Checklist DE Sécurité - MICROSOFT DEFENDER ANTIVIRUS

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v| — | 04 avril 2026 | · 196 controles

Sommaire

Section 1 — PROTECTION EN TEMPS RÉEL

1.0 — PROTECTION EN TEMPS RÉEL

1.1.1 *Activation de la protection en temps réel*

MITRE ATT&CK : T1562.001

DESCRIPTION :

La protection en temps réel doit être activée pour surveiller en permanence les fichiers, processus et activités système contre les menaces connues et inconnues.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableRealtimeMonitoring
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
- Intune: Endpoint Security > Antivirus > Real-time protection

REMÉDIATION :

1. Set-MpPreference -DisableRealtimeMonitoring
2. GPO: Computer Config > Admin Templates > Windows Components > Microsoft Defender Antivirus > Real-time Protection > Turn off real-time protection = Disabled
3. Intune: Devices > Configuration profiles > Endpoint protection > Microsoft Defender Antivirus

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.1.2 *Protection contre le téléchargement de fichiers*

MITRE ATT&CK : T1566.001

DESCRIPTION :

Contrôle l'analyse en temps réel des fichiers téléchargés depuis Internet pour bloquer les menaces avant leur exécution.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableIOAVProtection
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection

REMÉDIATION :

1. Set-MpPreference -DisableIOAVProtection
2. GPO: Turn off scanning of downloaded files and attachments = Disabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.1.3 *Surveillance des fichiers et programmes*

MITRE ATT&CK : T1204.002

DESCRIPTION :

Active la surveillance en temps réel de l'activité des fichiers et programmes sur le système pour détecter les comportements malveillants.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableOnAccessProtection
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection

REMÉDIATION :

1. Set-MpPreference -DisableOnAccessProtection
2. GPO: Turn off real-time file and program monitoring = Disabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.1.4 *Protection contre les scripts malveillants*

MITRE ATT&CK : T1059

DESCRIPTION :

Active la protection contre l'exécution de scripts malveillants via l'Antimalware Scan Interface (AMSI).

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableScriptScanning
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScriptScanning

REMÉDIATION :

1. Set-MpPreference -DisableScriptScanning
2. GPO: Configure script scanning = Enabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.1.5 *Protection de l'intégrité du comportement*

MITRE ATT&CK : T1055

DESCRIPTION :

Active la surveillance comportementale pour détecter les activités suspectes et les techniques d'évasion avancées.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableBehaviorMonitoring
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring

REMÉDIATION :

1. Set-MpPreference -DisableBehaviorMonitoring
2. GPO: Turn off behavior monitoring = Disabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.2.1 *Limite d'utilisation CPU pour l'analyse temps réel*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure la limitation d'utilisation CPU pour l'analyse en temps réel afin d'équilibrer sécurité et performance système.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanAvgCPULoadFactor
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan\AvgCPULoadFactor

REMÉDIATION :

1. Set-MpPreference -ScanAvgCPULoadFactor 50
2. GPO: Specify the maximum percentage of CPU utilization = 50%

VALEUR PAR DÉFAUT :

50%

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.2.2 *Analyse des processus nouveaux et modifiés*

MITRE ATT&CK : T1543

DESCRIPTION :

Configure l'analyse automatique des processus nouvellement créés ou modifiés pour détecter les activités malveillantes.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property RealTimeScanDirection

REMÉDIATION :

1. Set-MpPreference -RealTimeScanDirection Both
2. GPO: Monitor file and program activity on your computer = Incoming and outgoing files

VALEUR PAR DÉFAUT :

Incoming files only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.2.3 *Configuration des extensions de fichiers surveillées*

MITRE ATT&CK : T1036.005

DESCRIPTION :

Définit les extensions de fichiers à surveiller prioritairement pour optimiser les performances tout en maintenant la sécurité.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanParameters

REMÉDIATION :

1. Set-MpPreference -ScanParameters 1
2. GPO: Scan all downloaded files and attachments = Enabled

VALEUR PAR DÉFAUT :

Default extensions only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.2.4 *Analyse des archives et fichiers compressés*

MITRE ATT&CK : T1027.002

DESCRIPTION :

Configure l'analyse approfondie des fichiers d'archives pour détecter les malwares dissimulés dans les conteneurs compressés.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableArchiveScanning
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan\DisableArchiveScanning

REMÉDIATION :

1. Set-MpPreference -DisableArchiveScanning
2. GPO: Scan archive files = Enabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.2.5 *Surveillance des lecteurs réseau*

MITRE ATT&CK : T1021.002

DESCRIPTION :

Active l'analyse des fichiers accessibles via les partages réseau pour prévenir la propagation latérale des menaces.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableScanningNetworkFiles
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan\DisableScanningNetworkFiles

REMÉDIATION :

1. Set-MpPreference -DisableScanningNetworkFiles
2. GPO: Scan network files = Enabled

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.3.1 *Analyse des emails et pièces jointes*

MITRE ATT&CK : T1566.001

DESCRIPTION :

Active l'analyse des emails entrants et pièces jointes via l'intégration avec les clients de messagerie.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableEmailScanning
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan\DisableEmailScanning

REMÉDIATION :

1. Set-MpPreference -DisableEmailScanning
2. GPO: Scan e-mail = Enabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.3.2 *Protection contre les rootkits*

MITRE ATT&CK : T1014

DESCRIPTION :

Active la détection et suppression des rootkits via l'analyse au niveau noyau et les technologies de virtualisation.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object -Property AMEngineVersion,ProductStatus
- Event Viewer: Microsoft-Windows-Windows Defender/Operational

REMÉDIATION :

1. Protection automatique via Windows Defender
2. Utiliser Microsoft Defender Offline pour analyse approfondie

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.3.3 *Analyse des fichiers de démarrage*

MITRE ATT&CK : T1547

DESCRIPTION :

Surveille et analyse les fichiers et registres de démarrage automatique pour détecter la persistance malveillante.

AUDIT :

- PowerShell: Get-CimInstance Win32_StartupCommand
- Registre: Surveillance des clés de démarrage automatique

REMÉDIATION :

1. Configuration automatique via la protection en temps réel
2. Audit manuel avec msconfig ou autoruns

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.3.4 *Protection de l'intégrité des processus système*

MITRE ATT&CK : T1055

DESCRIPTION :

Protège les processus système critiques contre l'injection de code et la manipulation malveillante.

AUDIT :

- PowerShell: Get-ProcessMitigation -System
- Protection intégrée dans Windows Defender et Exploit Protection

REMÉDIATION :

1. Configuration via Exploit Protection (Section S9)
2. Set-ProcessMitigation -System -Enable DEP,SEHOP,ASLR

VALEUR PAR DÉFAUT :

Partially enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.3.5 *Surveillance des connexions réseau suspectes*

MITRE ATT&CK : T1071

DESCRIPTION :

Surveille les connexions réseau établies par les processus pour détecter les communications malveillantes.

AUDIT :

- PowerShell: Get-NetTCPConnection | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.State -eq 'Established'}
- Intégré dans Network Protection et Defender for Endpoint

REMÉDIATION :

1. Activer Network Protection (Section S7)
2. Déployer Defender for Endpoint pour surveillance avancée

VALEUR PAR DÉFAUT :

Basic monitoring

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.4.1 *Gestion des faux positifs en temps réel*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure la gestion automatisée des faux positifs pour réduire les interruptions tout en maintenant la sécurité.

AUDIT :

- PowerShell: Get-MpThreatDetection | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.ThreatName -like '*False*'}
- Event Viewer: Microsoft-Windows-Windows Defender/Operational

REMÉDIATION :

1. Configurer les exclusions appropriées (Section S5)
2. Utiliser Microsoft Security Intelligence pour rapporter les faux positifs

VALEUR PAR DÉFAUT :

Manual review required

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.4.2 *Notification des détections en temps réel*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure les notifications utilisateur et administrateur pour les détections de menaces en temps réel.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableRealtimeMonitoring,UILockdown
- Windows Security Center notifications

REMÉDIATION :

1. Configuration via Windows Security Center
2. GPO: Configure local setting override for reporting to Microsoft MAPS = Disabled

VALEUR PAR DÉFAUT :

Enabled for users

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.4.3 *Intégration avec SIEM pour temps réel*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure l'envoi des événements de détection en temps réel vers les solutions SIEM pour corrélation centralisée.

AUDIT :

- PowerShell: Get-WinEvent -ListLog *Defender* | Select-Object LogName,IsEnabled
- Event Viewer: Forwarded Events

REMÉDIATION :

1. Configurer Windows Event Forwarding (WEF)
2. wecutil es Microsoft-Windows-Windows-Defender%4Operational

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.4.4 *Performance de la protection temps réel*

MITRE ATT&CK : N/A

DESCRIPTION :

Surveille et optimise les performances de la protection en temps réel pour éviter l'impact sur la productivité.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object -Property *Performance*
- Performance Monitor: Windows Defender counters

REMÉDIATION :

1. Ajuster ScanAvgCPULoadFactor
2. Optimiser les exclusions (Section S5)

VALEUR PAR DÉFAUT :

Balanced

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.4.5 *Audit de la protection temps réel*

MITRE ATT&CK : N/A

DESCRIPTION :

Maintient un audit complet de l'activité de protection en temps réel pour analyse post-incident et conformité.

AUDIT :

- PowerShell: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows Defender/Operational'}
- Event retention policy configuration

REMÉDIATION :

1. Configurer la rétention des logs à 90 jours minimum
2. wevtutil sl Microsoft-Windows-Windows-Defender/Operational /ms:104857600

VALEUR PAR DÉFAUT :

30 days

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.5.1 *Redémarrage automatique après détection*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure le comportement de redémarrage automatique du système après détection et suppression de certaines menaces.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property *DefaultAction*
- Registre: HKLM\SOFTWARE\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction

REMÉDIATION :

1. Set-MpPreference -ThreatIDDefaultAction_Ids @(2,3,4,5) -ThreatIDDefaultAction_Actions @('Quarantine','Quarantine','Quarantine','Quarantine')
2. GPO: Configure remediation for low/medium/high/severe threats

VALEUR PAR DÉFAUT :

Quarantine for most threats

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.5.2 *Protection des fichiers de configuration Defender*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Protège les fichiers de configuration et bases de données de Microsoft Defender contre la modification malveillante.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property TamperProtection
- Microsoft 365 Security Center: Tamper Protection status

REMÉDIATION :

1. Activer via Microsoft 365 Security Center (nécessite Defender for Endpoint)
2. Configuration cloud-managed uniquement

VALEUR PAR DÉFAUT :

Enabled (with MDE)

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.5.3 *Surveillance de l'état des services Defender*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Surveille en continu l'état des services Microsoft Defender pour détecter les tentatives de désactivation.

