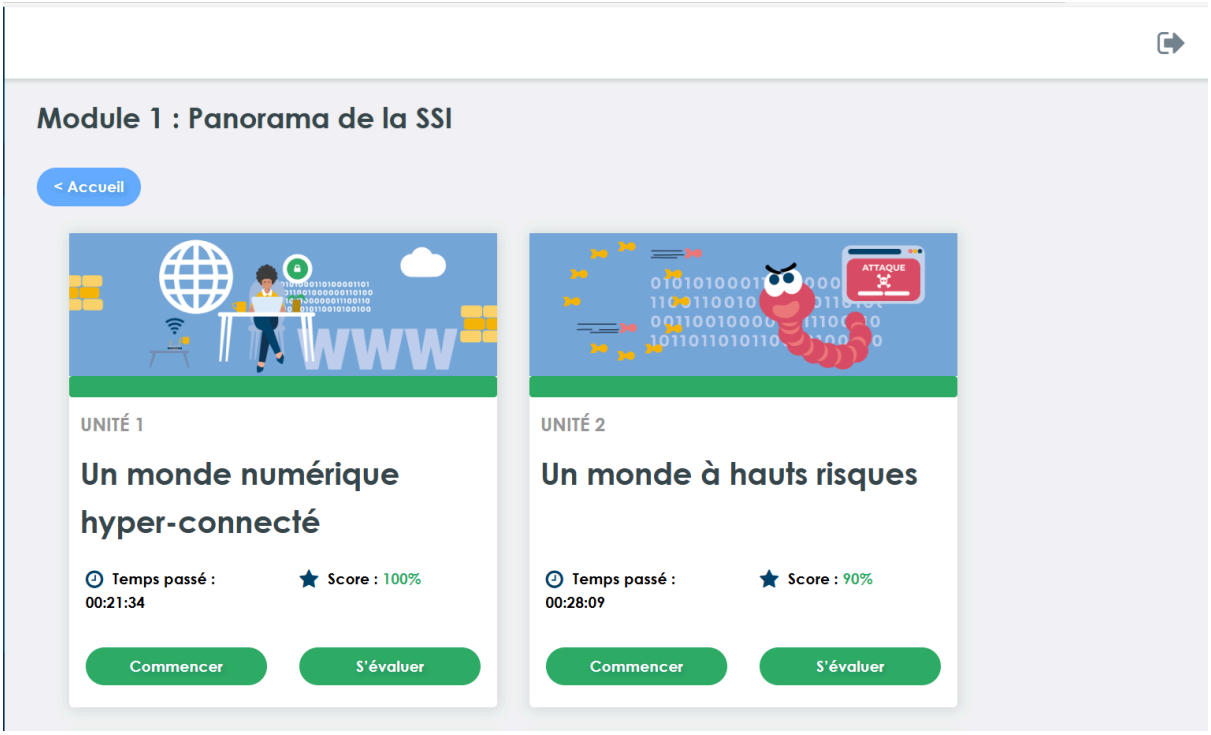
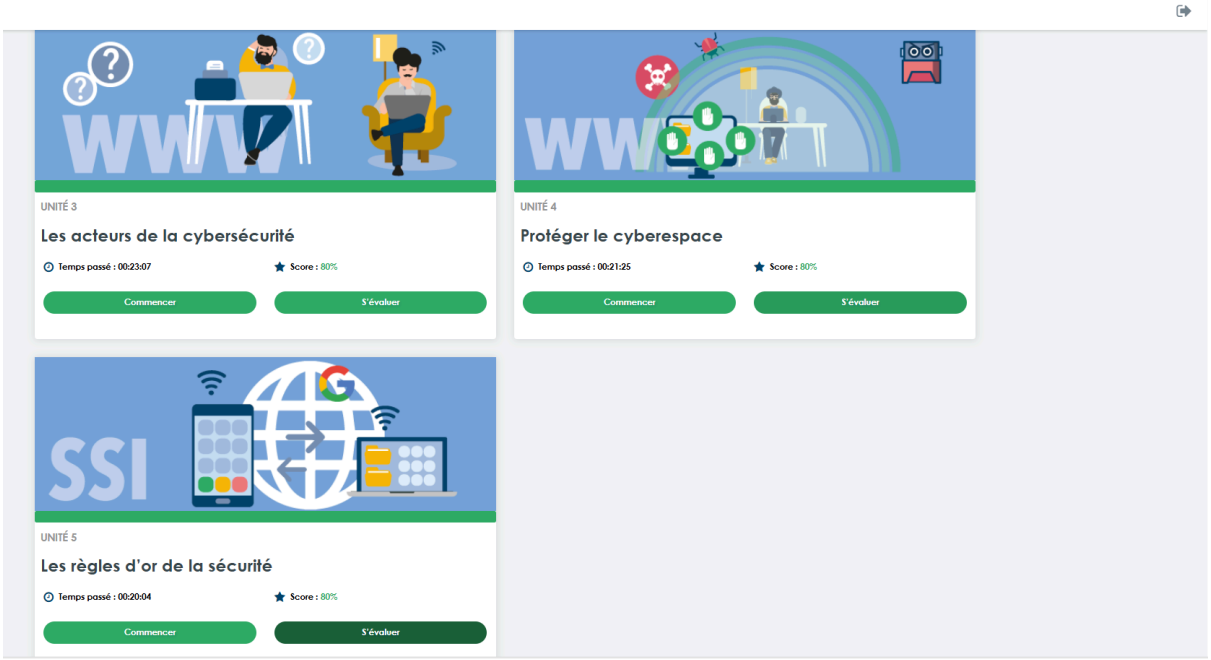
Mission 7 premier module





Compte rendu premier modul

Déjà, j'ai appris qu'en France, il y a des secteurs qu'on appelle "OIV" ça veut dire "Opérateurs d'Importance Vitale". Ce sont des domaines comme l'énergie, la santé, les transports… et il y en a 12 en tout. C'est super important de les protéger parce qu'ils sont essentiels pour le pays.

