Réponses types – Questions courantes en entretien Entra ID / M365

## Comment gères-tu l’activation MFA pour tous les utilisateurs ?

J’utilise des stratégies d’accès conditionnel pour appliquer le MFA en fonction de groupes, d’applications ou de niveaux de risque. Cela permet plus de flexibilité et évite de devoir l’activer manuellement utilisateur par utilisateur.

## Quels sont les niveaux de risque dans Microsoft Identity Protection ?

Il y a trois niveaux : faible, moyen et élevé. Ils sont basés sur des signaux tels que les connexions inhabituelles, les emplacements suspects, ou les fuites de mots de passe. Ces niveaux permettent d’adapter les réponses de sécurité.

## As-tu déjà travaillé avec les access reviews ? Pourquoi sont-elles importantes ?

Oui. Les access reviews permettent de s’assurer que les utilisateurs n’ont pas plus de droits que nécessaire. Elles sont utiles pour respecter le principe du moindre privilège et maintenir une sécurité continue dans l’entreprise.

## Peux-tu expliquer une stratégie d’accès conditionnel que tu mettrais en place ?

J’appliquerais une règle qui exige le MFA si l’utilisateur se connecte depuis un pays à risque ou un appareil inconnu. Je pourrais aussi bloquer l’accès à certaines applications sensibles en dehors du réseau d’entreprise.

## Comment limiter l’accès d’un compte à privilèges en mobilité ?

Je configure une politique d’accès conditionnel qui interdit l’utilisation de comptes à privilèges en dehors des emplacements approuvés, et j’impose MFA avec des sessions limitées dans le temps. Je recommande aussi d’utiliser un poste dédié sécurisé.

## Quelles sont les meilleures pratiques pour la gestion des mots de passe dans Microsoft 365 ?

Je recommande de : 1) imposer le MFA pour réduire la dépendance aux mots de passe, 2) désactiver l’expiration automatique mais suivre les activités, 3) activer la protection contre les mots de passe faibles via Azure AD Password Protection.

## Comment crées-tu un compte utilisateur en ligne de commande ?

Avec PowerShell et le module AzureAD ou MSOnline :  
`New-AzureADUser` ou `New-MsolUser` pour créer un compte, suivi de `Set-MsolUserLicense` pour assigner une licence.

## Quelles sont les étapes pour attribuer une licence M365 à un utilisateur via PowerShell ?

1) Connect-MsolService  
2) Get-MsolUser -UserPrincipalName user@domain.com  
3) Set-MsolUserLicense -UserPrincipalName user@domain.com -AddLicenses 'domain:ENTERPRISEPACK'

## Comment récupères-tu la liste des utilisateurs sans MFA ?

Avec PowerShell ou via le portail M365 (Azure AD -> MFA -> rapport des utilisateurs). On peut aussi utiliser le script :  
`Get-MsolUser | Where-Object { $\_.StrongAuthenticationMethods.Count -eq 0 }`

## Comment automatise-t-on la désactivation des comptes inactifs ?

Je programme une tâche PowerShell qui interroge les utilisateurs dont la dernière connexion date de plus de 30 jours, et désactive automatiquement ces comptes après alerte. On peut aussi le faire via un workflow d’Entra ID.

## Quelles différences entre RBAC et ABAC ?

RBAC attribue les droits selon des rôles prédéfinis (ex : administrateur). ABAC ajoute des attributs dynamiques (poste, service, lieu) pour définir les accès. ABAC est plus granulaire et adapté aux environnements complexes.

## Quels journaux examines-tu en priorité après une alerte de sécurité ?

Je commence par les journaux de connexions, les journaux d’audit d’Entra ID, et ceux de Microsoft Defender for Cloud Apps. Je cherche les heures, IPs, actions inhabituelles, et croisements avec d’autres alertes.

## Comment interpréter une série d’échecs MFA ?

Cela peut indiquer une tentative de brute force, une erreur utilisateur, ou un changement d’appareil. Je corrèle ces échecs avec les journaux d’accès et déclenche une alerte si le comportement est anormal.

## Quels sont les signaux d’un compte compromis ?

Connexion depuis un nouveau pays, échec MFA répété, modification de règles de messagerie, ajout inattendu à des groupes administrateurs, activité à des heures inhabituelles, ou transfert de données massif.

## Comment configurer une alerte automatique sur une activité suspecte ?

Dans le portail Microsoft Defender ou Azure AD Identity Protection, je définis une règle pour générer une alerte en cas de comportement à risque. On peut aussi utiliser Microsoft Sentinel ou Power Automate pour réagir automatiquement.

## As-tu utilisé Microsoft Defender for Cloud Apps ?

Oui. Il permet de superviser l’usage des applications cloud, détecter les comportements anormaux, bloquer certaines applications non approuvées et créer des politiques de protection des données sensibles.

## Quelle différence entre Azure Monitor et Log Analytics ?

Azure Monitor est le service global de supervision, tandis que Log Analytics est le moteur d’analyse des journaux collectés via Azure Monitor. Ils travaillent ensemble pour surveiller et diagnostiquer les performances et incidents.

## À quoi sert Microsoft Sentinel ?

Sentinel est un SIEM cloud de Microsoft. Il collecte, analyse et corrèle les données de sécurité pour détecter les menaces, avec des capacités d’automatisation et d’investigation avancées.

## Comment relies-tu Power BI à des journaux Microsoft 365 ?

En important les données via Microsoft Graph API, Azure Log Analytics, ou directement depuis des exports CSV. Cela permet de créer des tableaux de bord en temps réel pour suivre les indicateurs de sécurité.

## As-tu déjà utilisé les alertes dans le centre de conformité ?

Oui. On peut créer des alertes pour surveiller des actions sensibles : partage externe, suppression massive de données, ajout d’un admin, etc. Elles sont utiles pour une réponse rapide aux incidents.

## Comment réagis-tu en cas de pression (alerte critique ou urgence) ?

Je respire, je priorise. Je commence par contenir l’incident (bloquer accès, informer les bonnes personnes), puis j’analyse la situation étape par étape. Je garde toujours un comportement calme et méthodique.

## Raconte-moi une situation où tu as dû résoudre un problème seul.

Lors de mon stage, j’ai découvert une vulnérabilité SQLi sur un site Joomla. J’ai documenté, testé et proposé moi-même une solution au superviseur. Cela a été validé et appliqué immédiatement, montrant que je pouvais agir de manière autonome.

## Qu’as-tu fait lorsqu’on t’a confié une tâche que tu ne maîtrisais pas encore ?

J’ai cherché à comprendre. J’ai consulté les ressources disponibles, testé l’outil ou la commande, et posé des questions ciblées. Cette méthode m’a toujours permis de progresser rapidement et de livrer un travail fiable.

## As-tu déjà travaillé avec des collègues non techniques ? Comment as-tu communiqué ?

Oui. Je m’adapte à leur niveau, j’évite les termes techniques et j’utilise des exemples concrets. Je m’assure qu’ils comprennent l’impact sans être submergés par des détails techniques.

## Quelle est ta plus grande fierté dans ton parcours jusqu’ici ?

Avoir mené seule une analyse de vulnérabilités complète sur le site du PNLS, détecté plusieurs failles critiques, proposé des correctifs concrets, et contribué à la sécurisation du site. C’était une vraie mission de confiance et de responsabilité.