AUDIT :

- PowerShell: Get-Service -Name 'WinDefend','WdNisSvc','Sense' | Select-Object Name,Status,StartType
- Service status monitoring

REMÉDIATION :

1. Set-Service -Name WinDefend -StartupType Automatic
2. Configurer la surveillance des services critiques

VALEUR PAR DÉFAUT :

Automatic startup

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.5.4 *Protection contre la désactivation par malware*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Implémente des mesures de protection contre les tentatives de désactivation de Defender par des logiciels malveillants.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object AMEngineVersion,AntispywareEnabled,AntivirusEnabled
- Tamper Protection status

REMÉDIATION :

1. Activer Tamper Protection via Defender for Endpoint
2. Surveiller Event ID 5001 (service stopped) et 1150 (configuration changed)

VALEUR PAR DÉFAUT :

Basic protection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

1.5.5 *Récupération automatique après corruption*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure la récupération automatique de Microsoft Defender après corruption des fichiers ou configuration.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object ProductStatus,AMServiceEnabled
- Health status verification

REMÉDIATION :

1. Update-MpSignature -UpdateSource MicrosoftUpdateServer
2. Utiliser Microsoft Defender Offline pour récupération complète

VALEUR PAR DÉFAUT :

Manual recovery

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.0 — PROTECTION CLOUD (MAPS)

2.1.1 *Activation du service MAPS*

MITRE ATT&CK : T1562.001
DESCRIPTION :
Active Microsoft Advanced Protection Service pour la détection cloud des menaces inconnues et la classification en temps réel.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -Property MAPSReporting
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\SpynetReporting

REMÉDIATION :
1. Set-MpPreference -MAPSReporting Advanced
2. GPO: Join Microsoft MAPS = Advanced Membership

VALEUR PAR DÉFAUT :
Basic
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

2.1.2 *Configuration du niveau de rapport MAPS*

MITRE ATT&CK : T1071
DESCRIPTION :
Configure le niveau de détail des rapports envoyés à MAPS pour optimiser la détection tout en respectant la confidentialité.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -Property MAPSReporting
- Valeurs: 0=Disabled, 1=Basic, 2=Advanced

REMÉDIATION :
1. Set-MpPreference -MAPSReporting 2
2. GPO: Configure the 'Block at First Sight' feature = Enabled

VALEUR PAR DÉFAUT :
Basic (1)
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

2.1.3 *Block at First Sight (BAFS)*

MITRE ATT&CK : T1204
DESCRIPTION :
Active le blocage immédiat des fichiers suspects avant même la réception des définitions de signatures.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -Property DisableBlockAtFirstSeen
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\DisableBlockAtFirstSeen

REMÉDIATION :
1. Set-MpPreference -DisableBlockAtFirstSeen
2. GPO: Configure the 'Block at First Sight' feature = Enabled

VALEUR PAR DÉFAUT :
Enabled
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

2.1.4 *Soumission automatique d'échantillons*

MITRE ATT&CK : T1005
DESCRIPTION :
Configure la soumission automatique d'échantillons de fichiers suspects à Microsoft pour analyse approfondie.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -Property SubmitSamplesConsent
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\SubmitSamplesConsent

REMÉDIATION :
1. Set-MpPreference -SubmitSamplesConsent SendSafeSamples
2. GPO: Send file samples when further analysis is required = Send safe samples automatically

VALEUR PAR DÉFAUT :
Always prompt
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

2.1.5 *Délai d'attente cloud étendu*

MITRE ATT&CK : T1071

DESCRIPTION :

Configure un délai d'attente étendu pour les vérifications cloud afin d'améliorer la précision de détection.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property CloudExtendedTimeout
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine\MpCloudBlockLevel

REMÉDIATION :

1. Set-MpPreference -CloudExtendedTimeout 50
2. GPO: Configure extended cloud check timeout period = 50 seconds

VALEUR PAR DÉFAUT :

10 seconds

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.2.1 *Niveau de blocage cloud*

MITRE ATT&CK : T1204

DESCRIPTION :

Configure le niveau d'agressivité du blocage cloud pour équilibrer sécurité et faux positifs.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property CloudBlockLevel
- Valeurs: 0=Default, 1=Moderate, 2=High, 4=HighPlus, 6=ZeroTolerance

REMÉDIATION :

1. Set-MpPreference -CloudBlockLevel 2
2. GPO: Select cloud protection level = High blocking level

VALEUR PAR DÉFAUT :

Default (0)

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.2.2 *Protection renforcée contre les PUA*

MITRE ATT&CK : T1566.001

DESCRIPTION :

Active la détection cloud renforcée des applications potentiellement indésirables (PUA) via l'intelligence Microsoft.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property PUAProtection
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\PUAProtection

REMÉDIATION :

1. Set-MpPreference -PUAProtection Enabled
2. GPO: Configure detection for potentially unwanted applications = Enabled

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.2.3 *Analyse comportementale cloud*

MITRE ATT&CK : T1055

DESCRIPTION :

Active l'analyse comportementale cloud pour détecter les menaces basées sur les patterns de comportement.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableBehaviorMonitoring
- Intégration automatique avec MAPS Advanced

REMÉDIATION :

1. Assurez-vous que MAPS est en mode Advanced
2. Set-MpPreference -DisableBehaviorMonitoring

VALEUR PAR DÉFAUT :

Enabled with MAPS Advanced

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.2.4 *Classification des menaces en temps réel*

MITRE ATT&CK : T1071

DESCRIPTION :

Utilise l'intelligence cloud pour classifier les menaces en temps réel et adapter la réponse automatique.

AUDIT :

- PowerShell: Get-MpThreatDetection | Select-Object ThreatName,Resources,ProcessName
- Cloud threat intelligence integration

REMÉDIATION :

1. Configuration automatique via MAPS Advanced
2. Vérifier la connectivité cloud régulièrement

VALEUR PAR DÉFAUT :

Automatic with MAPS

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.2.5 *Réputation des fichiers et URLs*

MITRE ATT&CK : T1566

DESCRIPTION :

Utilise la base de données de réputation Microsoft pour évaluer la fiabilité des fichiers et URLs en temps réel.

AUDIT :

- PowerShell: Intégré dans la protection en temps réel
- SmartScreen integration pour URLs

REMÉDIATION :

1. Activer SmartScreen (Section S7)
2. Maintenir MAPS en mode Advanced

VALEUR PAR DÉFAUT :

Enabled with cloud protection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.3.1 *Connectivité cloud sécurisée*

MITRE ATT&CK : T1071

DESCRIPTION :

Assure la connectivité sécurisée vers les services cloud Microsoft pour les mises à jour et vérifications en temps réel.

AUDIT :

- PowerShell: Test-NetConnection -ComputerName wdcp.microsoft.com -Port 443
- Connectivité vers *.smartscreen.microsoft.com

REMÉDIATION :

1. Configurer le proxy si nécessaire
2. Ouvrir les ports requis (443, 80) vers les domaines Microsoft

VALEUR PAR DÉFAUT :

Direct connection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.3.2 *Configuration proxy pour MAPS*

MITRE ATT&CK : T1071

DESCRIPTION :

Configure l'utilisation de proxy d'entreprise pour les communications cloud tout en maintenant la sécurité.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ProxyServer,ProxyPacUrl
- netsh winhttp show proxy

REMÉDIATION :

1. Set-MpPreference -ProxyServer 'http://proxy.domain.com:8080'
2. Configurer l'authentification proxy si nécessaire

VALEUR PAR DÉFAUT :

Use system proxy settings

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.3.3 *Gestion des certificats cloud*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Vérifie l'intégrité des certificats SSL/TLS pour les communications cloud et gère les révocations.

AUDIT :

- PowerShell: Vérification automatique intégrée
- Certificate store validation

REMÉDIATION :

1. Maintenir les CA racines Microsoft à jour
2. Configurer la vérification CRL/OCSP

VALEUR PAR DÉFAUT :

Automatic validation

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.3.4 *Surveillance des performances cloud*

MITRE ATT&CK : N/A

DESCRIPTION :

Surveille les performances des requêtes cloud pour optimiser les temps de réponse et la disponibilité.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object *Cloud*
- Performance counters pour Defender

REMÉDIATION :

1. Ajuster CloudExtendedTimeout selon les performances réseau
2. Optimiser la configuration proxy

VALEUR PAR DÉFAUT :

Standard timeout

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.3.5 *Fallback en cas d'indisponibilité cloud*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure le comportement de fallback local quand les services cloud ne sont pas disponibles.

AUDIT :

- PowerShell: Configuration automatique intégrée
- Local signature fallback behavior

REMÉDIATION :

1. Maintenir les signatures locales à jour
2. Configuration automatique, pas d'action manuelle requise

VALEUR PAR DÉFAUT :

Automatic local fallback

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.4.1 *Audit des soumissions cloud*

MITRE ATT&CK : N/A

DESCRIPTION :

Maintient un audit des fichiers soumis au cloud pour analyse et respect des politiques de confidentialité.

AUDIT :

- PowerShell: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows Defender/Operational'; ID=1118}
- Event ID 1118 pour sample submission

REMÉDIATION :

1. Configurer la rétention des logs appropriée
2. Surveiller les soumissions via Event Viewer

VALEUR PAR DÉFAUT :

Basic logging

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.4.2 *Protection des données sensibles*

MITRE ATT&CK : T1005

DESCRIPTION :

Implémente la protection des données sensibles pour éviter leur soumission non autorisée au cloud.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property SubmitSamplesConsent
- Data Loss Prevention integration

REMÉDIATION :

1. Set-MpPreference -SubmitSamplesConsent SendSafeSamples
2. Configurer les exclusions pour données sensibles

VALEUR PAR DÉFAUT :

Prompt before sending

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.4.3 *Conformité réglementaire cloud*

MITRE ATT&CK : N/A

DESCRIPTION :

Assure la conformité avec les réglementations locales concernant le transfert de données vers le cloud Microsoft.

AUDIT :

- Documentation: Révision des contrats Microsoft MAPS
- Compliance documentation review

REMÉDIATION :

1. Réviser les accords de traitement des données Microsoft
2. Configurer selon les exigences réglementaires locales

VALEUR PAR DÉFAUT :

Standard Microsoft terms

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.4.4 *Intégration SIEM pour événements cloud*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure l'intégration SIEM pour collecter et analyser les événements liés aux interactions cloud.

AUDIT :

- PowerShell: Get-WinEvent -ListLog *Defender* | Where-Object {___BEGIN___COMMAND_OUTPUT_MARKER___.RecordCount -gt 0}
- SIEM connector configuration

REMÉDIATION :

1. Configurer Windows Event Forwarding
2. Filtrer les Event ID pertinents (1116, 1117, 1118, 1119)

VALEUR PAR DÉFAUT :

Local logging only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

2.4.5 *Optimisation continue de la protection cloud*

MITRE ATT&CK : N/A

DESCRIPTION :

Processus d'optimisation continue des paramètres cloud basé sur l'analyse des performances et détections.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object *Signature*,*Engine*
- Regular performance analysis

REMÉDIATION :

1. Révision mensuelle des paramètres cloud
2. Ajustement basé sur les métriques de performance

VALEUR PAR DÉFAUT :

Manual optimization

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.0 — MISES À JOUR DES DÉFINITIONS

3.1.1 *Fréquence des mises à jour automatiques*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure la fréquence optimale des mises à jour automatiques des définitions pour maintenir une protection maximale.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property SignatureUpdateInterval
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Signature Updates\SignatureUpdateInterval

REMÉDIATION :

1. Set-MpPreference -SignatureUpdateInterval 1
2. GPO: Define the number of hours to check for definition updates = 1 hour

VALEUR PAR DÉFAUT :

8 hours

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.1.2 *Source primaire de mise à jour*

MITRE ATT&CK : T1071

DESCRIPTION :

Configure la source primaire fiable pour les mises à jour de définitions antivirus (Microsoft Update, WSUS, etc.).

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property SignatureDefinitionUpdateFileSharesSources
- Windows Update configuration

REMÉDIATION :

1. Set-MpPreference -SignatureDefinitionUpdateFileSharesSources 'MicrosoftUpdateServer'
2. GPO: Define file shares for downloading definition updates

VALEUR PAR DÉFAUT :

Microsoft Update Server

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.1.3 *Sources de fallback configurées*

MITRE ATT&CK : T1071

DESCRIPTION :

Configure les sources de secours pour les mises à jour en cas d'indisponibilité de la source primaire.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property SignatureFallbackOrder
- Multiple update sources configuration

REMÉDIATION :

1. Set-MpPreference -SignatureFallbackOrder 'MicrosoftUpdateServer|MMPC|FileShares'
2. GPO: Define the order of sources for downloading definition updates

VALEUR PAR DÉFAUT :

Microsoft Update only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.1.4 *Mise à jour au démarrage du système*

MITRE ATT&CK : T1547

DESCRIPTION :

Force la vérification et mise à jour des définitions lors du démarrage système pour assurer la protection immédiate.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property CheckForSignaturesBeforeRunningScan
- Startup signature update policy

REMÉDIATION :

1. Set-MpPreference -CheckForSignaturesBeforeRunningScan
2. GPO: Check for the latest virus and spyware definitions on startup = Enabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.1.5 *Mise à jour différentielle optimisée*

MITRE ATT&CK : N/A

DESCRIPTION :

Active les mises à jour différentielles pour réduire la bande passante tout en maintenant la rapidité d'update.

AUDIT :

- PowerShell: Configuration automatique intégrée
- Differential update mechanism

REMÉDIATION :

1. Configuration automatique par Microsoft Update
2. Pas de paramétrage manuel requis

VALEUR PAR DÉFAUT :

Enabled automatically

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.2.1 *Mise à jour du moteur antivirus*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Assure la mise à jour régulière du moteur antivirus Microsoft Defender pour supporter les nouvelles techniques de détection.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object -Property AMEngineVersion
- Engine version check against latest

REMÉDIATION :

1. Update-MpSignature -UpdateSource MicrosoftUpdateServer
2. Configuration automatique via Windows Update

VALEUR PAR DÉFAUT :

Automatic with Windows Update

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.2.2 *Mise à jour de la plateforme Defender*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Maintient la plateforme Microsoft Defender à jour pour bénéficier des dernières fonctionnalités et corrections de sécurité.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object -Property AMProductVersion
- Platform version comparison

REMÉDIATION :

1. Configuration automatique via Windows Update
2. Manual: Update-MpSignature pour forcer la vérification

VALEUR PAR DÉFAUT :

Automatic with Windows Update

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.2.3 *Synchronisation des signatures réseau*

MITRE ATT&CK : T1071

DESCRIPTION :

Configure la synchronisation réseau des signatures pour les environnements déconnectés ou à bande passante limitée.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property SignatureDefinitionUpdateFileSharesSources
- Network share configuration

REMÉDIATION :

1. Set-MpPreference -SignatureDefinitionUpdateFileSharesSources '\\server\defender-updates'
2. GPO: Define file shares for downloading definition updates

VALEUR PAR DÉFAUT :

Direct Microsoft servers

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.2.4 *Validation de l'intégrité des signatures*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Vérifie l'intégrité cryptographique des signatures téléchargées pour éviter les signatures compromises.