Ensuite, j'ai vu que l'ANSSI est l'agence qui s'occupe de la sécurité informatique en France. Elle fait plein de choses : elle informe les gens, elle qualifie des produits, elle aide à détecter les attaques et elle accompagne les OIV. Par contre, elle ne déchiffre pas les données bloquées par des virus comme les rançongiciels, ça c'est autre chose.

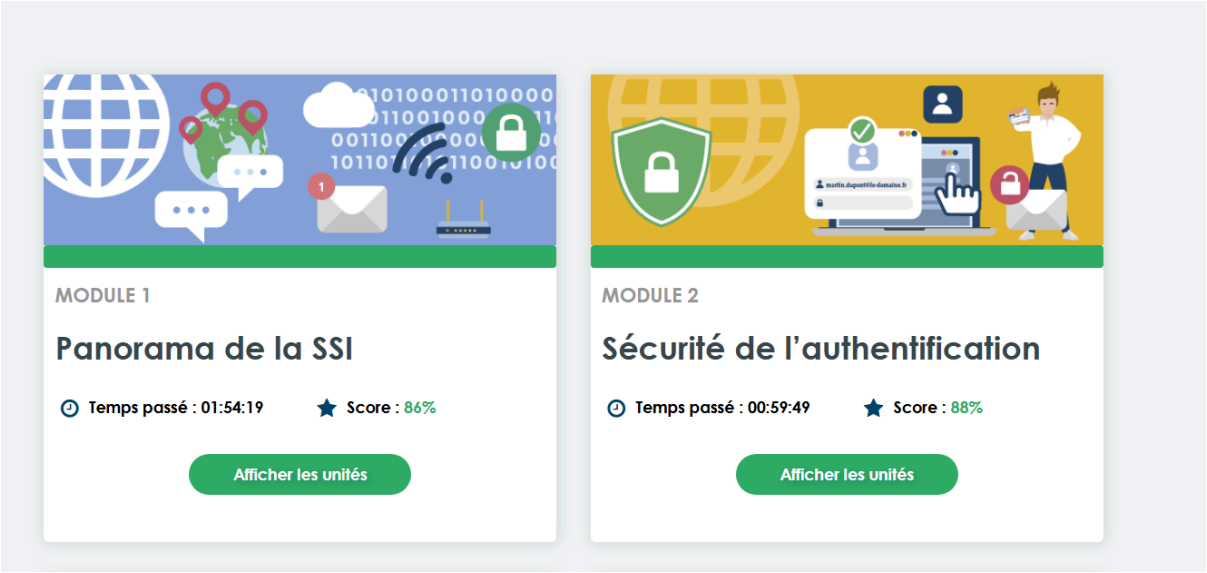
J'ai aussi découvert qu'il y a plusieurs acteurs qui travaillent dans la cybersécurité : la Gendarmerie, le Ministère de la Défense, la DGA, le CALID, le Ministère de la Justice… et même une unité spéciale de la police qui s'appelle l'OCLCTIC, qui lutte contre la criminalité sur Internet.

Côté pratique, j'ai compris que si on utilise un mot de passe trop simple, un pirate peut facilement accéder à nos infos, se faire passer pour nous, salir notre image ou même piéger nos contacts. Et si quelqu'un nous donne une clé USB, il ne faut surtout pas la brancher directement. Il vaut mieux la donner au service informatique ou la analyser avant.

J'ai aussi appris ce qu'est une donnée : c'est une information numérique, pas un objet physique ni une formation. Et il faut bien la protéger. Par exemple, si on envoie un mail à la mauvaise personne, ou si on se fait voler son téléphone ou son ordi, ça peut mettre en danger la confidentialité des données.

Pour bien stocker les données, il faut les chiffrer, les mettre dans un dossier privé et limiter les accès aux personnes autorisées. Et selon leur niveau de sensibilité, on peut définir comment elles doivent être échangées, stockées ou détruites.

Bref, j'ai compris que la cybersécurité, ce n'est pas juste pour les pros de l'informatique. Ça concerne tout le monde, et il y a plein de réflexes simples à avoir pour éviter les problèmes.



compte rendu 2 eme module

Ce module explique comment prouver son identité de manière fiable lorsqu'on se connecte à un service en ligne. Il montre la différence entre identification (dire qui on est) et authentification (prouver qu'on est bien cette personne).

On y découvre les trois facteurs d'authentification :

- quelque chose que l'on sait (mot de passe, code PIN),
- quelque chose que l'on possède (téléphone, carte à puce),
- quelque chose que l'on est (empreinte, visage).

Le cours insiste sur l'importance de mots de passe forts et uniques, et recommande d'utiliser un gestionnaire de mots de passe pour les stocker. Il encourage aussi à activer la double authentification (2FA), qui combine deux moyens différents pour se connecter plus sûrement.

Enfin, le module rappelle les bons réflexes : ne jamais partager ses identifiants, se méfier du phishing, et changer rapidement un mot de passe en cas de doute.