Checklist DE Sécurité AZURE FOUNDATIONS

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v1.0 — 04 Avril 2026 · 210 controles

Sommaire

1.0 — IDENTITÉ ET GESTION DES ACCÈS (IAM)

1.1.1 *MFA obligatoire pour les administrateurs Azure*

MITRE ATT&CK : T1078.004

DESCRIPTION :
L'authentification multi-facteurs doit être activée pour tous les comptes avec des privilèges administratifs dans Azure AD. Cela inclut les rôles Global Admin, Security Admin, et autres rôles privilégiés.

AUDIT :
- Portal > Azure AD > Security > Conditional Access > Policies
- CLI: az ad user list --query "[?accountEnabled].userPrincipalName" --output table
- PowerShell: Get-AzADUser | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.AccountEnabled -eq }

REMÉDIATION :
1. Portal > Azure AD > Security > Conditional Access
2. Create new policy "Require MFA for Admins"
3. Assign to admin groups/roles
4. Grant controls > Require MFA

VALEUR PAR DÉFAUT :
Désactivé

1.1.2 *MFA obligatoire pour tous les utilisateurs privilégiés*

MITRE ATT&CK : T1078.004

DESCRIPTION :
Tous les utilisateurs ayant des accès privilégiés aux ressources Azure doivent utiliser MFA, y compris les propriétaires de ressources et contributeurs sur des services critiques.

AUDIT :
- Portal > Azure AD > Sign-ins > Filter by Conditional Access status
- CLI: az ad signed-in-user show
- PowerShell: Get-AzContext

REMÉDIATION :
1. Identifier tous les comptes privilégiés
2. Créer une politique Conditional Access ciblée
3. Configurer l'exigence MFA
4. Test en mode report-only puis activation

VALEUR PAR DÉFAUT :
Désactivé

1.1.3 *Méthodes MFA sécurisées configurées*

MITRE ATT&CK : T1621

DESCRIPTION :
Les méthodes MFA faibles (SMS/appels vocaux) doivent être désactivées au profit des méthodes sécurisées (Microsoft Authenticator, FIDO2, Windows Hello).

AUDIT :
- Portal > Azure AD > Security > Authentication methods
- CLI: az rest --method get --url https://graph.microsoft.com/beta/policies/authenticationMethodsPolicy
- PowerShell: Get-MgPolicyAuthenticationMethodPolicy

REMÉDIATION :
1. Portal > Azure AD > Security > Authentication methods > Policies
2. Désactiver SMS et Voice call
3. Activer Microsoft Authenticator (passwordless)
4. Configurer FIDO2 security keys

VALEUR PAR DÉFAUT :
SMS et appels vocaux activés

1.2 — CONDITIONAL ACCESS

1.2.1 *Politique de blocage des pays à risque*

MITRE ATT&CK : T1078

DESCRIPTION :
Les connexions depuis des pays non autorisés doivent être bloquées automatiquement via Conditional Access pour réduire les risques de compromission.

AUDIT :
- Portal > Azure AD > Security > Conditional Access > Named locations
- CLI: az rest --method get --url https://graph.microsoft.com/v1.0/identity/conditionalAccess/policies
- PowerShell: Get-AzADConditionalAccessPolicy

REMÉDIATION :
1. Créer Named Locations pour pays autorisés
2. Créer politique CA "Block Risky Countries"
3. Condition : Locations (exclude trusted countries)
4. Grant : Block access

VALEUR PAR DÉFAUT :
Aucune restriction géographique

1.2.2 *Accès conditionnel basé sur les risques utilisateur*

MITRE ATT&CK : T1078.004

DESCRIPTION :
Azure AD Identity Protection doit détecter et bloquer automatiquement les connexions à haut risque basées sur le comportement utilisateur anormal.

AUDIT :
- Portal > Azure AD > Security > Identity Protection > User risk policy
- CLI: az rest --method get --url https://graph.microsoft.com/beta/identity/riskyUsers
- PowerShell: Get-AzADIdentityProtectionRiskyUser

REMÉDIATION :
1. Activer Azure AD P2 license
2. Portal > Identity Protection > User risk policy
3. Configuration : High risk = Block access
4. Medium risk = Require MFA + password change

VALEUR PAR DÉFAUT :
Désactivé (nécessite P2)

1.2.3 *Accès conditionnel pour applications cloud*

MITRE ATT&CK : T1078.004

DESCRIPTION :
Toutes les applications cloud critiques doivent avoir des politiques d'accès conditionnel spécifiques avec contrôles de sécurité appropriés.

AUDIT :
- Portal > Azure AD > Enterprise applications > Conditional Access
- CLI: az ad app list --query "[].{appId:appId,displayName:displayName}"
- PowerShell: Get-AzADApplication

REMÉDIATION :
1. Inventaire des applications critiques
2. Créer politiques CA par application
3. Conditions : Device compliance, Location, Risk
4. Grant controls : MFA, Compliant device, etc.

VALEUR PAR DÉFAUT :
Aucune politique spécifique

1.3 — PRIVILEGED IDENTITY MANAGEMENT (PIM)

1.3.1 *PIM activé pour les rôles administrateurs*

MITRE ATT&CK : T1078.003

DESCRIPTION :
Azure AD Privileged Identity Management doit être activé pour tous les rôles administratifs sensibles, permettant l'accès just-in-time et l'audit des privilèges.

AUDIT :
- Portal > Azure AD > Privileged Identity Management > Azure AD roles
- CLI: az rest --method get --url https://graph.microsoft.com/beta/privilegedAccess/azureAD/roleAssignments
- PowerShell: Get-AzADPIMEligibleRoleAssignment

REMÉDIATION :
1. Activer Azure AD P2 license
2. Portal > PIM > Azure AD roles > Discover resources
3. Configurer rôles éligibles (eligible assignments)
4. Supprimer assignations permanentes

VALEUR PAR DÉFAUT :
Désactivé (nécessite P2)

1.3.2 *Activation PIM avec justification obligatoire*

MITRE ATT&CK : T1078.003

DESCRIPTION :

L'activation des rôles privilégiés via PIM doit exiger une justification métier et une approbation selon le niveau de criticité du rôle.

AUDIT :

- Portal > PIM > Azure AD roles > Settings > Role settings
- CLI: Vérifier via Microsoft Graph API
- PowerShell: Get-AzADPIMRoleSettings

REMÉDIATION :

1. PIM > Role settings > Configure chaque rôle
2. Activation : Require justification
3. Activation : Require approval pour rôles critiques
4. Maximum duration : 8 heures maximum

VALEUR PAR DÉFAUT :

Aucune justification requise

1.3.3 *Révision d'accès PIM automatisée*

MITRE ATT&CK : T1078

DESCRIPTION :

Des révisions d'accès automatisées doivent être configurées pour valider périodiquement que les assignations de rôles privilégiés sont toujours justifiées.

AUDIT :

- Portal > PIM > Azure AD roles > Access reviews
- CLI: az rest --method get --url https://graph.microsoft.com/beta/accessReviews
- PowerShell: Get-AzADAccessReview

REMÉDIATION :

1. PIM > Access reviews > New access review
2. Scope : Eligible role assignments
3. Reviewers : Resource owners + managers
4. Recurrence : Quarterly pour rôles critiques

VALEUR PAR DÉFAUT :

Aucune révision automatisée

1.4 — RÔLES ET PERMISSIONS (RBAC)

1.4.1 *Principe du moindre privilège appliqué*

MITRE ATT&CK : T1078

DESCRIPTION :

Les utilisateurs et services doivent avoir uniquement les permissions minimales nécessaires pour accomplir leurs tâches, avec usage préférentiel des rôles intégrés plutôt que Owner ou Contributor.

AUDIT :

- Portal > Subscriptions > Access control (IAM) > Role assignments
- CLI: az role assignment list --include-inherited --include-groups
- PowerShell: Get-AzRoleAssignment

REMÉDIATION :

1. Audit des assignations actuelles
2. Identifier les sur-privilèges (Owner, Contributor)
3. Remplacer par rôles spécifiques (Reader, VM Contributor, etc.)
4. Documenter justifications métier

VALEUR PAR DÉFAUT :

Souvent sur-privilégié

1.4.2 *Limitation des propriétaires de souscriptions*

MITRE ATT&CK : T1078

DESCRIPTION :

Le nombre de propriétaires (Owner) de souscriptions Azure doit être limité au strict minimum (2-3 maximum) et faire l'objet d'un contrôle strict.

AUDIT :

- Portal > Subscriptions > Access control (IAM) > Filter by Owner role
- CLI: az role assignment list --role Owner --include-inherited
- PowerShell: Get-AzRoleAssignment | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.RoleDefinitionName -eq "Owner"}

REMÉDIATION :

1. Lister tous les propriétaires actuels
2. Révision métier : qui a vraiment besoin du rôle Owner ?
3. Remplacer par des rôles plus granulaires
4. Maintenir 2-3 Owners maximum par souscription

VALEUR PAR DÉFAUT :

Souvent trop de propriétaires

1.4.3 *Rôles personnalisés justifiés et documentés*

MITRE ATT&CK : T1078

DESCRIPTION :

Les rôles personnalisés ne doivent être créés que lorsqu'aucun rôle intégré ne répond au besoin, avec documentation complète des permissions accordées.

AUDIT :

- Portal > Subscriptions > Access control (IAM) > Roles > Type: Custom
- CLI: az role definition list --custom-role-only
- PowerShell: Get-AzRoleDefinition | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.IsCustom -eq }

REMÉDIATION :

1. Inventaire des rôles personnalisés
2. Révision : est-ce qu'un rôle intégré pourrait convenir ?
3. Documentation des rôles personnalisés conservés
4. Suppression des rôles obsolètes

VALEUR PAR DÉFAUT :

Aucun rôle personnalisé

1.5 — SERVICE PRINCIPALS ET MANAGED IDENTITIES

1.5.1 *Managed Identity privilégiée sur Service Principal*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les applications Azure doivent utiliser des Managed Identities plutôt que des Service Principals avec secrets pour l'authentification aux services Azure.

AUDIT :

- Portal > Azure AD > Enterprise applications > Managed identities
- CLI: az ad sp list --query "[?servicePrincipalType=='Application'].{appId:appId,displayName:displayName}"
- PowerShell: Get-AzADServicePrincipal | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.ServicePrincipalType -eq "Application"}

REMÉDIATION :

1. Inventaire des Service Principals actuels
2. Identifier lesquels peuvent utiliser Managed Identity
3. Migration : App Services, VMs, Function Apps
4. Suppression des secrets non nécessaires

VALEUR PAR DÉFAUT :

Service Principals avec secrets

1.5.2 *Rotation automatique des secrets Service Principal*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les secrets des Service Principals qui ne peuvent pas être remplacés par des Managed Identities doivent avoir une rotation automatisée et une durée de vie limitée (12 mois maximum).

AUDIT :

- Portal > Azure AD > App registrations > Certificates & secrets
- CLI: az ad app credential list --id
- PowerShell: Get-AzADAppCredential -ApplicationId

REMÉDIATION :

1. Audit des secrets existants et leurs dates d'expiration
2. Rotation des secrets > 12 mois
3. Mise en place d'alertes d'expiration
4. Processus de rotation automatisée (Key Vault + Logic Apps)

VALEUR PAR DÉFAUT :

Secrets à long terme (2 ans par défaut)

1.5.3 *Permissions minimales pour Service Principals*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les Service Principals doivent avoir uniquement les permissions Azure RBAC et API Graph strictement nécessaires pour leur fonction.

AUDIT :

- Portal > Azure AD > Enterprise applications > Permissions
- CLI: az ad sp show --id --query "oauth2PermissionGrants"
- PowerShell: Get-AzADServicePrincipal | Get-AzADServicePrincipalOAuth2PermissionGrant

REMÉDIATION :

1. Audit des permissions Graph API accordées
2. Révocation des permissions excessive (ex: Directory.ReadWrite.All)
3. Application du principe du moindre privilège
4. Test des applications après réduction des permissions

VALEUR PAR DÉFAUT :

Souvent sur-privilégié

1.6 — UTILISATEURS INVITÉS (GUEST)

1.6.1 *Restriction des invitations d'utilisateurs externes*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les invitations d'utilisateurs externes (B2B) doivent être restreintes aux administrateurs ou à un groupe défini, avec processus d'approbation formel.

AUDIT :

- Portal > Azure AD > External Identities > External collaboration settings
- CLI: az rest --method get --url https://graph.microsoft.com/v1.0/policies/externalIdentitiesPolicy
- PowerShell: Get-MgPolicyExternalIdentityPolicy

REMÉDIATION :

1. External Identities > External collaboration settings
2. Guest invite restrictions : "Only users assigned to specific admin roles"
3. OU créer groupe autorisé à inviter
4. Processus de validation métier des invitations

VALEUR PAR DÉFAUT :

Tous les utilisateurs peuvent inviter

1.6.2 *Révision périodique des utilisateurs invités*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les comptes utilisateurs invités doivent faire l'objet d'une révision d'accès trimestrielle pour s'assurer que leur accès est toujours justifié.

AUDIT :

- Portal > Azure AD > Identity Governance > Access reviews
- CLI: az ad user list --query "[?userType=='Guest'].{userPrincipalName:userPrincipalName,creationType:creationType}"
- PowerShell: Get-AzADUser | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.UserType -eq "Guest"}

REMÉDIATION :

1. Identity Governance > Access reviews > New access review
2. Scope : Guest users
3. Reviewers : Resource owners/sponsors
4. Recurrence : Quarterly

VALEUR PAR DÉFAUT :

Aucune révision automatisée

1.7 — COMPTES DE SERVICE ET BREAK-GLASS

1.7.1 *Comptes break-glass configurés et protégés*

MITRE ATT&CK : T1078

DESCRIPTION :

Au moins 2 comptes break-glass (urgence) doivent être configurés avec mot de passe complexe stocké de façon sécurisée, exclus des politiques Conditional Access.

AUDIT :

- Portal > Azure AD > Users > Filter par "emergency" ou "breakglass"
- CLI: az ad user list --query "[?contains(displayName,'emergency') || contains(displayName,'break')]"
- PowerShell: Get-AzADUser | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.DisplayName -like "*emergency*" -or ___BEGIN___COMMAND_OUTPUT_MARKER___.DisplayName -like "*break*"}

REMÉDIATION :

1. Créer 2 comptes : emergency-admin-01/02
2. Mot de passe complexe stocké offline sécurisé
3. Rôle Global Administrator
4. Exclusion des politiques Conditional Access
5. Monitoring spécifique des connexions

VALEUR PAR DÉFAUT :

Aucun compte break-glass

1.7.2 *Surveillance des comptes break-glass*

MITRE ATT&CK : T1078

DESCRIPTION :

Toute utilisation des comptes break-glass doit déclencher une alerte immédiate et faire l'objet d'un suivi d'incident de sécurité.

AUDIT :

- Portal > Azure Monitor > Logs > SigninLogs
- Requête KQL : SigninLogs | where UserPrincipalName contains "emergency"
- PowerShell: Get-AzActivityLog | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.Caller -like "*emergency*"}

REMÉDIATION :

1. Azure Monitor > Alerts > New alert rule
2. Condition : SigninLogs where UserPrincipalName contains emergency
3. Action Group : Email SOC + SMS responsables sécurité
4. Processus d'incident automatique

VALEUR PAR DÉFAUT :

Aucune surveillance spécifique

1.8 — POLITIQUES DE MOTS DE PASSE ET SÉCURITÉ

1.8.1 *Politique de mots de passe sécurisée*

MITRE ATT&CK : T1110

DESCRIPTION :

Les politiques de mots de passe doivent respecter les bonnes pratiques : longueur minimale, complexité, bannissement des mots de passe courants.

AUDIT :

- Portal > Azure AD > Security > Authentication methods > Password protection
- CLI: az rest --method get --url https://graph.microsoft.com/beta/policies/authenticationMethodsPolicy
- PowerShell: Get-MgPolicyAuthenticationMethodPolicy

REMÉDIATION :

1. Portal > Security > Authentication methods > Password protection
2. Activer "Enforce custom banned password list"
3. Ajouter termes spécifiques organisation
4. Mode : Enforced (pas Audit)

VALEUR PAR DÉFAUT :

Politique basique

1.8.2 *Protection contre le password spray*

MITRE ATT&CK : T1110.003

DESCRIPTION :

Azure AD Smart Lockout doit être configuré pour détecter et bloquer les attaques par pulvérisation de mots de passe.

AUDIT :

- Portal > Azure AD > Security > Authentication methods > Password protection
- CLI: Vérifier les paramètres via Graph API
- PowerShell: Vérification des politiques de verrouillage

REMÉDIATION :

1. Security > Authentication methods > Password protection
2. Smart Lockout : Threshold = 5 tentatives
3. Lockout duration : 60 secondes minimum
4. Monitoring des événements de verrouillage

VALEUR PAR DÉFAUT :

Lockout threshold = 10

1.9 — AUDIT ET SURVEILLANCE IAM

1.9.1 *Audit des changements de rôles privilégiés*

MITRE ATT&CK : T1078

DESCRIPTION :

Tous les changements d'attribution de rôles privilégiés doivent être audités et alerter automatiquement l'équipe de sécurité.

AUDIT :

- Portal > Azure AD > Audit logs > Activity: Add member to role
- CLI: az monitor activity-log list --filters "Category eq 'Administrative'"
- PowerShell: Get-AzLog -ResourceProvider "Microsoft.Authorization"

REMÉDIATION :

1. Azure Monitor > Logs > Recherche modifications RBAC
2. Création alerte : AuditLogs | where ActivityDisplayName contains "role"
3. Action Group : Notification équipe sécurité
4. Révision hebdomadaire des changements

VALEUR PAR DÉFAUT :

Audit activé, alertes non configurées

1.9.2 *Surveillance des connexions administrateur*

MITRE ATT&CK : T1078

DESCRIPTION :

Les connexions des comptes administrateur doivent être surveillées en continu avec alertes sur les comportements anormaux (géolocalisation, horaires, échecs répétés).

AUDIT :

- Portal > Azure AD > Sign-ins > Filter by admin roles
- CLI: az monitor activity-log list --filters "Category eq 'SigninLogs'"
- PowerShell: Search-AzGraph -Query "SigninLogs | where UserType == 'Admin'"

REMÉDIATION :

1. Configurer Identity Protection (Azure AD P2)
2. Surveillance géographique anormale
3. Alertes connexions à risque élevé
4. Dashboard SOC avec métriques admin

VALEUR PAR DÉFAUT :

Surveillance basique uniquement

1.7 — ACCÈS CONDITIONNEL AVANCÉ

1.7.1 *Politique d'accès basée sur les risques utilisateur*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Configurer des politiques d'accès conditionnel qui évaluent les risques des utilisateurs et sessions pour bloquer ou demander une authentification supplémentaire lors de connexions suspectes.

AUDIT :

- Portal > Azure AD > Security > Conditional Access > Policies
- CLI: az ad policy list --query "[?contains(displayName,'Risk')]"
- PowerShell: Get-AzureADMSConditionalAccessPolicy | Where-Object {$_.DisplayName -like "*Risk*"}

REMÉDIATION :

1. Activer Azure AD Identity Protection
2. Configurer les niveaux de risque utilisateur (Low, Medium, High)
3. Créer une politique CA "Block High Risk Users"
4. Tester en mode report-only avant activation

```
# Créer une politique de risque utilisateur
New-AzureADMSConditionalAccessPolicy -DisplayName "Block High Risk Users" -State "Enabled" -UserRiskLevels @("high") -SignInRiskLev
```

VALEUR PAR DÉFAUT :

Désactivé

1.7.2 *Accès conditionnel basé sur la géolocalisation*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Bloquer ou restreindre l'accès depuis des pays/régions non approuvés pour réduire les risques d'accès malveillants depuis des zones géographiques inattendues.

AUDIT :

- Portal > Azure AD > Security > Named locations
- CLI: az ad policy list --query "[?contains(displayName,'Location')]"
- PowerShell: Get-AzureADMSNamedLocationPolicy

REMÉDIATION :

1. Définir les emplacements nommés approuvés
2. Créer une politique de géolocalisation
3. Configurer le blocage des pays non approuvés

```
# Créer un emplacement nommé pour les pays approuvés
New-AzureADMSNamedLocationPolicy -OdataType "#microsoft.graph.countryNamedLocation" -DisplayName "Approved Countries" -CountriesAnd
```

VALEUR PAR DÉFAUT :

Désactivé

1.7.3 *Contrôle d'accès basé sur les appareils conformes*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Exiger que les appareils soient conformes aux politiques de sécurité ou joints au domaine avant d'autoriser l'accès aux ressources sensibles.

AUDIT :

- Portal > Azure AD > Devices > Device compliance
- CLI: az ad device list --query "[].{Name:displayName,Compliant:isCompliant}"
- PowerShell: Get-AzureADDevice | Select-Object DisplayName, IsCompliant

REMÉDIATION :

1. Configurer Microsoft Intune pour la gestion des appareils
2. Définir les politiques de conformité
3. Créer une politique CA exigeant des appareils conformes

```
# Créer une politique exigeant des appareils conformes
New-AzureADMSConditionalAccessPolicy -DisplayName "Require Compliant Device" -State "Enabled" -DeviceState @("compliant", "domainJo
```

VALEUR PAR DÉFAUT :

Désactivé

1.8 — PRIVILEGED IDENTITY MANAGEMENT (PIM)

1.8.1 *Activation JIT pour les rôles privilégiés*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Configurer PIM pour exiger une activation just-in-time des rôles administratifs avec approbation et justification métier.

AUDIT :

- Portal > Azure AD > Privileged Identity Management > Azure AD roles
- CLI: az rest --method GET --url "https://graph.microsoft.com/v1.0/privilegedAccess/azureResources/roleAssignments"
- PowerShell: Get-AzureADMSPrivilegedRoleAssignment

REMÉDIATION :

1. Activer PIM pour Azure AD
2. Configurer les paramètres d'activation pour chaque rôle
3. Définir les approbateurs et exigences de justification

```
# Configurer PIM pour le rôle Global Administrator
$roleDefinitionId = (Get-AzureADDirectoryRole | Where-Object {$_.DisplayName -eq "Global Administrator"}).ObjectId
Set-AzureADMSPrivilegedRoleAssignmentPolicy -ProviderId "aadRoles" -ResourceId "tenant" -RoleDefinitionId $roleDefinitionId -Activa
```

VALEUR PAR DÉFAUT :

Désactivé

1.8.2 *Révisions d'accès périodiques pour les rôles privilégiés*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Configurer des révisions d'accès automatiques pour tous les rôles privilégiés afin de s'assurer que les permissions restent nécessaires et appropriées.

AUDIT :

- Portal > Azure AD > Identity Governance > Access reviews
- CLI: az rest --method GET --url "https://graph.microsoft.com/v1.0/identityGovernance/accessReviews/definitions"
- PowerShell: Get-AzureADMSAccessReview

REMÉDIATION :

1. Créer des révisions d'accès pour tous les rôles privilégiés
2. Configurer la fréquence (recommandé : trimestrielle)
3. Définir les réviseurs appropriés

```
# Créer une révision d'accès pour les administrateurs globaux
New-AzureADMSAccessReview -DisplayName "Global Admin Review" -StartDate (Get-Date) -EndDate (Get-Date).AddDays(30) -ReviewedEntity
```

VALEUR PAR DÉFAUT :

Désactivé

1.8.3 *Alertes PIM configurées*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Configurer et surveiller les alertes PIM pour détecter les activations suspectes ou les modifications non autorisées des rôles privilégiés.

AUDIT :

- Portal > Azure AD > PIM > Azure AD roles > Alerts
- CLI: az monitor activity-log list --resource-group "PIM-Alerts"
- PowerShell: Get-AzureADAuditDirectoryLogs -Filter "category eq 'RoleManagement'"

REMÉDIATION :

1. Configurer les alertes PIM dans le portail
2. Définir les destinataires des notifications
3. Intégrer avec SIEM/Log Analytics

```
# Configurer une alerte pour les activations de rôles élevés
New-AzMetricAlertRuleV2 -Name "PIM-HighPrivilegeActivation" -ResourceGroupName "Security-Alerts" -TargetResourceId "/subscriptions/
```

VALEUR PAR DÉFAUT :

Alertes de base activées

1.9 — COMPTES D'URGENCE

1.9.1 *Comptes break-glass configurés et protégés*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Configurer et maintenir des comptes d'urgence (break-glass) pour l'accès d'urgence en cas de défaillance des systèmes d'authentification normaux.

