KUDELSKI SECURITY

SÉCURITÉ DES DONNÉES
CYBER VIGILANCE
DANS UN MONDE DIGITAL

Pascal Métral, VP Public Sector
pascal.metral@nagra.com
Nicolas Moniez, Sr. Security Engineer

AGENDA

- Introduction sur le Groupe Kudelski et Kudelski Security
- La sécurité des données
- Quelques questions à se poser (tests de sécurité et security awarness)
- Quelques solutions de Kudelski Security
- Conclusion

LE GROUPE KUDELSKI & KUDELSKI SECURITY

LE GROUPE KUDELSKI : UN TIERS DE CONFIANCE

NAGRA KUDELSKI

SÉCURITÉ
NUMERIQUE

KUDELSKI SECURITY

CYBER
SÉCURITÉ

SKIDATA
KUDELSKI GROUP

SÉCURITÉ
DES ACCÈS

- > 60 ans d'innovation technologique (depuis 1951)
- Groupe Suisse, Familial, (KUD: SIX Swiss EX)
- CHF 900M de CA, et CHF 200M+ de R&D par an
- 4'000+ brevets et des accords avec Cisco, Google, Netflix, etc.
- 3'000+ employés répartis sur 23 pays.
- Leader mondial de la sécurité numérique des médias
- Lancement en 2012 des activités cyber sécurité, sur la base de l'expérience acquise dans le domaine de la télévision numérique

LE GROUPE KUDELSKI AU TRAVERS LE MONDE

Basé en Suisse et opérant sur les cinq continents

47

47 sites au travers le monde

27

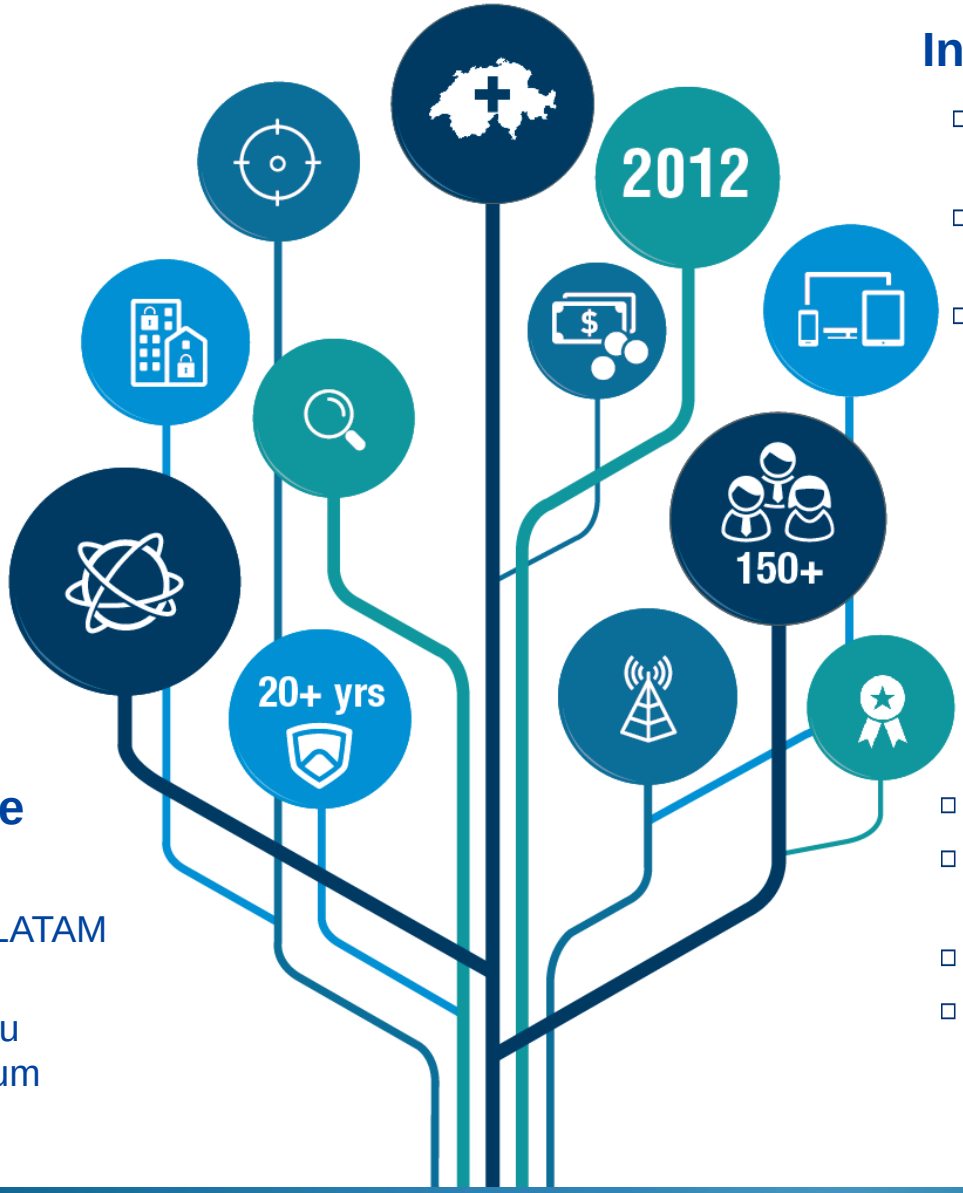
Operations dans 27 pays

■ Bureaux et centres de R&D

KUDELSKI SECURITY EN QUELQUES MOTS

4 verticales

- Services financiers
- Secteur public
- Défense
- Media & Telecom



Innovation en sécurité

- Division cybersecurité du groupe Kudelski
- Actif en sécurité digitale depuis plus de 20 ans
- Solution sur-mesure de cybersecurité

Indépendant et présence globale

- Basé en Suisse
- Présent en France, LATAM (Brésil), Inde, USA
- Partner stratégique du World Economic Forum

