Cybersécurité et IA – Risques et perspectives

L'*IA au service de la cybersécurité*

pwc

citédel'IA* *Intelligence Artificielle

MEDEF Lille Métropole
Réseau MEDEF Grand Lille

Agenda

1. Quelques éléments clés
2. La confiance dans l'évolution des menaces
3. La dualité de la cybersécurité intelligente
4. Conclusion

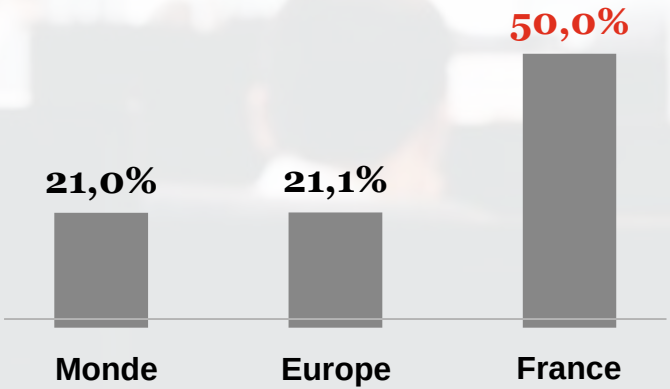
Ce que l'exécutif pense de la cybersécurité

85% *des PDG ne savent pas comment la cybersécurité est gérée au sein de leur organisation*

82% *des RSSI ne font pas confiance à la manière actuelle d'adresser la sécurité*

Seulement **1/3** *des PDG sont impliqués dans les problématiques cybersécurité*

65% *des PDG ne savent pas où sont localisées les données sensibles de leur organisation*



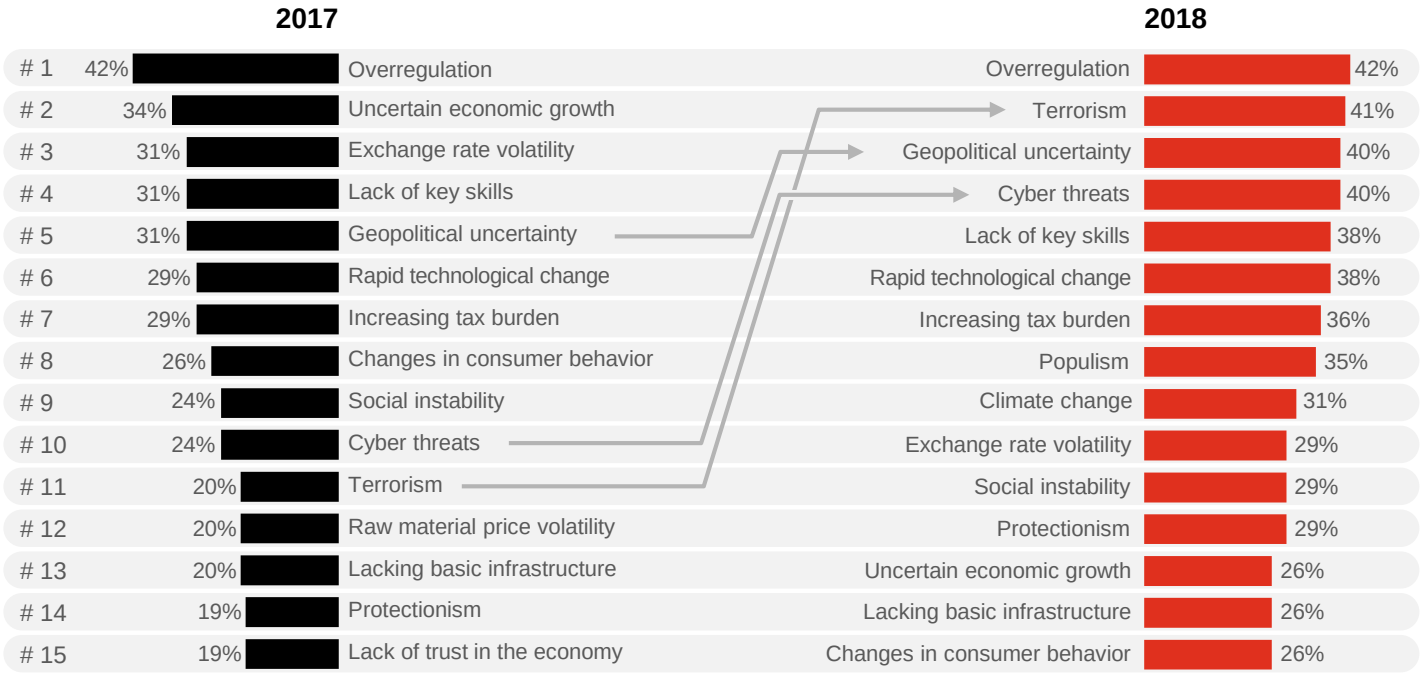
Les entreprises considèrent ne pas avoir suffisamment de ressources expertes en cybersécurité