AUDIT :

- Portal > Azure AD > Users > Rechercher comptes emergency/breakglass
- CLI: az ad user list --query "[?contains(userPrincipalName,'emergency')]"
- PowerShell: Get-AzureADUser | Where-Object {$_.UserPrincipalName -like "*emergency*"}

REMÉDIATION :

1. Créer 2 comptes d'urgence avec mots de passe forts
2. Exclure de toutes les politiques d'accès conditionnel
3. Stocker les identifiants dans un coffre-fort physique
4. Documenter les procédures d'utilisation

```
# Créer un compte d'urgence
New-AzureADUser -DisplayName "Emergency Admin 01" -UserPrincipalName "emergency01@domain.com" -PasswordProfile @{Password="ComplexP
```

VALEUR PAR DÉFAUT :

Non configuré

1.9.2 *Surveillance des comptes d'urgence*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Implémenter une surveillance stricte des comptes d'urgence avec alertes en temps réel pour toute utilisation.

AUDIT :

- Portal > Azure AD > Sign-ins > Filtrer par comptes emergency
- CLI: az monitor activity-log list --caller "emergency01@domain.com"
- PowerShell: Get-AzureADAuditSignInLogs -Filter "userPrincipalName eq 'emergency01@domain.com'"

REMÉDIATION :

1. Créer des alertes Log Analytics pour les connexions des comptes d'urgence
2. Configurer des notifications immé

RÉCAPITULATIF SECTION S1 - IAM

2.0 — MICROSOFT DEFENDER FOR CLOUD

2.1.1 *Defender for Cloud activé sur toutes les souscriptions*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Microsoft Defender for Cloud doit être activé avec niveau Standard/Paid sur toutes les souscriptions pour la détection de menaces et l'évaluation de sécurité continue.

AUDIT :
- Portal > Microsoft Defender for Cloud > Environment settings
- CLI: az security pricing list --query "value[].{name:name,tier:pricingTier}"
- PowerShell: Get-AzSecurityPricing

REMÉDIATION :
1. Defender for Cloud > Environment settings
2. Sélectionner chaque souscription
3. Activer tous les Defender plans (Servers, Storage, SQL, etc.)
4. Configurer Log Analytics workspace

VALEUR PAR DÉFAUT :
Free tier activé

2.1.2 *Plans Defender activés par type de ressource*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Tous les plans Defender spécialisés doivent être activés : Servers, App Service, Storage, SQL, Kubernetes, Container Registries, Key Vault, Resource Manager, DNS.

AUDIT :
- Portal > Defender for Cloud > Environment settings > Plans
- CLI: az security pricing show --name VirtualMachines
- PowerShell: Get-AzSecurityPricing | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.Name -eq "VirtualMachines"}

REMÉDIATION :
1. Environment settings > Subscription > Plans
2. Activer chaque plan individuellement :
3. Defender for Servers (Plan 2)
4. Defender for App Service
5. Defender for Storage
6. Defender for SQL
7. Defender for Kubernetes
8. Defender for Container Registries
9. Defender for Key Vault

VALEUR PAR DÉFAUT :
Plans désactivés individuellement

2.1.3 *Auto-provisioning activé pour agents de sécurité*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Le provisioning automatique des agents Log Analytics et Dependency Agent doit être activé pour permettre la collecte automatique des données de sécurité.

AUDIT :
- Portal > Defender for Cloud > Environment settings > Auto provisioning
- CLI: az security auto-provisioning-setting list
- PowerShell: Get-AzSecurityAutoProvisioningSetting

REMÉDIATION :
1. Environment settings > Auto provisioning
2. Log Analytics agent for Azure VMs : ON
3. Vulnerability assessment for machines : ON
4. Configurer workspace Log Analytics cible

VALEUR PAR DÉFAUT :
Auto-provisioning désactivé

2.2 — CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

2.2.1 *Secure Score monitoring et amélioration*

MITRE ATT&CK : T1562

DESCRIPTION :

Le Secure Score doit être surveillé régulièrement avec objectif d'amélioration continue. Score minimum acceptable : 70% pour production.

AUDIT :

- Portal > Defender for Cloud > Secure Score
- CLI: az security secure-score list
- PowerShell: Get-AzSecuritySecureScore

REMÉDIATION :

1. Établir baseline actuel du Secure Score
2. Prioriser recommandations High/Medium impact
3. Plan d'amélioration mensuel
4. Monitoring automatisé avec alertes si score < 70%

VALEUR PAR DÉFAUT :

Variable selon configuration

2.2.2 *Recommandations de sécurité priorisées et traitées*

MITRE ATT&CK : T1562

DESCRIPTION :

Les recommandations de sécurité critiques et de haut impact doivent être traitées dans les délais définis : 7 jours pour critique, 30 jours pour élevé.

AUDIT :

- Portal > Defender for Cloud > Recommendations
- CLI: az security task list --query "value[?state=='Active']"
- PowerShell: Get-AzSecurityTask | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.State -eq "Active"}

REMÉDIATION :

1. Classification des recommandations par criticité
2. Workflow de traitement avec SLA définis
3. Assignation responsables par type de recommandation
4. Tracking et reporting hebdomadaire

VALEUR PAR DÉFAUT :

Recommandations générées mais non traitées

2.2.3 *Compliance frameworks activés et surveillés*

MITRE ATT&CK : T1562

DESCRIPTION :

Les frameworks de compliance requis doivent être activés et surveillés : Azure Security Benchmark, CIS, PCI DSS, ISO 27001 selon les besoins métier.

AUDIT :

- Portal > Defender for Cloud > Regulatory compliance
- CLI: az security regulatory-compliance-standards list
- PowerShell: Get-AzSecurityRegulatoryComplianceStandard

REMÉDIATION :

1. Regulatory compliance > Add standards
2. Activer frameworks requis pour l'organisation
3. Monitoring des scores de compliance
4. Reporting compliance mensuel

VALEUR PAR DÉFAUT :

Azure Security Benchmark activé

2.3 — THREAT PROTECTION ET DETECTION

2.3.1 *Defender for Servers configuration avancée*

MITRE ATT&CK : T1055

DESCRIPTION :

Defender for Servers Plan 2 doit être configuré avec toutes les fonctionnalités de détection : comportemental, réseau, file integrity monitoring, adaptive application controls.

AUDIT :

- Portal > Defender for Cloud > Workload protections > Servers
- CLI: az security pricing show --name VirtualMachines
- PowerShell: Get-AzSecurityPricing -Name "VirtualMachines"

REMÉDIATION :

1. Activer Defender for Servers Plan 2
2. Configurer File Integrity Monitoring
3. Activer Adaptive Application Controls
4. Configurer Just-in-Time VM access

VALEUR PAR DÉFAUT :

Plan 1 ou désactivé

2.3.2 *Defender for Storage avec protection malware*

MITRE ATT&CK : T1204.002

DESCRIPTION :

Defender for Storage doit inclure la protection contre les malwares et la détection d'anomalies d'accès pour tous les comptes de stockage critiques.

AUDIT :

- Portal > Defender for Cloud > Workload protections > Storage
- CLI: az security pricing show --name StorageAccounts
- PowerShell: Get-AzSecurityPricing -Name "StorageAccounts"

REMÉDIATION :

1. Activer Defender for Storage
2. Configurer malware scanning
3. Activer sensitive data discovery
4. Configurer alertes accès anormaux

VALEUR PAR DÉFAUT :

Désactivé

2.3.3 *Defender for SQL avec Advanced Threat Protection*

MITRE ATT&CK : T1190

DESCRIPTION :

Defender for SQL doit être activé avec Advanced Threat Protection pour détecter injections SQL, accès anormaux, et activités suspectes.

AUDIT :

- Portal > Defender for Cloud > Workload protections > Databases
- CLI: az security pricing show --name SqlServers
- PowerShell: Get-AzSecurityPricing -Name "SqlServers"

REMÉDIATION :

1. Activer Defender for SQL servers
2. Activer Defender for SQL databases
3. Configurer email notifications
4. Intégration avec SIEM/Sentinel

VALEUR PAR DÉFAUT :

Désactivé

2.4 — INTÉGRATION ET ALERTING

2.4.1 *Intégration avec Azure Sentinel/SIEM*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Les alertes Defender for Cloud doivent être intégrées avec Azure Sentinel ou SIEM externe pour corrélation et réponse aux incidents.

AUDIT :

- Portal > Defender for Cloud > Security alerts > Export settings
- CLI: az security automation list
- PowerShell: Get-AzSecurityAutomation

REMÉDIATION :

1. Defender for Cloud > Security alerts > Export settings
2. Configurer continuous export vers Log Analytics
3. Ou configurer connector SIEM externe
4. Vérifier réception des alertes dans SIEM

VALEUR PAR DÉFAUT :

Pas d'export automatique

2.4.2 *Notifications email des alertes critiques*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Les alertes de sécurité de niveau High et Critical doivent déclencher des notifications email automatiques vers l'équipe de sécurité.

AUDIT :

- Portal > Defender for Cloud > Environment settings > Email notifications
- CLI: az security contact list
- PowerShell: Get-AzSecurityContact

REMÉDIATION :

1. Environment settings > Email notifications
2. Configurer email addresses SOC/Security team
3. Activer notifications pour alertes High severity
4. Tester réception des notifications

VALEUR PAR DÉFAUT :

Notifications désactivées

2.4.3 *Automation et réponse automatique*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des règles d'automation doivent être configurées pour répondre automatiquement aux alertes communes : isolement VM, blocage IP, escalade vers équipe sécurité.

AUDIT :

- Portal > Defender for Cloud > Workflow automation
- CLI: az security automation list
- PowerShell: Get-AzSecurityAutomation

REMÉDIATION :

1. Workflow automation > Add workflow automation
2. Trigger : Security alerts avec conditions
3. Actions : Logic Apps, Function Apps, ou Webhooks
4. Exemples : isolement network, ticket ITSM

VALEUR PAR DÉFAUT :

Aucune automation configurée

2.5 — VULNERABILITY MANAGEMENT

2.5.1 *Évaluation des vulnérabilités VMs activée*

MITRE ATT&CK : T1203

DESCRIPTION :

L'évaluation automatique des vulnérabilités doit être activée sur toutes les VMs avec remédiation priorisée selon CVSS score.

AUDIT :

- Portal > Defender for Cloud > Recommendations > Vulnerability findings
- CLI: az security va-solution list
- PowerShell: Get-AzSecurityVulnerabilityAssessment

REMÉDIATION :

1. Activer vulnerability assessment solution (Qualys ou Microsoft)
2. Déploiement automatique sur toutes VMs
3. Planification scans réguliers
4. Workflow remédiation vulnérabilités High/Critical

VALEUR PAR DÉFAUT :

Désactivé

2.5.2 *Container image vulnerability scanning*

MITRE ATT&CK : T1203

DESCRIPTION :

Les images de conteneurs doivent être scannées automatiquement pour les vulnérabilités lors du push vers Azure Container Registry.

AUDIT :

- Portal > Container Registry > Repository > Vulnerability scan results
- CLI: az acr task show --registry --name
- PowerShell: Get-AzContainerRegistryTask

REMÉDIATION :

1. Activer Defender for Container Registries
2. Configurer scan automatique au push
3. Politiques de blocage images vulnérables
4. Processus update régulier des base images

VALEUR PAR DÉFAUT :

Scan manuel uniquement

2.6 — COMPLIANCE ET GOUVERNANCE

2.6.1 *Azure Policy integration avec Defender*

MITRE ATT&CK : T1562

DESCRIPTION :

Les recommandations Defender for Cloud doivent être intégrées avec Azure Policy pour enforcement automatique des configurations de sécurité.

AUDIT :

- Portal > Policy > Assignments > Security Center initiatives
- CLI: az policy assignment list --query "[?contains(displayName,'Security')]"
- PowerShell: Get-AzPolicyAssignment | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.Properties.displayName -like "*Security*"}

REMÉDIATION :

1. Assign Azure Security Benchmark initiative
2. Configurer remediation automatique quand possible
3. Review non-compliance resources régulièrement
4. Exceptions documentées et approuvées

VALEUR PAR DÉFAUT :

Initiative ASB non assignée

2.6.2 *Inventaire et classification des assets*

MITRE ATT&CK : T1083

DESCRIPTION :

Un inventaire complet des ressources Azure doit être maintenu avec classification de criticité pour prioriser les efforts de sécurisation.

AUDIT :

- Portal > Defender for Cloud > Asset inventory
- CLI: az graph query -q "Resources | project name, type, resourceGroup, subscriptionId"
- PowerShell: Search-AzGraph -Query "Resources | project name, type, resourceGroup"

REMÉDIATION :

1. Utiliser Asset inventory de Defender for Cloud
2. Tagging des ressources avec niveau criticité
3. Filtres et vues par criticité/environnement
4. Révision inventaire mensuelle

VALEUR PAR DÉFAUT :

Inventaire basique sans classification

RÉCAPITULATIF SECTION S2 - DEFENDER FOR CLOUD

3.0 — SÉCURITÉ DU STOCKAGE

3.1.1 *Chiffrement au repos activé pour Storage Accounts*

MITRE ATT&CK : T1486

DESCRIPTION :
Le chiffrement au repos doit être activé sur tous les comptes de stockage Azure avec des clés managées par Microsoft ou Customer Managed Keys pour les données sensibles.

AUDIT :
- Portal > Storage accounts > Encryption
- CLI: az storage account show --name --query "encryption"
- PowerShell: Get-AzStorageAccount | Select-Object StorageAccountName,Encryption

REMÉDIATION :
1. Portal > Storage account > Security + networking > Encryption
2. Vérifier "Encryption at rest" activé
3. Pour données sensibles : configurer Customer Managed Keys
4. Rotation automatique des clés si CMK

VALEUR PAR DÉFAUT :
Chiffrement Microsoft-managed activé

3.1.2 *Secure transfer (HTTPS) obligatoire*

MITRE ATT&CK : T1040

DESCRIPTION :
L'option "Secure transfer required" doit être activée pour forcer l'utilisation de HTTPS/SMB 3.0 et bloquer les connexions HTTP non sécurisées.

AUDIT :
- Portal > Storage accounts > Configuration > Secure transfer required
- CLI: az storage account show --name --query "enableHttpsTrafficOnly"
- PowerShell: Get-AzStorageAccount | Select-Object StorageAccountName,EnableHttpsTrafficOnly

REMÉDIATION :
1. Storage account > Configuration
2. Secure transfer required : Enabled
3. Validation : tester qu'HTTP est bloqué
4. Mettre à jour applications pour utiliser HTTPS

VALEUR PAR DÉFAUT :
Enabled (depuis 2019)

3.1.3 *Minimum TLS version configurée (1.2)*

MITRE ATT&CK : T1040

DESCRIPTION :
La version TLS minimale acceptée doit être configurée à 1.2 pour éviter l'utilisation de protocoles cryptographiques faibles.

AUDIT :
- Portal > Storage accounts > Configuration > Minimum TLS version
- CLI: az storage account show --name --query "minimumTlsVersion"
- PowerShell: Get-AzStorageAccount | Select-Object StorageAccountName,MinimumTlsVersion

REMÉDIATION :
1. Storage account > Configuration
2. Minimum TLS version : Version 1.2
3. Tester compatibilité applications existantes
4. Monitoring des rejets de connexions TLS < 1.2

VALEUR PAR DÉFAUT :
TLS 1.0 (legacy)
3.2 — GESTION DES CLÉS ET ACCÈS

3.2.1 *Rotation automatique des clés d'accès*

MITRE ATT&CK : T1552.001

DESCRIPTION :

Les clés d'accès des comptes de stockage doivent être régénérées périodiquement (90 jours maximum) avec processus de rotation sans interruption.

AUDIT :

- Portal > Storage accounts > Access keys > Regenerate
- CLI: az storage account keys list --account-name
- PowerShell: Get-AzStorageAccountKey -ResourceGroupName -StorageAccountName

REMÉDIATION :

1. Documenter processus rotation (key1 puis key2)
2. Mettre à jour applications avec nouvelle clé
3. Automatisation via Key Vault + Logic Apps
4. Test avant suppression ancienne clé

VALEUR PAR DÉFAUT :

Pas de rotation automatique

3.2.2 *Shared Access Signatures (SAS) avec durée limitée*

MITRE ATT&CK : T1552.001

DESCRIPTION :

Les SAS tokens doivent avoir une durée de validité limitée (24 heures maximum pour production) et des permissions minimales selon le principe du moindre privilège.

AUDIT :

- Portal > Storage Explorer > Generate SAS
- CLI: az storage blob generate-sas --help (vérifier --expiry)
- PowerShell: New-AzStorageBlobSASToken -ExpiryTime

REMÉDIATION :

1. Audit des SAS existants et leur durée
2. Politique max 24h pour SAS de production
3. Permissions minimales (read-only si possible)
4. Utiliser Service/Account SAS plutôt que Ad-hoc

VALEUR PAR DÉFAUT :

Durée configurable, souvent excessive

3.2.3 *Stored Access Policies pour SAS management*

MITRE ATT&CK : T1552.001

DESCRIPTION :

Les Stored Access Policies doivent être utilisées pour gérer centralement les permissions SAS et permettre la révocation immédiate.

AUDIT :

- Portal > Storage account > Containers > Access policy
- CLI: az storage container policy list --container-name
- PowerShell: Get-AzStorageContainerStoredAccessPolicy

REMÉDIATION :

1. Créer Stored Access Policies par use case
2. Générer SAS basés sur ces policies
3. Révocation possible via suppression policy
4. Documentation des policies et leur usage

VALEUR PAR DÉFAUT :

Aucune policy pré-configurée

3.3 — CONTRÔLES D'ACCÈS RÉSEAU

3.3.1 *Firewall Storage Account configuré*

MITRE ATT&CK : T1095

DESCRIPTION :

Les règles de firewall doivent restreindre l'accès aux comptes de stockage aux réseaux autorisés uniquement, bloquant l'accès public par défaut.

AUDIT :

- Portal > Storage account > Security + networking > Firewalls and virtual networks
- CLI: az storage account show --name --query "networkRuleSet"
- PowerShell: Get-AzStorageAccount | Select-Object NetworkRuleSet

REMÉDIATION :

1. Storage account > Firewalls and virtual networks
2. Selected networks (pas "All networks")
3. Ajouter VNets/Subnets autorisés
4. Ajouter IPs publiques si nécessaire (bureaux)

VALEUR PAR DÉFAUT :

All networks (accès public)

3.3.2 *Private Endpoints pour accès sécurisé*

MITRE ATT&CK : T1095

DESCRIPTION :

Des Private Endpoints doivent être configurés pour l'accès aux comptes de stockage critiques depuis les VNets Azure, évitant le transit par Internet.

AUDIT :

- Portal > Storage account > Security + networking > Private endpoint connections
- CLI: az network private-endpoint list --query "[?privateLinkServiceConnections[0].groupIds[0]=='blob']"
- PowerShell: Get-AzPrivateEndpoint | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.PrivateLinkServiceConnections.GroupIds -contains "blob"}

REMÉDIATION :

1. Storage account > Private endpoint connections > Add
2. Créer Private Endpoint dans VNet cible
3. Configurer Private DNS zone
4. Tester connectivité interne

VALEUR PAR DÉFAUT :

Pas de Private Endpoint

3.3.3 *Disable public blob access si non requis*

MITRE ATT&CK : T1190

DESCRIPTION :

L'accès public aux blobs doit être désactivé au niveau du compte de stockage si aucun blob ne doit être accessible publiquement.

AUDIT :

- Portal > Storage account > Configuration > Allow Blob public access
- CLI: az storage account show --name --query "allowBlobPublicAccess"
- PowerShell: Get-AzStorageAccount | Select-Object StorageAccountName,AllowBlobPublicAccess

REMÉDIATION :

1. Storage account > Configuration
2. Allow Blob public access : Disabled
3. Validation : aucun container public requis
4. Alternative : SAS tokens pour accès externe

VALEUR PAR DÉFAUT :

Enabled

3.4 — LOGGING ET MONITORING

3.4.1 *Storage Analytics et monitoring activés*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Storage Analytics doit être activé pour logger toutes les opérations de lecture/écriture/suppression avec rétention appropriée (90 jours minimum).

AUDIT :

- Portal > Storage account > Monitoring > Insights
- CLI: az monitor diagnostic-settings list --resource
- PowerShell: Get-AzDiagnosticSetting -ResourceId

REMÉDIATION :

1. Storage account > Monitoring > Diagnostic settings
2. Activer logs pour Blob, Queue, Table, File
3. Destination : Log Analytics workspace
4. Retention : 90 jours minimum

VALEUR PAR DÉFAUT :

Logging minimal

3.4.2 *Alertes sur activités suspectes de stockage*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des alertes doivent être configurées pour détecter les activités anormales : accès depuis IPs non autorisées, volume de données anormal, suppressions en masse.

AUDIT :

- Portal > Azure Monitor > Alerts > Alert rules
- CLI: az monitor metrics alert list
- PowerShell: Get-AzMetricAlertRuleV2

REMÉDIATION :

1. Azure Monitor > Alerts > New alert rule
2. Scope : Storage account
3. Conditions : Transactions anomales, Errors, etc.
4. Action groups : notification équipe sécurité

VALEUR PAR DÉFAUT :

Pas d'alertes configurées

3.5 — PROTECTION AVANCÉE DES DONNÉES

3.5.1 *Advanced Threat Protection activé*

MITRE ATT&CK : T1204.002

DESCRIPTION :
Advanced Threat Protection (Defender for Storage) doit être activé pour détecter les malwares, accès anormaux, et exfiltration de données.

AUDIT :
- Portal > Defender for Cloud > Workload protections > Storage
- CLI: az security pricing show --name StorageAccounts
- PowerShell: Get-AzSecurityPricing -Name "StorageAccounts"

REMÉDIATION :
1. Defender for Cloud > Workload protections > Storage
2. Enable Defender for Storage
3. Configurer alertes et notifications
4. Intégration avec Sentinel/SIEM

VALEUR PAR DÉFAUT :
Désactivé

3.5.2 *Soft delete activé pour blobs et containers*

MITRE ATT&CK : T1485

DESCRIPTION :
La suppression réversible doit être activée pour les blobs et containers pour permettre la récupération après suppression accidentelle ou malveillante.

AUDIT :
- Portal > Storage account > Data protection > Recovery
- CLI: az storage account blob-service-properties show --account-name
- PowerShell: Get-AzStorageBlobServiceProperty

REMÉDIATION :
1. Storage account > Data protection > Recovery
2. Enable soft delete for blobs : 30 jours
3. Enable soft delete for containers : 30 jours
4. Test procédure de récupération

VALEUR PAR DÉFAUT :
Désactivé

3.5.3 *Versioning des blobs activé*

MITRE ATT&CK : T1485

DESCRIPTION :
Le versioning des blobs doit être activé pour les données critiques afin de maintenir l'historique des modifications et permettre la restauration.

AUDIT :
- Portal > Storage account > Data protection > Tracking
- CLI: az storage account blob-service-properties show --account-name --query "isVersioningEnabled"
- PowerShell: Get-AzStorageBlobServiceProperty | Select-Object IsVersioningEnabled

REMÉDIATION :
1. Storage account > Data protection > Tracking
2. Enable versioning for blobs
3. Configurer lifecycle management pour versions anciennes
4. Monitoring de la consommation de stockage

VALEUR PAR DÉFAUT :
Désactivé

3.6 — BACKUP ET DISASTER RECOVERY

3.6.1 *Géo-réplication configurée selon criticité*

MITRE ATT&CK : T1485

DESCRIPTION :
La géo-réplication appropriée doit être configurée selon la criticité des données : LRS pour dev/test, GRS/RA-GRS pour production critique.

AUDIT :
- Portal > Storage account > Overview > Replication
- CLI: az storage account show --name --query "sku.name"
- PowerShell: Get-AzStorageAccount | Select-Object StorageAccountName,Sku

REMÉDIATION :
1. Évaluer criticité des données par storage account
2. Production critique : Standard_RAGRS ou Standard_GZRS
3. Non-critique : Standard_LRS ou Standard_ZRS
4. Test procédures de failover

VALEUR PAR DÉFAUT :
LRS (réplication locale uniquement)

3.6.2 *Backup automatisé via Azure Backup*

MITRE ATT&CK : T1485

DESCRIPTION :

Les données critiques doivent être sauvegardées automatiquement via Azure Backup avec rétention selon les exigences métier (7-7-12 minimum).

