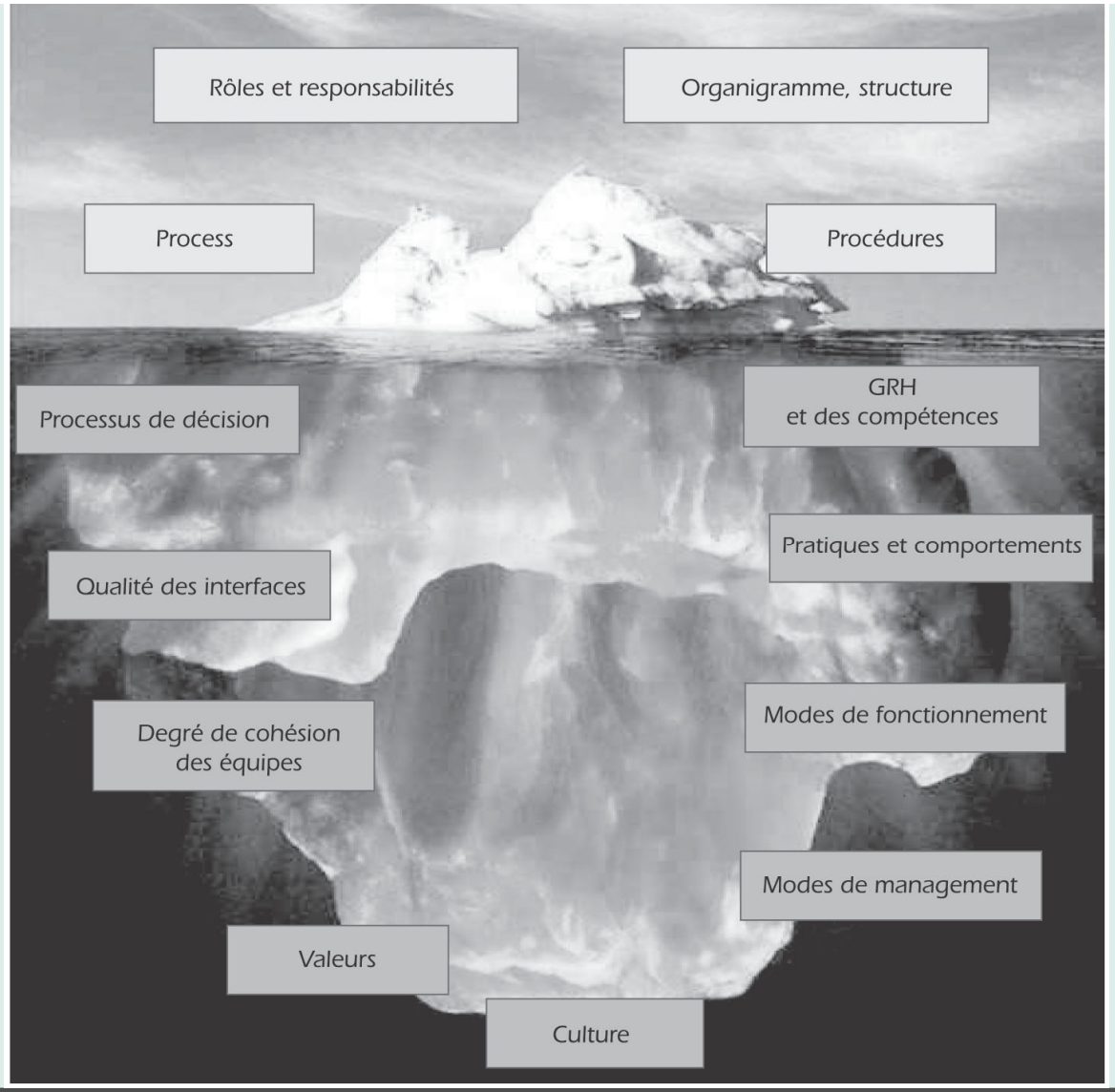
Amener du changement



Réorganisation

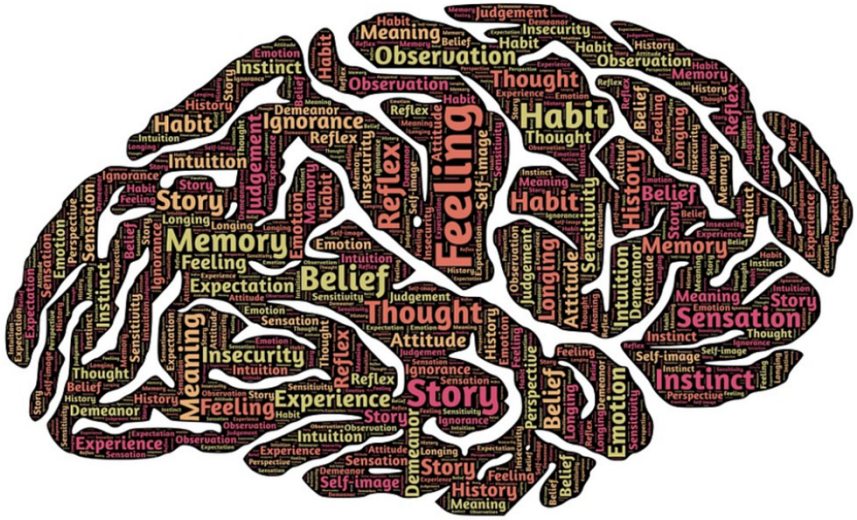
« YAKA - YFOKE »

