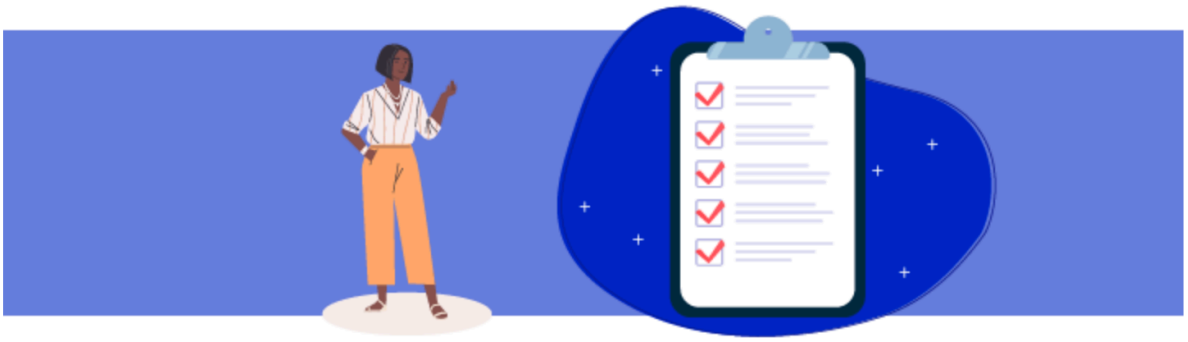
OPENCLASSROOMS

Découvrez l'univers de la cybersécurité

Ressources clés



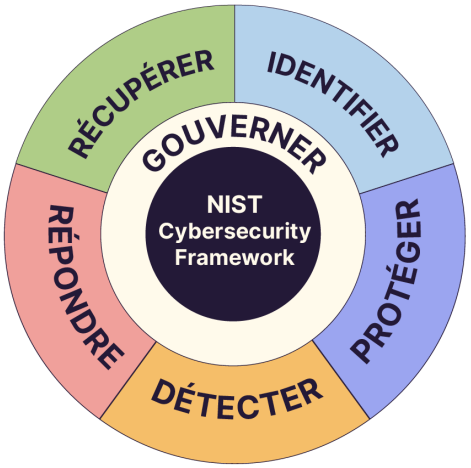
Il est facile de se perdre dans la profusion de ressources disponibles sur la cybersécurité. En voici une liste non exhaustive et perfectible, que nous vous encourageons à compléter selon vos découvertes ! Des sujets techniques aux sujets organisationnels, en passant par des ressources pour sensibiliser les collaborateurs ou citoyens, il y en a pour tous les goûts.

Les ressources fournies par les agences gouvernementales de cybersécurité

- Le site de l'ANSSI avec des ressources en français, et en particulier le guide d'hygiène informatique, utile pour connaître les sujets de sécurité les plus critiques à mettre en œuvre pour une organisation, ou tout document de la catégorie bonnes pratiques ;
- Le site cybermalveillance.gouv.fr fournit des conseils et des informations pour se protéger contre les cyberattaques et savoir y réagir ;
- Le site de l'ENISA avec des ressources disponibles en français et de nombreuses langues européennes ;
- Le site du NCSC avec des ressources disponibles uniquement en anglais ;
- Le site du CCB avec des ressources disponibles en français et anglais ;
- Le site du CISA avec des ressources disponibles uniquement en anglais.

Les standards ou normes liés à la cybersécurité

- L'ISO 27001 sur le management de la sécurité de l'information (document payant), qui définit la mise en place d'un système de management de la sécurité de l'information (SMSI), utile pour structurer et améliorer sa sécurité ;
- Le NIST cybersecurity framework (ressource en anglais accessible librement), qui décrit la cybersécurité à travers six grandes fonctions (gouverner, identifier, protéger, détecter, répondre et récupérer).