AUDIT :

- Portal > Recovery Services vault > Backup items > Azure Storage (Azure Files)
- CLI: az backup item list --resource-group --vault-name
- PowerShell: Get-AzRecoveryServicesBackupItem

REMÉDIATION :

1. Créer Recovery Services vault
2. Configurer backup policy (daily/weekly/monthly)
3. Activer backup pour Azure Files critiques
4. Tester procédures de restauration

VALEUR PAR DÉFAUT :

Pas de backup automatique

RÉCAPITULATIF SECTION S3 - STORAGE SECURITY

4.0 — SÉCURITÉ DES BASES DE DONNÉES

4.1.1 *Transparent Data Encryption (TDE) activé*

MITRE ATT&CK : T1486

DESCRIPTION :
Transparent Data Encryption doit être activé sur toutes les bases de données SQL Azure pour chiffrer les données au repos avec rotation automatique des clés.

AUDIT :
- Portal > SQL database > Security > Transparent data encryption
- CLI: az sql db tde show --database --server --resource-group
- PowerShell: Get-AzSqlDatabaseTransparentDataEncryption

REMÉDIATION :
1. SQL database > Security > Transparent data encryption
2. Status : ON (activé)
3. Pour données sensibles : Customer-managed key dans Key Vault
4. Vérifier performance impact négligeable

VALEUR PAR DÉFAUT :
Activé par défaut depuis 2017

4.1.2 *SQL Auditing activé avec rétention appropriée*

MITRE ATT&CK : T1562.001

DESCRIPTION :
L'audit SQL doit être activé au niveau serveur avec logs envoyés vers Log Analytics et rétention minimum 90 jours pour conformité et investigation.

AUDIT :
- Portal > SQL server > Security > Auditing
- CLI: az sql server audit-policy show --server --resource-group
- PowerShell: Get-AzSqlServerAudit

REMÉDIATION :
1. SQL server > Security > Auditing > ON
2. Destination : Log Analytics workspace
3. Retention : 90 jours minimum
4. Audit actions : All actions and groups

VALEUR PAR DÉFAUT :
Désactivé

4.1.3 *Advanced Data Security activé*

MITRE ATT&CK : T1190

DESCRIPTION :
Advanced Data Security (maintenant Defender for SQL) doit être activé pour la détection de menaces, évaluation des vulnérabilités et classification des données.

AUDIT :
- Portal > SQL server > Security > Microsoft Defender for Cloud
- CLI: az security pricing show --name SqlServers
- PowerShell: Get-AzSecurityPricing -Name "SqlServers"

REMÉDIATION :
1. SQL server > Security > Microsoft Defender for Cloud > Enable
2. Configurer notifications email pour alertes
3. Activer vulnerability assessment avec stockage résultats
4. Révision régulière des recommandations

VALEUR PAR DÉFAUT :
Désactivé

4.1.4 *Firewall SQL Server configuré restrictif*

MITRE ATT&CK : T1190

DESCRIPTION :
Les règles de firewall SQL Server doivent être configurées pour limiter l'accès aux IPs/réseaux autorisés uniquement, avec "Allow Azure services" désactivé si non requis.

AUDIT :
- Portal > SQL server > Security > Firewalls and virtual networks
- CLI: az sql server firewall-rule list --server --resource-group
- PowerShell: Get-AzSqlServerFirewallRule

REMÉDIATION :
1. SQL server > Firewalls and virtual networks
2. "Allow Azure services and resources to access this server" : OFF si non requis
3. Ajouter uniquement IPs/ranges nécessaires
4. Utiliser Virtual Network rules pour VNets

VALEUR PAR DÉFAUT :
"Allow Azure services" souvent activé

4.1.5 *Azure AD Authentication configurée*

MITRE ATT&CK : T1078.004

DESCRIPTION :
L'authentification Azure AD doit être configurée comme méthode d'authentification principale, avec désactivation optionnelle de l'authentification SQL.

AUDIT :
- Portal > SQL server > Security > Azure Active Directory admin
- CLI: az sql server ad-admin show --server --resource-group
- PowerShell: Get-AzSqlServerActiveDirectoryAdministrator

REMÉDIATION :
1. SQL server > Security > Azure Active Directory admin
2. Set admin : Configurer un groupe AD plutôt qu'un utilisateur
3. Considérer désactiver SQL authentication si AD seul suffisant
4. Utiliser Managed Identity pour applications

VALEUR PAR DÉFAUT :
SQL authentication uniquement
4.2 — AZURE SQL MANAGED INSTANCE

4.2.1 *Managed Instance dans VNet privé*

MITRE ATT&CK : T1095

DESCRIPTION :
Azure SQL Managed Instance doit être déployé dans un subnet dédié de VNet privé avec NSG appropriés pour isoler le trafic réseau.

AUDIT :
- Portal > SQL managed instance > Overview > Virtual network/subnet
- CLI: az sql mi show --name --resource-group --query "subnetId"
- PowerShell: Get-AzSqlInstance | Select-Object SubnetId

REMÉDIATION :
1. Déploiement dans subnet dédié (/27 minimum)
2. NSG avec règles restrictives
3. Route table configurée si nécessaire
4. Pas d'endpoint public sauf exception justifiée

VALEUR PAR DÉFAUT :
Configuration lors du déploiement

4.2.2 *TLS 1.2 minimum pour Managed Instance*

MITRE ATT&CK : T1040

DESCRIPTION :
La version TLS minimale doit être configurée à 1.2 pour toutes les connexions vers SQL Managed Instance.

AUDIT :
- Portal > SQL managed instance > Security > Networking
- CLI: az sql mi show --name --resource-group --query "minimalTlsVersion"
- PowerShell: Get-AzSqlInstance | Select-Object MinimalTlsVersion

REMÉDIATION :
1. SQL managed instance > Security > Networking
2. Minimal TLS version : 1.2
3. Tester compatibilité applications
4. Monitoring des rejets connexions TLS < 1.2

VALEUR PAR DÉFAUT :
TLS 1.0
4.3 — POSTGRESQL ET MYSQL

4.3.1 *SSL enforcement activé PostgreSQL/MySQL*

MITRE ATT&CK : T1040

DESCRIPTION :

L'application SSL doit être activée sur tous les serveurs Azure Database for PostgreSQL et MySQL pour chiffrer les communications.

AUDIT :

- Portal > Azure Database > Connection security > SSL enforcement
- CLI: az postgres server show --name --query "sslEnforcement"
- PowerShell: Get-AzPostgreSqlServer | Select-Object SslEnforcement

REMÉDIATION :

1. Azure Database > Connection security
2. SSL enforcement : ENABLED
3. Minimum TLS version : 1.2
4. Mettre à jour chaînes connexion applications

VALEUR PAR DÉFAUT :

ENABLED par défaut

4.3.2 *Firewall PostgreSQL/MySQL restrictif*

MITRE ATT&CK : T1190

DESCRIPTION :

Les règles de firewall des serveurs PostgreSQL/MySQL doivent être configurées pour limiter l'accès aux sources autorisées uniquement.

AUDIT :

- Portal > Azure Database > Connection security > Firewall rules
- CLI: az postgres server firewall-rule list --server-name
- PowerShell: Get-AzPostgreSqlFirewallRule

REMÉDIATION :

1. Azure Database > Connection security > Firewall rules
2. "Allow access to Azure services" : OFF si non requis
3. Ajouter uniquement IPs/ranges nécessaires
4. Utiliser Private Endpoints quand possible

VALEUR PAR DÉFAUT :

"Allow Azure services" souvent activé

4.3.3 *Backup automatique avec rétention appropriée*

MITRE ATT&CK : T1485

DESCRIPTION :

Les sauvegardes automatiques doivent être configurées avec rétention appropriée (7-35 jours) et géo-redondance pour les environnements critiques.

AUDIT :

- Portal > Azure Database > Overview > Backup retention period
- CLI: az postgres server show --name --query "backupRetentionDays"
- PowerShell: Get-AzPostgreSqlServer | Select-Object BackupRetentionDay

REMÉDIATION :

1. Configuration lors du déploiement ou via support
2. Retention period : 7 jours minimum, 35 pour production
3. Geo-redundant backup pour environnements critiques
4. Test procédures de restauration

VALEUR PAR DÉFAUT :

7 jours, locally redundant

4.4 — COSMOS DB SECURITY

4.4.1 *Chiffrement Cosmos DB avec Customer Managed Keys*

MITRE ATT&CK : T1486

DESCRIPTION :

Cosmos DB doit utiliser le chiffrement avec Customer Managed Keys stockées dans Azure Key Vault pour les données sensibles.

AUDIT :

- Portal > Cosmos DB account > Settings > Encryption
- CLI: az cosmosdb show --name --query "keyVaultKeyUri"
- PowerShell: Get-AzCosmosDBAccount | Select-Object KeyVaultKeyUri

REMÉDIATION :

1. Créer Key Vault avec clé de chiffrement
2. Cosmos DB > Settings > Encryption
3. Configurer Customer Managed Key
4. Vérifier rotation automatique des clés

VALEUR PAR DÉFAUT :

Microsoft-managed keys

4.4.2 *Firewall Cosmos DB configuré*

MITRE ATT&CK : T1190

DESCRIPTION :

Le firewall IP de Cosmos DB doit être configuré pour restreindre l'accès aux sources autorisées, avec désactivation de l'accès public si non requis.

AUDIT :

- Portal > Cosmos DB account > Settings > Firewalls and virtual networks
- CLI: az cosmosdb show --name --query "ipRules"
- PowerShell: Get-AzCosmosDBAccount | Select-Object IpRules

REMÉDIATION :

1. Cosmos DB > Firewalls and virtual networks
2. "Allow access from Azure Portal" : OFF si non requis
3. "Allow access from Azure datacenters" : OFF si non requis
4. Ajouter uniquement IPs autorisées

VALEUR PAR DÉFAUT :

Accès public autorisé

4.4.3 *Private Endpoints pour Cosmos DB*

MITRE ATT&CK : T1095

DESCRIPTION :

Des Private Endpoints doivent être configurés pour l'accès sécurisé à Cosmos DB depuis les VNets Azure sans transit par Internet.

AUDIT :

- Portal > Cosmos DB account > Settings > Private endpoint connections
- CLI: az network private-endpoint list --query "[?privateLinkServiceConnections[0].groupIds[0]=='Sql']"
- PowerShell: Get-AzPrivateEndpoint | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.PrivateLinkServiceConnections.GroupIds -contains "Sql"}

REMÉDIATION :

1. Cosmos DB > Private endpoint connections > Add
2. Créer Private Endpoint dans VNet approprié
3. Configurer Private DNS zone
4. Désactiver accès public après validation

VALEUR PAR DÉFAUT :

Pas de Private Endpoint

4.5 — DATABASE MONITORING ET COMPLIANCE

4.5.1 *Log Analytics intégration pour databases*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Tous les logs de base de données doivent être centralisés dans Log Analytics pour monitoring, alerting et investigation de sécurité.

AUDIT :

- Portal > Database > Monitoring > Diagnostic settings
- CLI: az monitor diagnostic-settings list --resource
- PowerShell: Get-AzDiagnosticSetting -ResourceId

REMÉDIATION :

1. Database > Monitoring > Diagnostic settings
2. Activer tous les logs pertinents (Audit, Errors, etc.)
3. Destination : Log Analytics workspace
4. Retention : 90 jours minimum

VALEUR PAR DÉFAUT :

Logging minimal

4.5.2 *Alertes sur activités suspectes base de données*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des alertes doivent être configurées pour détecter les activités anormales : connexions depuis IPs inhabituelles, requêtes suspectes, échecs d'authentification répétés.

AUDIT :

- Portal > Azure Monitor > Alerts > Alert rules (scope: databases)
- CLI: az monitor metrics alert list --resource-group
- PowerShell: Get-AzMetricAlertRuleV2

REMÉDIATION :

1. Azure Monitor > Alerts > New alert rule
2. Scope : Database resources
3. Conditions : Failed connections, CPU high, etc.
4. Action groups : SOC notification

VALEUR PAR DÉFAUT :

Pas d'alertes configurées

4.5.3 *Data Discovery et Classification activées*

MITRE ATT&CK : T1083

DESCRIPTION :

La découverte et classification automatique des données sensibles doit être activée pour identifier et protéger les informations personnelles et confidentielles.

AUDIT :

- Portal > SQL database > Security > Data Discovery & Classification
- CLI: Vérification via Azure Resource Graph ou API REST
- PowerShell: Utilisation des cmdlets SQL ou Resource Graph

REMÉDIATION :

1. SQL database > Security > Data Discovery & Classification
2. Lancer scan automatique
3. Révision et validation des classifications
4. Application labels de sensibilité

VALEUR PAR DÉFAUT :

Scan manuel

4.6 — ACCESS CONTROL ET PERMISSIONS

4.6.1 *Principe du moindre privilège pour accès DB*

MITRE ATT&CK : T1078

DESCRIPTION :

Les permissions d'accès aux bases de données doivent suivre le principe du moindre privilège avec séparation des environnements et rôles granulaires.

AUDIT :

- Portal > Database > Access control (IAM)
- SQL: SELECT name, type_desc FROM sys.database_principals
- PowerShell: Get-AzRoleAssignment -Scope

REMÉDIATION :

1. Audit des permissions actuelles
2. Création de rôles granulaires par fonction
3. Suppression des permissions excessives
4. Séparation prod/dev/test

VALEUR PAR DÉFAUT :

Permissions souvent excessives

4.6.2 *Comptes de service avec Managed Identity*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les applications doivent utiliser Managed Identity pour l'authentification aux bases de données Azure plutôt que des chaînes de connexion avec mots de passe.

AUDIT :

- Portal > Application > Identity > System assigned/User assigned
- Code : vérifier utilisation DefaultAzureCredential
- PowerShell: Get-AzWebApp | Select-Object Identity

REMÉDIATION :

1. Activer Managed Identity sur App Service/VM
2. Configurer permissions database pour l'identity
3. Modifier code application (DefaultAzureCredential)
4. Supprimer chaînes connexion avec mots de passe

VALEUR PAR DÉFAUT :

Chaînes de connexion avec mots de passe

RÉCAPITULATIF SECTION S4 - DATABASE SECURITY

5.0 — LOGGING ET SURVEILLANCE

5.1.1 *Activity Log retention configurée appropriée*

MITRE ATT&CK : T1562.001

DESCRIPTION :
L'Azure Activity Log doit être configuré avec une rétention de 90 jours minimum et exporté vers Log Analytics pour analyse et conformité réglementaire.

AUDIT :
- Portal > Monitor > Activity Log > Export Activity Logs
- CLI: az monitor diagnostic-settings list --resource "/subscriptions/"
- PowerShell: Get-AzDiagnosticSetting -ResourceId "/subscriptions/"

REMÉDIATION :
1. Monitor > Activity Log > Export Activity Logs
2. Diagnostic settings > Add diagnostic setting
3. Logs : Administrative, Security, Alert, Policy
4. Destination : Log Analytics workspace

VALEUR PAR DÉFAUT :
90 jours dans Activity Log, pas d'export

5.1.2 *Alertes Activity Log pour actions critiques*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Des alertes doivent être configurées pour les actions critiques dans Activity Log : création/suppression de ressources, modifications NSG, changements RBAC.

AUDIT :
- Portal > Monitor > Alerts > Alert rules
- CLI: az monitor activity-log alert list
- PowerShell: Get-AzActivityLogAlert

REMÉDIATION :
1. Monitor > Alerts > New alert rule
2. Scope : Subscription
3. Condition : Activity Log - Administrative
4. Filters : Create/Delete Resource, NSG changes, etc.

VALEUR PAR DÉFAUT :
Aucune alerte Activity Log

5.1.3 *Activity Log protection contre suppression*

MITRE ATT&CK : T1562.001

DESCRIPTION :
L'Activity Log exporté vers Log Analytics ou Storage doit être protégé contre la suppression non autorisée avec contrôles d'accès appropriés.

AUDIT :
- Portal > Log Analytics workspace > Access control (IAM)
- CLI: az role assignment list --scope
- PowerShell: Get-AzRoleAssignment -Scope

REMÉDIATION :
1. Limiter les permissions "Contributor" sur Log Analytics workspace
2. Utiliser "Log Analytics Reader" pour la majorité des utilisateurs
3. Resource lock sur workspace critique
4. Audit régulier des accès

VALEUR PAR DÉFAUT :
Permissions souvent excessives

5.2 — LOG ANALYTICS WORKSPACE

5.2.1 *Log Analytics workspace centralisé configuré*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Un workspace Log Analytics centralisé doit être configuré pour collecter tous les logs de sécurité avec rétention appropriée selon les exigences de conformité.

AUDIT :
- Portal > Log Analytics workspaces > Overview
- CLI: az monitor log-analytics workspace list
- PowerShell: Get-AzOperationalInsightsWorkspace

REMÉDIATION :
1. Créer Log Analytics workspace central
2. Configurer retention : 90 jours minimum
3. Data sources : Activity Logs, Security Events, etc.
4. Scaling selon volume de données

VALEUR PAR DÉFAUT :
Pas de workspace centralisé

5.2.2 *Solutions de sécurité installées dans Log Analytics*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Les solutions de sécurité doivent être installées dans Log Analytics : Security Center, Update Management, Change Tracking, Security & Audit.

AUDIT :
- Portal > Log Analytics workspace > Legacy solutions
- CLI: az monitor log-analytics solution list
- PowerShell: Get-AzOperationalInsightsIntelligencePack

REMÉDIATION :
1. Log Analytics workspace > Legacy solutions
2. Ajouter : Security & Audit, Update Management
3. Configurer Change Tracking si requis
4. Vérifier data collection

VALEUR PAR DÉFAUT :
Solutions de base uniquement

5.2.3 *Contrôle d'accès granulaire Log Analytics*

MITRE ATT&CK : T1562.001

DESCRIPTION :
L'accès au workspace Log Analytics doit être contrôlé avec permissions granulaires par table/ressource pour respecter la séparation des responsabilités.

AUDIT :
- Portal > Log Analytics workspace > Access control (IAM)
- Portal > Tables > Access control settings
- PowerShell: Get-AzRoleAssignment -Scope

REMÉDIATION :
1. Utiliser table-level RBAC plutôt que workspace-level
2. Rôles granulaires : Log Analytics Reader, Security Reader
3. Custom roles pour besoins spécifiques
4. Audit régulier des accès

VALEUR PAR DÉFAUT :
Workspace-level permissions

5.3 — DIAGNOSTIC SETTINGS

5.3.1 *Diagnostic settings activés pour toutes ressources critiques*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Les paramètres de diagnostic doivent être activés sur toutes les ressources critiques avec envoi des logs vers Log Analytics centralisé.

AUDIT :
- Portal > Resources > Monitoring > Diagnostic settings
- CLI: az monitor diagnostic-settings list --resource
- PowerShell: Get-AzDiagnosticSetting -ResourceId

REMÉDIATION :
1. Identifier toutes les ressources critiques
2. Activer diagnostic settings par ressource
3. Sélectionner tous les logs de sécurité pertinents
4. Destination : Log Analytics workspace central

VALEUR PAR DÉFAUT :
Diagnostic settings désactivés

5.3.2 *Azure Policy pour enforcement diagnostic settings*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Azure Policy doit être utilisé pour forcer automatiquement l'activation des diagnostic settings sur toutes les nouvelles ressources créées.

AUDIT :

- Portal > Policy > Assignments > Diagnostic settings policies
- CLI: az policy assignment list --query "[?contains(displayName,'diagnostic')]"
- PowerShell: Get-AzPolicyAssignment | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.Properties.displayName -like "*diagnostic*"}

REMÉDIATION :

1. Policy > Definitions > Rechercher "Configure diagnostic"
2. Assign policies pour chaque type de ressource
3. Configure remediation automatique
4. Monitor compliance dashboard

VALEUR PAR DÉFAUT :

Pas d'enforcement automatique

5.4 — AZURE MONITOR ALERTS

5.4.1 *Action Groups configurés pour équipes sécurité*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des Action Groups doivent être configurés avec les contacts appropriés (SOC, équipe sécurité, astreinte) pour notification des alertes de sécurité.

AUDIT :

- Portal > Monitor > Alerts > Action groups
- CLI: az monitor action-group list
- PowerShell: Get-AzActionGroup

REMÉDIATION :

1. Monitor > Alerts > Action groups > Add
2. Actions : Email, SMS, Azure app notification
3. Groupes : SOC 24/7, Security Team, Management
4. Test notifications

VALEUR PAR DÉFAUT :

Pas d'action groups configurés

5.4.2 *Alertes métriques pour ressources critiques*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des alertes métriques doivent être configurées pour surveiller la santé et performance des ressources critiques : CPU, mémoire, connexions, erreurs.

AUDIT :

- Portal > Monitor > Alerts > Alert rules (Metric alerts)
- CLI: az monitor metrics alert list
- PowerShell: Get-AzMetricAlertRuleV2

REMÉDIATION :

1. Identifier métriques critiques par type de ressource
2. Configurer seuils appropriés (CPU >90%, etc.)
3. Action groups pour escalade
4. Suppression alertes non actionnables

VALEUR PAR DÉFAUT :

Alertes basiques uniquement

5.4.3 *Log search alerts pour détection anomalies*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des alertes de recherche de logs (KQL) doivent être configurées pour détecter les activités suspectes et anomalies de sécurité.

AUDIT :

- Portal > Monitor > Alerts > Alert rules (Log search alerts)
- CLI: az monitor scheduled-query list
- PowerShell: Get-AzScheduledQueryRule

REMÉDIATION :

1. Développer requêtes KQL pour détection
2. Exemples : Failed logins, Privilege escalation
3. Fréquence appropriée (5-15 minutes)
4. Tuning pour réduire false positives

VALEUR PAR DÉFAUT :

Pas d'alertes log search

5.5 — NETWORK WATCHER

5.5.1 *Network Watcher activé dans toutes régions*

MITRE ATT&CK : T1040

DESCRIPTION :

Network Watcher doit être activé dans toutes les régions Azure utilisées pour permettre le monitoring réseau et l'investigation des incidents.

AUDIT :

- Portal > Network Watcher > Overview (toutes régions)
- CLI: az network watcher list
- PowerShell: Get-AzNetworkWatcher

REMÉDIATION :

1. Network Watcher > Overview
2. Vérifier activation dans chaque région utilisée
3. Activer si nécessaire
4. Configurer diagnostic settings

VALEUR PAR DÉFAUT :

Activé automatiquement dans certaines régions

5.5.2 *NSG Flow Logs activés pour NSGs critiques*

MITRE ATT&CK : T1040

DESCRIPTION :

Les NSG Flow Logs doivent être activés sur tous les NSG critiques avec stockage dans Storage Account et analyse via Traffic Analytics.

AUDIT :

- Portal > Network Watcher > NSG flow logs
- CLI: az network watcher flow-log list
- PowerShell: Get-AzNetworkWatcherFlowLogStatus

REMÉDIATION :

1. Network Watcher > NSG flow logs
2. Configurer pour chaque NSG critique
3. Storage account pour stockage logs
4. Activer Traffic Analytics avec Log Analytics

VALEUR PAR DÉFAUT :

Désactivé

5.5.3 *Traffic Analytics configuré*

MITRE ATT&CK : T1040

DESCRIPTION :

Traffic Analytics doit être configuré pour analyser les NSG Flow Logs et détecter les communications anormales ou non autorisées.

AUDIT :

- Portal > Network Watcher > Traffic Analytics
- CLI: Vérification via Network Watcher flow logs
- PowerShell: Vérification des paramètres Traffic Analytics

REMÉDIATION :

1. Network Watcher > Traffic Analytics
2. Configurer Log Analytics workspace
3. Interval : 10 minutes pour production
4. Révision régulière des insights

VALEUR PAR DÉFAUT :

Désactivé

5.6 — AZURE SENTINEL / SIEM

5.6.1 *Azure Sentinel ou SIEM externe configuré*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Une solution SIEM (Azure Sentinel ou externe) doit être configurée pour corrélation des événements de sécurité et réponse aux incidents.

AUDIT :

- Portal > Microsoft Sentinel > Overview
- CLI: az sentinel workspace list
- Ou vérification SIEM externe (Splunk, QRadar, etc.)

