

04
JUILLET

DE 8H30 À 11h00

HUBLAB PARIS 8e

**HUB TRENDS &
NETWORKING**

CYBER SÉCURITÉ

CMO, DRH, CFO, CTO

Pourquoi les risques cyber sont l'affaire de tous ?



HeadMind Partners



LEFEBVRE
SARRUT

ADVANT Altana



iwo
iad





[Welcome Speech]
CMO, DRH, CFO, CTO
**Pourquoi les risques
cyber sont l'affaire de
tous ?**



Perle Bagot

Associée fondatrice
HUB Institute

LA PLATEFORME D'ACCÉLÉRATION DES TRANSFORMATIONS **BUSINESS, DIGITALES & DURABLES**



Une plateforme unique qui promeut des services et des solutions à valeur ajoutée auprès de communautés professionnelles regroupant **100 000 décideurs**.

INDUSTRIES' COMMUNITIES



KEY FUNCTIONS' & CROSS INDUSTRIES COMMUNITIES



100 K décideurs nous suivent



+ 10 K cadres formés par an



+ 600 articles, rapports de tendances, études sectorielles



+ 150 événements online & offline



+ 120 entreprises membres
+ 20 secteurs d'activité axés sur le numérique et le développement durable

UN ÉCOSYSTÈME DE MEMBRES

ENGAGÉ À L'ANNÉE AVEC LES CONTENUS, FORUMS & ACTIVITÉS DU HUB INSTITUTE



Biens de consommation

Mode, Luxe & Beauté

Retail

Agroalimentaire & Co.



Acteurs financiers

Banque & Financement

Assurance & Mutuelle



Media

Médias & Agences



Infrastructure

Aménagement urbain

Centres commerciaux

Energies & Environnement

Voyage & Hôtellerie



Autres acteurs



Opérateur OEM

Mobilité & Logistique

Télécom & hardware

Équipementiers



Solutions



DÉCOUVREZ NOS

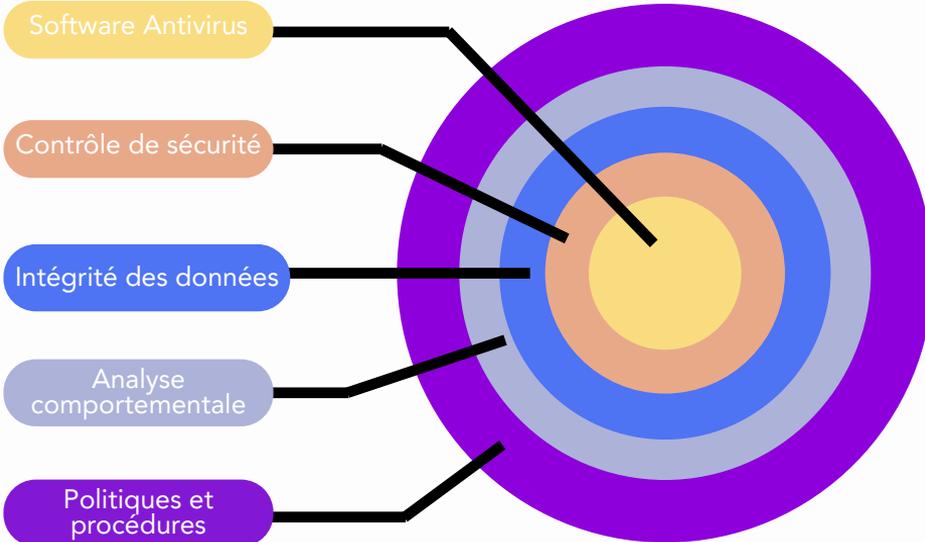
 **Review**

 **Reports**



QU'ENTENDONS-NOUS PAR CYBERSÉCURITÉ ?

STRATÉGIE D.I.D (Defense-in-depth)



CYBERSÉCURITÉ : DÉFINITION

La cybersécurité regroupe l'ensemble des processus et des outils destinés à **protéger les réseaux et les appareils contre les cyberattaques** : actions délibérément malveillantes à l'encontre d'un dispositif informatique.