Eléments clés

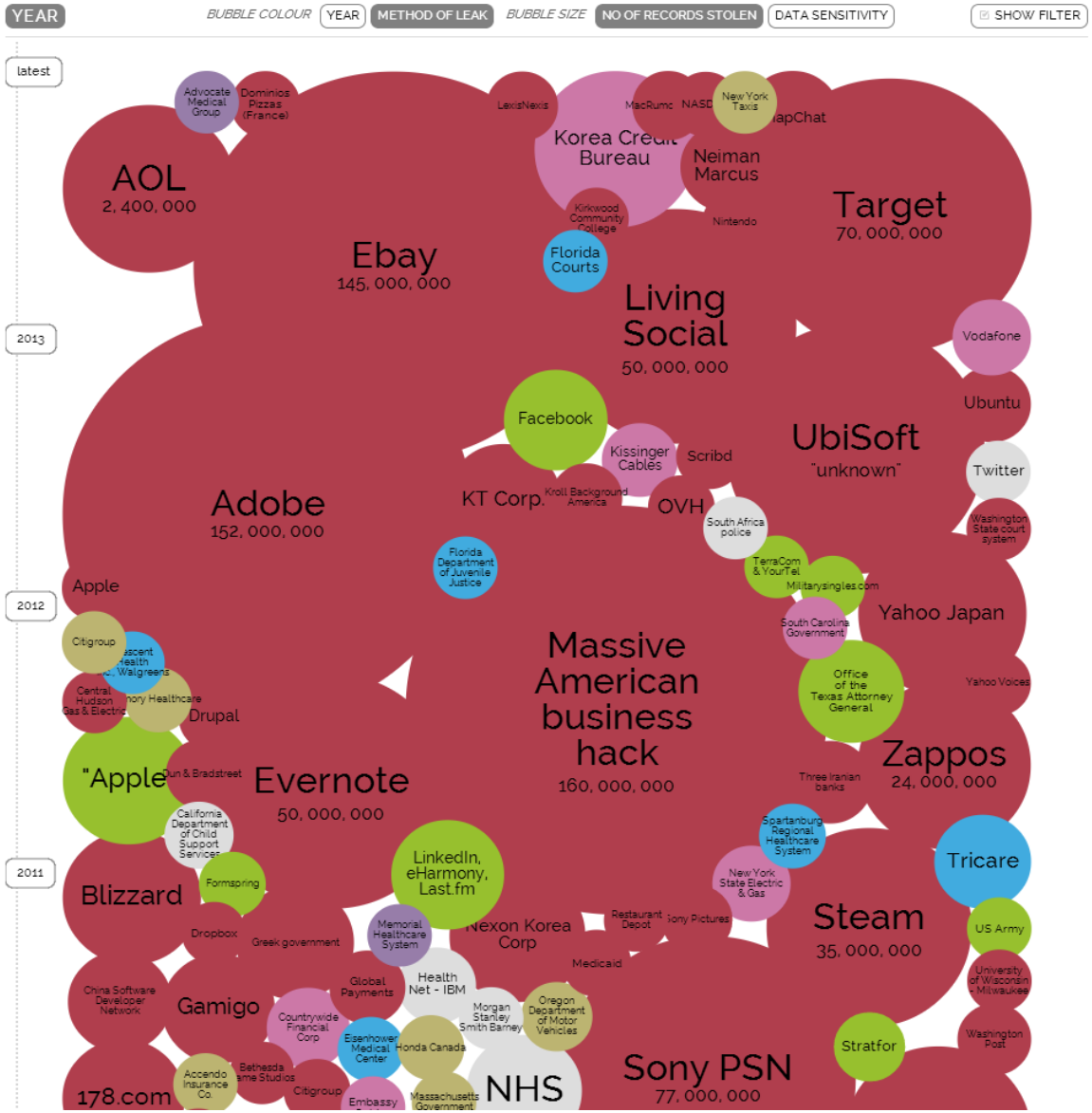
- Créé en novembre 2012
- 150+ professionnels en sécurité
- Certifié ISO 27001:2013
- Plus grand acteur suisse en cybersécurité

LA SÉCURITÉ DES DONNÉES

LA PROBLÉMATIQUE

KUDELSKI SECURITY

PLUS GROS CAS DE VOLS DE DONNÉES



METHODOLOGIES

- **All**
- **Accidentally published**
- **Hacked**
- **Inside job**
- **Lost / stolen computer**
- **Lost / stolen media**
- **Poor security**

Source: www.informationisbeautiful.net – July 14

3 TYPES DE MENACES

CRIMINELLE

- Information pour revente
- Personne à faire chanter
- Resource pour une attaque plus large

SPONSORISEE PAR UN ETAT

- Information à utiliser contre la cible
- Resource/équipement à contrôler

INTERNE

- Vengeance
- Profit

LA SÉCURITÉ DES DONNÉES

DEUX EXEMPLES CONCRETS

KUDELSKI SECURITY

VOL DE PROPRIÉTÉ INTELLECTUELLE

Vol du code source d'American Superconductor Inc. d'un logiciel liée à l'exploitation de l'énergie éolienne

→ Perte de **90% de la valeur de l'action**

s o u r c e : Michael A. Riley and Ashlee Vance, "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies," *Bloomberg Businessweek*, March 2013

VOL DE DONNÉES

Anthem Inc. medical data breach

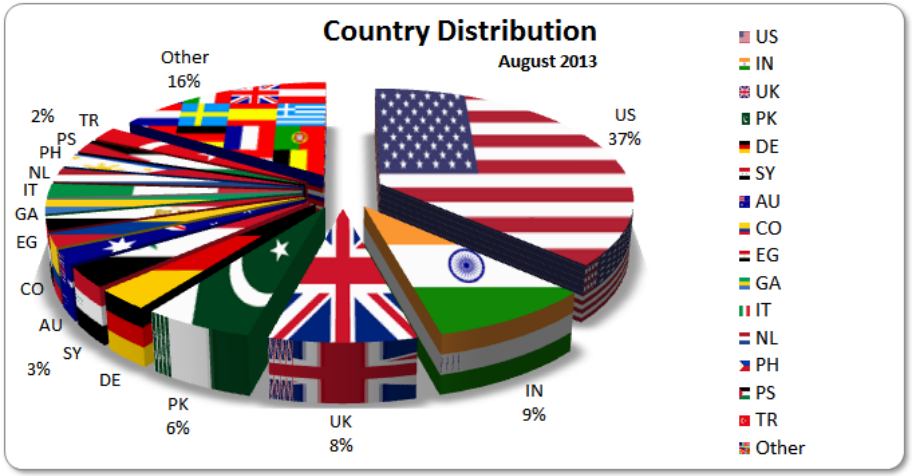
- 2ème plus grand assureur-maladie aux USA
- Vol de données personnelles afférentes à près de **80 millions d'assurés et membres du personnel**
- Noms, adresses, dates de naissance, données médicales, cartes de crédit, numéros de sécurité sociales, déclarations de revenus, informations professionnelles, etc.
- Les données volées seront vraisemblablement utilisées pour des attaques à venir
- **Les données n'étaient pas encryptées**…
- **Dommages pour Anthem? ……**
  - Un exemple concret: 80'000'000 x coût de remplacement d'une carte de crédit…