REMÉDIATION :

1. Évaluer Azure Sentinel vs SIEM existant
2. Si Sentinel : onboard Log Analytics workspace
3. Configurer data connectors appropriés
4. Développer règles de détection

VALEUR PAR DÉFAUT :

Aucune solution SIEM

5.6.2 *Data connectors Sentinel configurés*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Tous les connecteurs de données pertinents doivent être configurés dans Sentinel : Azure AD, Activity Log, Security Center, Office 365, etc.

AUDIT :

- Portal > Microsoft Sentinel > Data connectors
- CLI: az sentinel data-connector list
- PowerShell: Get-AzSentinelDataConnector

REMÉDIATION :

1. Sentinel > Data connectors
2. Activer : Azure Active Directory, Azure Activity
3. Security Events, Office 365 si applicable
4. Connecteurs tiers selon environnement

VALEUR PAR DÉFAUT :

Connecteurs de base uniquement

5.6.3 *Analytics rules et détections personnalisées*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des règles d'analyse et détections personnalisées doivent être configurées dans Sentinel pour détecter les menaces spécifiques à l'environnement.

AUDIT :

- Portal > Microsoft Sentinel > Analytics > Rules
- CLI: az sentinel alert-rule list
- PowerShell: Get-AzSentinelAlertRule

REMÉDIATION :

1. Sentinel > Analytics > Rule templates
2. Activer règles Microsoft appropriées
3. Créer règles personnalisées selon besoins
4. Tuning et réduction false positives

VALEUR PAR DÉFAUT :

Templates Microsoft uniquement

5.7 — COMPLIANCE ET AUDIT TRAIL

5.7.1 *Immutable logs pour compliance*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Pour les environnements soumis à conformité stricte, les logs doivent être stockés de manière immuable avec protection WORM.

AUDIT :

- Portal > Storage account > Data protection > Immutable storage
- CLI: az storage container immutability-policy show
- PowerShell: Get-AzStorageContainerImmutabilityPolicy

REMÉDIATION :

1. Storage account dédié pour logs d'audit
2. Immutable blob storage avec time-based retention
3. Legal hold si requis par régulation
4. Export logs critiques vers ce storage

VALEUR PAR DÉFAUT :

Stockage logs standard mutable

5.7.2 *Audit trail complet des modifications*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Un audit trail complet doit être maintenu pour toutes les modifications de configuration de sécurité avec traçabilité des responsables.

AUDIT :

- Portal > Monitor > Activity Log > Administrative category
- Requête KQL : AzureActivity | where CategoryValue == "Administrative"
- PowerShell: Get-AzLog -ResourceProvider "Microsoft.Authorization"

REMÉDIATION :

1. S'assurer Activity Log activé sur toutes souscriptions
2. Export vers Log Analytics avec rétention longue
3. Alertes sur modifications critiques
4. Reporting mensuel des changements

VALEUR PAR DÉFAUT :

Activity Log standard 90 jours

RÉCAPITULATIF SECTION S5 - LOGGING ET SURVEILLANCE

6.0 — SÉCURITÉ RÉSEAU

6.1.1 *Network Security Groups (NSG) configurés restrictifs*

MITRE ATT&CK : T1095

DESCRIPTION :

Les NSG doivent être configurés avec règles restrictives suivant le principe du moindre privilège pour contrôler le trafic réseau.

AUDIT :

- Portal > Virtual networks > Subnets > Network security group
- CLI: az network nsg rule list --nsg-name

REMÉDIATION :

1. Audit des règles NSG existantes
2. Suppression des règles "Any to Any"
3. Principe allow explicit, deny all

6.2.1 *Azure Firewall ou NVA déployé*

MITRE ATT&CK : T1095

DESCRIPTION :

Azure Firewall ou Network Virtual Appliance doit être déployé pour inspection et filtrage du trafic réseau centralisé.

AUDIT :

- Portal > Firewalls ou Network Virtual Appliances
- CLI: az network firewall list

REMÉDIATION :

1. Déploiement Azure Firewall dans hub VNet
2. Configuration des règles de filtrage
3. Route tables pour forcer passage par firewall

6.3.1 *DDoS Protection Standard activé*

MITRE ATT&CK : T1499

DESCRIPTION :

DDoS Protection Standard doit être activé sur les VNets exposés publiquement pour protection contre les attaques déni de service.

AUDIT :

- Portal > Virtual networks > DDoS protection
- CLI: az network ddos-protection list

REMÉDIATION :

1. Créer DDoS protection plan
2. Associer aux VNets publics
3. Configurer alertes DDoS

6.4 — AZURE FIREWALL PREMIUM ET WAF

6.4.1 *Azure Firewall Premium avec IDPS activé*

MITRE ATT&CK : T1190

DESCRIPTION :

Déployer Azure Firewall Premium avec les capacités IDPS (Intrusion Detection and Prevention System) pour détecter et bloquer les menaces réseau avancées.

AUDIT :

- Portal > Azure Firewall > Overview > Check SKU
- CLI: az network firewall show --name MyFirewall --resource-group MyRG --query "sku.tier"
- PowerShell: (Get-AzFirewall -Name "MyFirewall" -ResourceGroupName "MyRG").Sku.Tier

REMÉDIATION :

1. Upgrader vers Azure Firewall Premium
2. Activer les règles IDPS
3. Configurer les signatures de menaces

```
# Créer Azure Firewall Premium avec IDPS
$firewallPremium = New-AzFirewall -Name "MyFirewallPremium" -ResourceGroupName "MyRG" -Location "France Central" -VirtualNetwork $v
# Activer IDPS
$firewallPolicy = New-AzFirewallPolicy -Name "MyFirewallPolicy" -ResourceGroupName "MyRG" -Location "France Central" -ThreatIntelMo
```

VALEUR PAR DÉFAUT :

Standard SKU

6.4.2 *Web Application Firewall (WAF) avec règles OWASP*

MITRE ATT&CK : T1190

DESCRIPTION :

Configurer WAF avec les règles OWASP Core Rule Set pour protéger les applications web contre les attaques communes.

AUDIT :

- Portal > Application Gateway > Web application firewall
- CLI: az network application-gateway waf-config show --gateway-name MyAppGW --resource-group MyRG
- PowerShell: Get-AzApplicationGatewayWebApplicationFirewallConfiguration -ApplicationGateway $appgw

REMÉDIATION :

1. Activer WAF sur Application Gateway
2. Configurer OWASP Core Rule Set 3.2
3. Définir le mode de protection

```
# Configurer WAF avec OWASP
$appgw = Get-AzApplicationGateway -Name "MyAppGW" -ResourceGroupName "MyRG"
Set-AzApplicationGatewayWebApplicationFirewallConfiguration -ApplicationGateway $appgw -Enabled $true -FirewallMode "Prevention" -R
Set-AzApplicationGateway -ApplicationGateway $appgw
```

VALEUR PAR DÉFAUT :

Désactivé

6.5 — NSG ET FLOW LOGS

6.5.1 *NSG Flow Logs activés pour tous les NSG critiques*

MITRE ATT&CK : T1071

DESCRIPTION :

Activer les NSG Flow Logs pour surveiller et auditer le trafic réseau traversant les Network Security Groups.

AUDIT :

- Portal > Network Watcher > NSG flow logs
- CLI: az network watcher flow-log list --location francecentral
- PowerShell: Get-AzNetworkWatcherFlowLogStatus -NetworkWatcher $nw -TargetResourceId $nsg.Id

REMÉDIATION :

1. Créer un compte de stockage pour les logs
2. Activer Flow Logs sur tous les NSG critiques
3. Configurer Traffic Analytics si disponible

```
# Activer NSG Flow Logs
$nsg = Get-AzNetworkSecurityGroup -Name "MyNSG" -ResourceGroupName "MyRG"
$storageAccount = Get-AzStorageAccount -Name "flowlogsstorage" -ResourceGroupName "MyRG"
$nw = Get-AzNetworkWatcher -ResourceGroupName "NetworkWatcherRG" -Name "NetworkWatcher_francecentral"
Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher $nw -TargetResourceId $nsg.Id -StorageAccountId $storageAccount.Id -EnableFlowLog
```

VALEUR PAR DÉFAUT :

Désactivé

6.5.2 *Règles NSG avec principe du moindre privilège*

MITRE ATT&CK : T1071

DESCRIPTION :

Configurer les règles NSG selon le principe du moindre privilège, bloquant tout trafic par défaut et autorisant uniquement les flux nécessaires.

AUDIT :

- Portal > Network security group > Inbound/Outbound security rules
- CLI: az network nsg rule list --resource-group MyRG --nsg-name MyNSG
- PowerShell: Get-AzNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg

REMÉDIATION :

1. Auditer toutes les règles existantes
2. Supprimer les règles trop permissives
3. Implémenter des règles spécifiques par service

```
# Créer une règle NSG restrictive pour HTTPS
Add-AzNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "Allow-HTTPS-Inbound" -Protocol "Tcp" -Direction "Inbound" -Priori
Set-AzNetworkSecurityGroup -NetworkSecurityGroup $nsg
```

VALEUR PAR DÉFAUT :

Règles par défaut permissives

6.6 — DDOS PROTECTION

6.6.1 *DDoS Protection Standard activé*

MITRE ATT&CK : T1498

DESCRIPTION :

Activer DDoS Protection Standard pour protéger les adresses IP publiques contre les attaques de déni de service distribué.

AUDIT :

- Portal > Virtual network > DDoS protection
- CLI: az network ddos-protection list
- PowerShell: Get-AzDdosProtectionPlan

REMÉDIATION :

1. Créer un plan de protection DDoS Standard
2. Associer le plan aux réseaux virtuels
3. Configurer les alertes et métriques

```
# Créer et activer DDoS Protection
$ddosProtectionPlan = New-AzDdosProtectionPlan -Name "MyDdosProtectionPlan" -ResourceGroupName "MyRG" -Location "France Central"
$vnet = Get-AzVirtualNetwork -Name "MyVNet" -ResourceGroupName "MyRG"
$vnet.DdosProtectionPlan = New-Object Microsoft.Azure.Commands.Network.Models.PSResourceId
$vnet.DdosProtectionPlan.Id = $ddosProtectionPlan.Id
$vnet.EnableDdosProtection = $true
Set-AzVirtualNetwork -VirtualNetwork $vnet
```

VALEUR PAR DÉFAUT :

Basic (gratuit)

6.6.2 *Métriques et alertes DDoS configurées*

MITRE ATT&CK : T1498

DESCRIPTION :

Configurer la surveillance et les alertes pour les métriques DDoS afin de détecter et répondre rapidement aux attaques.

AUDIT :

- Portal > Monitor > Metrics > DDoS Protection
- CLI: az monitor metrics list --resource-type "Microsoft.Network/publicIPAddresses"
- PowerShell: Get-AzMetric -ResourceId $pip.Id -MetricName "IfUnderDDoSAttack"

REMÉDIATION :

1. Configurer des alertes sur les métriques DDoS
2. Créer des règles d'action automatisées
3. Intégrer avec les équipes de réponse

```
# Créer une alerte DDoS
$actionGroup = Get-AzActionGroup -ResourceGroupName "MyRG" -Name "SecurityTeam"
Add-AzMetricAlertRuleV2 -Name "DDoS-Attack-Alert" -ResourceGroupName "MyRG" -WindowSize "PT5M" -Frequency "PT1M" -TargetResourceId
```

VALEUR PAR DÉFAUT :

Pas d'alertes configurées

6.7 — PRIVATE ENDPOINTS ET SERVICE ENDPOINTS

6.7.1 *Private Endpoints pour tous les services PaaS critiques*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Configurer des Private Endpoints pour tous les services PaaS critiques afin d'éliminer l'exposition à Internet public.

AUDIT :

- Portal > Private Link Center > Private endpoints
- CLI: az network private-endpoint list
- PowerShell: Get-AzPrivateEndpoint

REMÉDIATION :

1. Identifier tous les services PaaS exposés publiquement
2. Créer des Private Endpoints appropriés
3. Configurer les zones DNS privées

```
# Créer un Private Endpoint pour SQL Database
$subnet = Get-AzVirtualNetworkSubnetConfig -Name "PrivateEndpointSubnet" -VirtualNetwork $vnet
New-AzPrivateEndpoint -ResourceGroupName "MyRG" -Name "sql-pe" -Location "France Central" -Subnet $subnet -PrivateLinkServiceId "/s
```

VALEUR PAR DÉFAUT :

Accès public autorisé

6.7.2 *Service Endpoints sécurisés configurés*

MITRE ATT&CK : T1071.001

DESCRIPTION :
Utiliser les Service Endpoints comme alternative aux Private Endpoints pour sécuriser l'accès aux services PaaS depuis des réseaux virtuels spécifiques.

AUDIT :

- Portal > Virtual network > Service endpoints
- CLI: az network vnet subnet show --vnet-name MyVNet --name MySubnet --resource-group MyRG --query "serviceEndpoints"
- PowerShell: (Get-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name "MySubnet").ServiceEndpoints

REMÉDIATION :

1. Configurer des Service Endpoints sur les sous-réseaux appropriés
2. Restreindre l'accès aux services depuis ces endpoints uniquement

```
# Configurer Service Endpoint pour Storage
$vnet = Get-AzVirtualNetwork -Name "MyVNet" -ResourceGroupName "MyRG"
$subnet = Get-AzVirtualNetworkSubnetConfig -Name "MySubnet" -VirtualNetwork $vnet
Add-AzVirtualNetworkSubnetConfig -Name "MySubnet" -VirtualNetwork $vnet -AddressPrefix $subnet.AddressPrefix -ServiceEndpoint "Micr
Set-AzVirtualNetwork -VirtualNetwork $vnet
```

VALEUR PAR DÉFAUT :
Pas de Service Endpoints
6.8 — NETWORK MONITORING ET ANALYTICS

6.8.1 *Connection Monitor configuré pour la surveillance réseau*

MITRE ATT&CK : T1071

DESCRIPTION :
Configurer Connection Monitor pour surveiller la connectivité réseau entre les ressources critiques et détecter les problèmes de performance.

AUDIT :

- Portal > Network Watcher > Connection monitor
- CLI: az network watcher connection-monitor list
- PowerShell: Get-AzNetworkWatcherConnectionMonitor

REMÉDIATION :

1. Créer des Connection Monitors pour les flux critiques
2. Configurer des seuils d'alertes
3. Intégrer avec Log Analytics

```
# Créer un Connection Monitor
$nw = Get-AzNetworkWatcher -ResourceGroupName "NetworkWatcherRG" -Name "NetworkWatcher_francecentral"
New-AzNetworkWatcherConnectionMonitor -NetworkWatcher $nw -Name "WebToDatabase" -SourceResourceId $vm1.Id -DestinationResourceId $v
```

VALEUR PAR DÉFAUT :
Non configuré

6.8.2 *Traffic Analytics activé*

MITRE ATT&CK : T1071

DESCRIPTION :
Activer Traffic Analytics pour analyser les patterns de trafic réseau et détecter les anomalies de communication.

AUDIT :

- Portal > Network Watcher > Traffic Analytics
- CLI: az network watcher flow-log show --location francecentral --name MyFlowLog
- PowerShell: Get-AzNetworkWatcherFlowLogStatus -NetworkWatcher $nw -TargetResourceId $nsg.Id

REMÉDIATION :

1. Créer un workspace Log Analytics
2. Activer Traffic Analytics sur les Flow Logs
3. Configurer des requêtes personnalisées

```
# Activer Traffic Analytics
$workspace = Get-AzOperationalInsightsWorkspace -ResourceGroupName "MyRG" -Name "MyWorkspace"
Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher $nw -TargetResourceId $nsg.Id -StorageAccountId $storageAccount.Id -EnableFlowLog
```

VALEUR PAR DÉFAUT :
Désactivé

7.0 — SÉCURITÉ DES MACHINES VIRTUELLES

7.1.1 *Disk encryption activé sur toutes les VMs*

MITRE ATT&CK : T1486

DESCRIPTION :

Azure Disk Encryption doit être activé sur tous les disques des VMs pour chiffrer les données au repos.

AUDIT :

- Portal > Virtual machines > Disks > Encryption
- CLI: az vm encryption show --name

REMÉDIATION :

1. Créer Key Vault avec access policies
2. Activer Azure Disk Encryption
3. Vérifier chiffrement OS et data disks

7.2.1 *Just-In-Time VM access configuré*

MITRE ATT&CK : T1078

DESCRIPTION :

Just-In-Time VM access doit être configuré pour limiter l'exposition RDP/SSH aux fenêtres de temps nécessaires.

AUDIT :

- Portal > Security Center > Just-in-time VM access
- CLI: az security jit-policy list

REMÉDIATION :

1. Activer JIT sur VMs critiques
2. Configurer ports et durées maximales
3. Processus d'approbation pour accès

7.3 — CHIFFREMENT ET PROTECTION DES DISQUES

7.3.1 *Azure Disk Encryption activé sur toutes les VM*

MITRE ATT&CK : T1486

DESCRIPTION :

Activer Azure Disk Encryption sur toutes les machines virtuelles pour chiffrer les disques OS et de données au repos.

AUDIT :

- Portal > Virtual machine > Disks > Encryption settings
- CLI: az vm encryption show --name MyVM --resource-group MyRG
- PowerShell: Get-AzVmDiskEncryptionStatus -ResourceGroupName "MyRG" -VMName "MyVM"

REMÉDIATION :

1. Créer un Azure Key Vault avec les bonnes permissions
2. Activer le chiffrement sur les VM existantes
3. Configurer le chiffrement par défaut pour les nouvelles VM

```
# Activer le chiffrement de disque
Set-AzVMDiskEncryptionExtension -ResourceGroupName "MyRG" -VMName "MyVM" -DiskEncryptionKeyVaultUrl "https://myvault.vault.azure.ne
```

VALEUR PAR DÉFAUT :

Désactivé

7.3.2 *Disques managés avec chiffrement côté serveur*

MITRE ATT&CK : T1486

DESCRIPTION :

Utiliser des disques managés avec chiffrement côté serveur et des clés gérées par le client pour un contrôle total du chiffrement.

AUDIT :

- Portal > Disks > Encryption type
- CLI: az disk show --name MyDisk --resource-group MyRG --query "encryption"
- PowerShell: (Get-AzDisk -ResourceGroupName "MyRG" -DiskName "MyDisk").Encryption

REMÉDIATION :

1. Créer un Disk Encryption Set avec Key Vault
2. Migrer vers des disques avec chiffrement CMK
3. Configurer la rotation automatique des clés

```
# Créer un Disk Encryption Set
$keyVault = Get-AzKeyVault -VaultName "MyVault" -ResourceGroupName "MyRG"
$key = Get-AzKeyVaultKey -VaultName "MyVault" -Name "DiskEncryptionKey"
New-AzDiskEncryptionSet -ResourceGroupName "MyRG" -Name "MyDiskEncryptionSet" -Location "France Central" -KeyUrl $key.Id -SourceVau
```

VALEUR PAR DÉFAUT :

Clés gérées par la plateforme

7.4 — JUST-IN-TIME ACCESS

7.4.1 *Just-In-Time VM Access configuré*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Configurer Just-In-Time VM Access pour limiter l'exposition des ports de gestion des machines virtuelles et réduire la surface d'attaque.

AUDIT :

- Portal > Security Center > Just-in-time VM access
- CLI: az security jit-policy list
- PowerShell: Get-AzJitNetworkAccessPolicy

REMÉDIATION :

1. Activer JIT Access dans Azure Security Center
2. Configurer les ports et durées d'accès
3. Former les utilisateurs aux procédures d'accès

```
# Configurer JIT pour RDP/SSH
$jitPolicy = @{
    "id" = "/subscriptions/{sub}/resourceGroups/MyRG/providers/Microsoft.Compute/virtualMachines/MyVM"
    "ports" = @(
        @{
            "number" = 22
            "protocol" = "TCP"
            "allowedSourceAddressPrefix" = "*"
            "maxRequestAccessDuration" = "PT3H"
        },
        @{
            "number" = 3389
            "protocol" = "TCP"
            "allowedSourceAddressPrefix" = "*"
            "maxRequestAccessDuration" = "PT3H"
        }
    )
}
Set-AzJitNetworkAccessPolicy -ResourceGroupName "MyRG" -Location "France Central" -Name "MyJitPolicy" -VirtualMachine $jitPolicy
```

VALEUR PAR DÉFAUT :

Désactivé

7.4.2 *Bastion Host déployé pour l'accès sécurisé*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Déployer Azure Bastion pour fournir un accès RDP/SSH sécurisé aux machines virtuelles sans exposer les adresses IP publiques.

AUDIT :

- Portal > Bastion > Check deployment status
- CLI: az network bastion list --resource-group MyRG
- PowerShell: Get-AzBastion -ResourceGroupName "MyRG"

REMÉDIATION :

1. Créer un sous-réseau AzureBastionSubnet (/27 minimum)
2. Déployer Azure Bastion dans le réseau virtuel
3. Supprimer les IP publiques des VM

```
# Déployer Azure Bastion
$vnet = Get-AzVirtualNetwork -Name "MyVNet" -ResourceGroupName "MyRG"
$pip = New-AzPublicIpAddress -Name "BastionIP" -ResourceGroupName "MyRG" -Location "France Central" -AllocationMethod "Static" -Sku
New-AzBastion -ResourceGroupName "MyRG" -Name "MyBastion" -PublicIpAddress $pip -VirtualNetwork $vnet
```

VALEUR PAR DÉFAUT :

Non déployé

7.5 — UPDATE MANAGEMENT ET PATCH COMPLIANCE

7.5.1 *Update Management automatisé configuré*

MITRE ATT&CK : T1068

DESCRIPTION :

Configurer Azure Update Management pour automatiser l'installation des mises à jour de sécurité sur toutes les machines virtuelles.

AUDIT :

- Portal > Automation Account > Update Management
- CLI: az vm assess-patches --name MyVM --resource-group MyRG
- PowerShell: Get-AzAutomationSoftwareUpdateConfiguration -AutomationAccountName "MyAutomation" -ResourceGroupName "MyRG"

REMÉDIATION :

1. Créer un compte Automation avec Update Management
2. Associer les VM au service Update Management
3. Configurer des planifications de maintenance

```
# Configurer Update Management
$automationAccount = Get-AzAutomationAccount -ResourceGroupName "MyRG" -Name "MyAutomation"
New-AzAutomationSoftwareUpdateConfiguration -AutomationAccountName "MyAutomation" -ResourceGroupName "MyRG" -Name "SecurityUpdates"
```

VALEUR PAR DÉFAUT :

Mise à jour manuelle

7.5.2 *Boot Diagnostics activé*

MITRE ATT&CK : T1068

DESCRIPTION :

Activer Boot Diagnostics pour surveiller le processus de démarrage des VM et diagnostiquer les problèmes de sécurité ou de performance.

AUDIT :

- Portal > Virtual machine > Boot diagnostics
- CLI: az vm boot-diagnostics get-boot-log --name MyVM --resource-group MyRG
- PowerShell: (Get-AzVM -ResourceGroupName "MyRG" -Name "MyVM").DiagnosticsProfile

REMÉDIATION :

1. Créer un compte de stockage pour les diagnostics
2. Activer Boot Diagnostics sur toutes les VM
3. Surveiller les logs de démarrage

```
# Activer Boot Diagnostics
$storageAccount = Get-AzStorageAccount -ResourceGroupName "MyRG" -Name "diagstorage"
$vm = Get-AzVM -ResourceGroupName "MyRG" -Name "MyVM"
Set-AzVMBootDiagnostic -VM $vm -Enable -ResourceGroupName "MyRG" -StorageAccountName "diagstorage"
Update-AzVM -ResourceGroupName "MyRG" -VM $vm
```

VALEUR PAR DÉFAUT :

Désactivé

7.6 — CONFIDENTIAL COMPUTING

7.6.1 *VM de calcul confidentiel pour données sensibles*

MITRE ATT&CK : T1486

DESCRIPTION :

Utiliser des VM de calcul confidentiel (DCsv2, DCsv3) pour traiter des données hautement sensibles avec chiffrement en mémoire.

AUDIT :

- Portal > Virtual machine > Size (Check DC series)
- CLI: az vm show --name MyVM --resource-group MyRG --query "hardwareProfile.vmSize"
- PowerShell: (Get-AzVM -ResourceGroupName "MyRG" -Name "MyVM").HardwareProfile.VmSize

REMÉDIATION :

1. Identifier les workloads nécessitant un calcul confidentiel
2. Migrer vers des VM DC series
3. Configurer l'attestation avec Azure Attestation

```
# Créer une VM de calcul confidentiel
New-AzVM -ResourceGroupName "MyRG" -Name "ConfidentialVM" -Location "France Central" -VirtualNetworkName "MyVNet" -SubnetName "Conf
```

VALEUR PAR DÉFAUT :

VM standard

7.6.2 *Azure Attestation configuré*

MITRE ATT&CK : T1486

DESCRIPTION :

Configurer Azure Attestation pour vérifier l'intégrité et l'authenticité des environnements de calcul confidentiel.

