Séance 2 : CyberShield (La Cybersécurité)

Durée totale : 75 minutes

Mise en contexte (15 min) :

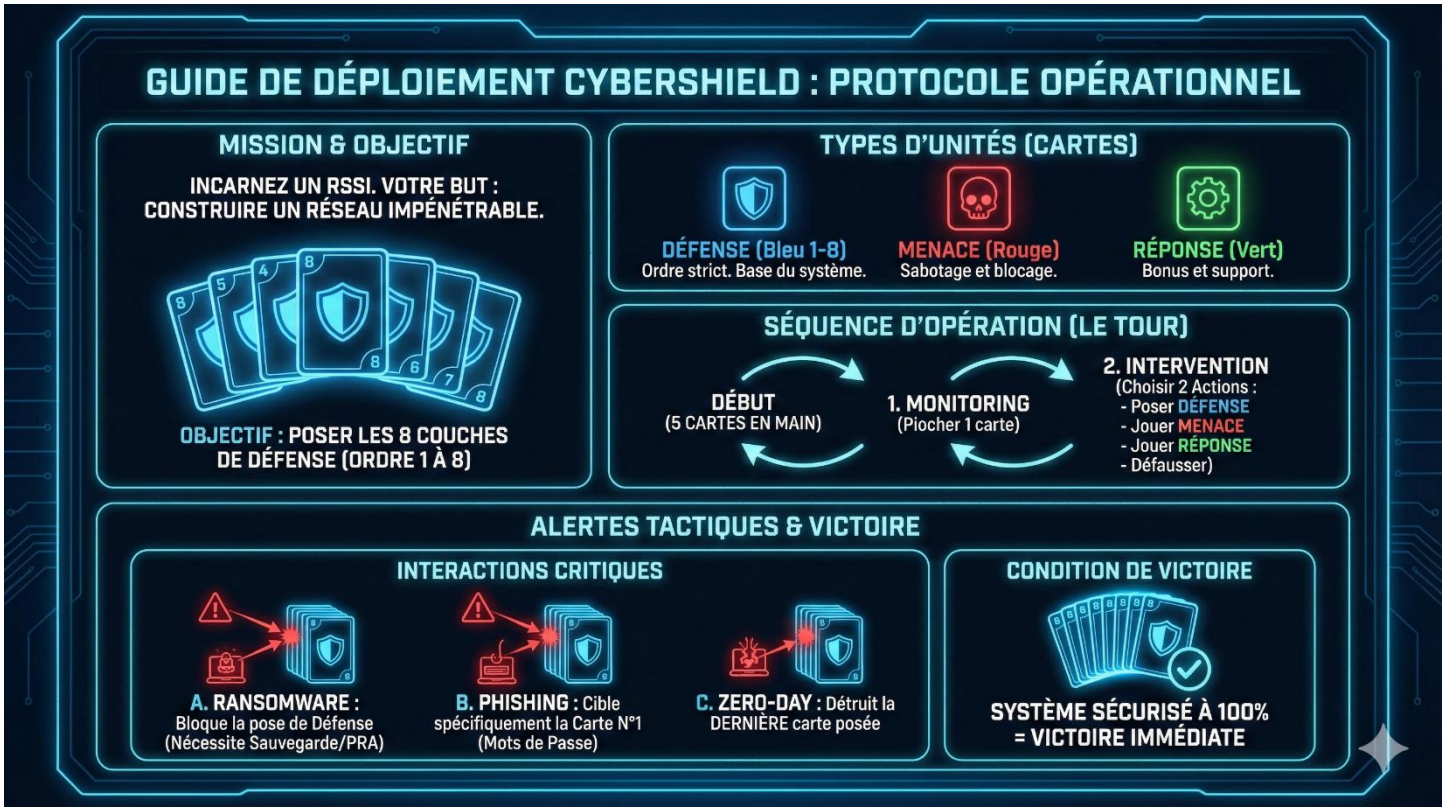
Scénario : "Vous êtes le responsable sécurité d'une mairie. Une cyberattaque mondiale est en cours. Votre mission : sécuriser vos serveurs."
Tour d'horizon des types d'attaques (Rouge) et de défenses (Bleu).

Mise en jeu (40 min) :

Partie de jeu : L'ambiance doit être un peu plus "tendue". L'animateur peut annoncer des "événements mondiaux" (ex : "Nouvelle faille Zero-Day découverte, tout le monde défausse sa dernière carte !") pour dynamiser.

Le Tour de Table de l'Expert (20 min) :

Analyse : "Quelle attaque a été la plus dévastatrice ? (Souvent le Ransomware). Comment la carte 'Sauvegarde' vous a-t-elle sauvé ?"
Transfert : "Dans votre vie professionnelle, quel est votre premier réflexe si vous recevez un mail suspect (Phishing) ?"
Conclusion : Rappel de la règle d'or : La sécurité est une chaîne, elle a la force de son maillon le plus faible.



1 MOTS DE PASSE FORTS

La première ligne de défense.

Utilisez des combinaisons longues, uniques et complexes pour verrouiller vos comptes.

2 DOUBLE AUTHENTIFICATION (MFA)

Une couche de sécurité supplémentaire.

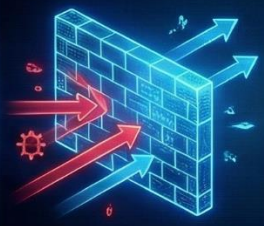
Exige un second facteur (code SMS, appli) pour valider l'accès.

3 CHIFFREMENT DES DONNÉES

Rend vos informations illisibles pour les pirates.

Seuls ceux qui possèdent la clé peuvent les déchiffrer.

4 PARE-FEU (FIREWALL)



Le garde-barrière du réseau.

Filtre le trafic entrant et sortant pour bloquer les connexions suspectes.

5 ANTIVIRUS / EDR

Détecte et neutralise les logiciels malveillants en temps réel.

L'EDR surveille aussi les comportements suspects.

6 MISES À JOUR (PATCHING)

Installe les derniers correctifs de sécurité.

Comble les failles avant que les pirates ne les exploitent.

7 VPN (RÉSEAU PRIVÉ VIRTUEL)

Crée un tunnel chiffré pour votre connexion internet.

Protège vos données et masque votre emplacement.

8 SAUVEGARDE (BACKUP)

La copie de sécurité ultime.

Permet de restaurer vos données en cas de perte, vol ou attaque ransomware.

AUDIT DE SÉCURITÉ

Permet de regarder la main d'un adversaire.

Révèle ses cartes Attaque et Défense.

PLAN DE REPRISE (PRA)

Permet de récupérer une carte de défense de votre choix dans la défausse et de l'ajouter à votre main.

SENSIBILISATION

Protège contre toutes les attaques de type "Phishing" ou "Clé USB Piégée" pendant votre prochain tour.

BUG BOUNTY

Vous trouvez une faille et la signalez.

Piochez immédiatement 2 cartes supplémentaires.

PHISHING (HAMEÇONNAGE)

Un faux email pour voler les identifiants.

Si l'attaque réussit, le joueur ciblé doit défausser sa carte "Mots de Passe Forts".

RANSOMWARE

Crypte les données.

Le joueur ciblé ne peut plus poser de carte de défense tant qu'il n'a pas joué une "Sauvegarde".

ATTAQUE BRUTE FORCE

Une machine teste des milliers de mots de passe.

Force le joueur ciblé à révéler sa main et à défausser une carte de défense.

ZERO-DAY (FAILLE INCONNUE)

Une faille critique sans correctif.

Contourne n'importe quelle défense. Le joueur ciblé doit retirer la dernière carte de défense qu'il a posée.