Transformation

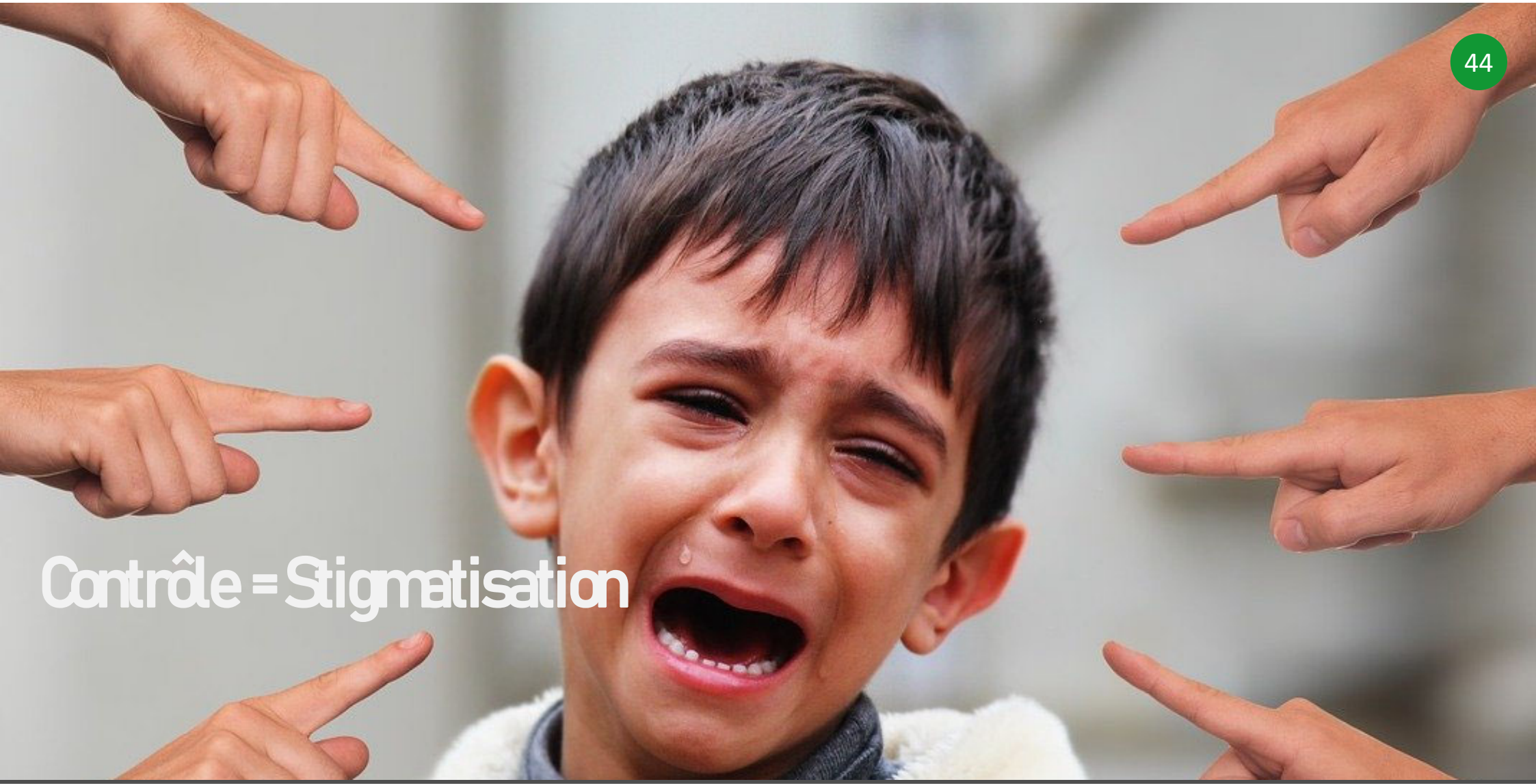


Srce: A. Tonnelé – Equipes autonomes

Réorganisation