AUDIT :

- Portal > Azure Attestation > Provider status
- CLI: az attestation list
- PowerShell: Get-AzAttestation

REMÉDIATION :

1. Créer un provider Azure Attestation
2. Configurer les politiques d'attestation
3. Intégrer avec les applications confidentielles

```
# Créer un provider d'attestation
New-AzAttestation -Name "MyAttestationProvider" -ResourceGroupName "MyRG" -Location "France Central"
```

VALEUR PAR DÉFAUT :

Non configuré

8.0 — AZURE KEY VAULT

8.1.1 *Key Vault avec RBAC et soft delete*

MITRE ATT&CK : T1552

DESCRIPTION :

Key Vault doit utiliser RBAC pour l'autorisation et avoir soft delete activé avec purge protection.

AUDIT :

- Portal > Key Vault > Access control (IAM)
- CLI: az keyvault show --name --query "properties.enableSoftDelete"

REMÉDIATION :

1. Migrer vers RBAC authorization
2. Activer soft delete et purge protection
3. Configurer permissions granulaires

8.2.1 *Rotation automatique des clés*

MITRE ATT&CK : T1552

DESCRIPTION :

Les clés dans Key Vault doivent avoir une rotation automatique configurée selon leur criticité.

AUDIT :

- Portal > Key Vault > Keys > Rotation policy
- CLI: az keyvault key rotation-policy show

REMÉDIATION :

1. Définir rotation policies par clé
2. Automatisation via Logic Apps si nécessaire
3. Test des processus de rotation

8.3 — POLITIQUES D'ACCÈS ET RBAC

8.3.1 *RBAC activé au lieu des politiques d'accès classiques*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Utiliser le modèle RBAC Azure pour Key Vault au lieu des politiques d'accès classiques pour une gestion des permissions plus granulaire et auditable.

AUDIT :

- Portal > Key Vault > Access policies > Permission model
- CLI: az keyvault show --name MyKeyVault --query "properties.enableRbacAuthorization"
- PowerShell: (Get-AzKeyVault -VaultName "MyKeyVault").EnableRbacAuthorization

REMÉDIATION :

1. Migrer vers le modèle de permissions RBAC
2. Assigner des rôles granulaires appropriés
3. Supprimer les anciennes politiques d'accès

```
# Activer RBAC sur Key Vault
Update-AzKeyVault -VaultName "MyKeyVault" -EnableRbacAuthorization $true
# Assigner un rôle Key Vault Secrets Officer
New-AzRoleAssignment -SignInName "user@domain.com" -RoleDefinitionName "Key Vault Secrets Officer" -Scope "/subscriptions/{sub}/res
```

VALEUR PAR DÉFAUT :

Politiques d'accès classiques

8.3.2 *Soft Delete et Purge Protection activés*

MITRE ATT&CK : T1485

DESCRIPTION :

Activer Soft Delete et Purge Protection sur tous les Key Vaults pour protéger contre la suppression accidentelle ou malveillante.

AUDIT :

- Portal > Key Vault > Properties > Soft-delete and Purge protection
- CLI: az keyvault show --name MyKeyVault --query "{SoftDelete:properties.enableSoftDelete, PurgeProtection:properties.enablePurgeProtection}"
- PowerShell: Get-AzKeyVault -VaultName "MyKeyVault" | Select-Object EnableSoftDelete, EnablePurgeProtection

REMÉDIATION :

1. Activer Soft Delete avec période de rétention appropriée
2. Activer Purge Protection pour empêcher la suppression définitive
3. Tester la récupération des objets supprimés

```
# Activer Soft Delete et Purge Protection
Update-AzKeyVault -VaultName "MyKeyVault" -EnableSoftDelete -EnablePurgeProtection
```

VALEUR PAR DÉFAUT :

Soft Delete activé, Purge Protection désactivé

8.4 — HSM ET CLÉS MATÉRIELLES

8.4.1 *HSM managé pour les clés critiques*

MITRE ATT&CK : T1552.004

DESCRIPTION :
Utiliser Azure Key Vault Managed HSM pour stocker les clés cryptographiques les plus critiques avec un niveau de sécurité FIPS 140-2 Level 3.

AUDIT :
- Portal > Key Vault > Managed HSM instances
- CLI: az keyvault list --resource-type hsm
- PowerShell: Get-AzKeyVaultManagedHsm

REMÉDIATION :
1. Créer un Managed HSM pour les clés critiques
2. Migrer les clés sensibles vers le HSM
3. Configurer la sauvegarde et la récupération

```
# Créer un Managed HSM
New-AzKeyVaultManagedHsm -Name "MyManagedHSM" -ResourceGroupName "MyRG" -Location "France Central" -Administrator "admin@domain.com
```

VALEUR PAR DÉFAUT :
Key Vault standard

8.4.2 *Clés HSM-backed pour le chiffrement d'infrastructure*

MITRE ATT&CK : T1552.004

DESCRIPTION :
Utiliser des clés protégées par HSM pour le chiffrement de l'infrastructure critique (disques, bases de données, stockage).

AUDIT :
- Portal > Key Vault > Keys > Check key type (HSM)
- CLI: az keyvault key show --vault-name MyKeyVault --name MyKey --query "key.kty"
- PowerShell: (Get-AzKeyVaultKey -VaultName "MyKeyVault" -Name "MyKey").Attributes.HSM

REMÉDIATION :
1. Créer des clés HSM dans Key Vault
2. Configurer les services pour utiliser des clés HSM
3. Documenter l'utilisation des clés HSM

```
# Créer une clé protégée par HSM
Add-AzKeyVaultKey -VaultName "MyKeyVault" -Name "HSMKey" -Destination HSM
```

VALEUR PAR DÉFAUT :
Clés logicielles

8.5 — ROTATION ET GESTION DES SECRETS

8.5.1 *Rotation automatique des secrets configurée*

MITRE ATT&CK : T1552.001

DESCRIPTION :
Configurer la rotation automatique des secrets et certificats dans Key Vault pour maintenir leur fraîcheur et réduire les risques de compromission.

AUDIT :
- Portal > Key Vault > Secrets/Certificates > Rotation policy
- CLI: az keyvault secret show --vault-name MyKeyVault --name MySecret --query "attributes.expires"
- PowerShell: Get-AzKeyVaultSecret -VaultName "MyKeyVault" -Name "MySecret"

REMÉDIATION :
1. Définir des politiques de rotation pour tous les secrets
2. Configurer des Azure Functions pour la rotation automatique
3. Intégrer avec les applications pour la gestion des secrets

```
# Configurer une politique de rotation pour un certificat
$policy = New-AzKeyVaultCertificatePolicy -SecretContentType "application/x-pkcs12" -SubjectName "CN=mycert" -RenewAtNumberOfDaysBe
Add-AzKeyVaultCertificate -VaultName "MyKeyVault" -Name "MyCertificate" -CertificatePolicy $policy
```

VALEUR PAR DÉFAUT :
Rotation manuelle

8.5.2 *Intégration avec Azure DevOps pour les secrets*

MITRE ATT&CK : T1552.001

DESCRIPTION :

Intégrer Key Vault avec Azure DevOps pour sécuriser la gestion des secrets dans les pipelines CI/CD.

AUDIT :

- Portal > Azure DevOps > Pipelines > Variable groups
- CLI: az devops configure --defaults organization=https://dev.azure.com/myorg project=myproject
- PowerShell: Vérification via REST API Azure DevOps

REMÉDIATION :

1. Créer des Service Connections vers Key Vault
2. Configurer des Variable Groups liés à Key Vault
3. Utiliser des Managed Identity pour l'authentification

```
# Assigner des permissions DevOps sur Key Vault
$spn = Get-AzADServicePrincipal -DisplayName "Azure DevOps Service Connection"
Set-AzKeyVaultAccessPolicy -VaultName "MyKeyVault" -ObjectId $spn.Id -PermissionsToSecrets get,list
```

VALEUR PAR DÉFAUT :

Secrets codés en dur

8.6 — SURVEILLANCE ET AUDIT

8.6.1 *Diagnostic settings configurés pour Key Vault*

MITRE ATT&CK : T1552.004

DESCRIPTION :

Configurer les paramètres de diagnostic pour surveiller et auditer toutes les opérations sur Key Vault.

AUDIT :

- Portal > Key Vault > Diagnostic settings
- CLI: az monitor diagnostic-settings list --resource MyKeyVault
- PowerShell: Get-AzDiagnosticSetting -ResourceId $keyVaultId

REMÉDIATION :

1. Créer des paramètres de diagnostic pour Key Vault
2. Envoyer les logs vers Log Analytics et Storage
3. Configurer des alertes sur les opérations sensibles

```
# Configurer les diagnostics Key Vault
$keyVault = Get-AzKeyVault -VaultName "MyKeyVault"
$workspace = Get-AzOperationalInsightsWorkspace -ResourceGroupName "MyRG" -Name "MyWorkspace"
Set-AzDiagnosticSetting -ResourceId $keyVault.ResourceId -WorkspaceId $workspace.ResourceId -Enabled $true -Category @("AuditEvent"
```

VALEUR PAR DÉFAUT :

Diagnostics désactivés

8.6.2 *Alertes configurées pour les accès Key Vault*

MITRE ATT&CK : T1552.004

DESCRIPTION :

Configurer des alertes pour détecter les accès anormaux ou suspects aux Key Vaults et leurs contenus.

AUDIT :

- Portal > Monitor > Alerts > Alert rules for Key Vault
- CLI: az monitor metrics alert list --resource-group MyRG
- PowerShell: Get-AzMetricAlertRuleV2 | Where-Object {$_.TargetResourceType -eq "Microsoft.KeyVault/vaults"}

REMÉDIATION :

1. Créer des alertes sur les métriques Key Vault
2. Configurer des alertes sur les requêtes Log Analytics
3. Intégrer avec les équipes de sécurité

```
# Créer une alerte pour les échecs d'authentification Key Vault
$actionGroup = Get-AzActionGroup -ResourceGroupName "MyRG" -Name "SecurityAlerts"
$keyVault = Get-AzKeyVault -VaultName "MyKeyVault"
Add-AzMetricAlertRuleV2 -Name "KeyVault-AuthFailures" -ResourceGroupName "MyRG" -WindowSize "PT5M" -Frequency "PT1M" -TargetResourc
```

VALEUR PAR DÉFAUT :

Pas d'alertes configurées

9.0 — APP SERVICE SECURITY

9.1.1 *HTTPS obligatoire et TLS 1.2 minimum*

MITRE ATT&CK : T1040

DESCRIPTION :

App Service doit forcer HTTPS avec TLS 1.2 minimum et désactiver les protocoles non sécurisés.

AUDIT :

- Portal > App Service > TLS/SSL settings
- CLI: az webapp config show --name --query "httpsOnly"

REMÉDIATION :

1. HTTPS Only : Enabled
2. Minimum TLS version : 1.2
3. Supprimer protocoles faibles

9.2.1 *Managed Identity pour authentification*

MITRE ATT&CK : T1078.004

DESCRIPTION :

App Service doit utiliser Managed Identity pour l'authentification aux services Azure.

AUDIT :

- Portal > App Service > Identity
- CLI: az webapp identity show --name

REMÉDIATION :

1. Activer System-assigned ou User-assigned identity
2. Configurer permissions aux ressources cibles
3. Modifier code pour utiliser DefaultAzureCredential

9.3 — IDENTITÉS MANAGÉES ET AUTHENTIFICATION

9.3.1 *Managed Identity activée pour tous les App Services*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Activer les identités managées (System-assigned ou User-assigned) pour tous les App Services afin d'éliminer l'utilisation de secrets codés en dur.

AUDIT :

- Portal > App Service > Identity
- CLI: az webapp identity show --name MyApp --resource-group MyRG
- PowerShell: (Get-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp").Identity

REMÉDIATION :

1. Activer System-assigned Managed Identity
2. Assigner les rôles nécessaires aux ressources Azure
3. Modifier le code pour utiliser DefaultAzureCredential

```
# Activer Managed Identity pour App Service
Set-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp" -AssignIdentity $true
# Assigner des permissions Key Vault
$webapp = Get-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp"
New-AzRoleAssignment -ObjectId $webapp.Identity.PrincipalId -RoleDefinitionName "Key Vault Secrets User" -Scope "/subscriptions/{su
```

VALEUR PAR DÉFAUT :

Désactivé

9.3.2 *Authentication/Authorization (EasyAuth) configuré*

MITRE ATT&CK : T1078.004

DESCRIPTION :
Configurer l'authentification et l'autorisation intégrées d'App Service (EasyAuth) pour sécuriser l'accès aux applications.

AUDIT :

- Portal > App Service > Authentication/Authorization
- CLI: az webapp auth show --name MyApp --resource-group MyRG
- PowerShell: Get-AzWebAppAuthSettings -ResourceGroupName "MyRG" -Name "MyApp"

REMÉDIATION :

1. Activer l'authentification App Service
2. Configurer Azure AD comme fournisseur d'identité
3. Définir les actions à effectuer avec les demandes non authentifiées

```
# Configurer l'authentification Azure AD
Set-AzWebAppAuthSettings -ResourceGroupName "MyRG" -Name "MyApp" -Enabled $true -DefaultProvider "AzureActiveDirectory" -Unauthenti
```

VALEUR PAR DÉFAUT :
Désactivé

9.4 — TLS ET CHIFFREMENT

9.4.1 *HTTPS Only obligatoire et TLS 1.2 minimum*

MITRE ATT&CK : T1040

DESCRIPTION :
Forcer HTTPS uniquement et configurer TLS 1.2 comme version minimale pour sécuriser toutes les communications avec l'App Service.

AUDIT :

- Portal > App Service > TLS/SSL settings
- CLI: az webapp show --name MyApp --resource-group MyRG --query "{HttpsOnly:httpsOnly,MinTlsVersion:siteConfig.minTlsVersion}"
- PowerShell: Get-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp" | Select-Object HttpsOnly, MinTlsVersion

REMÉDIATION :

1. Activer HTTPS Only dans les paramètres TLS/SSL
2. Configurer la version TLS minimale à 1.2
3. Tester l'accès HTTP pour vérifier la redirection

```
# Forcer HTTPS et TLS 1.2
Set-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp" -HttpsOnly $true
$webappConfig = (Get-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp").SiteConfig
$webappConfig.MinTlsVersion = "1.2"
Set-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp" -SiteConfig $webappConfig
```

VALEUR PAR DÉFAUT :
HTTP autorisé, TLS 1.0+

9.4.2 *Certificats SSL/TLS gérés automatiquement*

MITRE ATT&CK : T1040

DESCRIPTION :
Utiliser des certificats SSL/TLS gérés par Azure ou App Service pour simplifier la gestion et assurer le renouvellement automatique.

AUDIT :

- Portal > App Service > TLS/SSL settings > Private Key Certificates
- CLI: az webapp config ssl list --resource-group MyRG
- PowerShell: Get-AzWebAppSSLBinding -ResourceGroupName "MyRG" -WebAppName "MyApp"

REMÉDIATION :

1. Configurer un domaine personnalisé
2. Créer un certificat géré App Service gratuit
3. Lier le certificat au domaine

```
# Créer et lier un certificat géré
New-AzWebAppSSLBinding -ResourceGroupName "MyRG" -WebAppName "MyApp" -Name "www.mydomain.com" -CertificateFilePath $null -Thumbprin
```

VALEUR PAR DÉFAUT :
Certificat par défaut uniquement

9.5 — RESTRICTIONS D'ACCÈS ET SÉCURITÉ RÉSEAU

9.5.1 *Restrictions d'accès par IP configurées*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Configurer des restrictions d'accès par adresse IP pour limiter l'accès aux App Services depuis des sources autorisées uniquement.

AUDIT :

- Portal > App Service > Networking > Access restrictions
- CLI: az webapp config access-restriction show --name MyApp --resource-group MyRG
- PowerShell: Get-AzWebAppAccessRestrictionConfig -ResourceGroupName "MyRG" -Name "MyApp"

REMÉDIATION :

1. Identifier les plages IP autorisées
2. Configurer les règles de restriction d'accès
3. Tester l'accès depuis différentes sources

```
# Configurer des restrictions d'accès IP
Add-AzWebAppAccessRestrictionRule -ResourceGroupName "MyRG" -WebAppName "MyApp" -Name "OfficeNetwork" -IpAddress "203.0.113.0/24" -
Add-AzWebAppAccessRestrictionRule -ResourceGroupName "MyRG" -WebAppName "MyApp" -Name "VPN" -IpAddress "10.0.0.0/8" -Priority 110 -
```

VALEUR PAR DÉFAUT :

Accès ouvert

9.5.2 *Private Endpoints pour App Services Premium*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Configurer des Private Endpoints pour les App Services critiques afin d'éliminer l'exposition Internet public.

AUDIT :

- Portal > App Service > Networking > Private endpoints
- CLI: az network private-endpoint list --resource-group MyRG
- PowerShell: Get-AzPrivateEndpoint -ResourceGroupName "MyRG"

REMÉDIATION :

1. Upgrader vers un plan App Service Premium si nécessaire
2. Créer un Private Endpoint dans le réseau virtuel
3. Configurer la zone DNS privée

```
# Créer un Private Endpoint pour App Service
$subnet = Get-AzVirtualNetworkSubnetConfig -Name "PrivateEndpointSubnet" -VirtualNetwork $vnet
New-AzPrivateEndpoint -ResourceGroupName "MyRG" -Name "appservice-pe" -Location "France Central" -Subnet $subnet -PrivateLinkServic
```

VALEUR PAR DÉFAUT :

Accès public

9.6 — SURVEILLANCE ET DIAGNOSTIC

9.6.1 *Application Insights intégré et configuré*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Intégrer Application Insights pour surveiller les performances, diagnostiquer les problèmes et détecter les anomalies de sécurité.

AUDIT :

- Portal > App Service > Application Insights
- CLI: az monitor app-insights component show --app MyApp --resource-group MyRG
- PowerShell: Get-AzApplicationInsights -ResourceGroupName "MyRG" -Name "MyApp-insights"

REMÉDIATION :

1. Créer une ressource Application Insights
2. Connecter l'App Service à Application Insights
3. Configurer des alertes personnalisées

```
# Créer et configurer Application Insights
New-AzApplicationInsights -ResourceGroupName "MyRG" -Name "MyApp-insights" -Location "France Central" -Kind "web"
$insights = Get-AzApplicationInsights -ResourceGroupName "MyRG" -Name "MyApp-insights"
Set-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp" -AppSettings @{"APPINSIGHTS_INSTRUMENTATIONKEY" = $insights.InstrumentationKey
```

VALEUR PAR DÉFAUT :

Non configuré

9.6.2 *Logs de diagnostic configurés*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configurer les logs de diagnostic pour capturer et analyser les événements de sécurité et de performance des App Services.

AUDIT :

- Portal > App Service > Monitoring > Diagnostic settings
- CLI: az monitor diagnostic-settings list --resource MyApp
- PowerShell: Get-AzDiagnosticSetting -ResourceId $appServiceId

REMÉDIATION :

1. Activer les logs de diagnostic appropriés
2. Configurer l'envoi vers Log Analytics
3. Créer des requêtes de surveillance personnalisées

```
# Configurer les diagnostics App Service
$appService = Get-AzWebApp -ResourceGroupName "MyRG" -Name "MyApp"
$workspace = Get-AzOperationalInsightsWorkspace -ResourceGroupName "MyRG" -Name "MyWorkspace"
Set-AzDiagnosticSetting -ResourceId $appService.Id -WorkspaceId $workspace.ResourceId -Enabled $true -Category @("AppServiceHTTPLog
```

VALEUR PAR DÉFAUT :

Logs désactivés

10.0 — AZURE KUBERNETES SERVICE (AKS)

10.1.1 *Cluster AKS privé avec Azure AD integration*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les clusters AKS doivent être privés avec intégration Azure AD pour l'authentification et RBAC Kubernetes.

AUDIT :

- Portal > Kubernetes services > Networking
- CLI: az aks show --name --query "privateCluster"

REMÉDIATION :

1. Déploiement cluster privé
2. Intégration Azure AD
3. Configuration RBAC Kubernetes

10.2.1 *Network policies activées*

MITRE ATT&CK : T1095

DESCRIPTION :

Les network policies doivent être activées pour contrôler la communication entre pods dans le cluster AKS.

AUDIT :

- Portal > Kubernetes services > Networking > Network policy
- CLI: az aks show --name --query "networkProfile.networkPolicy"

REMÉDIATION :

1. Activer Azure Network Policy ou Calico
2. Définir network policies restrictives
3. Test de connectivité inter-pods

10.3 — SÉCURITÉ DES PODS ET RBAC

10.3.1 *Azure AD RBAC intégré pour AKS*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Intégrer Azure AD avec AKS et configurer RBAC pour contrôler l'accès aux ressources Kubernetes basé sur les identités Azure AD.

AUDIT :

- Portal > AKS cluster > Access control (IAM)
- CLI: az aks show --name MyAKS --resource-group MyRG --query "aadProfile"
- PowerShell: (Get-AzAksCluster -ResourceGroupName "MyRG" -Name "MyAKS").AadProfile

REMÉDIATION :

1. Activer l'intégration Azure AD lors de la création du cluster
2. Configurer des RoleBindings et ClusterRoleBindings
3. Assigner des utilisateurs/groupes aux rôles appropriés

```
# Créer un cluster AKS avec intégration Azure AD
New-AzAksCluster -ResourceGroupName "MyRG" -Name "MyAKS" -NodeCount 3 -EnableAadProfile -AadProfileManaged -EnableRbac
# Assigner des rôles AKS
New-AzRoleAssignment -SignInName "admin@domain.com" -RoleDefinitionName "Azure Kubernetes Service Cluster Admin Role" -Scope "/subs
```

VALEUR PAR DÉFAUT :

Authentification locale

10.3.2 *Pod Security Standards configurés*

MITRE ATT&CK : T1611

DESCRIPTION :

Implémenter les Pod Security Standards pour restreindre les capacités des pods et réduire la surface d'attaque.

AUDIT :

- CLI: kubectl get podsecuritypolicy
- CLI: az aks show --name MyAKS --resource-group MyRG --query "podSecurityProfile"
- PowerShell: kubectl get namespace default -o yaml | grep -i security

REMÉDIATION :

1. Activer Pod Security Standards au niveau du namespace
2. Configurer les profils de sécurité appropriés (restricted/baseline)
3. Tester les déploiements avec les nouvelles politiques

```
# Configurer Pod Security Standards
kubectl label namespace default pod-security.kubernetes.io/enforce=restricted
kubectl label namespace default pod-security.kubernetes.io/audit=restricted
kubectl label namespace default pod-security.kubernetes.io/warn=restricted
```

VALEUR PAR DÉFAUT :

Politiques permissives

10.4 — NETWORK POLICIES ET SEGMENTATION

10.4.1 *Network Policies Kubernetes activées*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Configurer des Network Policies Kubernetes pour contrôler le trafic réseau entre les pods et implémenter la segmentation.

AUDIT :

- CLI: kubectl get networkpolicies --all-namespaces
- CLI: az aks show --name MyAKS --resource-group MyRG --query "networkProfile.networkPolicy"
- PowerShell: kubectl describe networkpolicy

REMÉDIATION :

1. Activer Calico ou Azure Network Policy
2. Créer des NetworkPolicies par namespace
3. Implémenter le principe de moindre privilège réseau

```
# Exemple de Network Policy restrictive
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: deny-all-ingress
  namespace: production
spec:
  podSelector: {}
  policyTypes:
  - Ingress
```

VALEUR PAR DÉFAUT :

Pas de restrictions réseau

10.4.2 *Private Cluster avec API Server privé*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Configurer AKS comme cluster privé pour que l'API Server ne soit accessible que depuis des réseaux privés.