LA SÉCURITÉ DES DONNÉES

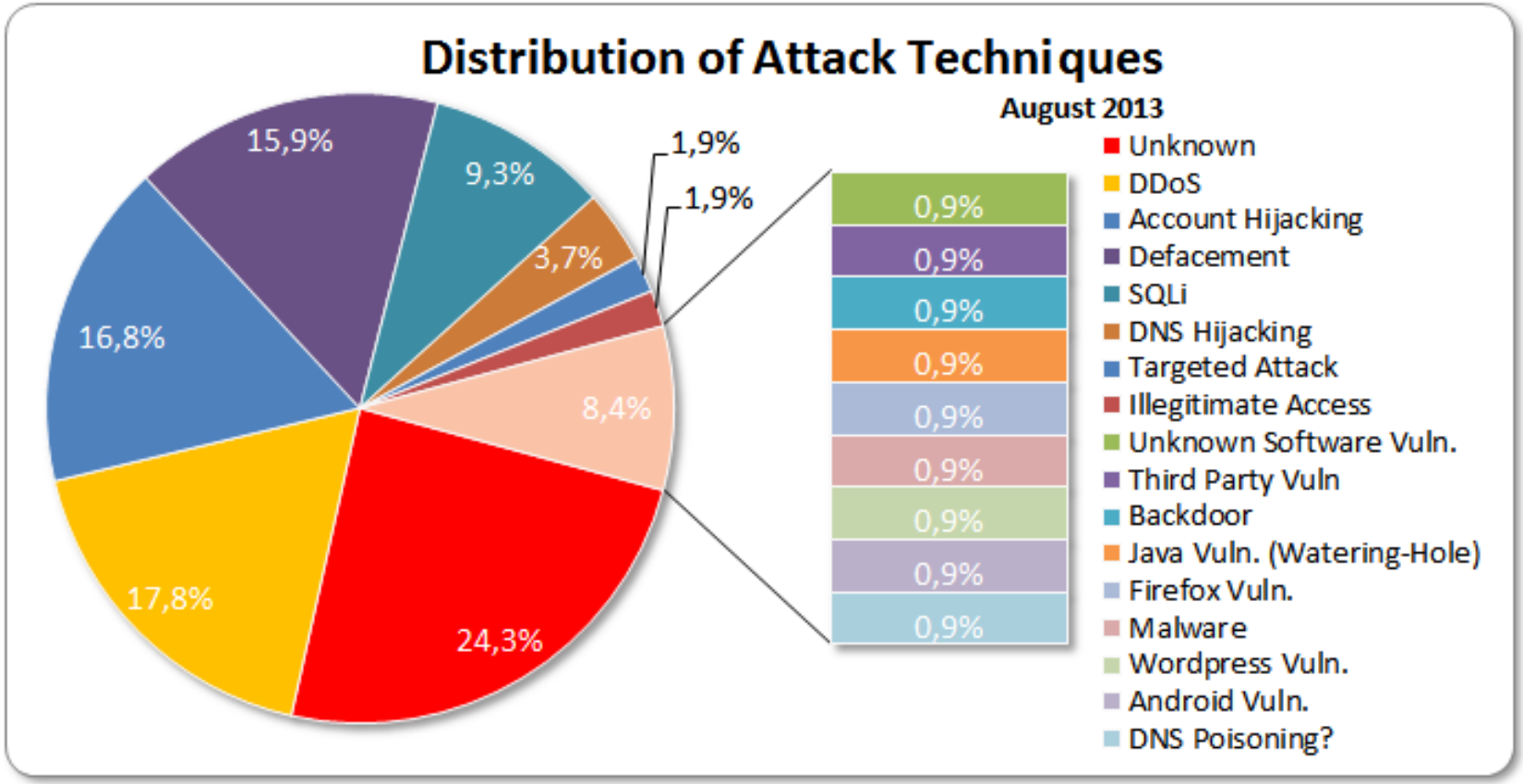
QUELQUES CHIFFRES

KUDELSKI SECURITY

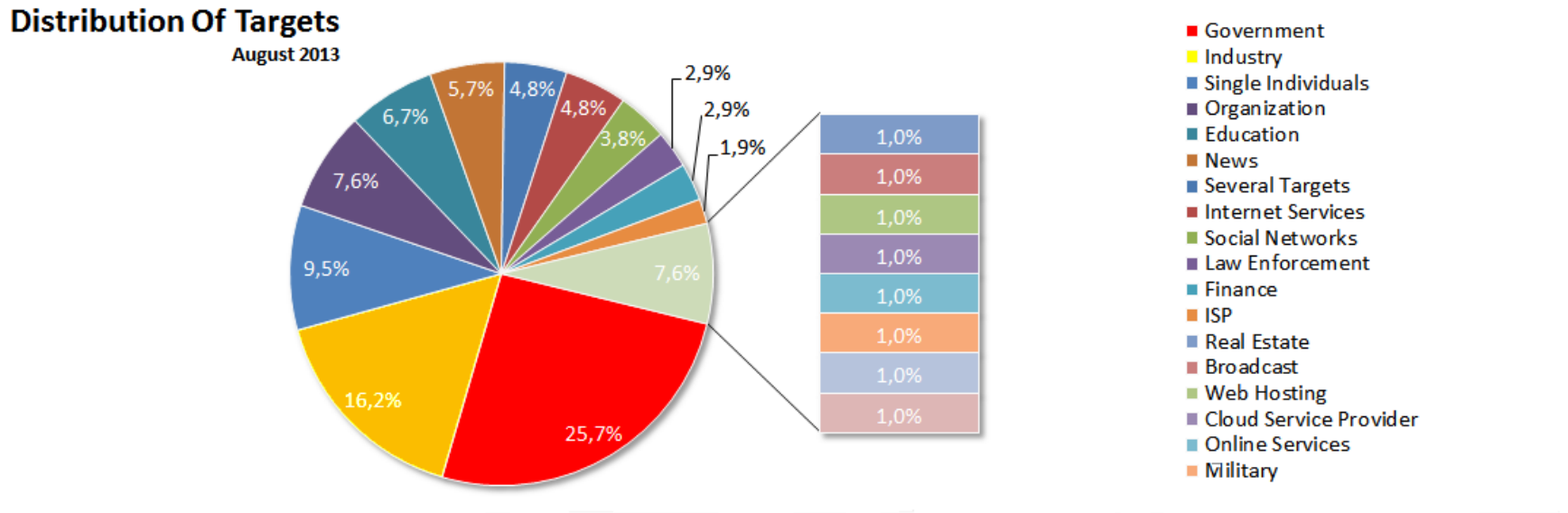
Les pays visés

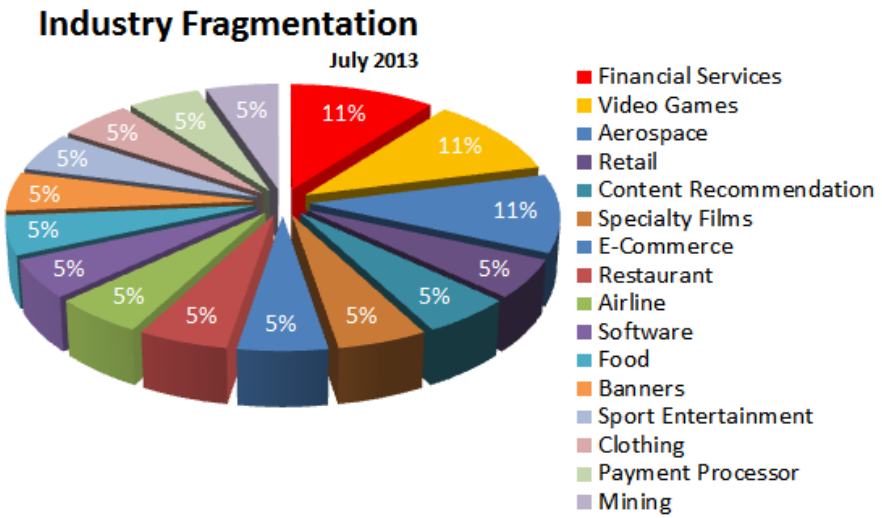


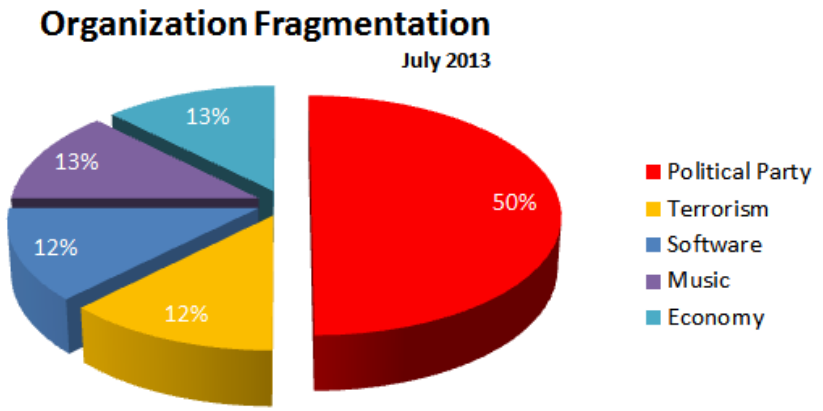
Les techniques d'attaque



LES CIBLES

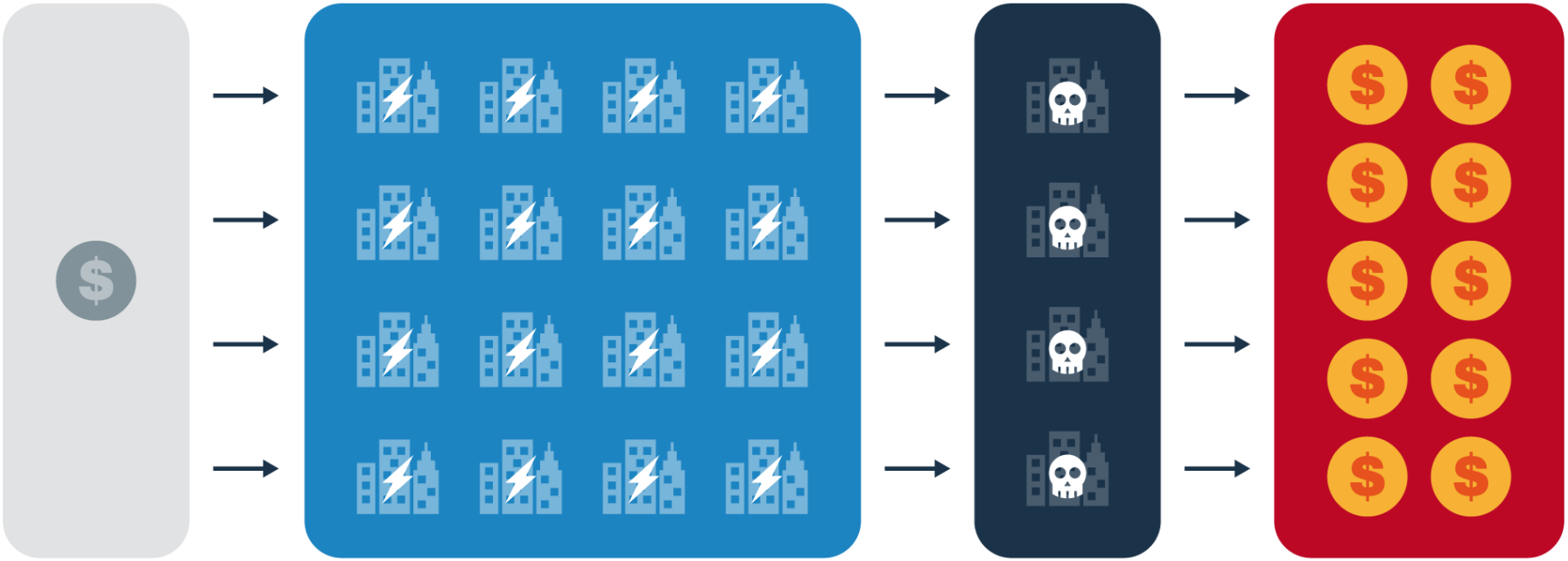






BILAN D'UNE ATTAQUE

DU POINT DE VUE DE L'ATTAQUANT



INVESTISSEMENT INITIAL	SOCIETES CIBLES	SOCIETES COMPROMISES	PRISE DE BENEFICES

$☠$ FORTEMENT POSITIF $☠$

KUDELSKI SECURITY

LES QUESTIONS A SE POSER

Suis-je à risque?	Ma sécurité est-elle compromise?	Suis-je prêt?	Ai-je été piraté?
Recherche de vulnérabilités	Evaluation de compromis	Revue de programme de sécurité	Service de réponse à incident
Test de pénétration avancés		Formation	
		Préparation à la gestion d'incident	
		Mise en place de service de gestion de la sécurité	

LA SÉCURITÉ DES DONNÉES

QUELQUES QUESTIONS A SE POSER (TESTS DE SÉCURITÉ ET SECURITY AWARNESS)

KUDELSKI SECURITY

LA SÉCURITÉ DES DONNÉES