DES ENTREPRISES MAL PRÉPARÉES

Plus de 77 % des entreprises n'ont pas établi de plan d'intervention en cas d'incident de sécurité. Il faut également noter qu'une grande partie des problèmes de cybersécurité sont liés à **des défaillances humaines**. Il est donc essentiel d'avoir une stratégie de défense.

General Data Protection Regulation

Le GDPR est un outil de prévention, car c'est le seul texte qui impose des mesures de cybersécurité sous peine de sanctions.

CYBERSÉCURITÉ : UN ENJEU POUR LES GÉANTS DE LA TECHNOLOGIE

UNE QUESTION D'AUTANT PLUS IMPORTANTE QUE L'ADMINISTRATION BIDEN CHERCHE À ÉTABLIR DES NORMES MINIMALES DE CYBERSECURITÉ FACE À LA MULTIPLICATION DES ATTAQUES



À la suite de nombreuses critiques concernant la désinformation et la protection des données, et sous la pression croissante des régulateurs, Facebook a investi plus de **13 milliards de dollars dans la cybersécurité**, a introduit des outils d'IA pour détecter la désinformation tels que SimSearchNet++ et a cessé d'utiliser son logiciel de reconnaissance faciale.



La sécurité est la priorité absolue d'Apple, c'est pourquoi l'entreprise exerce un **contrôle strict sur son écosystème de produits**, tant au niveau des appareils (iPhone, iWatch, etc.) que des logiciels. **Apple développe ses propres solutions de sécurité**, limite le partage de données avec des tiers et analyse chaque application avant son téléchargement.



En tant que fournisseur de logiciels, Microsoft accorde une attention particulière à la sécurité et a prévu un **budget de 20 milliards de dollars entre 2022 et 2027 pour améliorer la cybersécurité**. Elle a également cherché à améliorer la sécurité de son cloud Azure par le biais d'investissements et d'acquisitions (Aqua Security, CloudKnox, etc.).



A travers sa division AWS et son écosystème de partenaires, **Amazon opère sa cybersécurité en interne pour protéger l'identité, les données et l'infrastructure**. Amazon propose également AWS Security Hub, une solution qui centralise différents outils pour une protection unifiée.



Google a adopté un modèle de "confiance zéro", qui exige que chaque utilisateur et chaque système s'identifie pour accéder aux ressources, ce qui renforce la sécurité. Parallèlement, Google considère la cybersécurité comme une **opportunité de développement** et prévoit d'investir **10 milliards de dollars dans le développement de solutions de protection**.

De logiciels malveillants dits "Malware" à des attaques informatiques de type D.O.S (Denial-Of-Service), les cyberattaques prennent différentes formes.



Malware

Un malware est un logiciel malveillant et intrusif, téléchargé sans le consentement de l'utilisateur et destiné à nuire au système informatique.



Deepfakes

Utiliser de faux sons/images pour tromper les employés et contourner les protocoles de sécurité.



Data breach

Récupération des données personnelles et diffusion sur le dark web pour orchestrer des campagnes de phishing.



Ransomware

Logiciel d'extorsion conçu pour prendre en otage des données personnelles jusqu'à ce que la victime paie la rançon.



Malware-as-a-Service

Business Model qui vise à fournir aux pirates des logiciels malveillants pour leur éviter d'avoir à développer leur propre logiciel.



Cyber-espionnage

Ensemble d'actions menées dans le but d'infiltrer le système informatique d'une entreprise afin de s'emparer et d'exploiter des données/secrets industriels.



Advanced Persistent Threats (APT)

Ce sont des cyber-attaques ciblées, difficiles à tracer, au cours desquelles le pirate informatique accède au réseau sur une longue période.



Denial of Service (DoS)

Le DoS consiste pour un pirate informatique à inonder le site web d'une entreprise afin de provoquer une panne du serveur qui interrompt le service pour les utilisateurs.