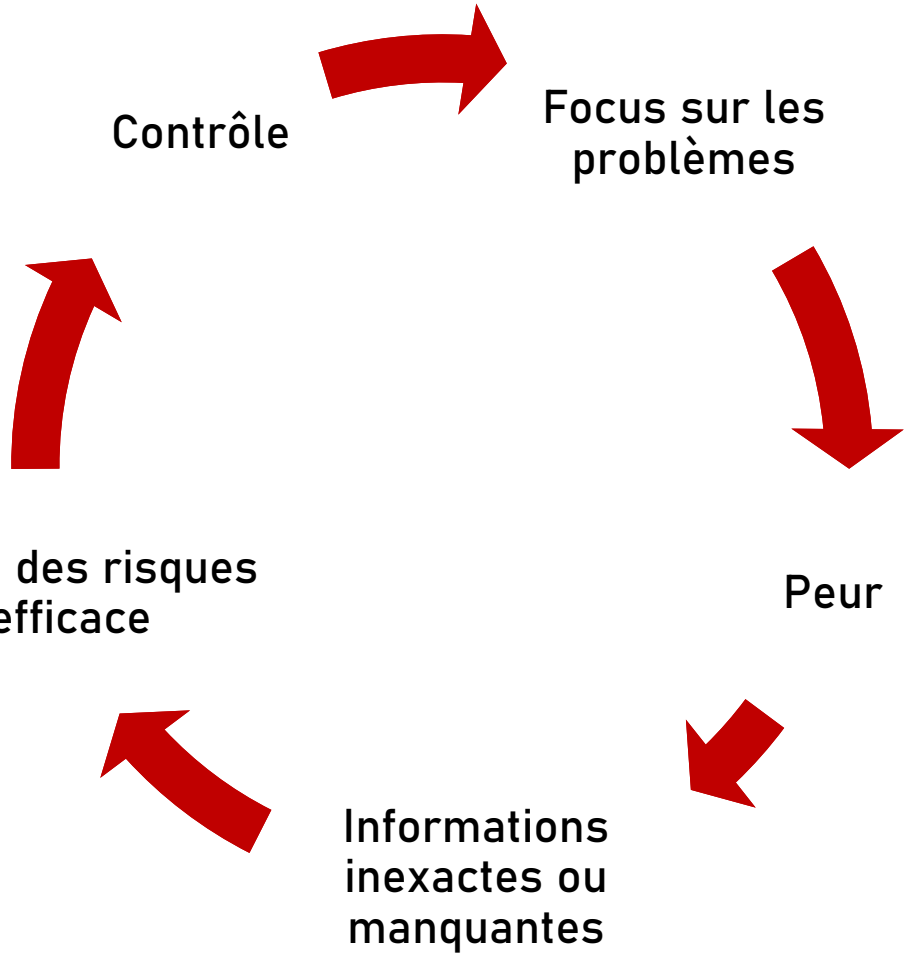


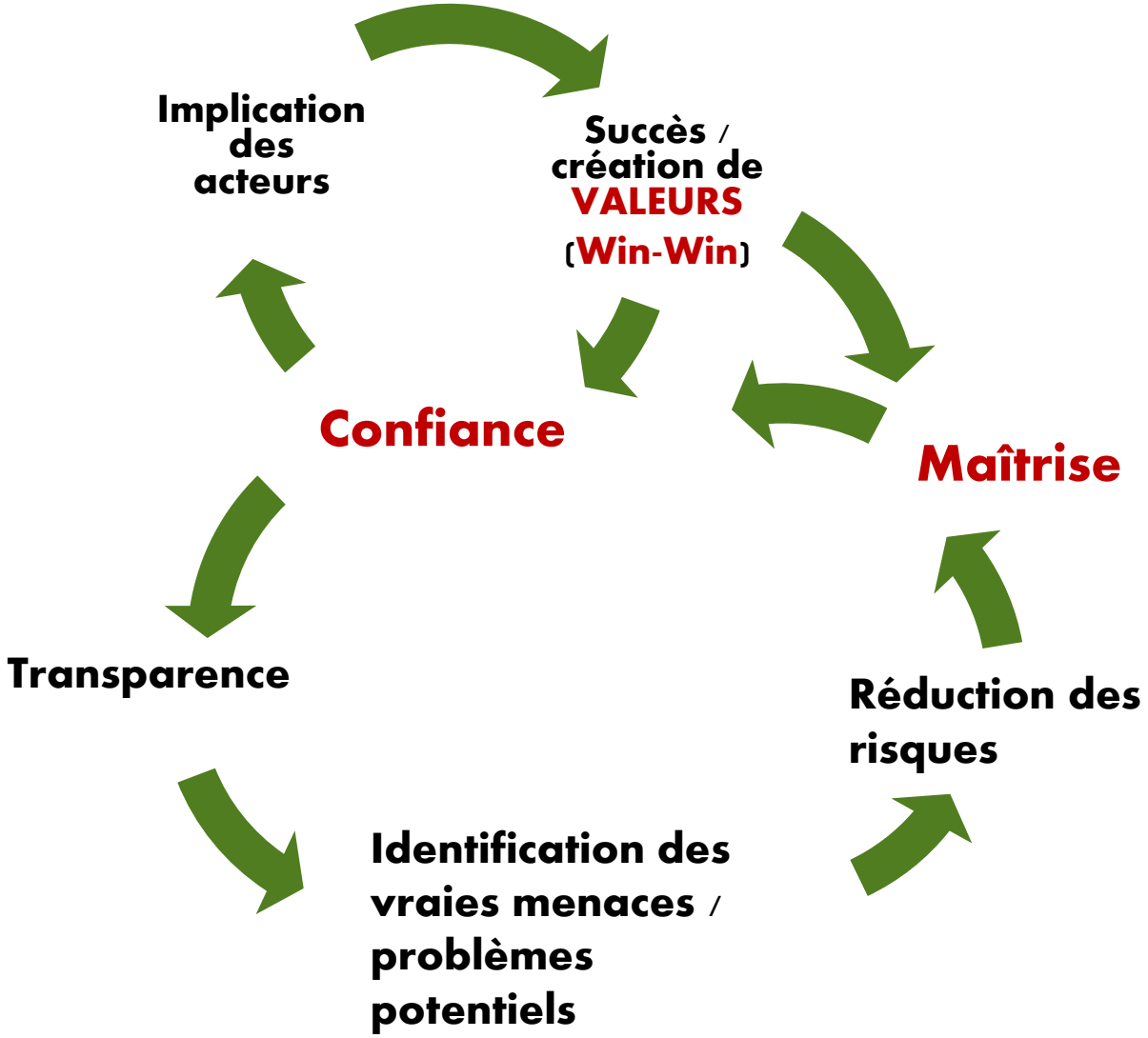
Transformation


Contrôle = Stigmatisation


CSI/DPO
Euh... OUI CHEF...
Cours toujours...

Procure une illusion de maîtrise (dans les organisations peu matures)