TESTS DE SÉCURITÉ

KUDELSKI SECURITY

QU'EST-CE QU'UN TEST DE SÉCURITÉ...

… et quels en sont les avantages ?

KUDELSKI SECURITY

QU'EST-CE QU'UN TEST DE SÉCURITÉ ?

«Une tentative d'accès à des données confidentielles auxquelles nous n'aurions pas accès en temps normal» ***SANS Institute*** [1]

[1]: http://www.sans.org

QU'EST-CE QU'UN TEST DE SÉCURITÉ ?

Processus en 4 étapes:

- Reconnaissance
- Identification des vulnérabilités
- Exploitation
- Contre-mesures

POURQUOI EFFECTUER UN 'PENTEST‘ ?

POURQUOI LES ENTREPRISES SONT-ELLES INTÉRESSÉES ?

Raison n°1:

Un pentest est un exercice grandeur nature permettant de vérifier la réactivé et la résistance d'un réseau face à une attaque.

POURQUOI LES ENTREPRISES SONT-ELLES INTÉRESSÉES ?

Raison n°2:

Un pentest permet de traduire les risques techniques en risques métier.

POURQUOI LES ENTREPRISES SONT-ELLES INTÉRESSÉES ?

Raison no°3:

Le pentest se concentre uniquement sur la sécurité, qui est un domaine à part entière.

KUDELSKI SECURITY NETSOP...