LES NOUVELLES TECHNOLOGIES À LA RESCOURSSE

POUR UNE PLUS GRANDE SÉCURITÉ DES DONNÉES

BLOCKCHAIN



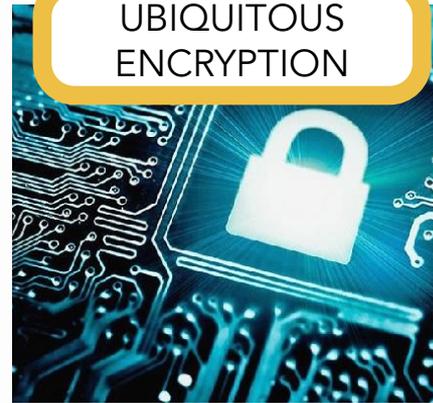
La start-up **ShareID** utilise la sécurité cryptographique combinée à l'IA pour créer une **identité numérique** sécurisée basée sur des documents officiels. **Dans le secteur du luxe, plusieurs marques se sont réunies pour former le Consortium Aura**, une solution blockchain globale pour garantir la transparence aux consommateurs.

SNOWPACK



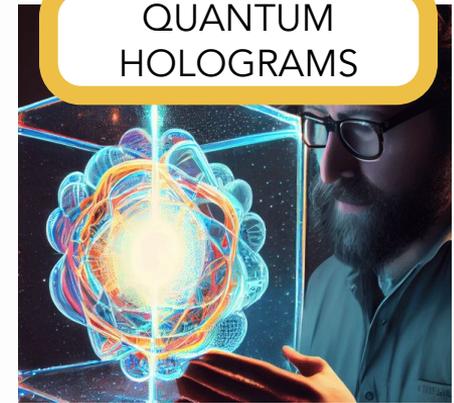
Snowpack a développé une solution qui **permet aux utilisateurs d'être anonymes sur Internet**. Snowpack cache les détails de l'utilisateur au niveau du réseau et de l'application sans stocker aucune donnée. Cela est possible grâce à des serveurs (nœuds) déployés sur les sites des clients de Snowpack.

UBIQUITOUS ENCRYPTION



Le chiffrement omniprésent est une technique qui permet de chiffrer les données partout et à tout moment, même dans le cloud. **Les données restent cryptées même lorsque des calculs sont effectués**, ce qui permet de les utiliser sans les révéler et donc sans les rendre vulnérables.

QUANTUM HOLOGRAMS



Des chercheurs ont réussi à créer des hologrammes en 3D à partir de photons intriqués. Cette technologie permet un **cryptage ultra-sécurisé des données** grâce au comportement des photons intriqués. Elle permet également le transfert de données à grande vitesse.



[Welcome Speech]
CMO, DRH, CFO, CTO
**Pourquoi les risques
cyber sont l'affaire de
tous ?**



Perle Bagot

Associée fondatrice
HUB Institute

Table ronde - Enjeux de la cybersécurité pour la performance et la compétitivité de l'entreprise



Virginie Duby-Muller

Députée de la Haute Savoie



Nicolas Arpagian

Vice-Président





Les Indicateurs Cyber au service du Middle Management



Benoît Fuzeau

Président
CLUSIF

[Table Ronde] **Sensibilisation et Formation des collaborateurs aux risques Cyber de l'Intelligence Artificielle générative, on fait le point !**



Candice Tran Dai

DSSI

LEFEBVRE
SARRUT



Laetitia Daage

Avocate à la Cour

ADVANT Altana



Manon Dubien

Vice-Présidente



Hakima Kadri

Head of Cybersecurity

iad

Carte d'identité du CFECYS

Association créée en

2016

sur l'initiative de
Nacira Salvan

Promouvoir les
métiers de la
cybersécurité
auprès des femmes
souhaitant accéder,
se reconverter ou
partager leur
expérience.



Membre du



4 missions

Sensibiliser
Promouvoir
Accompagner
Éclairer



Position d'
influenceur
dans l'écosystème
de la **cyber**

institutionnels,
organisations,
entreprises écoles,
medias

...