AUDIT :

- PowerShell: Vérification automatique intégrée
- Signature validation process

REMÉDIATION :

1. Configuration automatique par Windows Defender
2. Surveillance des échecs de validation dans Event Viewer

VALEUR PAR DÉFAUT :

Automatic validation

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.2.5 *Rollback des signatures défaillantes*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure la capacité de rollback automatique vers des signatures stables en cas de problème avec une mise à jour.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object -Property *Signature*
- Rollback mechanism status

REMÉDIATION :

1. Configuration automatique intégrée
2. Manual: Update-MpSignature -UpdateSource FallbackOrder

VALEUR PAR DÉFAUT :

Automatic rollback enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.3.1 *Programmation des vérifications de mise à jour*

MITRE ATT&CK : N/A

DESCRIPTION :

Programme les vérifications régulières de mises à jour à des heures optimales pour minimiser l'impact performance.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property *Update*
- Task Scheduler: Windows Defender tasks

REMÉDIATION :

1. Configuration via GPO ou Intune pour heures creuses
2. Utiliser Task Scheduler pour personnalisation avancée

VALEUR PAR DÉFAUT :

Every 8 hours

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.3.2 *Gestion de la bande passante pour les mises à jour*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure la limitation de bande passante pour les mises à jour afin de ne pas impacter les activités critiques.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property *Bandwidth*
- BITS configuration for updates

REMÉDIATION :

1. Configuration via BITS (Background Intelligent Transfer Service)
2. GPO: Configure BITS bandwidth throttling

VALEUR PAR DÉFAUT :

No bandwidth limitation

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.3.3 *Notification des échecs de mise à jour*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure les notifications automatiques en cas d'échec des mises à jour pour intervention rapide.

AUDIT :

- PowerShell: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows Defender/Operational'; ID=2001}
- Event ID 2001 pour update failures

REMÉDIATION :

1. Configurer les alertes Event Viewer
2. Intégration SIEM pour notifications centralisées

VALEUR PAR DÉFAUT :

Event logging only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.3.4 *Mise à jour prioritaire en cas de menace émergente*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Active les mises à jour prioritaires en cas de menaces émergentes critiques signalées par Microsoft.

AUDIT :

- PowerShell: Configuration automatique avec MAPS Advanced
- Emergency signature updates

REMÉDIATION :

1. Maintenir MAPS en mode Advanced
2. Assurer la connectivité cloud permanente

VALEUR PAR DÉFAUT :

Enabled with MAPS Advanced

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.3.5 *Historique des versions de signatures*

MITRE ATT&CK : N/A

DESCRIPTION :

Maintient un historique des versions de signatures installées pour traçabilité et dépannage.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object *Signature*
- Event Viewer: Signature update history

REMÉDIATION :

1. Configuration automatique des logs Windows
2. Rétention des événements sur 90 jours minimum

VALEUR PAR DÉFAUT :

30 days retention

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.4.1 *Cache local des signatures*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure un cache local efficace des signatures pour réduire les téléchargements répétitifs.

AUDIT :

- PowerShell: Get-ChildItem 'C:\ProgramData\Microsoft\Windows Defender\Definition Updates'
- Local cache directory inspection

REMÉDIATION :

1. Configuration automatique par Windows Defender
2. Surveiller l'espace disque disponible

VALEUR PAR DÉFAUT :

Automatic caching

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.4.2 *Nettoyage automatique des anciennes signatures*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure le nettoyage automatique des anciennes signatures pour optimiser l'espace disque.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanPurgeItemsAfterDelay
- Automatic cleanup configuration

REMÉDIATION :

1. Set-MpPreference -ScanPurgeItemsAfterDelay 30
2. Configuration automatique du nettoyage

VALEUR PAR DÉFAUT :

30 days

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.4.3 *Surveillance de l'espace disque pour signatures*

MITRE ATT&CK : N/A

DESCRIPTION :

Surveille l'espace disque disponible pour éviter les échecs de mise à jour dus au manque d'espace.

AUDIT :

- PowerShell: Get-PSDrive C | Select-Object Used,Free
- Disk space monitoring for definition updates

REMÉDIATION :

1. Configurer des alertes d'espace disque
2. Planifier le nettoyage régulier

VALEUR PAR DÉFAUT :

No specific monitoring

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.4.4 *Intégration avec la gestion des correctifs*

MITRE ATT&CK : N/A

DESCRIPTION :

Intègre les mises à jour Defender avec la stratégie globale de gestion des correctifs de l'organisation.

AUDIT :

- WSUS/SCCM: Configuration des mises à jour Defender
- Update management integration

REMÉDIATION :

1. Configurer WSUS pour inclure les mises à jour Defender
2. Coordonner avec l'équipe de gestion des correctifs

VALEUR PAR DÉFAUT :

Independent update process

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

3.4.5 *Métriques de performance des mises à jour*

MITRE ATT&CK : N/A

DESCRIPTION :

Collecte et analyse les métriques de performance des mises à jour pour optimisation continue.

AUDIT :

- PowerShell: Get-MpComputerStatus | Select-Object *Update*,*Age*
- Performance metrics collection

REMÉDIATION :

1. Établir des SLA pour les mises à jour
2. Surveillance continue des performances

VALEUR PAR DÉFAUT :

Basic metrics only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

6.0 — RÈGLES DE RÉDUCTION DE SURFACE D'ATTAQUE (ASR)

6.1.1 *Règle ASR: Bloquer l'exécutable créé par commandes Office*

MITRE ATT&CK : T1566.001
GUID ASR : BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550
DESCRIPTION :
Bloque la création et l'exécution d'exécutables par les applications Microsoft Office pour prévenir les macros malveillantes.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: Windows Defender Exploit Guard > Attack Surface Reduction > BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550 = Block
3. Intune: Endpoint Security > Attack Surface Reduction rules

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.1.2 *Règle ASR: Bloquer Office créant des processus enfants*

MITRE ATT&CK : T1566.001
GUID ASR : D4F940AB-401B-4EFC-AADC-AD5F3C50688A
DESCRIPTION :
Empêche les applications Office de créer des processus enfants, technique couramment utilisée par les malwares.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Vérifier la présence du GUID D4F940AB-401B-4EFC-AADC-AD5F3C50688A

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EFC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > D4F940AB-401B-4EFC-AADC-AD5F3C50688A = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.1.3 *Règle ASR: Bloquer injection dans processus Office*

MITRE ATT&CK : T1055
GUID ASR : 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
DESCRIPTION :
Bloque l'injection de code dans les processus Microsoft Office pour prévenir la compromission des applications légitimes.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Rechercher le GUID 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.1.4 *Règle ASR: Bloquer JavaScript/VBScript dans Office*

MITRE ATT&CK : T1059.007
GUID ASR : 3B576869-A4EC-4529-8536-B80A7769E899
DESCRIPTION :
Empêche l'exécution de JavaScript et VBScript lancés par Microsoft Office pour bloquer les scripts malveillants.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Vérifier 3B576869-A4EC-4529-8536-B80A7769E899

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 3B576869-A4EC-4529-8536-B80A7769E899 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 3B576869-A4EC-4529-8536-B80A7769E899 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.1.5 *Règle ASR: Bloquer macros Office avec contenu Web*

MITRE ATT&CK : T1566.001
GUID ASR : 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B
DESCRIPTION :
Bloque l'exécution de macros Office qui téléchargent du contenu depuis Internet pour prévenir les attaques par documents malveillants.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Confirmer 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.2.1 *Règle ASR: Bloquer exécutables suspects d'email*

MITRE ATT&CK : T1566.001
GUID ASR : BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46551
DESCRIPTION :
Bloque l'exécution d'exécutables provenant de clients email et webmail pour prévenir les attaques par pièces jointes.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Localiser BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46551

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46551 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46551 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.2.2 *Règle ASR: Bloquer vol de credentials Windows LSASS*

MITRE ATT&CK : T1003.001
GUID ASR : 9E6C4E1F-7D60-472F-BA1A-A39EF669E4B2
DESCRIPTION :
Protège le processus LSASS contre les tentatives de vol de credentials par des outils comme Mimikatz.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Vérifier 9E6C4E1F-7D60-472F-BA1A-A39EF669E4B2

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 9E6C4E1F-7D60-472F-BA1A-A39EF669E4B2 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 9E6C4E1F-7D60-472F-BA1A-A39EF669E4B2 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.2.3 *Règle ASR: Bloquer création processus via WMI*

MITRE ATT&CK : T1047
GUID ASR : D1E49AAC-8F56-4280-B9BA-993A6D77406C
DESCRIPTION :
Bloque la création de processus via les commandes WMI pour prévenir l'exécution de code à distance malveillant.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Localiser D1E49AAC-8F56-4280-B9BA-993A6D77406C

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids D1E49AAC-8F56-4280-B9BA-993A6D77406C -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > D1E49AAC-8F56-4280-B9BA-993A6D77406C = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.2.4 *Règle ASR: Bloquer processus non signés via USB*

MITRE ATT&CK : T1091
GUID ASR : B2B3F03D-6A65-4F7B-A9C7-1C7EF74A9BA4
DESCRIPTION :
Bloque l'exécution de processus non signés ou de confiance faible depuis des lecteurs USB amovibles.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Vérifier B2B3F03D-6A65-4F7B-A9C7-1C7EF74A9BA4

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids B2B3F03D-6A65-4F7B-A9C7-1C7EF74A9BA4 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > B2B3F03D-6A65-4F7B-A9C7-1C7EF74A9BA4 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.2.5 *Règle ASR: Bloquer scripts obfusqués suspects*

MITRE ATT&CK : T1027
GUID ASR : 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC
DESCRIPTION :
Bloque l'exécution de scripts JavaScript, VBScript et PowerShell obfusqués ou suspects.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Confirmer 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.3.1 *Règle ASR: Bloquer injection dans processus système*

MITRE ATT&CK : T1055
GUID ASR : 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
DESCRIPTION :
Empêche l'injection de code dans les processus système critiques pour maintenir l'intégrité du système.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Localiser 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.3.2 *Règle ASR: Bloquer téléchargements depuis navigateurs*

MITRE ATT&CK : T1566.002
GUID ASR : D3E037E1-3EB8-44C8-A917-57927947596D
DESCRIPTION :
Bloque l'exécution immédiate de fichiers téléchargés depuis les navigateurs web pour permettre l'analyse.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Vérifier D3E037E1-3EB8-44C8-A917-57927947596D

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids D3E037E1-3EB8-44C8-A917-57927947596D -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > D3E037E1-3EB8-44C8-A917-57927947596D = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.3.3 *Règle ASR: Bloquer communications avec ransomware*

MITRE ATT&CK : T1486
GUID ASR : C1DB55AB-C21A-4637-BB3F-A12568109D35
DESCRIPTION :
Bloque les communications réseau typiques des ransomwares pour interrompre leur fonctionnement.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Confirmer C1DB55AB-C21A-4637-BB3F-A12568109D35

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids C1DB55AB-C21A-4637-BB3F-A12568109D35 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > C1DB55AB-C21A-4637-BB3F-A12568109D35 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.3.4 *Règle ASR: Bloquer Adobe Reader processus enfants*

MITRE ATT&CK : T1566.001
GUID ASR : 7674BA52-37EB-4A4F-A9A1-F0F9A1619A2C
DESCRIPTION :
Empêche Adobe Reader de créer des processus enfants pour prévenir l'exploitation des vulnérabilités PDF.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Localiser 7674BA52-37EB-4A4F-A9A1-F0F9A1619A2C

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 7674BA52-37EB-4A4F-A9A1-F0F9A1619A2C -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 7674BA52-37EB-4A4F-A9A1-F0F9A1619A2C = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.3.5 *Règle ASR: Bloquer persistance via WMI*

MITRE ATT&CK : T1546.003
GUID ASR : E6DB77E5-3DF2-4CF1-B95A-636979351E5B
DESCRIPTION :
Bloque l'utilisation de souscriptions d'événements WMI pour établir la persistance malveillante.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Vérifier E6DB77E5-3DF2-4CF1-B95A-636979351E5B

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids E6DB77E5-3DF2-4CF1-B95A-636979351E5B -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > E6DB77E5-3DF2-4CF1-B95A-636979351E5B = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.4.1 *Configuration mode Audit vs Block*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure le mode d'évaluation (Audit) vs production (Block) pour les règles ASR selon la maturité organisationnelle.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Actions
- Valeurs: 0=Disabled, 1=Block, 2=Audit, 6=Warn

REMÉDIATION :

1. Phase 1 (Audit): Set-MpPreference -AttackSurfaceReductionRules_Actions AuditMode
2. Phase 2 (Production): Set-MpPreference -AttackSurfaceReductionRules_Actions Enabled
3. GPO: Configurer chaque règle individuellement

VALEUR PAR DÉFAUT :

Not configured

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

6.4.2 *Exclusions ASR documentées et justifiées*

MITRE ATT&CK : N/A

DESCRIPTION :

Maintient une liste documentée et justifiée des exclusions ASR pour les applications métier légitimes.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionOnlyExclusions
- Documentation des exclusions avec justifications business

REMÉDIATION :

1. Add-MpPreference -AttackSurfaceReductionOnlyExclusions 'C:\Program Files\Business App*'
2. Maintenir un registre des exclusions avec approbations
3. Révision trimestrielle des exclusions

VALEUR PAR DÉFAUT :

No exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

6.4.3 *Surveillance des déclenchements ASR*

MITRE ATT&CK : N/A

DESCRIPTION :

Surveille et analyse les déclenchements des règles ASR pour optimisation et détection d'attaques.