*… **qui** sommes-nous, et **comment** pouvons-nous vous aider ?*

KUDELSKI SECURITY NETSOP

NetSOp effectue des tests de sécurité internes et également pour des clients externes.

Nos facteurs de réussite sont:

- **Un haut niveau éthique**
- **La diversité de nos profils**
- **La passion de la technologie et de la sécurité de l'information**
- **Une combinaison gagnante de motivation, de formations intensives, et d'outils performants.**

NOS SERVICES

- Analyse d'architectures réseaux
- Pentest réseaux
- Pentest Wifi
- Pentest Web
- Pentest de machines
- Pentest d'applications mobiles
- Forensics
- Social Engineering
- “Security Awarness”

LA SÉCURITÉ DES DONNÉES

SECURITY AWARNESS

KUDELSKI SECURITY

QU'EST-CE QUE LE « SECURITY AWARNESS » ...

FORMATION « SECURITY AWARNESS » – EN RÉSUMÉ

- Formation donnée par 2 experts en sécurité
- Formation tout public d'une demi-journée
- Personnalisable en fonction de la demande
- Aborde les sujets principaux de la sécurité
- Explique le déroulement d'attaques
- Explique comment réagir
- Donne des moyens pour se protéger

LA SÉCURITÉ DES DONNÉES

QUELQUES SOLUTIONS

KUDELSKI SECURITY

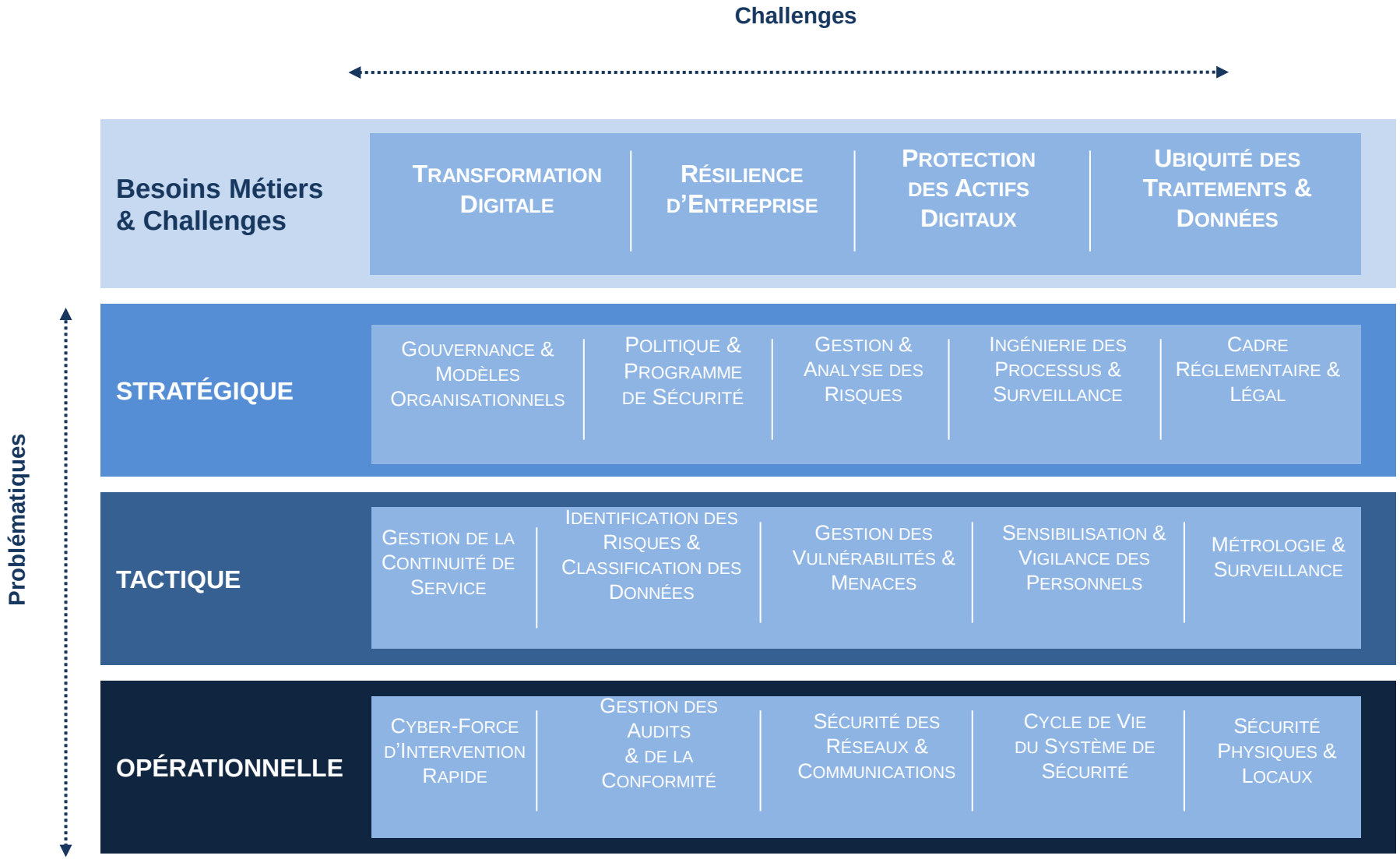
SERVICES ET SOLUTIONS DE KUDELSKI SECURITY

LA SÉCURITÉ DES DONNÉES

ACTIVITÉS DE CONSEIL

KUDELSKI SECURITY

VOUS ACCOMPAGNER À TOUS LES NIVEAUX



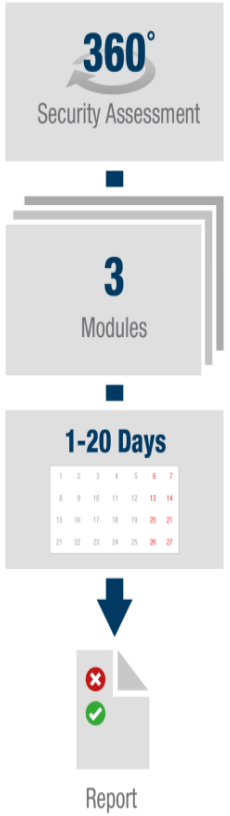
EVALUATIONS ET MODÉLISATION DES CYBER-RISQUES

➢ Analyse Fondamentale

- Questionnaires ISO-2700x avec une séance (à distance) d'interview
- Documentation des vulnérabilités techniques et technologiques
- Balayage de recherche à distance des vulnérabilités
- Rapport et recommandations sous une semaine

➢ Analyse étendue ou personnalisée

- Séance d'interview sur site
- Cadrage sur la base des actifs identifiés et du périmètre de sécurité
- Balayage de recherche des vulnérabilités sur site et périmétrique
- Définition du profil des menaces selon l'analyse de la criticité des actifs
- Rapport, identification des risques spécifiques et recommandations
- Sous 2 à 4 semaines



ZURICH

[1] Système de Management de la Sécurité l'Information (ISO 27001)