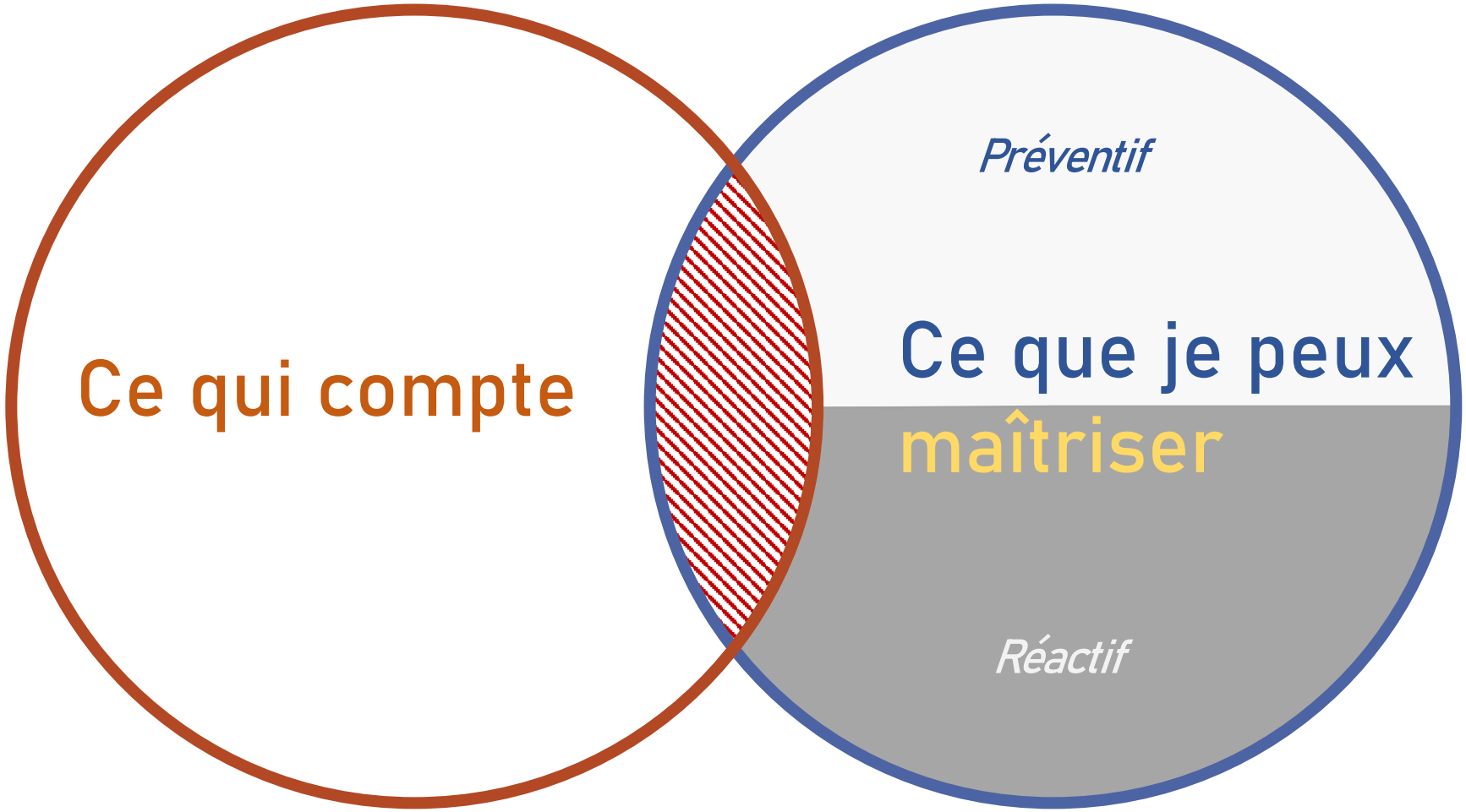



Implication des acteurs
Succès / création de VALEURS (Win-Win)
Confiance
Maîtrise
Transparence
Réduction des risques
Identification des vraies menaces / problèmes potentiels

Exemples de valeurs

- **Gouvernance des données :**
  - Qualité des données ⇒ meilleurs services aux citoyens/clients
  - Protection des données ⇒ protection des droits et libertés
- **Agilité :**
  - Mieux répondre aux enjeux sociétaux du moment
  - Efficience
  - Compétitivité % au privé
- **Image**


C’est toujours chouette avec vous, parce que vous venez toujours avec des solutions !


Ce qui compte
Préventif
Ce que je peux
maîtriser
Réactif

Erreurs

Accidents

Malveillances

Cybercriminalité organisée

Terrorisme

Structures spécialisées

Sûreté de l'État / Armée / Police

Ne nécessite pas moins d'expertise

Cyber Terrorisme

Sûreté de l'État / Armée / Police

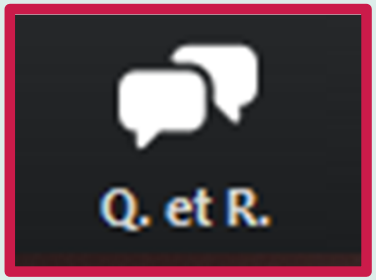
Responsables de traitement

SOC Wallon ?

CSIRT Wallon ?

Gestes barrières. Le reste est une affaire de spécialistes

Nous répondons à vos questions !



01 02 03 04

Réaliser son audit de sécurité : prévention et solution

Christophe TOURMENT

Ingénieur système en infrastructure IT et

responsable de la cellule de consultance

iMio

Pourquoi réaliser son audit de sécurité informatique ?

- Comprendre et avoir une vue exhaustive des forces et des faiblesses de la sécurité d'un SI à un instant T