AUDIT :

- PowerShell: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows Defender/Operational'; ID=1121,1122}
- Event ID 1121 (ASR Block), 1122 (ASR Audit)

REMÉDIATION :

1. Configurer la collecte centralisée des événements ASR
2. Établir des alertes pour déclenchements fréquents
3. Analyse hebdomadaire des patterns

VALEUR PAR DÉFAUT :

Local logging only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

6.4.4 *Intégration ASR avec SIEM*

MITRE ATT&CK : N/A

DESCRIPTION :

Intègre les événements ASR avec la solution SIEM pour corrélation avec d'autres événements de sécurité.

AUDIT :

- SIEM Configuration: Réception des Event ID 1121, 1122, 5007
- Windows Event Forwarding configuration

REMÉDIATION :

1. Configurer WEF pour transférer les événements ASR
2. Créer des règles de corrélation SIEM
3. Dashboard de supervision ASR

VALEUR PAR DÉFAUT :

No SIEM integration

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

6.4.5 *Règle ASR: Bloquer exécution depuis dossiers système*

MITRE ATT&CK : T1036.005
GUID ASR : 01443614-cd74-433a-b99e-2ecdc07bfc25
DESCRIPTION :
Bloque l'exécution d'exécutables depuis des dossiers système non autorisés pour prévenir le masquerading.
AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
- Vérifier 01443614-cd74-433a-b99e-2ecdc07bfc25

REMÉDIATION :
1. Add-MpPreference -AttackSurfaceReductionRules_Ids 01443614-cd74-433a-b99e-2ecdc07bfc25 -AttackSurfaceReductionRules_Actions Enabled
2. GPO: ASR Rules > 01443614-cd74-433a-b99e-2ecdc07bfc25 = Block

VALEUR PAR DÉFAUT :
Not configured
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.5.1 *Performance et impact des règles ASR*

MITRE ATT&CK : N/A
DESCRIPTION :
Évalue l'impact performance des règles ASR et optimise pour équilibrer sécurité et productivité.
AUDIT :
- PowerShell: Mesure des temps de démarrage et d'exécution d'applications
- Performance counters Windows Defender

REMÉDIATION :
1. Baseline des performances avant activation ASR
2. Monitoring continu post-déploiement
3. Ajustement des exclusions si nécessaire

VALEUR PAR DÉFAUT :
No performance monitoring
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.5.2 *Tests de régression ASR*

MITRE ATT&CK : N/A
DESCRIPTION :
Effectue des tests de régression réguliers pour s'assurer que les règles ASR n'impactent pas les applications métier.
AUDIT :
- Test Environment: Validation des applications critiques
- User Acceptance Testing results

REMÉDIATION :
1. Établir un environnement de test ASR
2. Scripts de tests automatisés pour applications critiques
3. Processus de validation avant mise en production

VALEUR PAR DÉFAUT :
No systematic testing
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.5.3 *Déploiement progressif des règles ASR*

MITRE ATT&CK : N/A
DESCRIPTION :
Implémente un déploiement progressif des règles ASR par phases pour minimiser les disruptions.
AUDIT :
- Deployment Phase Tracking: Audit > Warn > Block
- Group Policy ou Intune ring deployment

REMÉDIATION :
1. Phase 1: Mode Audit sur groupe pilote (2 semaines)
2. Phase 2: Mode Warn sur population élargie (2 semaines)
3. Phase 3: Mode Block sur toute l'organisation

VALEUR PAR DÉFAUT :
No phased deployment
État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A
Commentaires : _____

6.5.4 *Formation utilisateurs sur ASR*

MITRE ATT&CK : N/A

DESCRIPTION :

Forme les utilisateurs sur les impacts des règles ASR et les procédures d'escalade en cas de blocage légitime.

AUDIT :

- Training Completion Rate: Suivi des formations utilisateurs
- Help Desk ticket trends related to ASR

REMÉDIATION :

1. Matériel de formation sur les nouvelles restrictions
2. Procédures d'escalade pour demandes d'exclusion
3. FAQ et documentation utilisateur

VALEUR PAR DÉFAUT :

No user training

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

6.5.5 *Métriques et reporting ASR*

MITRE ATT&CK : N/A

DESCRIPTION :

Établit des métriques et reporting régulier de l'efficacité et de l'impact des règles ASR.

AUDIT :

- Monthly ASR Reports: Nombre de blocages, exclusions, performances
- Executive dashboard avec KPIs sécurité

REMÉDIATION :

1. Collecter métriques mensuelles ASR
2. Reports executifs sur efficacité sécurité
3. Recommandations d'optimisation basées sur données

VALEUR PAR DÉFAUT :

No systematic reporting

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.0 — ANALYSES PROGRAMMÉES

4.1.1 *Configuration de l'analyse complète hebdomadaire*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure une analyse complète hebdomadaire automatique pour détecter les menaces persistantes et dormantes.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanScheduleDay,ScanScheduleTime,ScanParameters
- Task Scheduler: Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan

REMÉDIATION :

1. Set-MpPreference -ScanScheduleDay 0 -ScanScheduleTime 02:00:00 -ScanParameters 2
2. GPO: Scan > Specify the scan type to use for a scheduled scan = Full scan
3. Configurer pour dimanche 2h00 du matin

VALEUR PAR DÉFAUT :

Quick scan daily

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.1.2 *Analyse rapide quotidienne*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Maintient une analyse rapide quotidienne pour détecter les menaces actives dans les emplacements critiques du système.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanScheduleQuickScanTime
- Daily quick scan configuration

REMÉDIATION :

1. Set-MpPreference -ScanScheduleQuickScanTime 12:00:00
2. GPO: Specify the time for a daily quick scan = 12:00
3. Programmer pendant les heures de faible activité

VALEUR PAR DÉFAUT :

2:00 AM daily

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.1.3 *Limitation CPU pour analyses programmées*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure la limitation d'utilisation CPU pendant les analyses pour préserver les performances système.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanAvgCPULoadFactor
- CPU usage limit configuration

REMÉDIATION :

1. Set-MpPreference -ScanAvgCPULoadFactor 30
2. GPO: Specify the maximum percentage of CPU utilization during a scan = 30%
3. Ajuster selon la charge de travail système

VALEUR PAR DÉFAUT :

50%

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.1.4 *Analyse de rattrapage pour systèmes hors ligne*

MITRE ATT&CK : N/A

DESCRIPTION :

Active l'analyse de rattrapage automatique pour les systèmes qui étaient hors ligne pendant l'analyse programmée.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableCatchupFullScan,DisableCatchupQuickScan
- Catch-up scan configuration

REMÉDIATION :

1. Set-MpPreference -DisableCatchupFullScan -DisableCatchupQuickScan
2. GPO: Start the scheduled scan only when computer is on but not in use = Disabled
3. Permettre les analyses de rattrapage

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.1.5 *Analyse uniquement si inactif*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure les analyses pour s'exécuter uniquement lorsque le système est inactif pour minimiser l'impact utilisateur.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanOnlyIfIdleEnabled
- Task Scheduler conditions for Defender scans

REMÉDIATION :

1. Set-MpPreference -ScanOnlyIfIdleEnabled
2. GPO: Start the scheduled scan only when computer is on but not in use = Enabled
3. Configurer seuil d'inactivité approprié

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.2.1 *Analyse des lecteurs réseau dans les scans programmés*

MITRE ATT&CK : T1021.002

DESCRIPTION :

Configure l'inclusion des lecteurs réseau mappés dans les analyses programmées selon les besoins de sécurité.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableScanningNetworkFiles
- Network drive scanning in scheduled scans

REMÉDIATION :

1. Set-MpPreference -DisableScanningNetworkFiles
2. GPO: Scan mapped network drives = Enabled
3. Évaluer l'impact performance réseau

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.2.2 *Analyse des archives dans les scans programmés*

MITRE ATT&CK : T1027.002

DESCRIPTION :

Active l'analyse approfondie des archives et fichiers compressés pendant les analyses programmées.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableArchiveScanning
- Archive scanning configuration

REMÉDIATION :

1. Set-MpPreference -DisableArchiveScanning
2. GPO: Scan archive files = Enabled
3. Considérer l'impact sur durée d'analyse

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.2.3 *Profondeur maximale d'analyse des archives*

MITRE ATT&CK : T1027.002

DESCRIPTION :

Configure la profondeur maximale d'analyse des archives imbriquées pour équilibrer sécurité et performance.

AUDIT :

- PowerShell: Configuration intégrée dans DisableArchiveScanning
- Archive depth scanning limits

REMÉDIATION :

1. Configuration automatique via Windows Defender
2. Surveillance des performances d'analyse
3. Ajustement si timeouts fréquents

VALEUR PAR DÉFAUT :

Standard depth

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.2.4 *Analyse des emails dans les scans programmés*

MITRE ATT&CK : T1566.001

DESCRIPTION :

Include l'analyse des fichiers email et bases de données de messagerie dans les analyses programmées.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableEmailScanning
- Email scanning in scheduled scans

REMÉDIATION :

1. Set-MpPreference -DisableEmailScanning
2. GPO: Scan e-mail = Enabled
3. Coordonner avec équipes messaging

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.2.5 *Analyse des supports amovibles*

MITRE ATT&CK : T1091

DESCRIPTION :

Configure l'analyse automatique des supports amovibles lors de leur connexion et pendant les scans programmés.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property DisableRemovableDriveScanning
- Removable drive scanning policy

REMÉDIATION :

1. Set-MpPreference -DisableRemovableDriveScanning
2. GPO: Scan removable drives = Enabled
3. Équilibrer sécurité et commodité utilisateur

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.3.1 *Mise à jour des signatures avant analyse*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Force la mise à jour des signatures antivirus avant chaque analyse programmée pour maximiser la détection.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property CheckForSignaturesBeforeRunningScan
- Pre-scan signature update policy

REMÉDIATION :

1. Set-MpPreference -CheckForSignaturesBeforeRunningScan
2. GPO: Check for the latest virus and spyware definitions before running a scheduled scan = Enabled

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.3.2 *Timeout pour analyses longues*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure un timeout raisonnable pour les analyses programmées afin d'éviter les blocages système prolongés.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanTimeout
- Scan timeout configuration

REMÉDIATION :

1. Configuration via GPO si nécessaire
2. Surveiller les analyses qui n'aboutissent pas
3. Ajuster selon la taille des systèmes

VALEUR PAR DÉFAUT :

No timeout

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.3.3 *Exclusions spécifiques aux analyses programmées*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure des exclusions spécifiques pour les analyses programmées pour optimiser les performances sans compromettre la sécurité.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ExclusionPath,ExclusionExtension
- Scheduled scan specific exclusions

REMÉDIATION :

1. Évaluer les exclusions nécessaires pour bases de données
2. Documenter et justifier chaque exclusion
3. Révision régulière des exclusions

VALEUR PAR DÉFAUT :

Global exclusions apply

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.3.4 *Priorité des processus d'analyse*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure la priorité des processus d'analyse programmée pour équilibrer sécurité et performance système.

