1. Identifier les différents types de pirates.

Il existe plusieurs types de pirates ayant des motifs d'attaques différents : du hacker isolé agissant par vengeance ou démonstration de compétence, au groupe de hackers organisé ayant pour objectif de revendre ses services pour déstabiliser des entreprises, ou de revendre des informations subtilisées dans des bases de données non-sécurisées comme des informations bancaires ou des données nominatives.

2. Lister et définir les types de menaces ainsi que les protections possibles pour s'en prémunir.

Les différents types de menaces sont :

Le phishing - Hameçonnage en français est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer ses données personnelles.
Le virus - C'est un programme malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire.
Le Cheval de Troie - Se présente comme un logiciel légitime ou anodin, mais une fois introduit dans le système, se comporte en réalité de façon malveillante.
Le déni de service ou DDoS - Rendre un service, un serveur ou une infrastructure indisponible. L'attaque peut prendre différentes formes : une saturation de la bande passante du serveur pour le rendre injoignable, un épuisement des ressources système de la machine, l'empêchant ainsi de répondre au trafic légitime. Il est recommandé de déployer des équipements de filtrage en bordure du système
Le Spyware - Logiciel malveillant qui infecte votre PC ou appareil mobile et qui collecte des informations vous concernant, vos habitudes de navigation et d'utilisation d'Internet ainsi que d'autres données. Il est recommandé de supprimer les logiciels espions de votre PC et d'utiliser un antivirus.
Le ver - Logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il est recommandé d'installer un logiciel de protection contre les programmes malveillants sur tous vos ordinateurs et périphériques et de le mettre régulièrement à jour.
Le Crypto virus/Ransomware - Logiciel malveillant disposant du même fonctionnement que le virus ransomware et le cheval de Troie. Pour empêcher ce virus, un antivirus ne sert à rien mais il est important de réaliser des sauvegardes régulières. Il est recommandé d'utiliser un Cloud.
Le botnet - Un ensemble d'appareils connectés à Internet sur lesquels s'exécutent un ou plusieurs robots. Les protections utiles sont de maintenir ses logiciels à jour, surveiller étroitement votre réseau, surveiller les tentatives de connexion ayant échoué et mettre en œuvre une solution avancée de détection des botnets.

3. Lister les motivations des pirates menant aux attaques.

Les motivations des pirates menant des attaques sont :
L'attaque étatique - Elles sont très ciblées, leur degré de sophistication et l'utilisation de vulnérabilités inconnues de manière coordonnée.
L'espionnage - Utilisée pour la recherche ou le Télécom, l'énergie, les petites entreprises, la santé et l'aéronautique.
La vengeance - Par exemple un ancien employé qui récupère les codes et peut attaquer les données et les revendre
Le vol des données - Les pirates accèdent à la machine de la victime, une fois fait il récupère les données et demande une rançon.

4. Lister les conséquences des attaques sur l'organisation les subissant.

Les conséquences des attaques sur l'organisation est la perte financière et l'atteinte à l'image

5. Compléter l'évaluation finale de cette unité jusqu'à obtenir un score satisfaisant

Votre score : 70%