Bureaux : Paris

Lille

Toulouse

Rennes

Marseille

Lyon



Rappel des Missions essentielles du CEFCYS

4 missions

Sensibiliser

Promouvoir

Accompagner

Éclairer

Sensibiliser

- Sensibiliser les entreprises, les partenaires éducatifs, les recruteurs à l'importance de la parité homme/femme et faire ainsi progresser la présence et l'impact des femmes.
- Nouer des partenariats avec des organismes permettant de reconnaître et faire progresser la présence et de l'impact des femmes dans le domaine de la SSI
- Le CEFCYS contribue à sensibiliser le grand public à la cybersécurité, en particulier les jeunes, pour la protection et l'éducation à l'usage sécurisé du numérique.

Promouvoir

- Valoriser et professionnaliser les femmes dans le domaine de la sécurité du numérique
- Proposer des programmes de mentorat aux jeunes femmes ayant des métiers relatifs à la SSI
- Organiser des évènements et conférences rassemblant les femmes travaillant ou aspirant à contribuer dans le domaine de la SSI pour :
 - Favoriser les échanges, la collaboration et retours d'expérience
 - Développer le réseau des femmes travaillant ou aspirant à travailler dans la sécurité des systèmes d'information

**Former &
Accompagner**

- Développer et participer à des programmes d'éducation, de sensibilisation et de formation dans le domaine de la SSI
- Accompagner dans la recherche d'emploi, organiser des salons de recrutement avec des entreprises partenaires

Eclairer

- Organiser et animer des groupes de travail traitant des tendances fortes de la SSI
- Publier des rapports, livres blancs, des supports de sensibilisation et des newsletters

[Table Ronde] **Sensibilisation et Formation des collaborateurs aux risques Cyber de l'Intelligence Artificielle générative, on fait le point !**



Candice Tran Dai

DSSI

LEFEBVRE
SARRUT



Laetitia Daage

Avocate à la Cour

ADVANT Altana



Manon Dubien

Vice-Présidente



Hakima Kadri

Head of Cybersecurity

iad



**IA Générative et
Cybersécurité –
du mythe à la
(probable) réalité**



Constant Bridon

Lead IA
HarfangLab



HUB Institute

IA générative & Cybersécurité

du mythe à la (probable)
réalité



L'IA GÉNÉRATIVE, CA (VA) MARCHE(R)



GAFAM

Intègre l'IA générative dans leurs produits historiques



SERVICES

Investit significativement dans la technologie "genAI"



INNOVATION

Levée de 100+ millions d'euros dans un contexte plus que contraint

QUID DU SECTEUR DE LA CYBER ?



LES FONCTIONS D'UN SECURITY OPERATION CENTER (SOC)

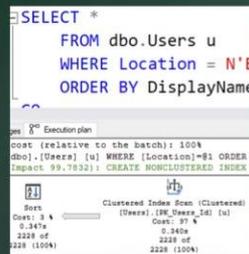


LES MANQUES DE L'IA « CLASSIQUE »



INFORMER

Veille technologique en continue
avec des sources de plus en plus
nombreuses



INTERAGIR

Requêtes sur des bases de données
hétérogènes avec des langages
parfois exotiques



REMEDIER

Diagnostic étant posé, quelle est
la prochaine action ?

IA GÉNÉRATIVE - LA SOLUTION À TOUS NOS PROBLÈMES



Veille

L'IA devient un outil de synthèse et d'interactions avec un contenu



Requête

Les requêtes n'ont plus besoin d'être exprimées dans un langage spécifique, en prenant en compte la technologie sous-jacente



Remédiation

Les procédures de remédiation identifiées n'ont plus à être générées explicitement, mais sont le produit de la spécialisation de l'IA à mon contexte

SEUL PROBLÈME : LES HALLUCINATIONS



CONCLUSIONS

CONCLUSIONS



Les analystes SOC ne seront pas remplacés

CONCLUSIONS



Les analystes SOC ne seront pas remplacés

DECATHLON

Le niveau de compétences requis à l'embauche va diminuer

CONCLUSIONS



Les analystes SOC ne seront pas remplacés

DECATHLON

Le niveau de compétences requis à l'embauche va diminuer



La montée en compétence en cyber va s'accélérer

CONCLUSIONS



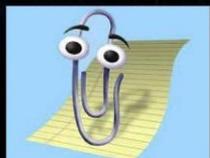
Les analystes SOC ne seront pas remplacés