AUDIT :

- PowerShell: Process priority configuration (automatique)
- Task Manager: Priorité des processus Defender

REMÉDIATION :

1. Configuration automatique par Windows Defender
2. Surveiller l'impact sur les performances
3. Ajustement via exclusions si nécessaire

VALEUR PAR DÉFAUT :

Normal priority

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.3.5 *Planification intelligente des analyses*

MITRE ATT&CK : N/A

DESCRIPTION :

Implémente une planification intelligente qui adapte les heures d'analyse selon les patterns d'utilisation système.

AUDIT :

- Task Scheduler: Conditions d'exécution adaptatives
- Machine Learning basé sur utilisation historique

REMÉDIATION :

1. Analyser les patterns d'utilisation système
2. Ajuster les heures d'analyse dynamiquement
3. Feedback utilisateur pour optimisation

VALEUR PAR DÉFAUT :

Fixed schedule

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.4.1 *Reporting des résultats d'analyses programmées*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure le reporting automatique des résultats d'analyses programmées pour suivi centralisé.

AUDIT :

- PowerShell: Get-MpThreatDetection pour historique
- Event Viewer: Microsoft-Windows-Windows Defender/Operational

REMÉDIATION :

1. Configurer la centralisation des logs d'analyse
2. Alertes automatiques en cas de détections
3. Rapports hebdomadaires de synthèse

VALEUR PAR DÉFAUT :

Local logging only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.4.2 *Surveillance des échecs d'analyses programmées*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Surveille et alerte sur les échecs d'analyses programmées pour intervention rapide.

AUDIT :

- PowerShell: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows Defender/Operational'; ID=1005}
- Event ID 1005 pour scan failures

REMÉDIATION :

1. Configurer alertes sur échecs d'analyse
2. Processus d'escalade automatique
3. Investigation des causes racines

VALEUR PAR DÉFAUT :

No automatic alerting

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.4.3 *Métriques de performance des analyses*

MITRE ATT&CK : N/A

DESCRIPTION :

Collecte et analyse les métriques de performance des analyses pour optimisation continue.

AUDIT :

- PowerShell: Durée d'analyse, fichiers scannés, détections
- Performance baselines et trending

REMÉDIATION :

1. Établir des baselines de performance
2. Monitoring des tendances de durée
3. Optimisation basée sur les données

VALEUR PAR DÉFAUT :

Basic metrics collection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.4.4 *Intégration avec outils de monitoring*

MITRE ATT&CK : N/A

DESCRIPTION :

Intègre les métriques d'analyses avec les outils de monitoring système pour vue d'ensemble.

AUDIT :

- SCOM/Nagios/Zabbix: Intégration des métriques Defender
- Dashboard centralisé de sécurité

REMÉDIATION :

1. Configurer les connecteurs monitoring
2. Seuils d'alerte appropriés
3. Corrélation avec autres métriques système

VALEUR PAR DÉFAUT :

No external integration

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

4.4.5 *Archivage des historiques d'analyse*

MITRE ATT&CK : N/A

DESCRIPTION :

Maintient un archivage approprié des historiques d'analyse pour audit et conformité.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ScanPurgeItemsAfterDelay
- Log retention policy configuration

REMÉDIATION :

1. Configurer rétention logs 12 mois minimum
2. Archivage automatique des anciens logs
3. Procédures de récupération pour audit

VALEUR PAR DÉFAUT :

30 days retention

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

Section 5 — GESTION DES EXCLUSIONS

5.0 — GESTION DES EXCLUSIONS

5.1.1 *Inventaire documenté des exclusions*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Maintient un inventaire complet et documenté de toutes les exclusions antivirus avec justifications métier.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property ExclusionPath,ExclusionExtension,ExclusionProcess
- Documentation formelle des exclusions avec approbations

REMÉDIATION :

1. Créer registre centralisé des exclusions
2. Justification métier obligatoire pour chaque exclusion
3. Approbation formelle par équipe sécurité

VALEUR PAR DÉFAUT :

No documented exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.1.2 *Exclusions de chemins avec wildcards sécurisés*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure les exclusions de chemins avec des wildcards spécifiques pour éviter les exclusions trop larges.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -ExpandProperty ExclusionPath
- Audit des wildcards potentiellement dangereux

REMÉDIATION :

1. Éviter les exclusions type 'C:*' ou '*.*'
2. Utiliser chemins spécifiques: 'C:\Program Files\AppName*'
3. Révision régulière des wildcards

VALEUR PAR DÉFAUT :

No path exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.1.3 *Exclusions d'extensions strictement limitées*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Limite strictement les exclusions d'extensions de fichiers aux besoins métier légitimes documentés.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -ExpandProperty ExclusionExtension
- Audit des extensions exclues potentiellement risquées

REMÉDIATION :

1. Interdire exclusions .exe, .dll, .scr, .bat, .cmd
2. Limiter aux extensions spécifiques métier (.dbf, .lck, etc.)
3. Révision mensuelle des exclusions d'extensions

VALEUR PAR DÉFAUT :

No extension exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.1.4 *Exclusions de processus avec validation sécurité*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Valide rigoureusement les exclusions de processus pour éviter l'exclusion de processus potentiellement malveillants.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -ExpandProperty ExclusionProcess
- Validation sécurité de chaque processus exclu

REMÉDIATION :

1. Signature numérique obligatoire pour processus exclus
2. Validation par équipe sécurité
3. Surveillance renforcée des processus exclus

VALEUR PAR DÉFAUT :

No process exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.1.5 *Exclusions temporaires avec échéance*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Implémente un système d'exclusions temporaires avec dates d'échéance automatiques pour révision.

AUDIT :

- Documentation: Suivi des dates d'échéance des exclusions temporaires
- Processus de révision automatique

REMÉDIATION :

1. Système de tickets avec dates d'échéance
2. Révision automatique mensuelle
3. Suppression auto des exclusions expirées

VALEUR PAR DÉFAUT :

No temporary exclusion system

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.2.1 *Exclusions pour applications métier critiques*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure des exclusions appropriées pour les applications métier critiques tout en maintenant la sécurité maximale.

AUDIT :

- PowerShell: Exclusions spécifiques aux applications identifiées
- Performance et stabilité des applications critiques

REMÉDIATION :

1. Identifier applications nécessitant exclusions
2. Exclusions minimales nécessaires uniquement
3. Monitoring renforcé des répertoires exclus

VALEUR PAR DÉFAUT :

No business application exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.2.2 *Exclusions pour bases de données*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure les exclusions appropriées pour les systèmes de bases de données selon les recommandations des éditeurs.

AUDIT :

- PowerShell: Exclusions pour SQL Server, Oracle, MongoDB, etc.
- Documentation éditeur des exclusions recommandées

REMÉDIATION :

1. Suivre recommendations Microsoft SQL Server
2. Exclusions spécifiques aux fichiers de données (.mdf, .ldf)
3. Surveillance des répertoires de données

VALEUR PAR DÉFAUT :

No database exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.2.3 *Exclusions pour systèmes de sauvegarde*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure les exclusions nécessaires pour les systèmes de sauvegarde pour éviter les corruptions et améliorer les performances.

AUDIT :

- PowerShell: Exclusions pour Veeam, Acronis, Backup Exec, etc.
- Performance et intégrité des sauvegardes

REMÉDIATION :

1. Exclusions selon documentation éditeur backup
2. Surveillance des performances de sauvegarde
3. Tests d'intégrité réguliers

VALEUR PAR DÉFAUT :

No backup system exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.2.4 *Exclusions pour outils de développement*

MITRE ATT&CK : T1127

DESCRIPTION :

Balance les exclusions pour outils de développement entre productivité et sécurité, avec surveillance renforcée.

AUDIT :

- PowerShell: Exclusions pour Visual Studio, compilers, etc.
- Monitoring activité dans répertoires de développement

REMÉDIATION :

1. Exclusions limitées aux répertoires projets
2. Surveillance renforcée activité développement
3. Formation développeurs sur sécurité

VALEUR PAR DÉFAUT :

No development tool exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.2.5 *Exclusions pour services système critiques*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure prudemment les exclusions pour les services système Windows critiques selon les guidelines Microsoft.

AUDIT :

- PowerShell: Exclusions pour services Windows essentiels
- Guidelines Microsoft pour exclusions système

REMÉDIATION :

1. Suivre strictement recommandations Microsoft
2. Exclusions minimales pour fonctionnement système
3. Documentation de chaque exclusion système

VALEUR PAR DÉFAUT :

Automatic system exclusions

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.3.1 *Processus d'approbation des exclusions*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Établit un processus formel d'approbation pour toutes les demandes d'exclusion avec validation sécurité.

AUDIT :

- Documentation: Processus d'approbation documenté et suivi
- Traçabilité des approbations et refus

REMÉDIATION :

1. Formulaire standardisé de demande d'exclusion
2. Validation obligatoire par équipe sécurité
3. Approbation du management pour exclusions critiques

VALEUR PAR DÉFAUT :

No formal approval process

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.3.2 *Tests d'impact avant exclusion*

MITRE ATT&CK : N/A

DESCRIPTION :

Effectue des tests d'impact sécurité avant d'implémenter de nouvelles exclusions.

AUDIT :

- Test Environment: Validation impact sécurité des exclusions
- Simulation d'attaques sur zones exclues

REMÉDIATION :

1. Tests en environnement isolé
2. Évaluation risques vs bénéfices
3. Plan de rollback en cas de problème

VALEUR PAR DÉFAUT :

No systematic testing

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.3.3 *Surveillance renforcée des zones exclues*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Implémente une surveillance sécurité renforcée des répertoires et processus exclus de l'antivirus.

AUDIT :

- SIEM: Monitoring activité dans zones exclues
- File Integrity Monitoring sur répertoires exclus

REMÉDIATION :

1. Configurer FIM sur tous répertoires exclus
2. Alertes sur modifications dans zones exclues
3. Corrélation avec autres événements sécurité

VALEUR PAR DÉFAUT :

No enhanced monitoring

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.3.4 *Révision périodique des exclusions*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Effectue une révision trimestrielle de toutes les exclusions pour valider leur pertinence continue.

AUDIT :

- Documentation: Planning et résultats des révisions trimestrielles
- Actions correctives suite aux révisions

REMÉDIATION :

1. Calendrier de révision trimestrielle
2. Validation continue de la nécessité métier
3. Suppression des exclusions obsolètes

VALEUR PAR DÉFAUT :

No periodic review

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

5.3.5 *Métriques et reporting des exclusions*

MITRE ATT&CK : N/A

DESCRIPTION :

Collecte des métriques sur l'utilisation des exclusions et leur impact sur la posture de sécurité.

AUDIT :

- Reporting: Nombre d'exclusions, types, évolution temporelle
- Métriques d'impact sécurité

REMÉDIATION :

1. Dashboard des exclusions actives
2. Métriques d'impact performance et sécurité
3. Rapports mensuels pour management

VALEUR PAR DÉFAUT :

No systematic metrics

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.0 — PROTECTION RÉSEAU

7.1.1 *Activation de la protection réseau*

MITRE ATT&CK : T1071

DESCRIPTION :

Active la protection réseau Microsoft Defender pour bloquer les connexions vers des domaines et IPs malveillants connus.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property EnableNetworkProtection
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection\EnableNetworkProtection

REMÉDIATION :

1. Set-MpPreference -EnableNetworkProtection Enabled
2. GPO: Prevent users and apps from accessing dangerous websites = Enabled (Block mode)
3. Intune: Endpoint Security > Attack Surface Reduction > Network Protection

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.1.2 *Configuration SmartScreen pour Microsoft Edge*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Active et configure Microsoft Defender SmartScreen dans Edge pour bloquer les sites web et téléchargements malveillants.

AUDIT :

- PowerShell: Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Edge' -Name SmartScreenEnabled
- Edge: edge://settings/privacy > Security

REMÉDIATION :

1. GPO: Computer Config > Administrative Templates > Microsoft Edge > SmartScreenEnabled = 1
2. GPO: SmartScreenPuaEnabled = 1
3. Intune: Administrative Templates > Microsoft Edge

VALEUR PAR DÉFAUT :

Enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.1.3 *SmartScreen pour applications et fichiers*

MITRE ATT&CK : T1204.002

DESCRIPTION :

Active SmartScreen pour vérifier la réputation des applications et fichiers téléchargés depuis Internet.