AUDIT :

- Portal > AKS cluster > Networking > Check Private cluster
- CLI: az aks show --name MyAKS --resource-group MyRG --query "apiServerAccessProfile"
- PowerShell: (Get-AzAksCluster -ResourceGroupName "MyRG" -Name "MyAKS").ApiServerAccessProfile

REMÉDIATION :

1. Créer un cluster AKS privé ou migrer un cluster existant
2. Configurer des plages IP autorisées si nécessaire
3. Utiliser Azure Bastion ou VPN pour l'accès administratif

```
# Créer un cluster AKS privé
New-AzAksCluster -ResourceGroupName "MyRG" -Name "MyPrivateAKS" -EnablePrivateCluster -PrivateDnsZone "System"
```

VALEUR PAR DÉFAUT :

API Server public

10.5 — SECRETS ET IDENTITÉS

10.5.1 *Azure Key Vault Provider for Secrets Store CSI Driver*

MITRE ATT&CK : T1552.007

DESCRIPTION :
Utiliser le CSI Driver Azure Key Vault pour injecter des secrets depuis Key Vault dans les pods AKS de manière sécurisée.

AUDIT :

- CLI: kubectl get pods -n kube-system | grep secrets-store-csi-driver
- CLI: az aks addon list --cluster-name MyAKS --resource-group MyRG
- PowerShell: kubectl get secretproviderclass

REMÉDIATION :

1. Activer l'addon Azure Key Vault Provider
2. Configurer des SecretProviderClass
3. Modifier les déploiements pour utiliser les volumes CSI

```
# Activer le CSI driver Key Vault
az aks enable-addons --addons azure-keyvault-secrets-provider --name MyAKS --resource-group MyRG
```

VALEUR PAR DÉFAUT :
Secrets Kubernetes natifs

10.5.2 *Workload Identity pour les pods*

MITRE ATT&CK : T1078.004

DESCRIPTION :
Configurer Azure AD Workload Identity pour permettre aux pods d'authentifier avec les services Azure sans stocker de secrets.

AUDIT :

- CLI: az aks show --name MyAKS --resource-group MyRG --query "oidcIssuerProfile"
- CLI: kubectl get serviceaccount -o yaml | grep azure.workload.identity
- PowerShell: Get-AzAksCluster -Name "MyAKS" -ResourceGroupName "MyRG"

REMÉDIATION :

1. Activer OIDC Issuer et Workload Identity sur AKS
2. Créer des identités managées utilisateur
3. Configurer la fédération d'identité

```
# Activer Workload Identity
az aks update --resource-group MyRG --name MyAKS --enable-oidc-issuer --enable-workload-identity
```

VALEUR PAR DÉFAUT :
Service Account tokens

10.6 — IMAGE SECURITY ET SCANNING

10.6.1 *Azure Defender for containers activé*

MITRE ATT&CK : T1611

DESCRIPTION :
Activer Azure Defender for containers pour scanner les vulnérabilités dans les images et surveiller l'activité des clusters.

AUDIT :

- Portal > Security Center > Pricing & settings > Containers
- CLI: az security pricing show --name "Containers"
- PowerShell: Get-AzSecurityPricing -Name "Containers"

REMÉDIATION :

1. Activer Defender for containers dans Security Center
2. Configurer les agents de surveillance
3. Examiner les recommandations de sécurité

```
# Activer Defender for containers
Set-AzSecurityPricing -Name "Containers" -PricingTier "Standard"
```

VALEUR PAR DÉFAUT :
Tier gratuit

10.6.2 *Admission controllers sécurisés configurés*

MITRE ATT&CK : T1611

DESCRIPTION :
Configurer des admission controllers pour valider et modifier les ressources Kubernetes avant leur création selon les politiques de sécurité.

AUDIT :

- CLI: kubectl get validatingadmissionwebhooks
- CLI: kubectl get mutatingadmissionwebhooks
- Portal > AKS > Policies (si Azure Policy addon activé)

REMÉDIATION :

1. Activer l'addon Azure Policy pour AKS
2. Assigner des définitions de politique appropriées
3. Configurer des admission controllers personnalisés si nécessaire

```
# Activer Azure Policy addon
az aks enable-addons --addons azure-policy --name MyAKS --resource-group MyRG
```

VALEUR PAR DÉFAUT :
Admission controllers de base uniquement

11.0 — GOVERNANCE ET COMPLIANCE

11.1.1 *Azure Policy initiatives assignées*

MITRE ATT&CK : T1562

DESCRIPTION :

Les initiatives Azure Policy pertinentes doivent être assignées : Azure Security Benchmark, CIS, compliance frameworks.

AUDIT :

- Portal > Policy > Assignments
- CLI: az policy assignment list

REMÉDIATION :

1. Assigner Azure Security Benchmark
2. Assigner initiatives compliance requises
3. Configurer remediation automatique

11.2.1 *Resource locks sur ressources critiques*

MITRE ATT&CK : T1485

DESCRIPTION :

Des verrous de ressources doivent être appliqués sur les ressources critiques pour prévenir la suppression accidentelle.

AUDIT :

- Portal > Resources > Locks
- CLI: az lock list

REMÉDIATION :

1. Identifier ressources critiques
2. Appliquer CanNotDelete locks
3. Documentation des exceptions

11.3 — AZURE POLICY ET BLUEPRINTS

11.3.1 *Azure Policy configuré avec initiatives de sécurité*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Implémenter Azure Policy avec les initiatives de sécurité intégrées pour assurer la conformité continue des ressources Azure.

AUDIT :

- Portal > Policy > Compliance
- CLI: az policy assignment list --scope /subscriptions/{subscription-id}
- PowerShell: Get-AzPolicyAssignment

REMÉDIATION :

1. Assigner l'initiative "Azure Security Benchmark"
2. Configurer des politiques personnalisées selon les besoins
3. Surveiller la conformité et corriger les non-conformités

```
# Assigner Azure Security Benchmark
$subscription = Get-AzSubscription
New-AzPolicyAssignment -Name "Azure-Security-Benchmark" -DisplayName "Azure Security Benchmark Initiative" -PolicySetDefinition "/p
```

VALEUR PAR DÉFAUT :

Pas de politiques assignées

11.3.2 *Azure Blueprints pour la gouvernance d'entreprise*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Utiliser Azure Blueprints pour déployer de manière cohérente des environnements conformes avec les politiques, rôles et ressources prédéfinies.

AUDIT :

- Portal > Blueprints > Blueprint definitions
- CLI: az blueprint list --management-group {mg-id}
- PowerShell: Get-AzBlueprint

REMÉDIATION :

1. Créer des définitions de blueprint pour chaque environnement
2. Inclure les politiques, rôles et templates ARM nécessaires
3. Assigner les blueprints aux scopes appropriés

```
# Créer un blueprint de sécurité
Import-AzBlueprintWithArtifact -InputPath "./security-blueprint" -ManagementGroupId "MyMG" -Name "SecurityBlueprint"
```

VALEUR PAR DÉFAUT :

Pas de blueprints configurés

11.4 — MANAGEMENT GROUPS ET STRUCTURE

11.4.1 *Management Groups hiérarchiques configurés*

MITRE ATT&CK : T1078.004

DESCRIPTION :
Structurer les abonnements Azure dans des Management Groups hiérarchiques pour appliquer des politiques et contrôles de gouvernance cohérents.

AUDIT :

- Portal > Management groups
- CLI: az account management-group list
- PowerShell: Get-AzManagementGroup

REMÉDIATION :

1. Créer une hiérarchie de Management Groups appropriée
2. Déplacer les abonnements dans les bons groupes
3. Appliquer des politiques au niveau des Management Groups

```
# Créer une structure de Management Groups
New-AzManagementGroup -GroupName "Corp" -DisplayName "Corporate"
New-AzManagementGroup -GroupName "Prod" -DisplayName "Production" -ParentId "/providers/Microsoft.Management/managementGroups/Corp"
New-AzManagementGroup -GroupName "Dev" -DisplayName "Development" -ParentId "/providers/Microsoft.Management/managementGroups/Corp"
```

VALEUR PAR DÉFAUT :
Structure plate

11.4.2 *Resource locks sur les ressources critiques*

MITRE ATT&CK : T1485

DESCRIPTION :
Appliquer des verrous de ressources (Resource Locks) sur les ressources critiques pour empêcher la suppression ou modification accidentelle.

AUDIT :

- Portal > Resource group > Locks
- CLI: az lock list --resource-group MyRG
- PowerShell: Get-AzResourceLock -ResourceGroupName "MyRG"

REMÉDIATION :

1. Identifier les ressources critiques nécessitant une protection
2. Appliquer des verrous ReadOnly ou CanNotDelete appropriés
3. Documenter les procédures de gestion des verrous

```
# Créer des verrous sur les ressources critiques
New-AzResourceLock -LockName "ProductionVNetLock" -LockLevel CanNotDelete -ResourceGroupName "Production-Network-RG" -ResourceName
```

VALEUR PAR DÉFAUT :
Pas de verrous
11.5 — COST MANAGEMENT ET ALERTES

11.5.1 *Budgets et alertes de coûts configurés*

MITRE ATT&CK : T1496

DESCRIPTION :
Configurer des budgets et alertes de coûts pour surveiller les dépenses Azure et détecter les anomalies de consommation qui pourraient indiquer une compromission.

AUDIT :

- Portal > Cost Management + Billing > Budgets
- CLI: az consumption budget list
- PowerShell: Get-AzConsumptionBudget

REMÉDIATION :

1. Créer des budgets par abonnement et resource group
2. Configurer des alertes à différents seuils (50%, 75%, 90%)
3. Intégrer les alertes avec les équipes de sécurité

```
# Créer un budget avec alertes
$budget = @{
    Amount = 1000
    TimeGrain = "Monthly"
    TimePeriod = @{
        StartDate = "2024-01-01T00:00:00Z"
        EndDate = "2024-12-31T23:59:59Z"
    }
}
New-AzConsumptionBudget -Name "Security-Budget" -Amount 1000 -Category "Cost" -TimeGrain "Monthly" -StartDate "2024-01-01" -EndDate
```

VALEUR PAR DÉFAUT :
Pas de budgets configurés

11.5.2 *Cost anomaly detection activé*

MITRE ATT&CK : T1496

DESCRIPTION :
Activer la détection d'anomalies de coûts pour identifier automatiquement les pics de consommation inhabituels qui pourraient indiquer une activité malveillante.

AUDIT :
- Portal > Cost Management + Billing > Cost alerts > Anomaly detection
- CLI: az consumption budget list --subscription {sub-id}
- PowerShell: Vérification via l'interface Cost Management

REMÉDIATION :
1. Activer la détection d'anomalies dans Cost Management
2. Configurer les destinataires des alertes d'anomalie
3. Établir des procédures de réponse aux anomalies de coût

```
# Configuration via PowerShell nécessite des appels REST API
# Exemple de configuration d'alerte de coût
$alertRule = @{
    name = "CostAnomalyAlert"
    properties = @{
        enabled = $true
        threshold = @{
            operator = "GreaterThan"
            value = 500
        }
    }
}
```

VALEUR PAR DÉFAUT :
Désactivé

11.6 — COMPLIANCE ET AUDITING

11.6.1 *Azure Compliance Manager configuré*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Utiliser Microsoft Compliance Manager pour évaluer et gérer la posture de conformité par rapport aux réglementations applicables.

AUDIT :
- Portal > Microsoft Purview compliance portal > Compliance Manager
- Vérification des scores de conformité et des actions d'amélioration
- Évaluation des contrôles selon les frameworks applicables

REMÉDIATION :
1. Configurer les évaluations appropriées (GDPR, ISO 27001, etc.)
2. Implémenter les actions d'amélioration recommandées
3. Surveiller régulièrement le score de conformité

```
# La gestion de Compliance Manager se fait principalement via le portail
# Exemple d'activation de la surveillance de conformité
Enable-AzSecurityContact -Email "compliance@company.com" -Phone "+33123456789" -AlertAdmin -AlertNotifications
```

VALEUR PAR DÉFAUT :
Non configuré

11.6.2 *Retention policies pour la gouvernance des données*

MITRE ATT&CK : T1485

DESCRIPTION :
Configurer des politiques de rétention pour les logs, données et ressources selon les exigences légales et de conformité.

AUDIT :
- Portal > Storage Account > Lifecycle management
- Portal > Log Analytics > Data retention
- CLI: az monitor log-analytics workspace show --workspace-name MyWorkspace --resource-group MyRG --query "retentionInDays"

REMÉDIATION :
1. Définir les exigences de rétention par type de données
2. Configurer des politiques de cycle de vie automatiques
3. Implémenter des politiques de suppression sécurisée

```
# Configurer la rétention dans Log Analytics
Set-AzOperationalInsightsWorkspace -ResourceGroupName "MyRG" -Name "MyWorkspace" -RetentionInDays 90
# Configurer le cycle de vie du stockage
$action = Add-AzStorageAccountManagementPolicyAction -BaseBlobAction Delete -daysAfterModificationGreaterThan 2555
$filter = New-AzStorageAccountManagementPolicyFilter -PrefixMatch "compliance-logs"
$rule = New-AzStorageAccountManagementPolicyRule -Name "ComplianceRetention" -Action $action -Filter $filter
Set-AzStorageAccountManagementPolicy -ResourceGroupName "MyRG" -StorageAccountName "compliancestorage" -Rule $rule
```

VALEUR PAR DÉFAUT :
Rétention par défaut (30 jours pour Log Analytics)

12.0 — SECRETS ET CHIFFREMENT

12.1.1 *Customer Managed Keys pour services critiques*

MITRE ATT&CK : T1486

DESCRIPTION :

Les services critiques doivent utiliser Customer Managed Keys pour le chiffrement plutôt que Microsoft Managed Keys.

AUDIT :

- Portal > Service > Encryption settings
- CLI: Vérification selon le service

REMÉDIATION :

1. Évaluer criticité des données
2. Configurer CMK dans Key Vault
3. Migration des services vers CMK

12.2.1 *Secrets rotation et lifecycle management*

MITRE ATT&CK : T1552

DESCRIPTION :

Tous les secrets doivent avoir une gestion de cycle de vie avec rotation automatique et alertes d'expiration.

AUDIT :

- Portal > Key Vault > Secrets > Expiration dates
- CLI: az keyvault secret list --vault-name --query "[].attributes.expires"

REMÉDIATION :

1. Audit des secrets sans expiration
2. Définir rotation policies
3. Alertes avant expiration

12.3 — CHIFFREMENT DE BOUT EN BOUT

12.3.1 *Always Encrypted pour SQL Database*

MITRE ATT&CK : T1486

DESCRIPTION :

Configurer Always Encrypted pour Azure SQL Database afin de chiffrer les données sensibles côté client et maintenir le contrôle des clés de chiffrement.

AUDIT :

- Portal > SQL Database > Security > Always Encrypted keys
- CLI: az sql db show --name MyDB --server MyServer --resource-group MyRG --query "encryption"
- PowerShell: Get-AzSqlDatabaseTransparentDataEncryption -ResourceGroupName "MyRG" -ServerName "MyServer" -DatabaseName "MyDB"

REMÉDIATION :

1. Configurer un Column Master Key dans Azure Key Vault
2. Créer des Column Encryption Keys
3. Chiffrer les colonnes sensibles avec SSMS ou T-SQL

```
# Configurer Always Encrypted via PowerShell
$keyVault = Get-AzKeyVault -VaultName "MyKeyVault"
New-AzKeyVaultKey -VaultName "MyKeyVault" -Name "AlwaysEncryptedKey" -Destination Software
# Configuration des colonnes chiffrées via SSMS ou scripts T-SQL
```

VALEUR PAR DÉFAUT :

Données en clair

12.3.2 *Chiffrement en transit obligatoire (TLS 1.2+)*

MITRE ATT&CK : T1040

DESCRIPTION :

Forcer le chiffrement TLS 1.2 ou supérieur pour toutes les communications avec les services Azure afin de protéger les données en transit.

AUDIT :

- Portal > SQL Server > Security > Firewalls and virtual networks > Minimum TLS version
- CLI: az sql server show --name MyServer --resource-group MyRG --query "minimalTlsVersion"
- PowerShell: (Get-AzSqlServer -ResourceGroupName "MyRG" -ServerName "MyServer").MinimalTlsVersion

REMÉDIATION :

1. Configurer TLS 1.2 minimum sur tous les services
2. Vérifier les applications clientes pour la compatibilité TLS 1.2
3. Tester les connexions après activation

```
# Forcer TLS 1.2 sur SQL Server
Set-AzSqlServer -ResourceGroupName "MyRG" -ServerName "MyServer" -MinimalTlsVersion "1.2"
# Pour Storage Account
Set-AzStorageAccount -ResourceGroupName "MyRG" -Name "mystorageaccount" -MinimumTlsVersion TLS1_2
```

VALEUR PAR DÉFAUT :

TLS 1.0+ autorisé

12.4 — GESTION DES CERTIFICATS

12.4.1 *Certificats avec renouvellement automatique*

MITRE ATT&CK : T1552.004

DESCRIPTION :

Configurer le renouvellement automatique des certificats SSL/TLS dans Key Vault pour éviter les expirations et maintenir la sécurité.

AUDIT :

- Portal > Key Vault > Certificates > Issuance policy
- CLI: az keyvault certificate show --vault-name MyKeyVault --name MyCert --query "policy"
- PowerShell: Get-AzKeyVaultCertificatePolicy -VaultName "MyKeyVault" -Name "MyCert"

REMÉDIATION :

1. Configurer des Certificate Authorities intégrées (DigiCert, GlobalSign)
2. Définir des politiques de renouvellement automatique
3. Configurer des notifications avant expiration

```
# Configurer une politique de certificat avec renouvellement auto
$policy = New-AzKeyVaultCertificatePolicy -SecretContentType "application/x-pkcs12" -SubjectName "CN=www.mydomain.com" -IssuerName
Add-AzKeyVaultCertificate -VaultName "MyKeyVault" -Name "WebsiteCert" -CertificatePolicy $policy
```

VALEUR PAR DÉFAUT :

Renouvellement manuel

12.4.2 *Monitoring des expirations de certificats*

MITRE ATT&CK : T1552.004

DESCRIPTION :

Surveiller les dates d'expiration des certificats et configurer des alertes pour éviter les interruptions de service.

AUDIT :

- Portal > Key Vault > Certificates > Check expiration dates
- CLI: az keyvault certificate list --vault-name MyKeyVault --query "[].{Name:name,Expires:attributes.expires}"
- PowerShell: Get-AzKeyVaultCertificate -VaultName "MyKeyVault" | Select-Object Name, Expires

REMÉDIATION :

1. Créer des requêtes Log Analytics pour surveiller les expirations
2. Configurer des alertes à 90, 30 et 7 jours avant expiration
3. Automatiser les notifications aux équipes responsables

```
# Créer une alerte pour les certificats expirant bientôt
$actionGroup = Get-AzActionGroup -ResourceGroupName "MyRG" -Name "CertificateAlerts"
# Requête KQL pour les certificats expirant dans 30 jours
$query = "KeyVaultData | where OperationName == 'CertificateNearExpiry' | where TimeGenerated > ago(1d)"
```

VALEUR PAR DÉFAUT :

Pas de surveillance automatique

12.5 — HARDWARE SECURITY MODULES (HSM)

12.5.1 *Dedicated HSM pour les workloads ultra-sensibles*

MITRE ATT&CK : T1552.004

DESCRIPTION :
Utiliser Azure Dedicated HSM pour les workloads nécessitant un contrôle exclusif du matériel cryptographique et une certification FIPS 140-2 Level 3.

AUDIT :

- Portal > Azure Dedicated HSM
- CLI: az dedicated-hsm list
- PowerShell: Get-AzDedicatedHsm

REMÉDIATION :

1. Évaluer les besoins en HSM dédié vs Managed HSM
2. Déployer Dedicated HSM dans un réseau virtuel
3. Configurer la haute disponibilité et la sauvegarde

```
# Déployer un Dedicated HSM (nécessite une planification préalable)
New-AzDedicatedHsm -Name "MyDedicatedHSM" -ResourceGroupName "MyRG" -Location "France Central" -NetworkProfile $networkProfile
```

VALEUR PAR DÉFAUT :
Non disponible

12.5.2 *Key Management interoperable avec PKCS#11*

MITRE ATT&CK : T1552.004

DESCRIPTION :
Configurer la gestion des clés avec support PKCS#11 pour l'interopérabilité avec les applications existantes utilisant des standards HSM.

AUDIT :

- Documentation technique des HSM déployés
- Test de compatibilité PKCS#11 avec les applications
- Vérification des interfaces cryptographiques

REMÉDIATION :

1. Configurer les bibliothèques PKCS#11 appropriées
2. Tester l'intégration avec les applications critiques
3. Documenter les procédures d'utilisation PKCS#11

```
# Configuration PKCS#11 (exemple pour Linux)
# Installation des bibliothèques HSM
sudo apt-get install opensc-pkcs11
# Configuration des applications pour utiliser PKCS#11
export PKCS11_MODULE="/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so"
```

VALEUR PAR DÉFAUT :
APIs propriétaires uniquement

13.0 — CONTAINERS ET REGISTRIES

13.1.1 *Container Registry scanning des vulnérabilités*

MITRE ATT&CK : T1203

DESCRIPTION :

Azure Container Registry doit scanner automatiquement les images pour détecter les vulnérabilités.

AUDIT :

- Portal > Container Registry > Repositories > Scan results
- CLI: az acr task list --registry

REMÉDIATION :

1. Activer vulnerability scanning
2. Policies de blocage images vulnérables
3. Processus de remediation

13.2.1 *Container Registry access restreint*

MITRE ATT&CK : T1190

DESCRIPTION :

L'accès à Container Registry doit être restreint avec authentification appropriée et network rules.

AUDIT :

- Portal > Container Registry > Access control (IAM)
- CLI: az acr show --name --query "networkRuleSet"

REMÉDIATION :

1. RBAC avec rôles granulaires
2. Network rules restrictives
3. Private endpoints si requis

13.3 — AZURE CONTAINER REGISTRY SECURITY

13.3.1 *Vulnerability scanning activé sur ACR*

MITRE ATT&CK : T1610

DESCRIPTION :

Activer l'analyse des vulnérabilités sur Azure Container Registry pour scanner automatiquement toutes les images pusheés et détecter les failles de sécurité.

AUDIT :

- Portal > Container Registry > Security > Vulnerability scanning
- CLI: az acr task list --registry MyACR --resource-group MyRG
- PowerShell: Get-AzContainerRegistryReplication -RegistryName "MyACR" -ResourceGroupName "MyRG"

REMÉDIATION :

1. Upgrader vers ACR Premium tier si nécessaire
2. Activer Defender for container registries
3. Configurer des politiques de quarantaine pour les images vulnérables

```
# Activer Defender for container registries
Set-AzSecurityPricing -Name "ContainerRegistry" -PricingTier "Standard"
# Créer un ACR Premium avec scanning
New-AzContainerRegistry -ResourceGroupName "MyRG" -Name "MyACR" -Sku "Premium" -Location "France Central" -EnableAdminUser $false
```

VALEUR PAR DÉFAUT :

Scanning désactivé

13.3.2 *Content Trust et signature d'images*

MITRE ATT&CK : T1195.001

DESCRIPTION :
Activer Docker Content Trust et la signature d'images pour garantir l'intégrité et l'authenticité des images de conteneurs.

AUDIT :

- Portal > Container Registry > Policies > Content trust
- CLI: az acr config content-trust show --registry MyACR
- PowerShell: Vérification via Azure REST API

REMÉDIATION :

1. Activer Content Trust sur ACR Premium
2. Configurer Notary pour la signature d'images
3. Forcer la vérification de signature dans les clusters

```
# Activer Content Trust (nécessite ACR Premium)
az acr config content-trust update --registry MyACR --status enabled
```

VALEUR PAR DÉFAUT :
Content Trust désactivé
13.4 — POLITIQUES DE SÉCURITÉ CONTAINERS

13.4.1 *Quarantine policy pour les images vulnérables*

MITRE ATT&CK : T1610

DESCRIPTION :
Configurer des politiques de quarantaine automatique pour bloquer le déploiement d'images contenant des vulnérabilités critiques ou élevées.

AUDIT :

- Portal > Container Registry > Policies > Quarantine policy
- CLI: az acr config quarantine show --registry MyACR
- PowerShell: Vérification via les métriques de sécurité ACR

REMÉDIATION :

1. Configurer la quarantaine automatique basée sur les scores CVSS
2. Définir des exceptions pour les images approuvées
3. Intégrer avec les pipelines CI/CD pour bloquer les déploiements

```
# Activer la quarantaine pour les vulnérabilités élevées
az acr config quarantine update --registry MyACR --status enabled --policy-type "VulnerabilityBasedPolicy"
```

VALEUR PAR DÉFAUT :
Pas de quarantaine automatique

13.4.2 *Image scanning automatisé dans les pipelines*

MITRE ATT&CK : T1610

DESCRIPTION :
Intégrer l'analyse de sécurité des images dans les pipelines CI/CD pour détecter les vulnérabilités avant le déploiement en production.