1 à 2 millions
de postes en cybersécurité à pourvoir

pwc *Source: CEO Survey*

Comment construire la confiance dans un contexte d'évolution des menaces?

Quel est votre niveau inquiétude sur l'impact de chaque menace dans la croissance de votre organisation?



Source: CEO Survey

La cybersécurité intélligente – Une dualité inévitable

Attaque

Reconnaissance de menaces

Une capacité de reconnaissance automatisée basée sur des processus d'apprentissage cycliques

Des attaques mieux ciblées

Des moteurs d'IA qui adoptent des stratégies améliorées et des cibles tactiques dans les infrastructures

Gestion de crise

Une exécution efficace des procédures de gestion de crise, avec une diminution des délais observés

Contournement des defenses existantes

Manipulation des technologies de cyberdéfense basées sur des règles d'identification préétablies, suite à leur adoption à large échelle

Analyse comportementale

Construction des profils utilisateur pour l'amélioration des pratiques de la sécurité, et détection des acteurs malveillants

De nouveaux scenarios et vecteurs d'attaque

Détournement des flux, manipulation des utilisateurs, sabotage de la surveillance…

Assistance et resolution des incidents

Construction des profils utilisateur pour l'amélioration des pratiques de la sécurité, et détection des acteurs malveillants

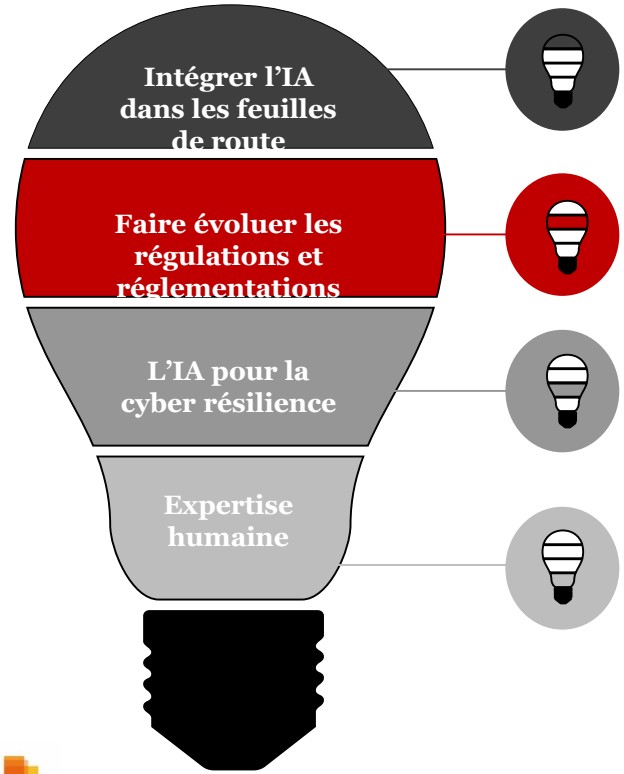
Camouflage et dissimulation améliorée

L'emploi d'entité IA soulève des obstacles importants quant à l'identification des acteurs malveillants et leur reconnaissance

Défense

pwc

Conclusion



Les idées clés à retenir:

- L'IA fera partie intégrante de l'écosystème des entreprises
- Eviter les points de vue extrêmes lors de l'analyse du potentiel de l'IA dans la cybersécurité

- Les régulations et réglementations doivent permettre une adoption facilitée et une clarification des usages autorisés pour la cybersécurité

- Les meilleurs mécanismes de résiliences seront non seulement réactifs, mais proactifs, et l'IA est un des moyens les plus efficaces pour cela

- L'obstacle principal à l'adoption de l'IA sera l'absence d'experts humains
- Les technologies d'IA sont paradoxalement fortement liées à la couche humaine

Merci !