AUDIT :

- PowerShell: Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer' -Name SmartScreenEnabled
- Windows Security: App & browser control > Reputation-based protection

REMÉDIATION :

1. GPO: Computer Config > Administrative Templates > Windows Components > File Explorer > Configure Windows Defender SmartScreen = Enabled
2. Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer' -Name SmartScreenEnabled -Value 'RequireAdmin'

VALEUR PAR DÉFAUT :

Enabled (Warn)

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.1.4 *Protection contre les applications potentiellement indésirables (PUA)*

MITRE ATT&CK : T1566.001

DESCRIPTION :

Active la détection et le blocage des applications potentiellement indésirables (PUA) via SmartScreen et Defender.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property PUAProtection
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\PUAProtection

REMÉDIATION :

1. Set-MpPreference -PUAProtection Enabled
2. GPO: Configure detection for potentially unwanted applications = Enabled
3. SmartScreen PUA protection in browsers

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.1.5 *Filtrage DNS avec protection contre le DNS poisoning*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Configure la protection DNS pour bloquer les requêtes vers des domaines malveillants et prévenir le DNS poisoning.

AUDIT :

- PowerShell: Get-DnsClientServerAddress pour vérifier serveurs DNS sécurisés
- Network Protection integration avec DNS filtering

REMÉDIATION :

1. Configurer DNS sécurisés (1.1.1.1, 8.8.8.8, ou DNS d'entreprise filtrants)
2. Activer Network Protection pour filtrage complémentaire
3. Monitorer requêtes DNS suspectes

VALEUR PAR DÉFAUT :

ISP DNS

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.2.1 *Blocage des connexions sortantes suspectes*

MITRE ATT&CK : T1071

DESCRIPTION :

Configure le blocage automatique des connexions sortantes vers des IPs et domaines identifiés comme malveillants.

AUDIT :

- PowerShell: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows Defender/Operational'; ID=1125,1126}
- Network Protection block events

REMÉDIATION :

1. Activer Network Protection en mode Block
2. Surveiller Event ID 1125 (Network Protection block)
3. Whitelist des domaines légitimes si nécessaire

VALEUR PAR DÉFAUT :

No automatic blocking

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.2.2 *Protection contre l'exfiltration de données*

MITRE ATT&CK : T1041

DESCRIPTION :

Surveille et bloque les tentatives d'exfiltration de données vers des destinations non autorisées.

AUDIT :

- Network Protection: Surveillance des connexions suspectes
- Integration avec DLP policies

REMÉDIATION :

1. Configurer Network Protection pour surveillance avancée
2. Intégrer avec Microsoft 365 DLP
3. Alertes sur volumes de données inhabituels

VALEUR PAR DÉFAUT :

Basic monitoring

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.2.3 *Blocage des communications C&C (Command and Control)*

MITRE ATT&CK : T1071

DESCRIPTION :

Détecte et bloque les communications avec des serveurs de commande et contrôle de malwares.

AUDIT :

- Network Protection: Détection patterns C&C
- Threat Intelligence integration

REMÉDIATION :

1. Maintenir Network Protection à jour
2. Intégrer feeds de threat intelligence
3. Surveillance des connexions périodiques suspectes

VALEUR PAR DÉFAUT :

Included in Network Protection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.2.4 *Protection contre les attaques par déni de service*

MITRE ATT&CK : T1498

DESCRIPTION :

Configure la protection contre les attaques DoS locales et aide à la détection des participations à des DDoS.

AUDIT :

- Network Protection: Détection de patterns DoS
- Windows Firewall advanced rules

REMÉDIATION :

1. Configurer Windows Firewall avec règles anti-DoS
2. Surveillance des connexions anormalement élevées
3. Limitation des connexions sortantes par processus

VALEUR PAR DÉFAUT :

Basic Windows Firewall protection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.2.5 *Inspection SSL/TLS et détection de certificats malveillants*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Configure la validation des certificats SSL/TLS et la détection de certificats compromis ou malveillants.

AUDIT :

- Certificate Store: Validation des autorités de certification
- SmartScreen certificate validation

REMÉDIATION :

1. Maintenir à jour les listes de révocation
2. Configurer la validation stricte des certificats
3. Alertes sur certificats auto-signés suspects

VALEUR PAR DÉFAUT :

Standard certificate validation

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.3.1 *Intégration avec Windows Firewall*

MITRE ATT&CK : T1562.004

DESCRIPTION :

Intègre Network Protection avec Windows Firewall pour une défense en profondeur coordonnée.

AUDIT :

- PowerShell: Get-NetFirewallProfile | Select-Object -Property Name,Enabled,DefaultInboundAction,DefaultOutboundAction
- Windows Firewall coordination avec Network Protection

REMÉDIATION :

1. Maintenir Windows Firewall activé sur tous profils
2. Coordonner règles Firewall avec Network Protection
3. Logging centralisé des événements firewall

VALEUR PAR DÉFAUT :

Basic integration

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.3.2 *Configuration proxy et inspection du trafic*

MITRE ATT&CK : T1071

DESCRIPTION :

Configure l'inspection du trafic via proxy d'entreprise en coordination avec Network Protection.

AUDIT :

- PowerShell: netsh winhttp show proxy
- Proxy configuration et inspection SSL

REMÉDIATION :

1. Configurer proxy transparent si possible
2. Coordination avec Network Protection
3. Bypass appropriés pour services Microsoft

VALEUR PAR DÉFAUT :

Direct connection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.3.3 *Surveillance des connexions P2P et BitTorrent*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Détecte et contrôle les connexions peer-to-peer et BitTorrent pour prévenir les fuites de données et malwares.

AUDIT :

- Network monitoring: Détection protocols P2P
- Traffic analysis pour patterns BitTorrent

REMÉDIATION :

1. Configurer détection de trafic P2P
2. Bloquer ports BitTorrent standards
3. Alertes sur utilisation de protocoles P2P

VALEUR PAR DÉFAUT :

No specific P2P monitoring

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.3.4 *Protection contre les attaques de réseaux sans fil*

MITRE ATT&CK : T1200

DESCRIPTION :

Configure la protection contre les attaques via réseaux WiFi compromis et points d'accès malveillants.

AUDIT :

- Windows WiFi profiles et sécurité
- Network Protection sur connexions sans fil

REMÉDIATION :

1. Désactiver auto-connexion réseaux ouverts
2. Forcer WPA3 ou WPA2 minimum
3. Surveillance des connexions WiFi suspectes

VALEUR PAR DÉFAUT :

Basic WiFi security

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

7.3.5 *Reporting et métriques de protection réseau*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure le reporting détaillé des activités de protection réseau pour analyse et optimisation.

AUDIT :

- PowerShell: Get-WinEvent Network Protection events
- SIEM integration pour événements réseau

REMÉDIATION :

1. Configurer logging détaillé Network Protection
2. Dashboards de surveillance réseau
3. Métriques d'efficacité de blocage

VALEUR PAR DÉFAUT :

Basic event logging

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.0 — MICROSOFT DEFENDER FOR ENDPOINT

10.1.1 *Déploiement et onboarding MDE*

MITRE ATT&CK : N/A

DESCRIPTION :

Déploie et configure l'onboarding Microsoft Defender for Endpoint sur tous les endpoints de l'organisation.

AUDIT :

- PowerShell: Get-Service -Name Sense | Select-Object Name,Status,StartType
- Microsoft 365 Defender Portal: Device inventory et health status

REMÉDIATION :

1. Télécharger package d'onboarding depuis M365 Defender Portal
2. Déployer via GPO, Intune, ou SCCM
3. Vérifier connectivity: Test-NetConnection winatp-gw-cus.microsoft.com -Port 443

VALEUR PAR DÉFAUT :

Not deployed

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.1.2 *Configuration des politiques de détection EDR*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure les politiques de détection EDR (Endpoint Detection and Response) pour une surveillance comportementale avancée.

AUDIT :

- M365 Defender Portal: Settings > Endpoints > Advanced features
- EDR in block mode configuration

REMÉDIATION :

1. Activer EDR in block mode
2. Configurer les règles de détection personnalisées
3. Ajuster sensibilité selon environnement

VALEUR PAR DÉFAUT :

Standard detection rules

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.1.3 *Configuration de l'investigation automatisée (AIR)*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Active et configure l'investigation et réponse automatisées (AIR) pour réduire les temps de réponse aux incidents.

AUDIT :

- M365 Defender Portal: Settings > Endpoints > Advanced features > Automated investigation
- AIR automation level configuration

REMÉDIATION :

1. Configurer automation level: Semi-automated ou Full automated
2. Définir actions automatiques approuvées
3. Surveillance des actions AIR

VALEUR PAR DÉFAUT :

Semi-automated

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.1.4 *Configuration Advanced Hunting*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure et utilise Advanced Hunting pour la recherche proactive de menaces avec des requêtes KQL personnalisées.

AUDIT :

- M365 Defender Portal: Hunting > Advanced hunting
- Bibliothèque de requêtes personnalisées

REMÉDIATION :

1. Créer requêtes de chasse personnalisées
2. Programmer des requêtes récurrentes
3. Intégrer résultats avec workflows d'investigation

VALEUR PAR DÉFAUT :

Basic hunting capabilities

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.1.5 *Intégration avec Microsoft Sentinel*

MITRE ATT&CK : N/A

DESCRIPTION :

Intègre MDE avec Microsoft Sentinel pour une analyse SIEM centralisée et une corrélation de sécurité avancée.

AUDIT :

- Microsoft Sentinel: Data connectors > Microsoft 365 Defender
- Flux de données MDE vers Sentinel

REMÉDIATION :

1. Configurer connecteur MDE dans Sentinel
2. Créer règles de corrélation personnalisées
3. Dashboards unifiés de sécurité

VALEUR PAR DÉFAUT :

No SIEM integration

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.2.1 *Gestion des indicateurs de compromission (IOCs)*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure la gestion centralisée des IOCs pour bloquer automatiquement les indicateurs de menaces connus.

AUDIT :

- M365 Defender Portal: Settings > Endpoints > Indicators
- Liste des IOCs actifs et leurs actions

REMÉDIATION :

1. Importer feeds de threat intelligence
2. Créer IOCs personnalisés basés sur incidents
3. Configurer actions automatiques (Alert, Block, etc.)

VALEUR PAR DÉFAUT :

No custom IOCs

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.2.2 *Configuration des groupes d'appareils*

MITRE ATT&CK : N/A

DESCRIPTION :

Organise les endpoints en groupes logiques pour appliquer des politiques de sécurité différenciées.

AUDIT :

- M365 Defender Portal: Settings > Endpoints > Device groups
- Attribution des devices aux groupes appropriés

REMÉDIATION :

1. Créer groupes par criticité (Critical, Standard, Dev)
2. Définir politiques spécifiques par groupe
3. Attribution automatique basée sur tags

VALEUR PAR DÉFAUT :

Single default group

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.2.3 *Configuration des notifications et alertes*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure les notifications personnalisées pour les incidents critiques et les détections importantes.

AUDIT :

- M365 Defender Portal: Settings > Endpoints > Email notifications
- Règles de notification configurées

REMÉDIATION :

1. Configurer notifications email par criticité
2. Intégration avec outils de ticketing (ServiceNow, etc.)
3. Escalade automatique pour incidents critiques

VALEUR PAR DÉFAUT :

Basic email notifications

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.2.4 *Configuration du live response*

MITRE ATT&CK : T1105

DESCRIPTION :

Active et configure les capacités de réponse en temps réel pour investigation et remédiation à distance.

AUDIT :

- M365 Defender Portal: Settings > Endpoints > Advanced features > Live response
- Permissions et accès live response

REMÉDIATION :

1. Activer live response avec restrictions appropriées
2. Définir utilisateurs autorisés
3. Procédures d'utilisation documentées

VALEUR PAR DÉFAUT :

Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.2.5 *Configuration de l'analyse comportementale*

MITRE ATT&CK : T1055

DESCRIPTION :

Configure l'analyse comportementale avancée pour détecter les techniques d'évasion et les attaques sophistiquées.

AUDIT :

- MDE behavioral analysis settings
- Cloud-powered protection activation

REMÉDIATION :

1. Maintenir protection cloud activée
2. Configurer seuils de détection appropriés
3. Surveillance des faux positifs

VALEUR PAR DÉFAUT :

Standard behavioral analysis

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.3.1 *Threat and Vulnerability Management (TVM)*

MITRE ATT&CK : T1190

DESCRIPTION :

Active et configure TVM pour identifier et prioriser les vulnérabilités selon le risque réel d'exploitation.

AUDIT :

- M365 Defender Portal: Vulnerability management > Dashboard
- Inventaire des vulnérabilités et recommandations

REMÉDIATION :

1. Activer toutes les fonctionnalités TVM
2. Intégrer avec processus de patch management
3. Priorisation basée sur exploitabilité

VALEUR PAR DÉFAUT :

Basic vulnerability detection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.3.2 *Microsoft Secure Score intégration*

MITRE ATT&CK : N/A

DESCRIPTION :

Utilise Microsoft Secure Score pour mesurer et améliorer continuellement la posture de sécurité.

