Thème 2 Chapitre 3 : *Préserver l'identité numérique de l'organisation*

TP 1
Protéger l'identité numérique de M@Banque

Bloc 3 - Cybersécurité des services informatiques

EVALUATION DES COMPETENCES VISEES						
Compétence(s) Visée(s)	**Savoir-Faire(s)**	**Niveau d'acquisition**				
		A	B	C	D	E
B3.2 Préserver l'identité numérique de l'organisation	**Protéger l'identité numérique d'une organisation**					

Mission

La défiguration du site de M@Banque a montré la nécessité d'informer les clients sur les moyens de vérification de l'intégrité d'un site Web pour éviter que leurs outils numériques (smartphones, ordinateurs, tablettes, etc.) ne soient infectés.

Cette action doit apporter une contre-mesure utile pour rétablir la confiance des clients en démontrant la capacité de M@Banque à protéger son identité numérique.

Votre mission est de tester et réaliser un comparatif de solutions permettant l'audit du site Web de M@Banque.

Pour ce travail, vous allez prendre pour exemple le site de votre concurrent direct : **https://n26.com/fr-fr**

Travail à faire

1 - Complétez le tableau d'organisation de la veille technologique.

Document 1

Fiches méthode 1 et 2, p203 et p205

Utilisez un tableau pour comparer plusieurs sources d'information. Cela vous aidera dans votre veille technologique. Les sources d'information choisies peuvent provenir de différents supports (sites, blog, magazine, livre, vidéo…).

Vous trouverez dans le tableau ci-dessous un exemple déjà complété et un autre à compléter. Trouvez-en 1 ou 2 autres supplémentaires (à vous de choisir).

Chaque critère d'évaluation de la qualité et de la pertinence de l'information sera noté de 1 à 4 (1 étant la note signalant que le critère n'est pas du tout respecté).

Objectif de la veille technologique	**Comparer des solutions permettant l'audit du site Web de M@Banque**					
Sources d'information	**Crédibilité de l'auteur**	**Fiabilité de la source**	**Objectivité de l'information**	**Exactitude de l'information**	**Actualité de l'information**	**Pertinence de l'information**
Exemple 1 site **Blog :** https://blog.hubspot.fr/marketing/outils-seo-analyser-site	**1** **Erell Le Gall (blogueuse pour la société HubSpot)**	**1** **(Société commerciale HubSpot)**	**2** **(Société commerciale qui propose des logiciels favorisant le référencement de site)**	**2** **(Société commerciale HubSpot)**	**3** **(22/09/2022)**	**3** **(L'article répond au sujet traité.)**
Exemple 2 site **Site :** https://www.journalducm.com/realiser-audit-site-web/						

2 - Préparez et paramétrez un dispositif de veille juridique sur les outils d'audits de sécurité de sites Web. Ce dispositif doit comprendre un outil de collecte, de traitement, de curation, de partage de l'information.

Document 2 et fiches méthode 1 et 2

L'objectif ici est de préparer et de paramétrer un **dispositif de veille technologique** et non de veille juridique. Ce travail peut prendre appui sur la fiche méthode 2, p. 205.

L'objectif, pour vous, est de comprendre le processus d'une veille technologique (fiche méthode 1) et de maîtriser les outils qu'elle met en place. Plusieurs outils sont présentés dans la fiche méthode 2 mais la liste n'est pas exhaustive.

2.1 - Proposez et mettez en place au moins un outil de collecte

2.2 - Proposez et mettez en place au moins un outil de traitement ou de curation

2.3 - Proposez et mettez en place au moins un outil de partage et de diffusion des résultats de la veille

2.4 - Il y a aussi les sites Web et wiki…

3 - Retrouvez au moins un autre outil d'audits de sécurité de sites Web à l'aide des résultats de vos recherches.

Voici un exemple d'outils supplémentaires d'audit de sécurité d'un site web :

Dubbed Observatory (https://observatory.mozilla.org) : outils de vérification des mécanismes de sécurité développés par un ingénieur en sécurité de Mozilla.

Il évalue notamment la configuration SSL/TLS (cf. article sur le sujet : https://www.lemondeinformatique.fr/actualites/lire-mozilla-lance-un-outil-gratuit-d-analyse-de-la-securite-des-sites-web-65748.html).

4 - Testez les outils d'audits de sécurité de sites Web en prenant pour cible celui de votre principal concurrent. Complétez le tableau comparatif mis à disposition.

Documents 3 et 4

Critères d'analyse	Google Safe-Browsing	UrlVoid	Dubbed Observatory
Protection des cookies			
Content security policy (abrégé CSP) est un mécanisme de sécurité standardisé permettant de restreindre l'origine du contenu (tel qu'un script Javascript, une feuille de style, etc.) dans une page web à certains sites autorisés. Il permet notamment de mieux se prémunir contre des attaques d'injection de code.			
Utilisation du protocole HTTPS			
Spywares*, virus ou *adwares			
Injection de code SQL ou XML			
Site douteux			
URL outil			
...			

5 - Rédiger une note à l'intention de M^{me} Schmitt, la *community manager*, afin de lui fournir les informations lui permettant d'adresser aux clients un courrier présentant clairement la nécessité d'utiliser la solution retenue pour vérifier l'intégrité du site de M@Banque.

Document 1

La qualité et la pertinence des informations collectées

Objectifs de la veille technologique						
Sources d'informations	Crédibilité de l'auteur	Fiabilité de la source	Objectivité de l'information	Exactitude de l'information	Actualité de l'information	Pertinence de l'information
Exemple : site Web...						
Évaluation						

Chaque critère d'évaluation de la qualité des sources d'information sera noté de 1 à 4 (1 étant la note indiquant que le critère n'est pas du tout respecté).

Document 2

Les outils de collecte, traitement, curation et partage de l'information

	Outil de collecte de l'information	Outil de traitement de l'information	Outil de curation de l'information	Outil de partage des résultats
Nom de l'outil				
Avantages				
Inconvénients				

Document 3

Tester en ligne la sécurité d'un site Web

Le test de sécurité permet de s'assurer qu'un site n'est pas infecté par un malware, victime d'une défiguration, blacklisté ou encore utilisé pour spammer. L'attaque d'un site devient visible et problématique quand :

- une marque concurrente informe l'entreprise que son site est utilisé pour vendre illégalement des produits
- quand le site se met à dysfonctionner.

Il existe de nombreux outils en ligne gratuits pour tester et vérifier l'intégrité d'un site Web. Ces outils ne mesurent pas l'intégrité des sites selon les mêmes critères et sont plus ou moins performants. Il existe, par exemple :

- le Google Safe Browsing : https://transparencyreport.google.com/safe-browsing/search
- le URLVoid : https://www.urlvoid.com/

Document 4

Un tableau comparatif des outils d'audits de sécurité de site Web

Critères d'analyse	Google Safe Browsing	URLVoid
Malware		
Spam		
...		