AUDIT :

- Portal > Azure DevOps > Pipelines > Security tasks
- Vérification des tasks de scanning dans les YAML pipelines
- Review des rapports de sécurité des builds

REMÉDIATION :

1. Ajouter des tasks de scanning dans les pipelines Azure DevOps
2. Configurer des gates de sécurité pour bloquer les déploiements
3. Intégrer avec des outils comme Twistlock, Aqua ou Defender for DevOps

```
# Exemple de pipeline Azure DevOps avec scanning
- task: ContainerScan@0
  displayName: 'Scan container images'
  inputs:
    containerRegistry: 'MyACR'
    repository: 'myapp'
    tag: '$(Build.BuildId)'
    scanType: 'Basic'
```

VALEUR PAR DÉFAUT :
Pas de scanning automatisé
13.5 — RUNTIME SECURITY

13.5.1 *Runtime protection avec Defender for Containers*

MITRE ATT&CK : T1611

DESCRIPTION :
Activer Defender for Containers pour la protection runtime et la détection de menaces dans les environnements de conteneurs.

AUDIT :
- Portal > Security Center > Pricing & settings > Containers plan
- CLI: az security pricing show --name "Containers"
- PowerShell: Get-AzSecurityPricing -Name "Containers"

REMÉDIATION :
1. Activer Defender for Containers sur tous les clusters
2. Configurer les agents de surveillance sur les nœuds
3. Surveiller les alertes de sécurité runtime

```
# Activer Defender for Containers
Set-AzSecurityPricing -Name "Containers" -PricingTier "Standard"
# Installer l'extension Defender sur AKS
az k8s-extension create --name microsoft.azuresecuritypack.defender --cluster-type managedClusters --cluster-name MyAKS --resource-
```

VALEUR PAR DÉFAUT :
Protection de base uniquement

13.5.2 *Network segmentation pour containers*

MITRE ATT&CK : T1071.001

DESCRIPTION :
Implémenter la segmentation réseau pour isoler les workloads de conteneurs et limiter la propagation latérale en cas de compromission.

AUDIT :
- CLI: kubectl get networkpolicies --all-namespaces
- Portal > AKS > Networking > Network policy
- Vérification des règles de micro-segmentation

REMÉDIATION :
1. Créer des Network Policies Kubernetes granulaires
2. Implémenter la segmentation par namespace et labels
3. Utiliser des solutions comme Calico ou Azure Network Policy

```
# Exemple de Network Policy pour isolation
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: deny-all-ingress
  namespace: production
spec:
  podSelector: {}
  policyTypes:
  - Ingress
  - Egress
  egress:
  - to: []
    ports:
    - protocol: TCP
      port: 443
    - protocol: TCP
      port: 53
    - protocol: UDP
      port: 53
```

VALEUR PAR DÉFAUT :
Communication ouverte entre pods

13.6 — COMPLIANCE ET GOUVERNANCE

13.6.1 *Image compliance policies avec OPA Gatekeeper*

MITRE ATT&CK : T1610

DESCRIPTION :

Utiliser OPA Gatekeeper pour implémenter des politiques de conformité des images et empêcher le déploiement d'images non conformes.

AUDIT :

- CLI: kubectl get constraint
- CLI: kubectl get constrainttemplate
- Portal > AKS > Policies (si Azure Policy est activé)

REMÉDIATION :

1. Installer OPA Gatekeeper sur le cluster AKS
2. Créer des ConstraintTemplates pour la validation d'images
3. Appliquer des Constraints pour enforcer les politiques

```
# Exemple de constraint pour images approuvées uniquement
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
  name: allowedrepos
spec:
  crd:
    spec:
      names:
        kind: AllowedRepos
      validation:
        type: object
        properties:
          repos:
            type: array
            items:
              type: string
  targets:
    - target: admission.k8s.gatekeeper.sh
      rego: |
        package allowedrepos
        violation[{"msg": msg}] {
          container := input.review.object.spec.containers[_]
          not starts_with(container.image, input.parameters.repos[_])
          msg := "Image not from approved registry"
        }
```

VALEUR PAR DÉFAUT :

Pas de validation d'images automatisée

14.0 — BACKUP ET DISASTER RECOVERY

14.1.1 *Azure Backup configuré pour ressources critiques*

MITRE ATT&CK : T1485

DESCRIPTION :

Azure Backup doit être configuré pour toutes les ressources critiques avec politique de rétention appropriée.

AUDIT :

- Portal > Recovery Services vault > Backup items
- CLI: az backup item list --vault-name

REMÉDIATION :

1. Identifier ressources à sauvegarder
2. Configurer backup policies
3. Test de restauration réguliers

14.2.1 *Site Recovery pour continuité d'activité*

MITRE ATT&CK : T1485

DESCRIPTION :

Azure Site Recovery doit être configuré pour les applications critiques nécessitant un RTO faible.

AUDIT :

- Portal > Recovery Services vault > Site Recovery
- CLI: az site-recovery vault list

REMÉDIATION :

1. Évaluer besoins RTO/RPO
2. Configurer réplication vers région secondaire
3. Tests de failover réguliers

14.3 — AZURE BACKUP AVANCÉ

14.3.1 *Backup cross-region pour la continuité d'activité*

MITRE ATT&CK : T1485

DESCRIPTION :

Configurer des sauvegardes cross-region avec Azure Backup pour assurer la récupération en cas de défaillance régionale majeure.

AUDIT :

- Portal > Recovery Services vault > Backup items > Check geo-replication
- CLI: az backup vault show --name MyVault --resource-group MyRG --query "properties.storageType"
- PowerShell: Get-AzRecoveryServicesVault -ResourceGroupName "MyRG" -Name "MyVault"

REMÉDIATION :

1. Configurer le stockage géo-redondant (GRS) sur les Recovery Services vaults
2. Activer Cross Region Restore si disponible
3. Tester la restauration depuis la région secondaire

```
# Configurer le stockage géo-redondant
$vault = Get-AzRecoveryServicesVault -ResourceGroupName "MyRG" -Name "MyVault"
Set-AzRecoveryServicesVaultContext -Vault $vault
Set-AzRecoveryServicesBackupProperty -Vault $vault -BackupStorageRedundancy GeoRedundant
```

VALEUR PAR DÉFAUT :

Stockage localement redondant (LRS)

14.3.2 *Immutable backup pour protection ransomware*

MITRE ATT&CK : T1486

DESCRIPTION :
Activer les sauvegardes immuables pour protéger les données de sauvegarde contre la suppression ou modification malveillante, notamment lors d'attaques ransomware.

AUDIT :
- Portal > Recovery Services vault > Properties > Security Settings > Immutability
- CLI: az backup vault backup-properties show --resource-group MyRG --vault-name MyVault
- PowerShell: Get-AzRecoveryServicesVaultProperty -VaultId $vault.ID

REMÉDIATION :
1. Activer Immutability sur le Recovery Services vault
2. Configurer la durée de rétention minimale
3. Tester l'impossibilité de suppression des points de récupération

```
# Activer l'immutabilité des sauvegardes
Set-AzRecoveryServicesVaultProperty -VaultId $vault.ID -ImmutabilityState "Unlocked"
# Verrouiller après configuration
Set-AzRecoveryServicesVaultProperty -VaultId $vault.ID -ImmutabilityState "Locked"
```

VALEUR PAR DÉFAUT :
Sauvegardes modifiables
14.4 — DISASTER RECOVERY AUTOMATION

14.4.1 *Azure Site Recovery pour les VM critiques*

MITRE ATT&CK : T1485

DESCRIPTION :
Configurer Azure Site Recovery pour la réplication automatique et le basculement des machines virtuelles critiques vers une région secondaire.

AUDIT :
- Portal > Recovery Services vault > Site Recovery > Replicated items
- CLI: az backup protection show --container-name MyContainer --item-name MyVM --resource-group MyRG --vault-name MyVault
- PowerShell: Get-AzRecoveryServicesAsrReplicationProtectedItem

REMÉDIATION :
1. Configurer la réplication vers une région Azure secondaire
2. Créer des plans de récupération automatisés
3. Effectuer des tests de basculement réguliers

```
# Configurer Site Recovery pour une VM
$vault = Get-AzRecoveryServicesVault -ResourceGroupName "MyRG" -Name "MyVault"
Set-AzRecoveryServicesAsrVaultContext -Vault $vault
$fabric = Get-AzRecoveryServicesAsrFabric -Name "AzureFabric"
$container = Get-AzRecoveryServicesAsrProtectionContainer -Fabric $fabric
Enable-AzRecoveryServicesAsrProtection -ReplicationProtectedItem $vm -ProtectionContainer $container -Policy $policy
```

VALEUR PAR DÉFAUT :
Pas de réplication automatique

14.4.2 *Runbooks automatisés pour le disaster recovery*

MITRE ATT&CK : T1485

DESCRIPTION :
Créer des runbooks Azure Automation pour automatiser les procédures de récupération d'urgence et réduire les temps de récupération (RTO).

AUDIT :
- Portal > Automation Account > Runbooks > DR procedures
- CLI: az automation runbook list --automation-account-name MyAutomation --resource-group MyRG
- PowerShell: Get-AzAutomationRunbook -AutomationAccountName "MyAutomation" -ResourceGroupName "MyRG"

REMÉDIATION :
1. Créer des runbooks pour les procédures de basculement
2. Configurer des webhooks pour l'activation automatique
3. Tester régulièrement les runbooks DR

```
# Créer un runbook de disaster recovery
Import-AzAutomationRunbook -AutomationAccountName "MyAutomation" -ResourceGroupName "MyRG" -Name "DR-Failover" -Type PowerShell -Pa
Publish-AzAutomationRunbook -AutomationAccountName "MyAutomation" -ResourceGroupName "MyRG" -Name "DR-Failover"
```

VALEUR PAR DÉFAUT :
Procédures manuelles
14.5 — TESTS ET VALIDATION DR

14.5.1 *Tests de disaster recovery automatisés*

MITRE ATT&CK : T1485

DESCRIPTION :

Implémenter des tests automatisés réguliers des procédures de disaster recovery pour valider les RTO/RPO et identifier les problèmes.

AUDIT :

- Portal > Site Recovery > Recovery plans > Test failover history
- Logs des tests de basculement dans Log Analytics
- Métriques de performance des tests DR

REMÉDIATION :

1. Programmer des tests de basculement mensuels automatisés
2. Créer des métriques pour mesurer RTO/RPO réels
3. Documenter et corriger les écarts identifiés

```
# Programmer un test de basculement automatisé
$recoveryPlan = Get-AzRecoveryServicesAsrRecoveryPlan -Name "MyDRPlan"
Start-AzRecoveryServicesAsrTestFailoverJob -RecoveryPlan $recoveryPlan -Direction "PrimaryToRecovery" -NetworkId $testNetwork.Id
```

VALEUR PAR DÉFAUT :

Tests manuels ad-hoc

14.5.2 *Monitoring des métriques RTO/RPO*

MITRE ATT&CK : T1485

DESCRIPTION :

Surveiller en continu les métriques RTO (Recovery Time Objective) et RPO (Recovery Point Objective) pour s'assurer du respect des SLA de récupération.

AUDIT :

- Portal > Monitor > Metrics > Site Recovery metrics
- Dashboards personnalisés pour RTO/RPO tracking
- Alertes configurées sur les déviations

REMÉDIATION :

1. Créer des dashboards Azure Monitor pour RTO/RPO
2. Configurer des alertes sur les dépassements d'objectifs
3. Intégrer les métriques dans les rapports de gouvernance

```
# Créer une alerte sur les métriques RPO
$actionGroup = Get-AzActionGroup -ResourceGroupName "MyRG" -Name "DRAlerts"
Add-AzMetricAlertRuleV2 -Name "RPO-Exceeded" -ResourceGroupName "MyRG" -WindowSize "PT15M" -Frequency "PT5M" -TargetResourceId $vau
```

VALEUR PAR DÉFAUT :

Pas de monitoring automatisé

15.0 — SENTINEL ET SOC

15.1.1 *Sentinel workbooks et dashboards*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des workbooks et dashboards Sentinel doivent être configurés pour monitoring proactif de la sécurité.

AUDIT :

- Portal > Sentinel > Workbooks
- Templates disponibles et customization

REMÉDIATION :

1. Déployer workbooks Microsoft
2. Customisation selon environnement
3. Dashboards pour différents rôles

15.2.1 *Playbooks automatisation réponse incident*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des playbooks de réponse automatique doivent être configurés pour les incidents de sécurité courants.

AUDIT :

- Portal > Sentinel > Automation > Playbooks
- Logic Apps integration

REMÉDIATION :

1. Développer playbooks pour cas d'usage communs
2. Intégration avec analytics rules
3. Test et amélioration continue

15.3 — AZURE SENTINEL SIEM AVANCÉ

15.3.1 *Data connectors configurés pour toutes les sources*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configurer tous les connecteurs de données Azure Sentinel nécessaires pour ingérer les logs de sécurité de l'ensemble de l'infrastructure Azure et hybride.

AUDIT :

- Portal > Sentinel > Data connectors > Status of connectors
- CLI: az sentinel data-connector list --resource-group MyRG --workspace-name MyWorkspace
- PowerShell: Get-AzSentinelDataConnector -ResourceGroupName "MyRG" -WorkspaceName "MyWorkspace"

REMÉDIATION :

1. Activer Azure Activity, Azure AD, Office 365 connectors
2. Configurer les connecteurs pour Azure Security Center
3. Ajouter les connecteurs tiers (AWS, GCP, Firewalls)

```
# Activer le connecteur Azure Activity
New-AzSentinelDataConnector -ResourceGroupName "MyRG" -WorkspaceName "MyWorkspace" -Kind "AzureActivity" -SubscriptionId $subscript
# Activer Azure AD connector
New-AzSentinelDataConnector -ResourceGroupName "MyRG" -WorkspaceName "MyWorkspace" -Kind "AzureActiveDirectory" -TenantId $tenantId
```

VALEUR PAR DÉFAUT :

Connecteurs de base uniquement

15.3.2 *Analytics rules pour détection de menaces*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configurer et personnaliser les règles d'analytique Sentinel pour détecter les menaces spécifiques à l'environnement Azure.

AUDIT :

- Portal > Sentinel > Analytics > Active rules count
- CLI: az sentinel alert-rule list --resource-group MyRG --workspace-name MyWorkspace
- PowerShell: Get-AzSentinelAlertRule -ResourceGroupName "MyRG" -WorkspaceName "MyWorkspace"

REMÉDIATION :

1. Activer les règles prêtes à l'emploi Microsoft
2. Créer des règles personnalisées basées sur KQL
3. Ajuster les seuils et fréquences selon l'environnement

```
# Créer une règle d'analytics personnalisée
$rule = @{
    DisplayName = "Suspicious Azure AD Sign-ins"
    Description = "Détecte les connexions Azure AD suspectes"
    Query = "SigninLogs | where RiskLevelDuringSignIn == 'high' | where ResultType == 0"
    QueryFrequency = "PT5M"
    QueryPeriod = "PT6H"
    TriggerOperator = "GreaterThan"
    TriggerThreshold = 0
    Severity = "High"
}
New-AzSentinelAlertRule -ResourceGroupName "MyRG" -WorkspaceName "MyWorkspace" @rule
```

VALEUR PAR DÉFAUT :

Règles de base Microsoft

15.3.3 *Playbooks automatisés pour la réponse aux incidents*

MITRE ATT&CK : T1059

DESCRIPTION :

Développer des playbooks Logic Apps pour automatiser la réponse aux incidents de sécurité détectés par Sentinel.

AUDIT :

- Portal > Sentinel > Automation > Playbooks
- CLI: az logic workflow list --resource-group MyRG
- PowerShell: Get-AzLogicApp -ResourceGroupName "MyRG"

REMÉDIATION :

1. Créer des playbooks pour les cas d'usage courants
2. Intégrer avec Azure AD pour disable des comptes compromis
3. Configurer des notifications automatiques aux équipes

```
# Créer un playbook de désactivation automatique de compte
$workflow = @{
    Name = "DisableCompromisedUser"
    ResourceGroupName = "MyRG"
    Location = "France Central"
    Definition = $playbook_definition
}
New-AzLogicApp @workflow
```

VALEUR PAR DÉFAUT :

Réponse manuelle uniquement

15.4 — THREAT HUNTING AVANCÉ

15.4.1 *Hunting queries personnalisées développées*

MITRE ATT&CK : T1057

DESCRIPTION :

Développer et maintenir des requêtes de chasse aux menaces personnalisées basées sur les Tactics, Techniques, and Procedures (TTP) pertinents pour l'environnement.

AUDIT :

- Portal > Sentinel > Hunting > Custom hunting queries
- Notebook Jupyter avec requêtes KQL avancées
- Métriques d'utilisation des hunting queries

REMÉDIATION :

1. Développer des hunting queries pour chaque technique MITRE ATT&CK
2. Créer des notebooks Jupyter pour l'analyse avancée
3. Programmer des hunts automatisés avec Azure Automation

```
// Exemple de hunting query pour persistence via scheduled tasks
let timeframe = 7d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 4698 // Scheduled task created
| where Process =~ "schtasks.exe"
| extend TaskName = extract(@'TaskName:\s*([^
]+)', 1, CommandLine)
| where TaskName !~ "Microsoft"
| summarize count() by Computer, Account, TaskName, CommandLine
| where count_ > 1
```

VALEUR PAR DÉFAUT :

Hunting queries Microsoft de base

15.4.2 *Threat intelligence feeds intégrés*

MITRE ATT&CK : T1590

DESCRIPTION :

Intégrer des flux de threat intelligence externes et internes dans Sentinel pour enrichir les détections et le contexte des incidents.

AUDIT :

- Portal > Sentinel > Threat intelligence > Indicators
- API calls pour vérifier l'ingestion des IOCs
- Métriques d'enrichissement des alertes

REMÉDIATION :

1. Configurer des connecteurs vers des fournisseurs TI (Microsoft TI, ThreatConnect)
2. Développer des connecteurs personnalisés pour sources internes
3. Créer des règles d'analytics utilisant les IOCs

```
# Importer des IOCs via PowerShell
$indicators = @(
    @{
        Pattern = "malicious-domain.com"
        PatternType = "domain-name"
        Source = "Internal Research"
        ThreatType = "malicious-activity"
        Confidence = 85
    }
)
Import-AzSentinelThreatIntelligence -ResourceGroupName "MyRG" -WorkspaceName "MyWorkspace" -Indicators $indicators
```

VALEUR PAR DÉFAUT :

Microsoft TI uniquement

15.5 — SOC OPERATIONS

15.5.1 *Incident response workflows standardisés*

MITRE ATT&CK : T1059

DESCRIPTION :
Établir des workflows d'incident response standardisés intégrés dans Sentinel pour assurer une réponse cohérente et efficace aux menaces.

AUDIT :
- Portal > Sentinel > Incidents > Response templates
- Documentation des procédures d'incident response
- Métriques de temps de réponse (MTTR)

REMÉDIATION :
1. Créer des templates d'incident par type de menace
2. Définir des niveaux d'escalation automatiques
3. Intégrer avec les systèmes de ticketing (ServiceNow, JIRA)

```
{
  "incident_template": {
    "severity": "High",
    "title": "Compromised Account Detected",
    "description": "Automated response for compromised user account",
    "tasks": [
      {
        "name": "Disable user account",
        "automation": "playbook:disable-user"
      },
      {
        "name": "Reset user credentials",
        "automation": "manual"
      }
    ]
  }
}
```

VALEUR PAR DÉFAUT :
Incidents génériques

15.5.2 *Métriques SOC et dashboards de performance*

MITRE ATT&CK : T1562.001

DESCRIPTION :
Créer des dashboards et métriques pour surveiller la performance du SOC et l'efficacité des détections de sécurité.

AUDIT :
- Portal > Sentinel > Workbooks > SOC performance dashboards
- Métriques MTTR, MTTD, taux de faux positifs
- Rapports de performance mensuels automatisés

REMÉDIATION :
1. Créer des workbooks Sentinel pour les métriques SOC
2. Configurer des alertes sur les SLA de réponse
3. Automatiser la génération de rapports de performance

```
// Métriques de performance SOC
SecurityIncident
| where TimeGenerated >= ago(30d)
| summarize
    TotalIncidents = count(),
    AvgTimeToClose = avg(datetime_diff('minute', ClosedTime, CreatedTime)),
    HighSeverityIncidents = countif(Severity == "High"),
    AutomatedResponse = countif(isnotempty(PlaybookRunId))
| extend
    AutomationRate = AutomatedResponse * 100.0 / TotalIncidents,
    HighSeverityRate = HighSeverityIncidents * 100.0 / TotalIncidents
```

VALEUR PAR DÉFAUT :
Métriques de base uniquement

16.0 — SÉCURITÉ API

16.1.1 *API Management avec authentification forte*

MITRE ATT&CK : T1190

DESCRIPTION :

Azure API Management doit être configuré avec authentification forte et politiques de sécurité pour toutes les APIs.

AUDIT :

- Portal > API Management > APIs > Security
- Policies de validation et authentification

REMÉDIATION :

1. OAuth 2.0 ou certificats client
2. Rate limiting et throttling
3. Validation input/output

16.2.1 *WAF protection pour APIs publiques*

MITRE ATT&CK : T1190

DESCRIPTION :

Web Application Firewall doit protéger les APIs publiques contre les attaques communes OWASP.

AUDIT :

- Portal > Application Gateway > Web application firewall
- Frontend avec WAF rules

REMÉDIATION :

1. Déployer WAF devant APIs
2. OWASP Core Rule Set
3. Custom rules selon besoins

16.3 — AZURE API MANAGEMENT SECURITY

16.3.1 *API Management avec WAF et rate limiting*

MITRE ATT&CK : T1499.004

DESCRIPTION :

Configurer Azure API Management avec Web Application Firewall et limitations de débit pour protéger les APIs contre les attaques par déni de service et injection.

AUDIT :

- Portal > API Management > Security > WAF policies
- Portal > API Management > APIs > Rate limiting policies
- CLI: az apim api policy show --service-name MyAPIService --resource-group MyRG --api-id MyAPI

REMÉDIATION :

1. Déployer APIM derrière Application Gateway avec WAF
2. Configurer des politiques de rate limiting granulaires
3. Implémenter l'authentification OAuth 2.0/JWT

```
<!-- Exemple de politique APIM avec rate limiting -->
<policies>
    <inbound>
        <rate-limit calls="100" renewal-period="60" />
        <quota calls="1000" renewal-period="3600" />
        <validate-jwt header-name="Authorization" failed-validation-httpcode="401">
            <openid-config url="https://login.microsoftonline.com/{tenant}/.well-known/openid_configuration" />
        </validate-jwt>
    </inbound>
</policies>
```

VALEUR PAR DÉFAUT :

Pas de protection APIM

16.3.2 *Authentication et authorization robustes*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Implémenter une authentification et autorisation robustes pour toutes les APIs avec OAuth 2.0, JWT, et scopes appropriés.

AUDIT :

- Portal > App registrations > API permissions
- Portal > API Management > Security > OAuth 2.0
- Tests d'authentification avec différents tokens

REMÉDIATION :

1. Configurer Azure AD comme serveur d'autorisation
2. Implémenter des scopes OAuth granulaires
3. Valider les JWT tokens dans APIM

```
# Créer un app registration pour l'API
$app = New-AzADApplication -DisplayName "MySecureAPI" -ReplyUrls @("https://api.mycompany.com/oauth/callback")
New-AzADServicePrincipal -ApplicationId $app.ApplicationId
# Configurer les scopes OAuth appropriés
```

VALEUR PAR DÉFAUT :

Authentification basique ou API keys

16.3.3 *API monitoring et anomaly detection*

MITRE ATT&CK : T1190

DESCRIPTION :

Configurer la surveillance avancée des APIs avec détection d'anomalies pour identifier les patterns d'attaque et comportements suspects.