AUDIT :

- M365 Defender Portal: Secure Score dashboard
- Progression et actions recommandées

REMÉDIATION :

1. Révision mensuelle du Secure Score
2. Priorisation des améliorations high-impact
3. Suivi des métriques de progression

VALEUR PAR DÉFAUT :

Default scoring

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.3.3 *Configuration des simulations d'attaque*

MITRE ATT&CK : T1204

DESCRIPTION :

Configure et utilise les simulations d'attaque intégrées pour tester les défenses et former les utilisateurs.

AUDIT :

- M365 Defender Portal: Evaluation and tutorials
- Attack simulation training results

REMÉDIATION :

1. Programmer simulations régulières
2. Analyser résultats et améliorer formations
3. Mesurer amélioration awareness utilisateurs

VALEUR PAR DÉFAUT :

No regular simulations

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.3.4 *Intégration avec Microsoft 365 Defender*

MITRE ATT&CK : N/A

DESCRIPTION :

Intègre pleinement MDE avec l'écosystème M365 Defender pour une protection coordonnée cross-platform.

AUDIT :

- M365 Defender Portal: Unified incident management
- Cross-service correlation et investigation

REMÉDIATION :

1. Activer toutes les intégrations M365 Defender
2. Unified incident response workflows
3. Corrélation avec Defender for Office 365, Cloud Apps

VALEUR PAR DÉFAUT :

Basic integration

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.3.5 *Configuration du machine learning et IA*

MITRE ATT&CK : N/A

DESCRIPTION :

Optimise les capacités de machine learning et d'IA pour améliorer la précision de détection et réduire les faux positifs.

AUDIT :

- Cloud-powered protection status
- ML-based detection effectiveness metrics

REMÉDIATION :

1. Maintenir cloud connectivity pour ML updates
2. Feedback sur faux positifs pour améliorer ML
3. Surveillance performance des modèles IA

VALEUR PAR DÉFAUT :

Standard ML capabilities

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.4.1 *Collecte et analyse des données télémétrie*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure la collecte optimale de télémétrie pour alimenter les analyses de sécurité sans impacter les performances.

AUDIT :

- Telemetry collection settings
- Data retention policies

REMÉDIATION :

1. Configurer niveau de télémétrie approprié
2. Balance entre détection et privacy
3. Rétention données selon réglementations

VALEUR PAR DÉFAUT :

Standard telemetry

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.4.2 *Configuration des playbooks de réponse*

MITRE ATT&CK : N/A

DESCRIPTION :

Développe et configure des playbooks de réponse automatisée pour les types d'incidents courants.

AUDIT :

- Automated investigation playbooks
- Custom response actions

REMÉDIATION :

1. Créer playbooks pour incidents fréquents
2. Tester et ajuster réponses automatiques
3. Escalade vers humains si nécessaire

VALEUR PAR DÉFAUT :

Basic automated responses

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.4.3 *Gestion des permissions et RBAC*

MITRE ATT&CK : T1078

DESCRIPTION :

Configure un contrôle d'accès basé sur les rôles (RBAC) strict pour limiter l'accès aux fonctions MDE sensibles.

AUDIT :

- M365 Defender Portal: Permissions & roles
- Audit des accès et permissions accordées

REMÉDIATION :

1. Implémenter principe de moindre privilège
2. Rôles personnalisés selon besoins métier
3. Révision régulière des permissions

VALEUR PAR DÉFAUT :

Basic role assignments

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.4.4 *Monitoring et métriques de performance MDE*

MITRE ATT&CK : N/A

DESCRIPTION :

Surveille les performances et l'efficacité de MDE avec des métriques et KPIs appropriés.

AUDIT :

- Device health et connectivity status
- Performance impact metrics

REMÉDIATION :

1. Dashboard de santé des endpoints MDE
2. Métriques MTTR (Mean Time To Response)
3. KPIs d'efficacité de détection

VALEUR PAR DÉFAUT :

Basic health monitoring

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.4.5 *Processus de mise à jour et maintenance MDE*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Établit des processus de mise à jour et maintenance régulière pour maintenir l'efficacité de MDE.

AUDIT :

- Update compliance status
- Feature rollout management

REMÉDIATION :

1. Processus de validation des updates MDE
2. Ring deployment pour nouvelles fonctionnalités
3. Rollback procedures en cas de problème

VALEUR PAR DÉFAUT :

Automatic updates

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.5.1 *Formation et certification des équipes*

MITRE ATT&CK : N/A

DESCRIPTION :

Assure la formation continue des équipes de sécurité sur les capacités et l'utilisation optimale de MDE.

AUDIT :

- Training completion status
- Certification levels des analystes

REMÉDIATION :

1. Programme de formation MDE structuré
2. Certifications Microsoft Defender recommandées
3. Mise à jour compétences sur nouvelles fonctionnalités

VALEUR PAR DÉFAUT :

Basic product knowledge

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.5.2 *Documentation et procédures opérationnelles*

MITRE ATT&CK : N/A

DESCRIPTION :

Maintient une documentation complète des procédures d'utilisation et de maintenance de MDE.

AUDIT :

- Runbook completeness
- Procedure documentation currency

REMÉDIATION :

1. Runbooks détaillés pour toutes les opérations MDE
2. Procédures d'escalade documentées
3. Mise à jour régulière de la documentation

VALEUR PAR DÉFAUT :

Basic documentation

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.5.3 *Tests et validation des capacités MDE*

MITRE ATT&CK : N/A

DESCRIPTION :

Effectue des tests réguliers pour valider l'efficacité des détections et réponses MDE.

AUDIT :

- Purple team exercise results
- Detection validation testing

REMÉDIATION :

1. Tests mensuels de détection avec outils simulés
2. Purple team exercises trimestriels
3. Validation après chaque mise à jour majeure

VALEUR PAR DÉFAUT :

No systematic testing

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.5.4 *Intégration avec processus ITSM*

MITRE ATT&CK : N/A

DESCRIPTION :

Intègre les alertes et incidents MDE avec les processus ITSM existants pour une gestion unifiée.

AUDIT :

- ServiceNow/Remedy integration status
- Ticket automation et workflow

REMÉDIATION :

1. Connecteurs vers outils ITSM
2. Automatisation création tickets
3. Escalade basée sur criticité

VALEUR PAR DÉFAUT :

Manual ticket creation

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

10.5.5 *Métriques business et ROI de MDE*

MITRE ATT&CK : N/A

DESCRIPTION :

Mesure et reporte les métriques business et le retour sur investissement de MDE.

AUDIT :

- ROI calculation methodology
- Business impact metrics

REMÉDIATION :

1. Métriques de réduction des incidents
2. Calcul des coûts évités grâce à MDE
3. Rapports réguliers pour management

VALEUR PAR DÉFAUT :

No formal ROI measurement

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

8.0 — ACCÈS CONTRÔLÉ AUX DOSSIERS

8.1.1 *Activation de l'accès contrôlé aux dossiers*

MITRE ATT&CK : T1486

DESCRIPTION :
Active la protection des dossiers système et utilisateur contre les modifications par des applications non autorisées.

AUDIT :
- PowerShell: Get-MpPreference | Select-Object -Property EnableControlledFolderAccess
- Registre: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Controlled Folder Access\EnableControlledFolderAccess

REMÉDIATION :
1. Set-MpPreference -EnableControlledFolderAccess Enabled
2. GPO: Windows Defender Exploit Guard > Controlled folder access > Configure Controlled folder access = Enabled
3. Intune: Endpoint Security > Attack Surface Reduction > Controlled folder access

VALEUR PAR DÉFAUT :
Disabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

8.1.2 *Configuration des dossiers protégés*

MITRE ATT&CK : T1486

DESCRIPTION :
Configure la liste des dossiers protégés incluant les répertoires système critiques et dossiers utilisateur importants.

AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty ControlledFolderAccessProtectedFolders
- Liste des dossiers actuellement protégés

REMÉDIATION :
1. Add-MpPreference -ControlledFolderAccessProtectedFolders 'C:\Users*\Documents'
2. Add-MpPreference -ControlledFolderAccessProtectedFolders 'C:\Users*\Desktop'
3. Inclure dossiers métier critiques

VALEUR PAR DÉFAUT :
System default folders only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

8.1.3 *Applications autorisées pour accès contrôlé*

MITRE ATT&CK : T1486

DESCRIPTION :
Maintient une liste d'applications autorisées à modifier les dossiers protégés avec validation de sécurité.

AUDIT :
- PowerShell: Get-MpPreference | Select-Object -ExpandProperty ControlledFolderAccessAllowedApplications
- Audit des applications autorisées

REMÉDIATION :
1. Add-MpPreference -ControlledFolderAccessAllowedApplications 'C:\Program Files\TrustedApp\app.exe'
2. Validation signature numérique obligatoire
3. Documentation de chaque autorisation

VALEUR PAR DÉFAUT :
Windows built-in applications only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

8.2.1 *Protection des dossiers de sauvegarde*

MITRE ATT&CK : T1486

DESCRIPTION :

Étend la protection aux dossiers de sauvegarde locaux pour prévenir le chiffrement par ransomware.

AUDIT :

- Protection des répertoires de sauvegarde configurée
- Exclusions appropriées pour logiciels de sauvegarde légitimes

REMÉDIATION :

1. Add-MpPreference -ControlledFolderAccessProtectedFolders 'D:\Backups'
2. Autoriser uniquement logiciels de sauvegarde validés
3. Surveillance des accès aux dossiers de sauvegarde

VALEUR PAR DÉFAUT :

No backup folder protection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

8.2.2 *Surveillance des tentatives d'accès bloquées*

MITRE ATT&CK : T1486

DESCRIPTION :

Surveille et analyse les tentatives d'accès bloquées pour détecter les activités malveillantes.

AUDIT :

- PowerShell: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows Defender/Operational'; ID=1123}
- Event ID 1123 pour blocked access attempts

REMÉDIATION :

1. Configurer alertes sur tentatives d'accès bloquées
2. Corrélation avec autres événements de sécurité
3. Investigation des applications légitimes bloquées

VALEUR PAR DÉFAUT :

Basic event logging

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

9.0 — PROTECTION CONTRE L'EXPLOITATION

9.1.1 *Activation de l'ASLR système*

MITRE ATT&CK : T1055

DESCRIPTION :

Active l'Address Space Layout Randomization (ASLR) au niveau système pour compliquer les attaques d'exploitation mémoire.

AUDIT :

- PowerShell: Get-ProcessMitigation -System | Select-Object -Property ASLR
- Registre: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\MoveImages

REMÉDIATION :

1. Set-ProcessMitigation -System -Enable ForceRelocateImages
2. GPO: System Settings > Optional subsystems > Set to 1
3. bcdedit /set nx OptIn

VALEUR PAR DÉFAUT :

Enabled on modern systems

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

9.1.2 *Configuration du DEP (Data Execution Prevention)*

MITRE ATT&CK : T1055

DESCRIPTION :

Configure la prévention d'exécution des données (DEP) pour bloquer l'exécution de code dans les zones de données.

AUDIT :

- PowerShell: Get-ProcessMitigation -System | Select-Object -Property DEP
- bcdedit /enum | findstr nx

REMÉDIATION :

1. Set-ProcessMitigation -System -Enable DEP
2. bcdedit /set {current} nx AlwaysOn
3. Redémarrage requis pour application

VALEUR PAR DÉFAUT :

OptIn on modern systems

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

9.1.3 *Protection SEHOP (Structured Exception Handler Overwrite Protection)*

MITRE ATT&CK : T1055

DESCRIPTION :

Active SEHOP pour protéger contre l'exploitation des gestionnaires d'exception structurés.

AUDIT :

- PowerShell: Get-ProcessMitigation -System | Select-Object -Property SEHOP
- Registre: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\kernel\DisableExceptionChainValidation

REMÉDIATION :

1. Set-ProcessMitigation -System -Enable SEHOP
2. Registre: DisableExceptionChainValidation = 0
3. Test de compatibilité avec applications legacy

VALEUR PAR DÉFAUT :

Enabled on Windows 8+

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

9.2.1 *Mitigations par application*

MITRE ATT&CK : T1055

DESCRIPTION :

Configure des protections d'exploitation spécifiques par application pour les logiciels à haut risque.