Les formations

Il existe de nombreuses formations certifiantes ou non. Parmi les certifications en cybersécurité les plus connues, nous pouvons citer :

- ISO 27001 lead implementer ou lead auditor : pour se préparer à faire certifier son organisation ou à devenir auditeur ;
- CISSP (Certified Information Systems Security Professional ou Professionnel Certifié en Sécurité des Systèmes d'Information) : une des certifications les plus exigeantes car elle couvre tous les sujets de la cybersécurité et demande plusieurs mois de préparation.

Les référentiels des métiers de la cybersécurité

- Le panorama des métiers de la cybersécurité par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)

- Le cadre référentiel européen de compétences cybersécurité par l'agence européenne de la cybersécurité (ENISA, en Anglais).
- L'initiative nationale pour l'éducation en cybersécurité (NICE) par l'institut national des standards et de la technologie américain (NIST)
- Le référentiel des compétences des métiers de la cyber par le campus cyber

Les ressources privilégiées par métier ou équipe

Métier	Ressources
Équipe de surveillance et détection (SOC)	• Les référentiels du MITRE ATT&CK et du MITRE D3FEND
Analyste de la menace	• Les plateformes du MISP (plateforme open source permettant de s'échanger des informations sur les menaces) ou d'OpenCTI
Gestionnaire de crise	Les guides de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) sur : • La gestion de la crise cyber • La communication de crise cyber • L'organisation d'un exercice de crise cyber
Équipe de réponse à incident (CERT / CSIRT)	• La base de connaissances du MITRE ATT&CK • Les alertes de sécurité du CERT-FR

Équipe de sécurité applicative	• Le top 10 de l'OWASP (rapport régulièrement mis à jour qui liste les 10 vulnérabilités les plus critiques affectant les applications web) • Le catalogue de vulnérabilités du MITRE CVE • Le référentiel du MITRE D3FEND • La base de connaissances Secure Flag (en anglais) utile aux développeurs pour comprendre les vulnérabilités pouvant affecter le code et comment s'en prémunir • Les recommandations de l'ANSSI pour la sécurisation des sites web
Architecte sécurité	• Le référentiel du MITRE D3FEND
Pentester (auditeur technique)	• Le top 10 de l'OWASP • Les outils Payload Box et Kali Linux
Analyste des risques cybersécurité	• La méthodologie d'analyse de risques EBIOS Risk Manager • La norme ISO 27005:2022 (Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information)
Chargé de conformité	• Les grandes normes de cybersécurité : ISO 27001, ISO 27002, ISO 27701, etc. • Le site de la CNIL pour la mise en conformité avec le RGPD
RSSI	• Les grands référentiels de cybersécurité tels que l'ISO 27001 et le NIST

	cybersecurity framework • Le guide d'hygiène informatique de l'ANSSI

Les ressources pour les développeurs

Si vous souhaitez en savoir plus sur l'application des bonnes pratiques dans le développement, la CNIL a publié un guide RGPD pour les développeurs. Il est centré sur la protection des données personnelles mais présente aussi quelques attaques communes contre lesquelles les développeurs peuvent agir (fiche n°18).

Encore une fois, de nombreux guides de l'ANSSI donnent des bonnes pratiques, comme ces recommandations pour la mise en œuvre d'un site web, à destination des développeurs.

Enfin, il existe des ressources (en anglais) de l'organisation à but non lucratif SAFECode qui œuvre pour le développement sécurisé.

Les ressources sur la sécurité "by design"

Vous trouverez ci-dessous quelques ressources permettant de progresser dans cette démarche de sécurité dès la conception :

- Les recommandations du Comité Européen de la Protection des Données (EDPB) traitant de la protection des données personnelles dès la conception et par défaut (en anglais) ;
- Un guide de l'ANSSI sur l'agilité et la sécurité numérique à destination des équipes projets.

Les ressources sur le modèle Zero Trust

L'ANSSI a publié un avis scientifique et technique sur le sujet.
Le NIST a publié un document sur l'architecture Zero Trust (en anglais).