Atelier IAM – SSO, OAuth2, OIDC et SAML

Exercice 1 – Comprendre le SSO

1. Expliquer simplement ce que signifie *SSO*.
2. Donner un exemple où l'on utilise du SSO.
3. Pourquoi le SSO est-il utile dans une entreprise qui utilise 10 applications différentes ?
4. Quels risques le SSO peut-il introduire s'il est mal configuré ?

Exercice 2 – OAuth2 : délégation d'accès

1. Identifier les 4 acteurs d'OAuth2 et leur rôle.
2. Pourquoi dit-on qu'OAuth2 est un protocole de délégation et pas d'authentification ?
3. Donner un exemple concret d'application qui utilise OAuth2.
4. Explique le rôle du **jeton d'accès**..

Exercice 3 – De OAuth2 vers OIDC

1. Quelle est la principale limite d'OAuth2 si on veut l'utiliser comme un système de connexion (SSO) ?
2. Qu'ajoute OpenID Connect (OIDC) à OAuth2 pour résoudre ce problème ?
3. Dans OIDC, quel est le rôle de l'**ID Token** par rapport au **Access Token** ?
4. Citer un exemple concret d'application qui utilise OIDC aujourd'hui.

Exercice 4 – Comparaison OIDC et SAML

1. Classer chaque technologie dans sa catégorie : SAML ou OIDC ?
    - Basé sur XML
    - Basé sur JSON
    - Utilisé surtout dans les environnements historiques, entreprise
    - Utilisé surtout dans les applications modernes, web et mobiles
2. Donner un cas où une entreprise préférerait SAML, et un cas où elle préférerait OIDC.
3. Résumer en une phrase la différence majeure entre SAML et OIDC.

Exercice 5 – Cas pratique

Tu es RSSI d'une PME. Tu dois mettre en place un SSO pour :

- Accéder à Microsoft 365
- Accéder à une application SaaS moderne (Slack)
- Accéder à un vieux portail interne basé sur Java et XML

Questions :

1. Quel protocole utiliserais-tu pour Microsoft 365 ?
2. Quel protocole utiliserais-tu pour Slack ?
3. Quel protocole utiliserais-tu pour le portail interne ?
4. Pourquoi ne pas utiliser uniquement un seul protocole pour tout ?