AUDIT :

- Portal > API Management > Monitoring > Analytics
- Portal > Application Insights > API performance metrics
- Alertes configurées sur les anomalies d'utilisation

REMÉDIATION :

1. Intégrer APIM avec Application Insights
2. Configurer des alertes sur les patterns d'attaque
3. Implémenter la détection d'anomalies ML

```
# Configurer Application Insights pour APIM
$appInsights = New-AzApplicationInsights -ResourceGroupName "MyRG" -Name "APIM-Insights" -Location "France Central"
# Lier APIM à Application Insights
Set-AzApiManagementLogger -Context $apimContext -LoggerId "appinsights" -Name "Application Insights Logger"
```

VALEUR PAR DÉFAUT :

Logs de base uniquement

16.4 — API GATEWAY SECURITY

16.4.1 *Private endpoints pour APIs internes*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Configurer des private endpoints pour les APIs internes afin d'éliminer l'exposition Internet public et sécuriser la communication interne.

AUDIT :

- Portal > API Management > Network > Virtual network
- CLI: az network private-endpoint list --resource-group MyRG
- Test de connectivité depuis les réseaux internes uniquement

REMÉDIATION :

1. Déployer APIM en mode internal dans un VNet
2. Créer des private endpoints pour l'accès interne
3. Configurer des NSGs appropriées

```
# Configurer APIM en mode internal
$vnet = Get-AzVirtualNetwork -Name "MyVNet" -ResourceGroupName "MyRG"
$subnet = Get-AzVirtualNetworkSubnetConfig -Name "APIMSubnet" -VirtualNetwork $vnet
Set-AzApiManagement -ResourceGroupName "MyRG" -Name "MyAPIM" -VirtualNetwork $subnet -VpnType "Internal"
```

VALEUR PAR DÉFAUT :

APIM external/public

16.4.2 *Certificate pinning et mTLS*

MITRE ATT&CK : T1040

DESCRIPTION :

Implémenter le certificate pinning et mutual TLS (mTLS) pour sécuriser les communications entre les clients API et les backends.

AUDIT :

- Portal > API Management > Security > Client certificates
- Vérification des certificats clients configurés
- Tests de connexion mTLS

REMÉDIATION :

1. Configurer l'authentification par certificat client
2. Implémenter le certificate pinning côté client
3. Valider les certificats dans les politiques APIM

```
<!-- Politique APIM pour validation de certificat client -->
<policies>
    <inbound>
        <choose>
            <when condition="@(context.Request.Certificate == null || !context.Request.Certificate.Verify())">
                <return-response>
                    <set-status code="403" reason="Invalid client certificate" />
                </return-response>
            </when>
        </choose>
    </inbound>
</policies>
```

VALEUR PAR DÉFAUT :

TLS simple sans validation client

16.5 — OWASP API SECURITY

16.5.1 *Protection contre OWASP API Top 10*

MITRE ATT&CK : T1190

DESCRIPTION :

Implémenter des protections contre les 10 risques de sécurité API les plus critiques selon OWASP API Security Top 10.

AUDIT :

- Tests de sécurité automatisés pour OWASP API Top 10
- Review des politiques APIM pour chaque risque
- Scans de vulnérabilités API réguliers

REMÉDIATION :

1. Configurer des politiques APIM pour chaque risque OWASP
2. Implémenter la validation de schéma JSON/XML
3. Configurer le logging et monitoring appropriés

```
<!-- Protection contre injection et data exposure -->
<policies>
    <inbound>
        <validate-content unspecified-content-type-action="prevent" max-size="102400" size-exceeded-action="prevent" errors-variabl
            <content type="application/json" validate-as="json" action="prevent" />
        </validate-content>
        <set-header name="X-Content-Type-Options" exists-action="override">
            <value>nosniff</value>
        </set-header>
    </inbound>
    <outbound>
        <set-header name="X-Frame-Options" exists-action="override">
            <value>DENY</value>
        </set-header>
    </outbound>
</policies>
```

VALEUR PAR DÉFAUT :

Protections de base uniquement

16.5.2 *API versioning et deprecation sécurisée*

MITRE ATT&CK : T1190

DESCRIPTION :

Gérer le versioning des APIs et la dépréciation sécurisée des anciennes versions pour éviter l'exposition de vulnérabilités dans les versions obsolètes.

AUDIT :

- Portal > API Management > APIs > Version management
- Inventory des versions API actives
- Politiques de dépréciation documentées

REMÉDIATION :

1. Implémenter un strategy de versioning cohérent
2. Définir des timelines de dépréciation claires
3. Migrer proactivement les clients vers les nouvelles versions

```
# Créer une nouvelle version d'API
New-AzApiManagementApiVersionSet -Context $apimContext -Id "myapi-versions" -Name "MyAPI Versions" -Scheme "Path" -PathValue "v{ver
New-AzApiManagementApi -Context $apimContext -ApiId "myapi-v2" -Name "MyAPI v2.0" -ServiceUrl "https://backend.api.com/v2" -Path "a
```

VALEUR PAR DÉFAUT :

Pas de gestion de versions formelle

17.0 — RÉPONSE AUX INCIDENTS

17.1.1 *Plan de réponse incidents documenté*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Un plan de réponse aux incidents de sécurité doit être documenté avec procédures claires et contacts d'escalade.

AUDIT :

- Documentation disponible et à jour
- Formation équipes sur procédures

REMÉDIATION :

1. Rédaction plan de réponse
2. Définition des rôles et responsabilités
3. Exercices de simulation réguliers

17.2.1 *Forensic capabilities et preservation*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Des capacités de forensic numérique doivent être disponibles avec procédures de préservation des preuves.

AUDIT :

- Outils et procédures forensic
- Chain of custody documentation

REMÉDIATION :

1. Outils forensic cloud (Azure tools)
2. Procédures preservation logs
3. Formation équipes techniques

18.0 — CONFORMITÉ RÉGLEMENTAIRE

18.1.1 *Compliance frameworks mapping*

MITRE ATT&CK : T1562

DESCRIPTION :

Les contrôles de sécurité doivent être mappés aux frameworks de conformité applicables (RGPD, NIS2, ISO27001, etc.).

AUDIT :

- Documentation mapping controls
- Compliance dashboard et reporting

REMÉDIATION :

1. Identification réglementations applicables
2. Mapping des contrôles
3. Reporting conformité régulier

18.2.1 *Audit trail pour compliance*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Un audit trail complet doit être maintenu pour répondre aux exigences de conformité réglementaire.

AUDIT :

- Logs avec timestamps et intégrité
- Rétention selon exigences légales

REMÉDIATION :

1. Centralisation logs dans SIEM
2. Protection intégrité (signatures)
3. Rétention selon réglementations

RÉCAPITULATIFS SECTIONS S6-S18

Annexe : Checklist (210 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — IDENTITÉ ET GESTION DES ACCÈS (IAM)					
1.1.1	MFA obligatoire pour les administrateurs Azure	●	☐	☐	☐
1.1.2	MFA obligatoire pour tous les utilisateurs privilégiés	●	☐	☐	☐
1.1.3	Méthodes MFA sécurisées configurées	●	☐	☐	☐
1.2.1	Politique de blocage des pays à risque	●	☐	☐	☐
1.2.2	Accès conditionnel basé sur les risques utilisateur	●	☐	☐	☐
1.2.3	Accès conditionnel pour applications cloud	●	☐	☐	☐
1.3.1	PIM activé pour les rôles administrateurs	●	☐	☐	☐
1.3.2	Activation PIM avec justification obligatoire	●	☐	☐	☐
1.3.3	Révision d'accès PIM automatisée	●	☐	☐	☐
1.4.1	Principe du moindre privilège appliqué	●	☐	☐	☐
1.4.2	Limitation des propriétaires de souscriptions	●	☐	☐	☐
1.4.3	Rôles personnalisés justifiés et documentés	●	☐	☐	☐
1.5.1	Managed Identity privilégiée sur Service Principal	●	☐	☐	☐
1.5.2	Rotation automatique des secrets Service Principal	●	☐	☐	☐
1.5.3	Permissions minimales pour Service Principals	●	☐	☐	☐
1.6.1	Restriction des invitations d'utilisateurs externes	●	☐	☐	☐
1.6.2	Révision périodique des utilisateurs invités	●	☐	☐	☐
1.7.1	Comptes break-glass configurés et protégés	●	☐	☐	☐
1.7.2	Surveillance des comptes break-glass	●	☐	☐	☐
1.8.1	Politique de mots de passe sécurisée	●	☐	☐	☐
1.8.2	Protection contre le password spray	●	☐	☐	☐
1.9.1	Audit des changements de rôles privilégiés	●	☐	☐	☐
1.9.2	Surveillance des connexions administrateur	●	☐	☐	☐
1.7.1	Politique d'accès basée sur les risques utilisateur	●	☐	☐	☐
1.7.2	Accès conditionnel basé sur la géolocalisation	●	☐	☐	☐
1.7.3	Contrôle d'accès basé sur les appareils conformes	●	☐	☐	☐
1.8.1	Activation JIT pour les rôles privilégiés	●	☐	☐	☐
1.8.2	Révisions d'accès périodiques pour les rôles privilégiés	●	☐	☐	☐
1.8.3	Alertes PIM configurées	●	☐	☐	☐
1.9.1	Comptes break-glass configurés et protégés	●	☐	☐	☐
1.9.2	Surveillance des comptes d'urgence	●	☐	☐	☐
Section 2 — MICROSOFT DEFENDER FOR CLOUD					
2.1.1	Defender for Cloud activé sur toutes les souscriptions	●	☐	☐	☐
2.1.2	Plans Defender activés par type de ressource	●	☐	☐	☐
2.1.3	Auto-provisioning activé pour agents de sécurité	●	☐	☐	☐
2.2.1	Secure Score monitoring et amélioration	●	☐	☐	☐
2.2.2	Recommandations de sécurité priorisées et traitées	●	☐	☐	☐
2.2.3	Compliance frameworks activés et surveillés	●	☐	☐	☐
2.3.1	Defender for Servers configuration avancée	●	☐	☐	☐
2.3.2	Defender for Storage avec protection malware	●	☐	☐	☐
2.3.3	Defender for SQL avec Advanced Threat Protection	●	☐	☐	☐
2.4.1	Intégration avec Azure Sentinel/SIEM	●	☐	☐	☐
2.4.2	Notifications email des alertes critiques	●	☐	☐	☐
2.4.3	Automation et réponse automatique	●	☐	☐	☐
2.5.1	Évaluation des vulnérabilités VMs activée	●	☐	☐	☐
2.5.2	Container image vulnerability scanning	●	☐	☐	☐
2.6.1	Azure Policy integration avec Defender	●	☐	☐	☐
2.6.2	Inventaire et classification des assets	●	☐	☐	☐
Section 3 — SÉCURITÉ DU STOCKAGE					
3.1.1	Chiffrement au repos activé pour Storage Accounts	●	☐	☐	☐
3.1.2	Secure transfer (HTTPS) obligatoire	●	☐	☐	☐
3.1.3	Minimum TLS version configurée (1.2)	●	☐	☐	☐
3.2.1	Rotation automatique des clés d'accès	●	☐	☐	☐
3.2.2	Shared Access Signatures (SAS) avec durée limitée	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
3.2.3	Stored Access Policies pour SAS management	●	☐	☐	☐
3.3.1	Firewall Storage Account configuré	●	☐	☐	☐
3.3.2	Private Endpoints pour accès sécurisé	●	☐	☐	☐
3.3.3	Disable public blob access si non requis	●	☐	☐	☐
3.4.1	Storage Analytics et monitoring activés	●	☐	☐	☐
3.4.2	Alertes sur activités suspectes de stockage	●	☐	☐	☐
3.5.1	Advanced Threat Protection activé	●	☐	☐	☐
3.5.2	Soft delete activé pour blobs et containers	●	☐	☐	☐
3.5.3	Versioning des blobs activé	●	☐	☐	☐
3.6.1	Géo-réplication configurée selon criticité	●	☐	☐	☐
3.6.2	Backup automatisé via Azure Backup	●	☐	☐	☐
Section 4 — SÉCURITÉ DES BASES DE DONNÉES					
4.1.1	Transparent Data Encryption (TDE) activé	●	☐	☐	☐
4.1.2	SQL Auditing activé avec rétention appropriée	●	☐	☐	☐
4.1.3	Advanced Data Security activé	●	☐	☐	☐
4.1.4	Firewall SQL Server configuré restrictif	●	☐	☐	☐
4.1.5	Azure AD Authentication configurée	●	☐	☐	☐
4.2.1	Managed Instance dans VNet privé	●	☐	☐	☐
4.2.2	TLS 1.2 minimum pour Managed Instance	●	☐	☐	☐
4.3.1	SSL enforcement activé PostgreSQL/MySQL	●	☐	☐	☐
4.3.2	Firewall PostgreSQL/MySQL restrictif	●	☐	☐	☐
4.3.3	Backup automatique avec rétention appropriée	●	☐	☐	☐
4.4.1	Chiffrement Cosmos DB avec Customer Managed Keys	●	☐	☐	☐
4.4.2	Firewall Cosmos DB configuré	●	☐	☐	☐
4.4.3	Private Endpoints pour Cosmos DB	●	☐	☐	☐
4.5.1	Log Analytics intégration pour databases	●	☐	☐	☐
4.5.2	Alertes sur activités suspectes base de données	●	☐	☐	☐
4.5.3	Data Discovery et Classification activées	●	☐	☐	☐
4.6.1	Principe du moindre privilège pour accès DB	●	☐	☐	☐
4.6.2	Comptes de service avec Managed Identity	●	☐	☐	☐
Section 5 — LOGGING ET SURVEILLANCE					
5.1.1	Activity Log retention configurée appropriée	●	☐	☐	☐
5.1.2	Alertes Activity Log pour actions critiques	●	☐	☐	☐
5.1.3	Activity Log protection contre suppression	●	☐	☐	☐
5.2.1	Log Analytics workspace centralisé configuré	●	☐	☐	☐
5.2.2	Solutions de sécurité installées dans Log Analytics	●	☐	☐	☐
5.2.3	Contrôle d'accès granulaire Log Analytics	●	☐	☐	☐
5.3.1	Diagnostic settings activés pour toutes ressources critiques	●	☐	☐	☐
5.3.2	Azure Policy pour enforcement diagnostic settings	●	☐	☐	☐
5.4.1	Action Groups configurés pour équipes sécurité	●	☐	☐	☐
5.4.2	Alertes métriques pour ressources critiques	●	☐	☐	☐
5.4.3	Log search alerts pour détection anomalies	●	☐	☐	☐
5.5.1	Network Watcher activé dans toutes régions	●	☐	☐	☐
5.5.2	NSG Flow Logs activés pour NSGs critiques	●	☐	☐	☐
5.5.3	Traffic Analytics configuré	●	☐	☐	☐
5.6.1	Azure Sentinel ou SIEM externe configuré	●	☐	☐	☐
5.6.2	Data connectors Sentinel configurés	●	☐	☐	☐
5.6.3	Analytics rules et détections personnalisées	●	☐	☐	☐
5.7.1	Immutable logs pour compliance	●	☐	☐	☐
5.7.2	Audit trail complet des modifications	●	☐	☐	☐
Section 6 — SÉCURITÉ RÉSEAU					
6.1.1	Network Security Groups (NSG) configurés restrictifs	●	☐	☐	☐
6.2.1	Azure Firewall ou NVA déployé	●	☐	☐	☐
6.3.1	DDoS Protection Standard activé	●	☐	☐	☐
6.4.1	Azure Firewall Premium avec IDPS activé	●	☐	☐	☐
6.4.2	Web Application Firewall (WAF) avec règles OWASP	●	☐	☐	☐
6.5.1	NSG Flow Logs activés pour tous les NSG critiques	●	☐	☐	☐
6.5.2	Règles NSG avec principe du moindre privilège	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
6.6.1	DDoS Protection Standard activé	●	☐	☐	☐
6.6.2	Métriques et alertes DDoS configurées	●	☐	☐	☐
6.7.1	Private Endpoints pour tous les services PaaS critiques	●	☐	☐	☐
6.7.2	Service Endpoints sécurisés configurés	●	☐	☐	☐
6.8.1	Connection Monitor configuré pour la surveillance réseau	●	☐	☐	☐
6.8.2	Traffic Analytics activé	●	☐	☐	☐
Section 7 — SÉCURITÉ DES MACHINES VIRTUELLES					
7.1.1	Disk encryption activé sur toutes les VMs	●	☐	☐	☐
7.2.1	Just-In-Time VM access configuré	●	☐	☐	☐
7.3.1	Azure Disk Encryption activé sur toutes les VM	●	☐	☐	☐
7.3.2	Disques managés avec chiffrement côté serveur	●	☐	☐	☐
7.4.1	Just-In-Time VM Access configuré	●	☐	☐	☐
7.4.2	Bastion Host déployé pour l'accès sécurisé	●	☐	☐	☐
7.5.1	Update Management automatisé configuré	●	☐	☐	☐
7.5.2	Boot Diagnostics activé	●	☐	☐	☐
7.6.1	VM de calcul confidentiel pour données sensibles	●	☐	☐	☐
7.6.2	Azure Attestation configuré	●	☐	☐	☐
Section 8 — AZURE KEY VAULT					
8.1.1	Key Vault avec RBAC et soft delete	●	☐	☐	☐
8.2.1	Rotation automatique des clés	●	☐	☐	☐
8.3.1	RBAC activé au lieu des politiques d'accès classiques	●	☐	☐	☐
8.3.2	Soft Delete et Purge Protection activés	●	☐	☐	☐
8.4.1	HSM managé pour les clés critiques	●	☐	☐	☐
8.4.2	Clés HSM-backed pour le chiffrement d'infrastructure	●	☐	☐	☐
8.5.1	Rotation automatique des secrets configurée	●	☐	☐	☐
8.5.2	Intégration avec Azure DevOps pour les secrets	●	☐	☐	☐
8.6.1	Diagnostic settings configurés pour Key Vault	●	☐	☐	☐
8.6.2	Alertes configurées pour les accès Key Vault	●	☐	☐	☐
Section 9 — APP SERVICE SECURITY					
9.1.1	HTTPS obligatoire et TLS 1.2 minimum	●	☐	☐	☐
9.2.1	Managed Identity pour authentification	●	☐	☐	☐
9.3.1	Managed Identity activée pour tous les App Services	●	☐	☐	☐
9.3.2	Authentication/Authorization (EasyAuth) configuré	●	☐	☐	☐
9.4.1	HTTPS Only obligatoire et TLS 1.2 minimum	●	☐	☐	☐
9.4.2	Certificats SSL/TLS gérés automatiquement	●	☐	☐	☐
9.5.1	Restrictions d'accès par IP configurées	●	☐	☐	☐
9.5.2	Private Endpoints pour App Services Premium	●	☐	☐	☐
9.6.1	Application Insights intégré et configuré	●	☐	☐	☐
9.6.2	Logs de diagnostic configurés	●	☐	☐	☐
Section 10 — AZURE KUBERNETES SERVICE (AKS)					
10.1.1	Cluster AKS privé avec Azure AD integration	●	☐	☐	☐
10.2.1	Network policies activées	●	☐	☐	☐
10.3.1	Azure AD RBAC intégré pour AKS	●	☐	☐	☐
10.3.2	Pod Security Standards configurés	●	☐	☐	☐
10.4.1	Network Policies Kubernetes activées	●	☐	☐	☐
10.4.2	Private Cluster avec API Server privé	●	☐	☐	☐
10.5.1	Azure Key Vault Provider for Secrets Store CSI Driver	●	☐	☐	☐
10.5.2	Workload Identity pour les pods	●	☐	☐	☐
10.6.1	Azure Defender for containers activé	●	☐	☐	☐
10.6.2	Admission controllers sécurisés configurés	●	☐	☐	☐
Section 11 — GOVERNANCE ET COMPLIANCE					
11.1.1	Azure Policy initiatives assignées	●	☐	☐	☐
11.2.1	Resource locks sur ressources critiques	●	☐	☐	☐
11.3.1	Azure Policy configuré avec initiatives de sécurité	●	☐	☐	☐
11.3.2	Azure Blueprints pour la gouvernance d'entreprise	●	☐	☐	☐
11.4.1	Management Groups hiérarchiques configurés	●	☐	☐	☐
11.4.2	Resource locks sur les ressources critiques	●	☐	☐	☐
11.5.1	Budgets et alertes de coûts configurés	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
11.5.2	Cost anomaly detection activé	●	☐	☐	☐
11.6.1	Azure Compliance Manager configuré	●	☐	☐	☐
11.6.2	Retention policies pour la gouvernance des données	●	☐	☐	☐
Section 12 — SECRETS ET CHIFFREMENT					
12.1.1	Customer Managed Keys pour services critiques	●	☐	☐	☐
12.2.1	Secrets rotation et lifecycle management	●	☐	☐	☐
12.3.1	Always Encrypted pour SQL Database	●	☐	☐	☐
12.3.2	Chiffrement en transit obligatoire (TLS 1.2+)	●	☐	☐	☐
12.4.1	Certificats avec renouvellement automatique	●	☐	☐	☐
12.4.2	Monitoring des expirations de certificats	●	☐	☐	☐
12.5.1	Dedicated HSM pour les workloads ultra-sensibles	●	☐	☐	☐
12.5.2	Key Management interoperable avec PKCS#11	●	☐	☐	☐
Section 13 — CONTAINERS ET REGISTRIES					
13.1.1	Container Registry scanning des vulnérabilités	●	☐	☐	☐
13.2.1	Container Registry access restreint	●	☐	☐	☐
13.3.1	Vulnerability scanning activé sur ACR	●	☐	☐	☐
13.3.2	Content Trust et signature d'images	●	☐	☐	☐
13.4.1	Quarantine policy pour les images vulnérables	●	☐	☐	☐
13.4.2	Image scanning automatisé dans les pipelines	●	☐	☐	☐
13.5.1	Runtime protection avec Defender for Containers	●	☐	☐	☐
13.5.2	Network segmentation pour containers	●	☐	☐	☐
13.6.1	Image compliance policies avec OPA Gatekeeper	●	☐	☐	☐
Section 14 — BACKUP ET DISASTER RECOVERY					
14.1.1	Azure Backup configuré pour ressources critiques	●	☐	☐	☐
14.2.1	Site Recovery pour continuité d'activité	●	☐	☐	☐
14.3.1	Backup cross-region pour la continuité d'activité	●	☐	☐	☐
14.3.2	Immutable backup pour protection ransomware	●	☐	☐	☐
14.4.1	Azure Site Recovery pour les VM critiques	●	☐	☐	☐
14.4.2	Runbooks automatisés pour le disaster recovery	●	☐	☐	☐
14.5.1	Tests de disaster recovery automatisés	●	☐	☐	☐
14.5.2	Monitoring des métriques RTO/RPO	●	☐	☐	☐
Section 15 — SENTINEL ET SOC					
15.1.1	Sentinel workbooks et dashboards	●	☐	☐	☐
15.2.1	Playbooks automatisation réponse incident	●	☐	☐	☐
15.3.1	Data connectors configurés pour toutes les sources	●	☐	☐	☐
15.3.2	Analytics rules pour détection de menaces	●	☐	☐	☐
15.3.3	Playbooks automatisés pour la réponse aux incidents	●	☐	☐	☐
15.4.1	Hunting queries personnalisées développées	●	☐	☐	☐
15.4.2	Threat intelligence feeds intégrés	●	☐	☐	☐
15.5.1	Incident response workflows standardisés	●	☐	☐	☐
15.5.2	Métriques SOC et dashboards de performance	●	☐	☐	☐
Section 16 — SÉCURITÉ API					
16.1.1	API Management avec authentification forte	●	☐	☐	☐
16.2.1	WAF protection pour APIs publiques	●	☐	☐	☐
16.3.1	API Management avec WAF et rate limiting	●	☐	☐	☐
16.3.2	Authentication et authorization robustes	●	☐	☐	☐
16.3.3	API monitoring et anomaly detection	●	☐	☐	☐
16.4.1	Private endpoints pour APIs internes	●	☐	☐	☐
16.4.2	Certificate pinning et mTLS	●	☐	☐	☐
16.5.1	Protection contre OWASP API Top 10	●	☐	☐	☐
16.5.2	API versioning et deprecation sécurisée	●	☐	☐	☐
Section 17 — RÉPONSE AUX INCIDENTS					
17.1.1	Plan de réponse incidents documenté	●	☐	☐	☐
17.2.1	Forensic capabilities et preservation	●	☐	☐	☐
Section 18 — CONFORMITÉ RÉGLEMENTAIRE					
18.1.1	Compliance frameworks mapping	●	☐	☐	☐
18.2.1	Audit trail pour compliance	●	☐	☐	☐