KUDELSKI SECURITY

LA SÉCURITÉ DES DONNÉES

LA FORMATION

KUDELSKI SECURITY

DES CENTRES DE FORMATION EN EUROPE

Exemples de formations:

- *Recherches OSINT (Open Source Intelligence)*[1]
- ***Sensibilisation à la cyber sécurité (« Security Awareness Training »)***[1]
- *Executive Cyber Security Coaching avec certification CISM*
- Certified Information Security Manager (CISM)
- ISO 27005 Gestionnaire des Risques
- ISO 27001 Lead Auditor
- ISO 27001 Lead Implementer
- ISO 22301 Lead Auditor
- ISO 22301 Lead Implementer
- Sécurité iOS pour Test d'Intrusion et Audit des Applications
- *Gestion de Crise*[1]
- *Etc.*

https://www.kudelskisecurity.com/solutions/training-programs.html

[1] formation spécifiquement conçue par Kudelski Security

LA SÉCURITÉ DES DONNÉES

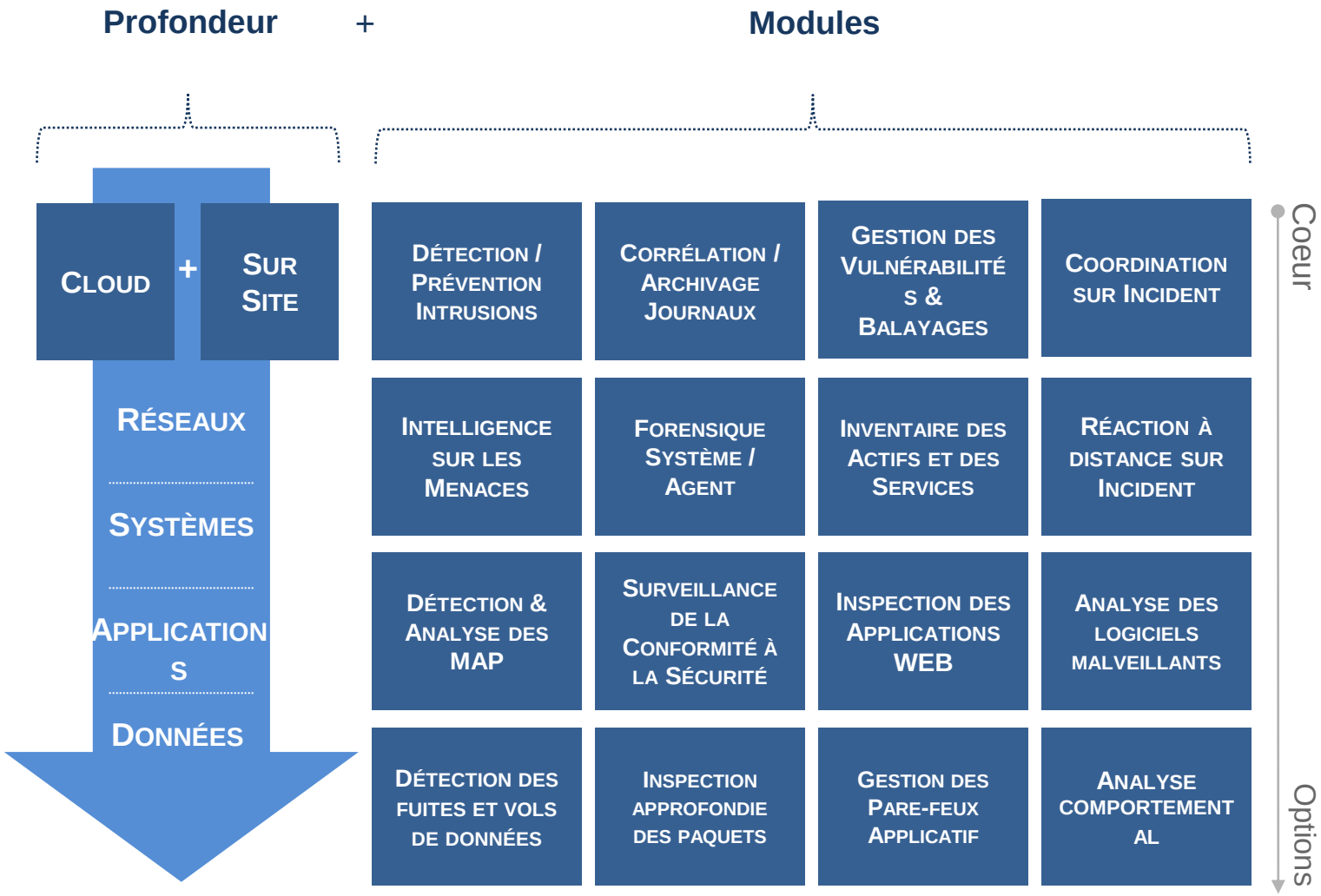
LE MONITORING ET LA DÉTECTION

KUDELSKI SECURITY

CYBER FUSION CENTER

KUDELSKI SECURITY

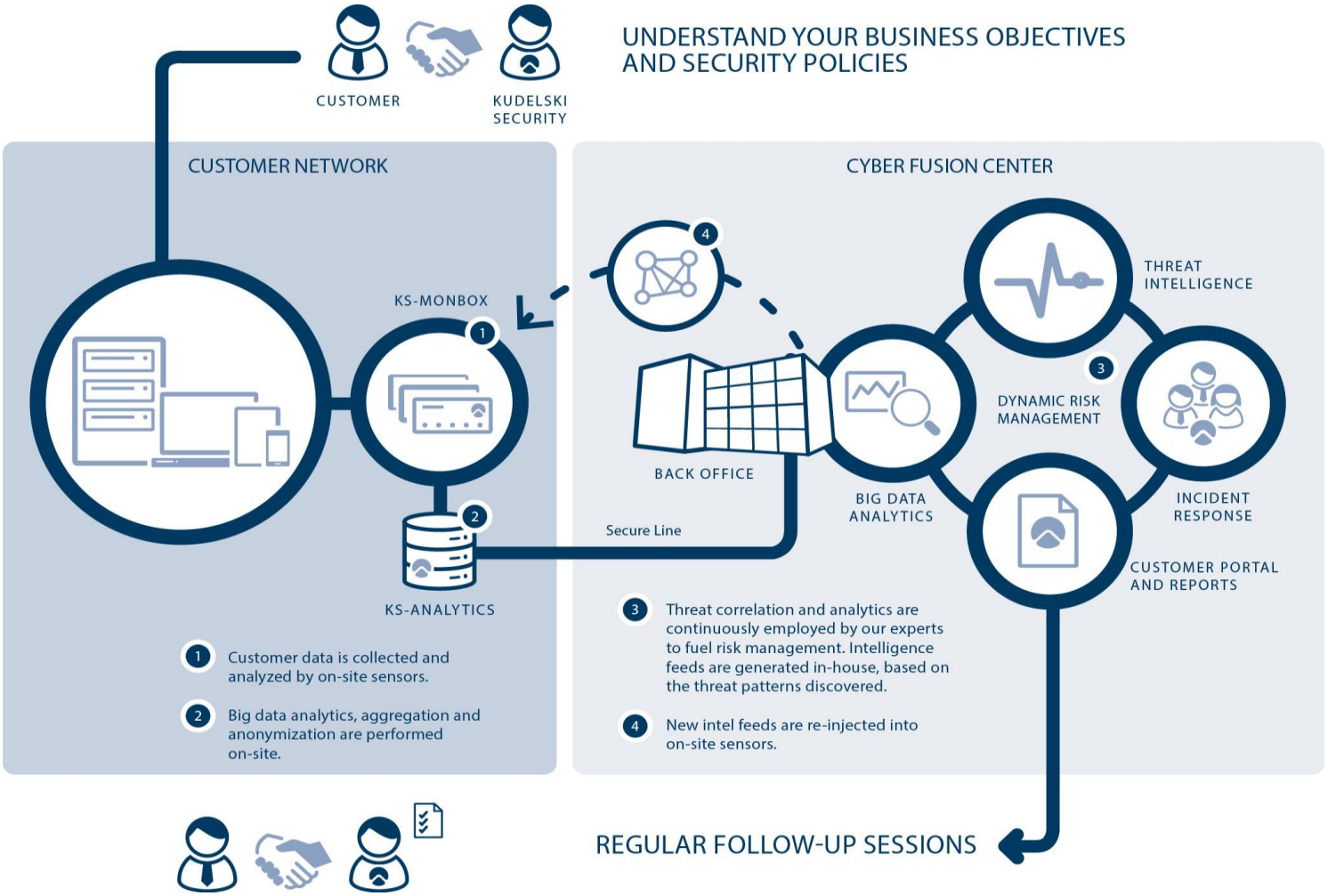
UN CYBER FUSION CENTER[1] (CFC) À VOTRE SERVICE



