masters insights

les évolutions de nos métiers

CLUB CYBERSÉCURITÉ

Les métiers de la cybersécurité face aux transformations de 2030

« L'IA devient un multiplicateur de capacités pour les deux camps. »

UNE ANALYSE MASTERS INSIGHTS

Édition Août 2026

SOMMAIRE

Table des matières

01 —

Le métier en 2026

La cybersécurité est devenue une fonction stratégique pour toutes les organisations.

La généralisation du cloud, du télétravail, de l'intelligence artificielle, des objets connectés et des infrastructures critiques augmente considérablement la surface d'attaque des entreprises.

Parallèlement, les cybercriminels utilisent eux aussi l'intelligence artificielle pour automatiser certaines attaques, produire des campagnes de phishing plus crédibles ou accélérer la découverte de vulnérabilités.

La cybersécurité n'est plus uniquement un sujet informatique. Elle est devenue un sujet de gouvernance, de continuité d'activité, de souveraineté et de compétitivité.

02 —

Les faits

Les cyberattaques continuent d'augmenter

Les organismes européens et français observent une hausse constante des attaques visant les entreprises, les collectivités et les infrastructures critiques.

Les rançongiciels, le phishing, les compromissions d'identité et les attaques contre la chaîne d'approvisionnement figurent parmi les principales menaces.

La pénurie de compétences reste importante

Les entreprises rencontrent toujours des difficultés à recruter des profils expérimentés en cybersécurité, notamment dans les domaines de l'architecture, de la gouvernance, de la réponse aux incidents et du cloud.

Les réglementations se renforcent

Les nouvelles réglementations européennes, notamment NIS2 et le Cyber Resilience Act, renforcent les obligations des entreprises en matière de cybersécurité, de gouvernance et de gestion des risques.

03 —

Les grandes transformations du métier

L'intelligence artificielle

L'IA permet désormais :

- d'accélérer la détection des menaces
- d'automatiser certaines investigations
- d'analyser des millions d'événements de sécurité
- d'assister les analystes SOC
- de produire des rapports plus rapidement

Mais elle permet également aux attaquants :

- de personnaliser les campagnes de phishing
- d'automatiser certaines attaques
- de produire du code malveillant plus rapidement
- d'améliorer les techniques d'ingénierie sociale

> ***« L'IA devient un multiplicateur de capacités pour les deux camps. »***

La gouvernance cyber

La cybersécurité est désormais pilotée au niveau des directions générales et des conseils d'administration. Les responsables cyber doivent dialoguer avec :

- les dirigeants
- les juristes
- les responsables des risques
- les métiers
- les autorités de régulation

La sécurisation de l'IA

Les entreprises doivent désormais protéger :

- leurs modèles d'IA
- leurs données d'entraînement
- leurs agents IA

- leurs infrastructures cloud

La sécurité de l'intelligence artificielle devient un nouveau domaine d'expertise.

04 —

Les 10 killer compétences

1. **Gestion des risques cyber**
   Identifier, hiérarchiser et traiter les risques.
2. **Architecture de sécurité**
   Concevoir des systèmes résilients.
3. **Réponse aux incidents**
   Limiter rapidement les impacts d'une attaque.
4. **Gouvernance cyber**
   Intégrer la cybersécurité dans la stratégie de l'entreprise.
5. **Sécurité cloud**
   Sécuriser les infrastructures modernes.
6. **Sécurité de l'IA**
   Comprendre les nouvelles vulnérabilités liées aux modèles d'IA.
7. **Gestion de crise**
   Piloter une organisation pendant un incident majeur.
8. **Communication**
   Expliquer les risques aux dirigeants et aux métiers.
9. **Veille technologique**
   Anticiper l'évolution des menaces.
10. **Leadership**
    Développer une véritable culture de cybersécurité dans l'organisation.

05 —

Les compétences qui perdent de la valeur

- Approche exclusivement périmétrique de la sécurité
- Contrôles manuels répétitifs
- Réponse réactive sans anticipation
- Sécurité pensée uniquement par la DSI
- Gestion isolée des risques sans dialogue avec les métiers

06 —

Les principaux risques

- Utilisation malveillante de l'IA
- Attaques sur la chaîne d'approvisionnement
- Pénurie persistante de talents
- Explosion des obligations réglementaires
- Dépendance aux fournisseurs cloud
- Sophistication croissante des cybercriminels

07 —

Les opportunités des cinq prochaines années

Les besoins continueront de croître dans :

- la gouvernance cyber
- la sécurité des infrastructures critiques
- la sécurité du cloud
- la sécurité de l'IA
- la gestion des identités
- la réponse aux incidents
- les audits de conformité
- les fonctions de RSSI externalisé ou Fractional CISO

Les profils expérimentés ayant une vision stratégique seront particulièrement recherchés.

08 —

Les compétences à développer dès aujourd'hui

- Gouvernance des risques
- Intelligence artificielle appliquée à la cybersécurité
- Cloud Security
- Zero Trust
- Gestion de crise
- Réglementation européenne
- Communication avec les dirigeants
- Leadership

09 —

Les outils à connaître

- ChatGPT
- Microsoft Security Copilot
- Google Gemini
- Perplexity
- Microsoft Defender XDR
- CrowdStrike Falcon
- Palo Alto Cortex XSIAM
- Splunk
- SentinelOne
- Wiz

Ces outils renforcent les capacités de détection et d'analyse, mais ne remplacent ni l'expertise humaine ni le jugement face à des situations inédites.

10 —

Ce que disent les faits

- Les agences européennes et françaises considèrent la cybersécurité comme un enjeu majeur de souveraineté économique et de résilience.
- Les nouvelles réglementations renforcent la responsabilité des dirigeants dans la gestion des risques cyber.
- L'intelligence artificielle transforme aussi bien les moyens de défense que les capacités des attaquants, ce qui augmente la nécessité d'une supervision humaine qualifiée.

11 —

Les 5 questions clés

Que tout expert cybersécurité devrait se poser :

01 *Mon expertise couvre-t-elle uniquement la technique ou également la gouvernance ?*

02 *Suis-je prêt à sécuriser des systèmes intégrant de l'intelligence artificielle ?*

03 *Comment expliquer les risques cyber à un comité exécutif ou à un conseil d'administration ?*

04 *Est-ce que je développe des compétences en gestion de crise et en communication ?*

05 *Mon expérience pourrait-elle être valorisée comme RSSI externalisé, Board Advisor ou consultant stratégique ?*

12 —

Sources

INSTITUTIONS

- Agence nationale de la sécurité des systèmes d'information (ANSSI)
- European Union Agency for Cybersecurity (ENISA)
- Commission européenne
- Agence de l'Union européenne pour la cybersécurité (NIS2, Cyber Resilience Act)

RÉFÉRENCES INTERNATIONALES

- National Institute of Standards and Technology (NIST)
- Cybersecurity and Infrastructure Security Agency (CISA)
- MITRE ATT&CK

CABINETS ET INSTITUTS

- Gartner
- IBM – Cost of a Data Breach Report
- Microsoft – Digital Defense Report
- Verizon – Data Breach Investigations Report
- PwC – Global Digital Trust Insights
- Deloitte – Global Future of Cyber Survey
- Accenture – State of Cybersecurity Resilience

RECHERCHE

- Stanford AI Index
- World Economic Forum – Global Cybersecurity Outlook