DECATHLON

Le niveau de compétences requis à l'embauche va diminuer



La montée en compétence en cyber va s'accélérer



Clippy va revenir

MERCI



Constant Bridon

Lead IA at HarfangLab



Besoins et enjeux des entreprises en termes de formation des profils Cyber



Cédric Martins

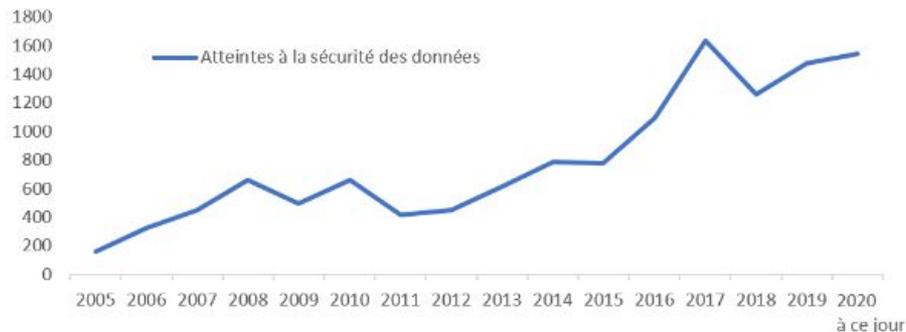
Directeur

School of Cyber

L'explosion de la Cyber

Augmentation des menaces

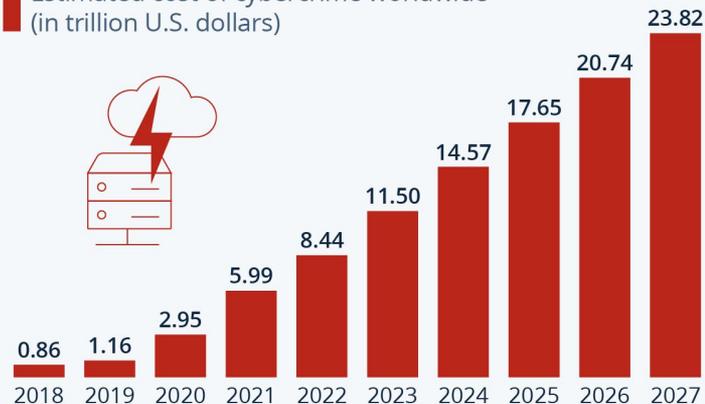
Explosion du nombre de cyberattaques.



Source : Identity Theft Resource Center.

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF



statista



Personne n'est épargné !

Toutes les
14 sec



une entreprise est victime
d'une attaque par ransomware

50k€

Coût médian



27%
du CA annuel



115

milliards € de
dépenses Cyber
d'ici 2025

(EN 2022)

Enjeux de Cybersécurité pour les entreprises



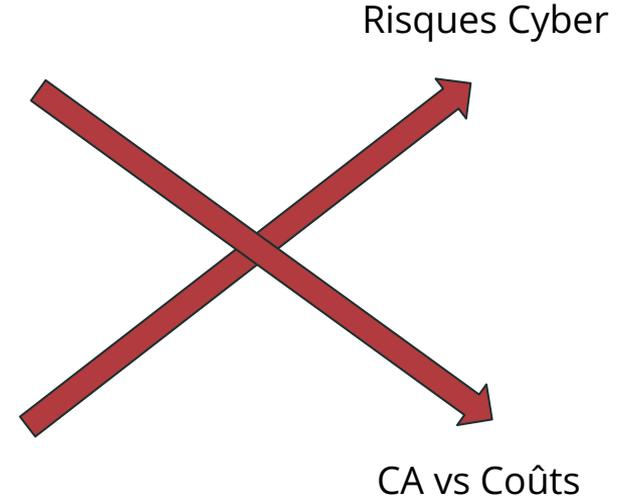
Selon l'ANSSI, **831 intrusions** ont ainsi été constatées en France en 2022. Hôpitaux, collectivités, grandes et plus récemment petites et moyennes entreprises...