([1]) Centre des Opérations de Sécurité

LE CYBER FUSION CENTER EN BREF

Managed Security Services overview



AU SEIN DU CFC: LE PASSÉ, LE PRÉSENT & LE FUTUR

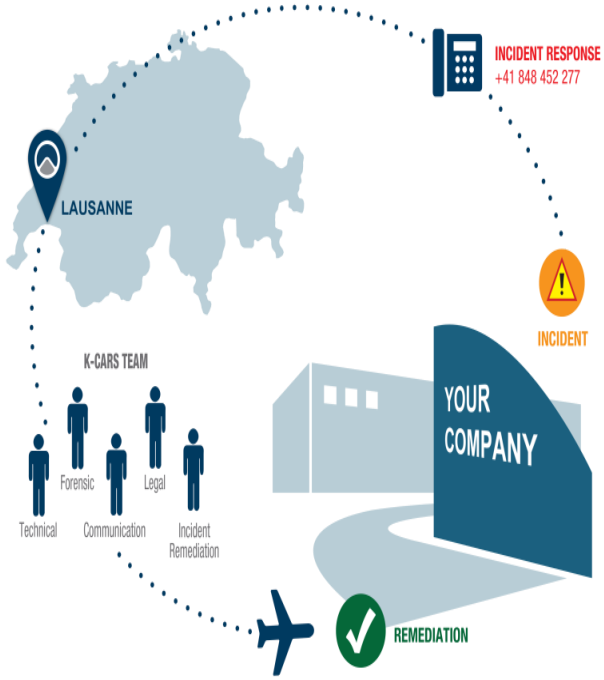
LA SÉCURITÉ DES DONNÉES

LA GESTION D'INCIDENTS DE SÉCURITÉ

KUDELSKI SECURITY

CYBER-FORCE D'INTERVENTION RAPIDE

- Depuis 2013, Kudelski Security dispose de son propre CERT[1] , et fait parti du FIRST, association internationale de coordination des CERT.
- La Cyber-Force d'Intervention Rapide (K-CARS) est prêt à intervenir 24/7, en réponse à tout incident, jusqu'à la mise en oeuvre du plan de reprise d'activité.
- Notre expertise:
  - Gestion d'incidents et crises
  - Investigation cyber-criminel et forensique
  - Communication de crise
  - Assistance juridique
  - Représentation auprès des instances de polices (ie. InterPol, EuroPol)
- Ce service est offert par Zurich Insurance dans le cadre des ses polices de Cyber-Assurance.