- Faire appel à un expert en sécurité informatique appelé « auditeur » est la meilleure solution

Il est possible de réaliser soi-même son audit en appliquant une méthodologie définie par les experts

- Auditer son infrastructure informatique permet de remédier aux brèches pouvant engendrer une intrusion informatique
- Définir le périmètre du SI et concevoir un référentiel informatique
  - Une cartographie du parc informatique et du réseau
  - Une documentation du fonctionnement des outils développés en interne
  - Un règlement propre à l'entreprise

Comment réaliser un audit de sécurité informatique ?

- Comprendre l'utilisation de l'outil informatique dans l'entreprise grâce à l'interview du personnel
- Tests d'intrusions et de la recherche de vulnérabilités
  - Test de pénétration dit « black box » ou boîte noire
  - Test de pénétration dit « grey box » ou boîte grise
  - Test de pénétration dit « white box », « crystal box » ou boîte blanche
- Préconisations et conseils
  - Accompagnement à la mise en œuvre de ces recommandations

Comment se protéger ? Prendre des mesures préventives simples mais efficaces

- Mettre à jour votre système d'exploitation et vos logiciels, dès que cela est nécessaire
- Former et informer les utilisateurs
- Choisir des mots de passe efficaces
- Sauvegarder régulièrement ses fichiers
- Chiffrer ses données, conversations ou les envois de fichiers importants
- Banaliser les appareils nomades

Quelles sont les solutions pour me protéger ?