La question n'est pas de savoir si on va subir une attaque mais quand ?

- Accélération du numérique → **Augmentation du risque Cyber**
- Confiance implicite → **Zéro Trust**
- Besoin de talents pour accompagner ce changement

La pénurie de Talents

- Ambition du gouvernement de créer **37.000 emplois** d'ici 2025
- Selon une étude Wavestone, plus de **15.000 postes** ne seraient pas pourvus
- A l'échelle mondiale, la pénurie s'élèverait à **3,5 millions de personnes**
- **Tous les métiers sont concernés** : des ingénieurs aux consultants en passant par les architectes en cybersécurité



Panorama des formations

2 Filières :

- Ingénieur
- **Management**

3 Niveaux :

- BAC +3 (Niv 6) → Technicien ou poursuite d'études
- **BAC +5 (Niv 7) → Expert**
- Formation continue → Spécialisation, mise à niveau et reconversion



Les 4 grandes familles de métiers de la Cyber

GESTION DE LA SÉCURITÉ ET PILOTAGE DES PROJETS DE SÉCURITÉ

- **Directeur Cybersécurité**
- **Responsable de la Sécurité des Systèmes d'Information**
 - Déclinaison pour le Responsable de sécurité des SI
 - Coordinateur sécurité
 - Directeur de programme de sécurité
 - Responsable de projet de sécurité

CONCEPTION ET MAINTIEN D'UN SI SÉCURISÉ

- **Chef sécurité de projet**
- **Auditeur de sécurité organisationnelle**
 - Architecte sécurité
 - Spécialiste sécurité d'un domaine technique
 - Spécialiste en développement sécurisé
 - Cryptologue
 - Administrateur de solutions de sécurité
 - Auditeur de sécurité technique

GESTION DES INCIDENTS ET DES CRISES DE SÉCURITÉ

- **Analyste réponse aux incidents de sécurité**
- **Gestionnaire de crise de cybersécurité**
 - Responsable du SOC
 - Opérateur analyste SOC
 - Responsable du CSIRT
 - Analyste de la menace cybersécurité

CONSEIL, SERVICES ET RECHERCHE

- **Consultant en cybersécurité**
- **Formateur en cybersécurité**
 - Chercheur en sécurité des systèmes d'information
 - Évaluateur de la sécurité des technologies de l'information
 - Développeur de solutions de sécurité
 - Intégrateur de solutions de sécurité

Source :



Pourquoi School of Cyber ?

- **Certification Qualiopi** délivrée pour nos formations
- Des **intervenants experts** pour former les jeunes à la Cybersécurité
- Les étudiants profitent de l'**écosystème du Hub Institute varié**
- **Comité de pilotage** composé d'experts des métiers de la Cyber



Notre Campus - Paris 8ème

Lieu de formation :

- Salle de cours
- Lieu de vie
- Administration

Lieu d'événements :

- Conférences
- Masterclass





Besoins et enjeux des entreprises en termes de formation des profils Cyber



Cédric Martins

Directeur

School of Cyber



Mot de clôture



Perle Bagot

Associée fondatrice

HUB Institute

gamers dans le monde

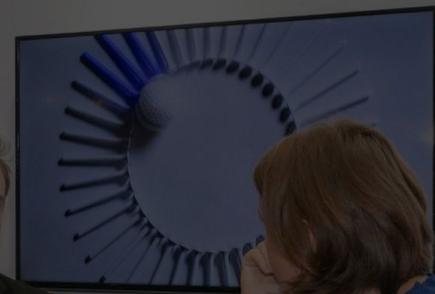
- La vente de produits digitaux a atteint 67,5 milliards de \$ en 2022

HUB CYBER

FORUM & NETWORKING

Mardi 12 Décembre 2023
9h00 - 17h00
HUBLOFT, Paris 8ème

Créons →
une IA avec intégrité, sa



MERCI À TOUS



HeadMind Partners



LEFEBVRE
SARRUT

ADVANT Altana



in
iad

