Mini-cartographie des outils cyber gratuits[1] (2024)

- technique

Côté Perso

Grand public

Tester mon niveau de sensibilisation cyber :	SecNum académie	Lien
Savoir si un de mes comptes a été compromis[2] :	';--have i been pwned?	Lien
Générer et stocker mes mots de passe :	KeePass	Lien
Tester la robustesse de mon mot de passe :	Solidité mot de passe	Lien

Gestes de premiers secours cyber

Obtenir de l'aide suite à une cybermalveillance :	CYBER MALVEILLANCE GOUV.FR	Lien
Signaler aux autorités une escroquerie en ligne :	PHAROS	Lien
Porter plainte en ligne (si arnaque à caractère financier) :	THESEE	Lien

Sauvegarder mes données[3] :	Nextcloud	Lien
Chiffrer (protéger) mes données sensibles :	VeraCrypt	Lien
Déterminer si un fichier téléchargé est malveillant :	VIRUSTOTAL	Lien
M'initier au hacking éthique :	KALI	Lien

Côté Pro

Dirigeant

Sensibiliser mes employés à la cybersécurité :	La Mallette Cyber	Lien
Auto-évaluer la maturité cyber de mon entreprise :	nc3 Fit4Cybersecurity	Lien
Auto-évaluer mon dispositif de gestion de crise cyber:	(ANSSI)	Lien

RSSI

Réaliser une analyse d'impact (en appui du/de la DPO) :	Pia (CNIL)	Lien
Outiller mon analyse de risques (méthode EBIOS RM) :	EBIOS-RM	Lien
Homologuer un système (entité publique uniquement) :	MonService Sécurisé (ANSSI)	Lien
Suivre les principales alertes et avis de sécurité :	CERT-FR	Lien

Administrateur

Auditer la sécurité de l'Active Directory :	PING CASTLE	Lien
Générer gratuitement des certificats SSL/TLS :	Let's Encrypt	Lien
Auditer la sécurité de la configuration de mes serveurs :	Lynis	Lien
Suivre les vulnérabilités des composants de mon SI :	OpenCVE	Lien

Développeur

Chasser les secrets de mes dépôts Git :	gitLeaks	Lien
Analyser la sécurité de mes dépendances :	DEPENDENCY-CHECK	Lien
Intégrer des fonctions cryptographiques dans mon code :	libsodium	Lien
Tester la sécurité de mon application :	ZAP	Lien

+ technique

(1) Liste non-exhaustive d'outils gratuits recommandés par l'auteur de la publication, lequel n'a **aucun lien avec leur(s) créateur(s) respectif(s).** Lesdits outils ont ici été sélectionnés car développés et maintenus par les autorités françaises et/ou répandus au sein de l'écosystème francophone de la cybersécurité. L'auteur encourage cependant le lectorat à étudier les alternatives à chacun des outils cités avant leur utilisation.

(2) Il est déconseillé de saisir un mot de passe associé à un compte existant dans la page de la plateforme prévue à cet effet.

(3) Cet outil de cloud privé Open Source constitue une alternative à la méthode « traditionnelle » de sauvegarde manuelle des fichiers et leur stockage sur un support dédié (ex: disque dur externe ou clé USB).

A propos de l'auteur : **Nicolas GENET**
Consultant en cybersécurité

Contact :