Il faut bien comprendre que le risque zéro n'existe pas. Il faut alors :

- se prémunir d'un firewall avec un IPS ou IDS intégrer ou séparer
- avoir un logiciel antivirus moderne
- posséder un portefeuille de mot de passe
- opter pour une stratégie de back-up préventive
- utiliser un logiciel de cryptage
- mettre en place d'un règlement d'accès au SI

Cas pratique chez iMio

Il y a 2 ans, iMio a subit une attaque de ransomware sur deux de ses applications, IA.Tech et IA.Gpec

- IA.Tech : application des services techniques
- IA.Gpec : application des ressources humaines.

Grâce à l'application des règles citées précédemment, le drame a pu être évité.

En effet, 20 minutes après la détection de l'inaccessibilité des deux instances, les utilisateurs de ces deux communes ont pu retravailler.

- La perte des données pour le client IA.Tech s'est élevée à 4h de travail, ce qui représente 17 interventions à réencoder sur 12.849 contenues dans la base de données.

Nous répondons à vos questions !

01 02 03 04

Une cyberattaque, que faire ?

Olivier BOGAERT

Commissaire de Police

Computer Crime Unit

Police Fédérale

Exemples récents

- Plusieurs structures hospitalières visées ces derniers mois
- Avec, notamment, des serveurs bloqués par cryptage
- Mais aussi, communications rendues impossible entre services et membres du personnel
- Hypothèse : le logiciel malveillant qui a pu rentrer suite à un mail reçu contenant une pièce jointe

L’utilisateur peut être un détecteur

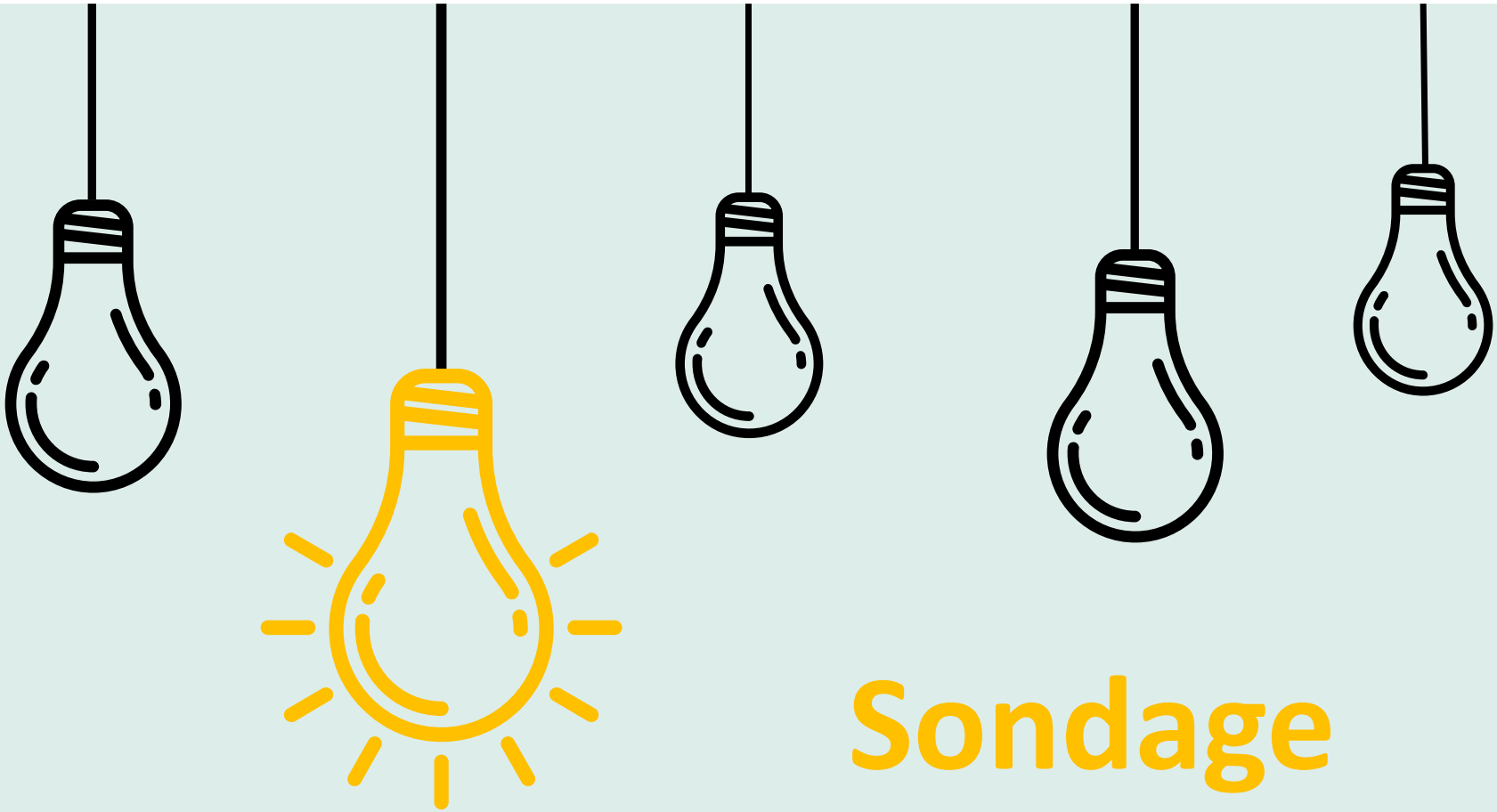
- Des fichiers de son ordinateur ont disparu
- Problème de connexion vers sa machine ou vers les serveurs de sa structure
- Le système de fichiers est endommagé
- Il y a eu des modifications de mots de passe
- En regardant l’historique, il y a des connexions ou des activités inhabituelles depuis la machine
- Il y a la création ou la destruction de compte
- Des fichiers ont été créés mais ce n’est pas lui