ZURICH

[1] Computer Emergency Response Team
[2] http://www.first.org/

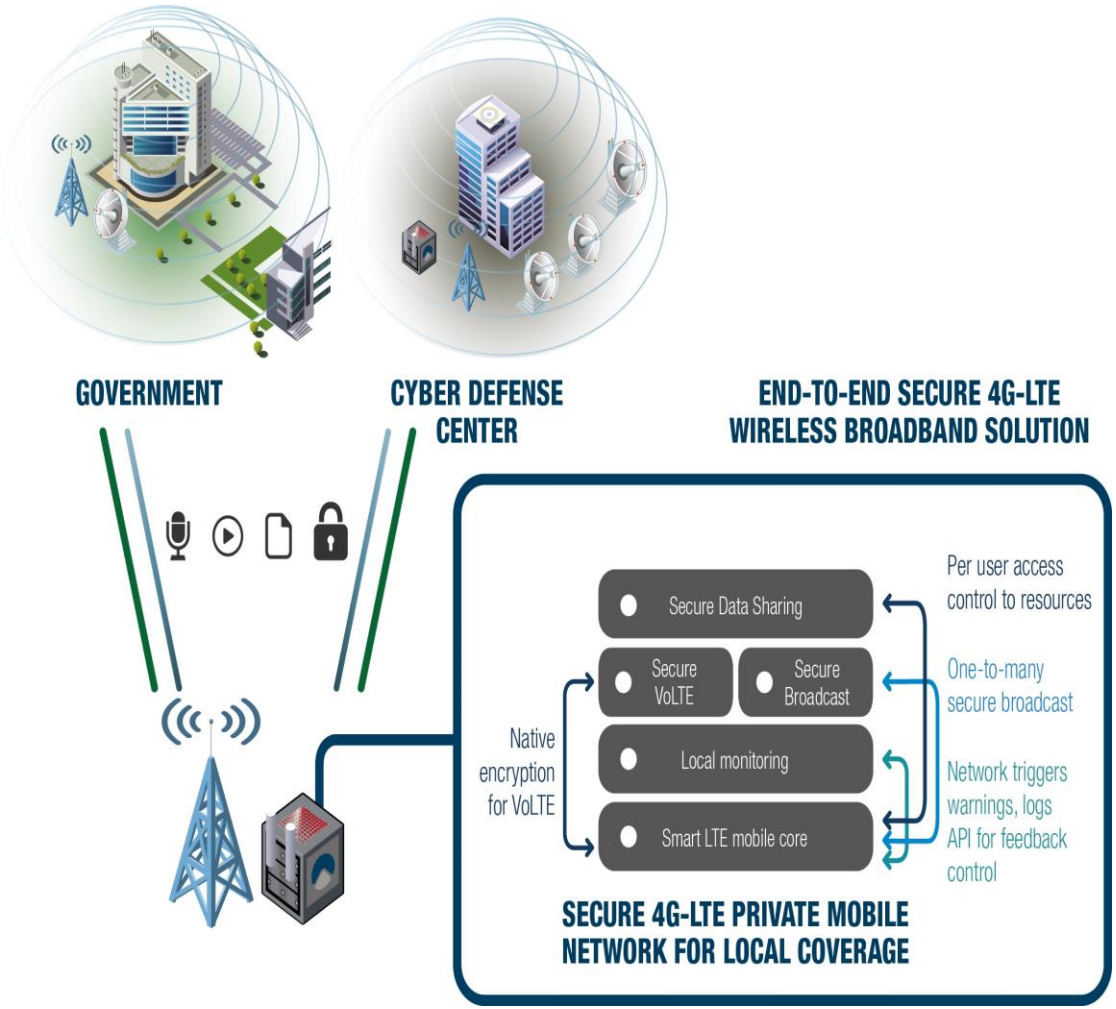
KUDELSKI SECURITY

LA SÉCURITÉ DES DONNÉES

LES TÉLÉCOMMUNICATIONS SÉCURISÉES

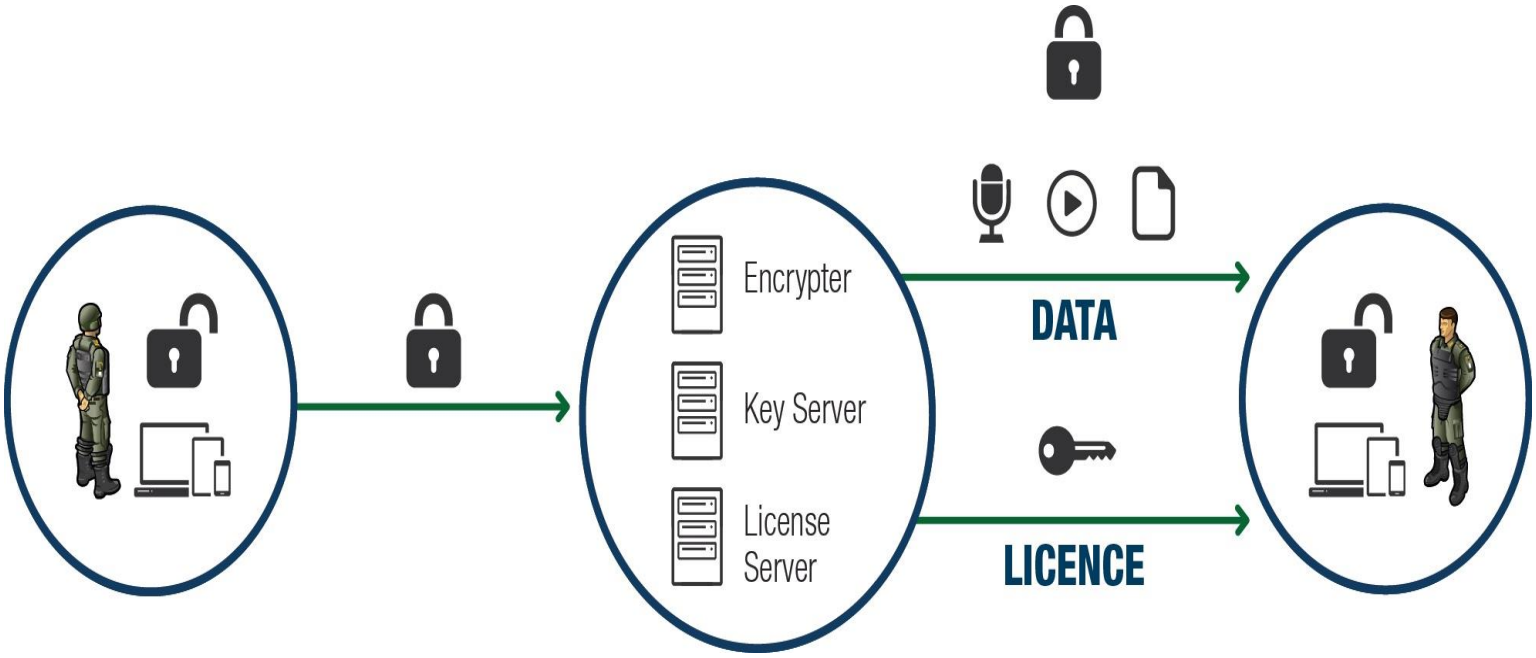
KUDELSKI SECURITY

RESEAU SECURISE DE COMMUNICATION 4G - LTE



- RESEAU CELLULAIRE PRIVEE
  - INDEPENDANT DES OPERATEURS DE TELEPHONIE MOBILE
- RESISTANT, COMPACT ET MOBILE
  - DIVISIONS & BRIGADES MOBILES
- RESEAU COMPLET, FIABILISE ET SECURISE
  - ALGORITHME SUR MESURE ET SURVEILLANCE DES MENACES

PARTAGE SÉCURISÉ DE DONNÉES
CONTRÔLE SUR L'ACCÈS AUX DONNÉES ET LEUR UTILISATION



- PARTAGE SECURISE DE TOUS TYPES DE DONNEES
  - DOCUMENT, VOIX, IMAGES, VIDEOS, ETC.
- PARTAGE AVEC DES INDIVIDUS OU DES GROUPES
  - A LA FOIS A L'INTERIEUR ET/OU A L'EXTERIEUR DU PERIMETRE DE CONFIANCE
- SERVEURS DE POLITIQUES DE SECURITE SUR SITE
  - DROITS D'ACCESS SELON LA CLASSIFICATION DES DONNEES

TÉLÉPHONE ET “HEADSET” SÉCURISÉS

Embedded White Noise SE *(with SPI interface)*

Microcontroller *(capable of lightning protocol)*

Apple authentication chip *(for use of lightning data connectivity)*

Lightning male connector *(data stream conduit + phone battery power supply)*

Battery (capacity tbd – 3200mAh?)

Female lightning connector *(charges case battery + phone battery)*

OR

Secure Bluetooth headset with embedded Kudelski Secure Element

SWISS MADE

CONCLUSION

- La gamme des services proposés par Kudelski Security est complète :
  - Cyber Fusion Center
  - Conseil en architecture des installations IT
  - Tests d'intrusion et audits de sécurité
  - Gestion d'incidents et de crises
  - Formation à la cyber sécurité des collaborateurs
  - Action légales pour faire fermer des sites pirates ou lutter contre la contrefaçon
  - Cryptage des télécommunications et des documents
- En fonction des besoins exprimés par un client, Kudelski Security élabore une offre sur mesure, adaptée au périmètre et à la nature des menaces à traiter


KUDELSKI
SECURITY
THANK YOU!
www.kudelskisecurity.com
cyber security unit of Kudelski Group