SECURITY

Les anti-virus

Objectif

- Expliquer l'utilité d'un antivirus dans la protection d'un système informatique.
- Décrire les principaux types de logiciels malveillants pris en charge par un antivirus.
- Comprendre les méthodes de détection : signatures, heuristique, analyse comportementale.
- Expliquer le principe de la quarantaine.
- Identifier les limites d'un antivirus et les bonnes pratiques à adopter pour compléter la protection.

Qu’est-ce qu’un antivirus ?

- Programme conçu pour protéger un ordinateur contre les logiciels malveillants.
- Surveille le système en permanence.
- Empêche, détecte et supprime les menaces.

Pourquoi un antivirus est-il indispensable ?

- Les malwares peuvent voler des données ou endommager le système.
- Les attaques sont fréquentes : mails piégés, téléchargements douteux, sites compromis.
- L'antivirus réduit les risques et protège l'utilisateur.

Les types de menaces détectées

- Virus classiques
- Vers, chevaux de Troie
- Ransomwares
- Spywares et adwares

Principe de fonctionnement général

- Analyse des fichiers et programmes.
- Détection grâce aux signatures (base de données).
- Détection comportementale (analyse en temps réel).

Analyse par signatures

- L'antivirus compare les fichiers à une base de données de malwares connus.
- Très efficace contre les menaces déjà identifiées.
- Nécessite des mises à jour régulières.

Analyse heuristique et comportementale

- Observation des actions suspectes (modification du registre, accès réseau anormal…).
- Permet de détecter des menaces inconnues (zero-day).
- Réduit les risques d'infection avant mise à jour des signatures.

Analyse en temps réel

- Vérifie chaque fichier ouvert ou exécuté.
- Bloque l'action avant qu'elle n'endommage le système.
- Fonctionne en arrière-plan.

Quarantaine

- Isolement d'un fichier suspect.
- Permet de vérifier s'il s'agit d'un vrai malware ou d'un faux positif.
- Empêche toute exécution dangereuse.

Limites d’un antivirus

- Ne protège pas à 100 %.
- Ne compense pas des comportements imprudents (téléchargements, clics hasardeux).
- Complément nécessaire : pare-feu, mises à jour, bonnes pratiques.

Bonnes pratiques de sécurité

- Mettre l'antivirus à jour.
- Analyser régulièrement le système.
- Ne pas ouvrir de pièces jointes douteuses.
- Télécharger uniquement depuis des sources fiables.