UNE ATTAQUE ?

- Déconnecter la machine du réseau, sans l'éteindre
- Cela permet de conserver les traces de la cyberattaque et notamment les processus qui étaient actifs au moment de l'intrusion
- Prévenir la hiérarchie et le responsable sécurité
- Faire une copie physique du disque
- La copie aura toute son importance si vous décidez de lancer une procédure judiciaire. Elle servira à montrer l'état du système au moment de la découverte de l'intrusion

UNE ATTAQUE ?

- Rechercher les traces disponibles sur l'ensemble du réseau
- Lorsqu'un système est attaqué, les traces laissées par les pirates ne le sont pas que sur la machine de l'utilisateur. Un pirate laisse également des traces sur l'ensemble des équipements du réseau : firewall, routeurs…
- Ne pas rentrer en contact directement avec le pirate
- Entrer en contact avec le pirate est inutile car cela peut lui fournir des informations qui pourront l'aider
- Dépôt de la plainte à la CCU de votre arrondissement



Sondage

Qu’avez-vous pensé de ce webinaire ?

En conclusion et…

pour aller plus loin

Formation UVCW
Comment mener une analyse d'impact ?
(1 jour)
https://www.uvcw.be/formations/1971

Réseau des informaticiens communaux (RIC)
La maîtrise de son informatique, au sein d'un pouvoir local
http://www.ric.be/public/maitrise/view

Nos webinaires en replay
Vers des sites internet communaux accessibles à tous, Budget participatif, …
http://uvcw.be/espaces/formations/922.cfm

Votre espace eCampus
Procédure de connexion :
https://vimeo.com/518713611/f3c95176c9

Espace "E-gov, TIC et simplification administrative" - Site UVCW
https://www.uvcw.be/e-gov/accueil

Merci pour votre participation !

Nous revenons vers vous pour…

- Vous permettre de revoir le webinaire

À bientôt !