# TP 01 d'utilisation de Python/Pandas dans le cadre de la cybersécurité

**Table des matières**

*On va analyser des fichiers de logs pour détecter des activités suspectes, telles que des tentatives répétées de connexion échouée.*

# I. Détection de tentatives de connexion échouées

## A. Étape 1 : Charger les données de logs

On suppose que nous avons un fichier de logs au format CSV contenant des informations comme l'adresse IP, la date, et le statut de la connexion.

### 1. Exemple de fichier logs.csv :

timestamp,ip_address,status

2025-01-05 12:34:56,192.168.1.10,success

2025-01-05 12:35:01,192.168.1.11,failed

2025-01-05 12:35:05,192.168.1.11,failed

2025-01-05 12:35:10,192.168.1.11,failed

2025-01-05 12:36:00,192.168.1.12,success

## B. Étape 2 : Code Python pour analyser les logs

Créer en python avec la librairie Pandas, l'algorithme suivant :

- Charger les données (le fichier logs.csv)
- Filtrer uniquement les connexions échouées
- Compter le nombre de tentatives échouées par adresse IP
- Détecter les IPs avec plus de 2 tentatives échouées
- Afficher le résultat à l'écran

## C. Étape 3 : Résultat attendu

En exécutant ce script, vous obtiendrez une liste des adresses IP suspectes avec un nombre élevé de connexions échouées :

Adresses IP suspectes :

ip_address failed_count

1 192.168.1.11 3

## D. Explications :

1. **Filtrage** : On isole les tentatives de connexion échouées.
2. **Groupement** : On regroupe par adresse IP pour compter les échecs.
3. **Détection** : On identifie les IPs ayant dépassé un seuil défini (ici 2 échecs).
   Ce type d'analyse peut être utilisé pour alimenter un système de détection d'intrusion ou générer des alertes.