AUDIT :

- PowerShell: Get-ProcessMitigation -Name 'chrome.exe','firefox.exe','winword.exe'
- Configuration des mitigations par process

REMÉDIATION :

1. Set-ProcessMitigation -Name 'chrome.exe' -Enable DEP,ASLR,SEHOP
2. Configuration via GPO Exploit Protection
3. Tests de compatibilité nécessaires

VALEUR PAR DÉFAUT :

System defaults only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

9.2.2 *Protection Control Flow Guard (CFG)*

MITRE ATT&CK : T1055

DESCRIPTION :

Active Control Flow Guard pour protéger contre les attaques de type ROP/JOP (Return/Jump Oriented Programming).

AUDIT :

- PowerShell: Get-ProcessMitigation -System | Select-Object -Property CFG
- Applications compilées avec support CFG

REMÉDIATION :

1. Set-ProcessMitigation -System -Enable CFG
2. Vérifier support CFG dans applications critiques
3. Mise à jour applications si nécessaire

VALEUR PAR DÉFAUT :

Application dependent

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

11.0 — PROTECTION CONTRE LA FALSIFICATION (TAMPER PROTECTION)

11.1.1 *Activation de la protection contre la falsification*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Active Tamper Protection pour empêcher la désactivation malveillante de Microsoft Defender et ses composants.

AUDIT :

- Microsoft 365 Security Center: Device security > Tamper protection
- PowerShell: Vérification via cloud management uniquement

REMÉDIATION :

1. Activer via Microsoft 365 Security Center
2. Déploiement requis de Microsoft Defender for Endpoint
3. Gestion centralisée cloud obligatoire

VALEUR PAR DÉFAUT :

Disabled (requires MDE)

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

11.1.2 *Protection des services Windows Defender*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Protège les services critiques de Windows Defender contre l'arrêt et la modification non autorisés.

AUDIT :

- PowerShell: Get-Service WinDefend,WdNisSvc,Sense | Select-Object Name,Status,StartType
- Protection des services par Tamper Protection

REMÉDIATION :

1. Tamper Protection protège automatiquement les services
2. Surveillance des tentatives d'arrêt de services
3. Alertes sur modifications de configuration service

VALEUR PAR DÉFAUT :

Protected when Tamper Protection enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

11.1.3 *Protection des clés de registre Defender*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Protège les clés de registre critiques de Microsoft Defender contre les modifications malveillantes.

AUDIT :

- Registre: Protection des clés HKLM\SOFTWARE\Microsoft\Windows Defender
- Tamper Protection impact sur modifications registre

REMÉDIATION :

1. Protection automatique via Tamper Protection
2. Monitoring des tentatives de modification registre
3. Gestion centralisée des changements de configuration

VALEUR PAR DÉFAUT :

Protected when Tamper Protection enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

11.2.1 *Gestion centralisée de Tamper Protection*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Assure la gestion centralisée de Tamper Protection via Microsoft 365 Security Center avec traçabilité.

AUDIT :

- M365 Security Center: Centralized tamper protection management
- Audit trail des changements de configuration

REMÉDIATION :

1. Configuration exclusivement via cloud management
2. Traçabilité de tous les changements
3. Approbation pour désactivation temporaire

VALEUR PAR DÉFAUT :

Cloud-managed when enabled

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

12.0 — INTÉGRATION INTUNE/MEM

12.1.1 *Déploiement des politiques Defender via Intune*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure et déploie les politiques Microsoft Defender via Intune pour une gestion centralisée et cohérente.

AUDIT :

- Intune Admin Center: Endpoint security > Antivirus policies
- Device compliance et policy deployment status

REMÉDIATION :

1. Créer profils de configuration Defender dans Intune
2. Déploiement par groupes d'appareils
3. Monitoring du compliance status

VALEUR PAR DÉFAUT :

No centralized policy management

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

12.1.2 *Configuration des règles de conformité*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Établit des règles de conformité Intune pour assurer que tous les appareils respectent les standards de sécurité Defender.

AUDIT :

- Intune: Device compliance policies
- Compliance reporting et non-compliant devices

REMÉDIATION :

1. Créer règles de conformité pour Defender activation
2. Actions automatiques pour non-compliance
3. Reporting régulier de conformité

VALEUR PAR DÉFAUT :

No compliance rules

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

12.1.3 *Accès conditionnel basé sur la sécurité Defender*

MITRE ATT&CK : T1078

DESCRIPTION :

Configure l'accès conditionnel Azure AD basé sur l'état de sécurité et conformité Defender des appareils.

AUDIT :

- Azure AD: Conditional Access policies
- Device risk et compliance integration

REMÉDIATION :

1. Politiques d'accès conditionnel basées sur device compliance
2. Blocage des appareils non conformes Defender
3. Intégration avec Microsoft Defender for Endpoint risk assessment

VALEUR PAR DÉFAUT :

No conditional access based on Defender

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

12.2.1 *Automatisation des déploiements Defender*

MITRE ATT&CK : N/A

DESCRIPTION :

Automatise le déploiement et la configuration de Microsoft Defender sur les nouveaux appareils via Intune Autopilot.

AUDIT :

- Intune: Autopilot deployment profiles
- Automatic Defender configuration during device enrollment

REMÉDIATION :

1. Intégrer Defender dans profils Autopilot
2. Configuration automatique des paramètres de sécurité
3. Validation post-déploiement automatisée

VALEUR PAR DÉFAUT :

Manual Defender configuration

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

12.2.2 *Rapports et dashboards Intune-Defender*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure des rapports et dashboards unifiés pour surveiller l'état Defender via Intune.

AUDIT :

- Intune: Reports > Endpoint security
- Defender health status across managed devices

REMÉDIATION :

1. Configurer rapports automatisés Defender
2. Dashboards executifs de sécurité
3. Alertes proactives sur problèmes de configuration

VALEUR PAR DÉFAUT :

Basic reporting only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

13.0 — QUARANTAINE ET RÉPONSE

13.1.1 *Configuration de la quarantaine automatique*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure la quarantaine automatique des fichiers malveillants détectés selon le niveau de menace.

AUDIT :

- PowerShell: Get-MpPreference | Select-Object -Property *DefaultAction*
- Actions automatiques par niveau de menace configurées

REMÉDIATION :

1. Set-MpPreference -LowThreatDefaultAction Quarantine
2. Set-MpPreference -ModerateThreatDefaultAction Quarantine
3. Set-MpPreference -HighThreatDefaultAction Quarantine

VALEUR PAR DÉFAUT :

Quarantine for most threats

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

13.1.2 *Gestion des faux positifs en quarantaine*

MITRE ATT&CK : N/A

DESCRIPTION :

Établit des procédures de gestion des faux positifs avec restauration sécurisée depuis la quarantaine.

AUDIT :

- Processus documenté de gestion des faux positifs
- PowerShell: Get-MpThreatDetection pour révision

REMÉDIATION :

1. Procédure de validation avant restauration
2. Soumission à Microsoft Security Intelligence
3. Mise à jour des exclusions si approprié

VALEUR PAR DÉFAUT :

Manual review required

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

14.0 — GESTION DES INDICATEURS DE COMPROMISSION (IOC)

14.1.1 *Intégration des feeds de threat intelligence*

MITRE ATT&CK : T1071

DESCRIPTION :

Intègre des feeds de threat intelligence externes pour enrichir la détection avec des IOCs actualisés.

AUDIT :

- M365 Defender: Settings > Endpoints > Indicators
- Feeds de threat intelligence configurés et actifs

REMÉDIATION :

1. Configurer feeds de threat intelligence réputés
2. Automatisation de l'import d'IOCs
3. Validation et scoring des IOCs

VALEUR PAR DÉFAUT :

Microsoft intelligence only

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

14.1.2 *Création d'IOCs personnalisés*

MITRE ATT&CK : T1071

DESCRIPTION :

Développe des IOCs personnalisés basés sur les incidents locaux et l'intelligence de menaces spécifique.

AUDIT :

- Processus de création d'IOCs personnalisés
- Validation et tests des IOCs créés

REMÉDIATION :

1. Processus formalisé de création d'IOCs
2. Validation technique des IOCs
3. Cycle de vie et expiration des IOCs

VALEUR PAR DÉFAUT :

No custom IOCs

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

15.0 — REPORTING ET DASHBOARDS

15.1.1 *Dashboards de supervision opérationnelle*

MITRE ATT&CK : N/A

DESCRIPTION :

Configure des dashboards temps réel pour la supervision opérationnelle de l'état et des performances Defender.

AUDIT :

- Dashboards configurés et accessibles aux équipes
- Métriques clés de santé système affichées

REMÉDIATION :

1. Power BI ou outils de reporting configurés
2. KPIs de santé Defender en temps réel
3. Alertes sur dégradation de service

VALEUR PAR DÉFAUT :

Basic Windows Security interface

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

15.1.2 *Rapports exécutifs mensuels*

MITRE ATT&CK : N/A

DESCRIPTION :

Génère des rapports exécutifs mensuels synthétisant l'efficacité et les incidents de sécurité Defender.

AUDIT :

- Template de rapport exécutif établi
- Automatisation de la génération mensuelle

REMÉDIATION :

1. Template standardisé de rapport mensuel
2. Automatisation via Power Automate ou scripts
3. Distribution automatique aux stakeholders

VALEUR PAR DÉFAUT :

No executive reporting

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

16.0 — SCÉNARIOS SERVEURS

16.1.1 *Optimisation Defender pour serveurs*

MITRE ATT&CK : N/A

DESCRIPTION :

Optimise la configuration Defender pour les serveurs en équilibrant sécurité et performance critique.

AUDIT :

- Configuration spécifique serveurs documentée
- Tests de performance avec Defender activé

REMÉDIATION :

1. Profils de configuration spécifiques serveurs
2. Exclusions optimisées pour workloads serveurs
3. Planification analyses pendant fenêtres maintenance

VALEUR PAR DÉFAUT :

Desktop configuration

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

16.1.2 *Defender pour serveurs critiques*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Configure une protection renforcée pour les serveurs critiques avec surveillance 24/7.

AUDIT :

- Serveurs critiques identifiés et protégés
- Monitoring et alerting renforcés configurés

REMÉDIATION :

1. Classification des serveurs par criticité
2. Protection renforcée pour Tier 0/1
3. Surveillance continue et alerting immédiat

VALEUR PAR DÉFAUT :

Standard server protection

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

17.0 — RÉPONSE AUX INCIDENTS

17.1.1 *Playbooks de réponse automatisée*

MITRE ATT&CK : N/A

DESCRIPTION :

Développe des playbooks de réponse automatisée utilisant les capacités Defender for Endpoint et AIR.

AUDIT :

- Playbooks documentés et testés
- Intégration avec systèmes de ticketing

REMÉDIATION :

1. Playbooks pour incidents types (malware, ransomware, etc.)
2. Automatisation via Microsoft Power Automate
3. Escalade automatique selon criticité

VALEUR PAR DÉFAUT :

Manual incident response

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

17.1.2 *Collecte forensique avec Live Response*

MITRE ATT&CK : T1005

DESCRIPTION :

Utilise les capacités Live Response de MDE pour la collecte forensique rapide lors d'incidents.

AUDIT :

- Procédures Live Response documentées
- Formation équipes sur outils forensiques MDE

REMÉDIATION :

1. Scripts Live Response standardisés
2. Formation équipes investigation
3. Procédures de préservation des preuves

VALEUR PAR DÉFAUT :

No standardized forensic procedures

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

18.0 — GOUVERNANCE ET CONFORMITÉ

18.1.1 *Politiques de gouvernance Defender*

MITRE ATT&CK : N/A

DESCRIPTION :

Établit des politiques de gouvernance formelles pour la gestion et l'évolution de Microsoft Defender.

AUDIT :

- Politiques de gouvernance documentées et approuvées
- Comité de gouvernance sécurité établi

REMÉDIATION :

1. Charte de gouvernance sécurité
2. Processus de prise de décision documenté
3. Révisions périodiques des politiques

VALEUR PAR DÉFAUT :

No formal governance

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

18.1.2 *Conformité réglementaire (RGPD, SOX, etc.)*

MITRE ATT&CK : N/A

DESCRIPTION :

Assure la conformité de l'implémentation Defender avec les réglementations applicables.

AUDIT :

- Mapping conformité réglementaire documenté
- Audits de conformité réguliers

REMÉDIATION :

1. Analyse des exigences réglementaires
2. Configuration selon requirements compliance
3. Documentation pour audits externes

VALEUR PAR DÉFAUT :

Basic compliance considerations

État : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

Commentaires : _____

Annexe : Checklist (196 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — PROTECTION EN TEMPS RÉEL					
1.1.1	Activation de la protection en temps réel	●	☐	☐	☐
1.1.2	Protection contre le téléchargement de fichiers	●	☐	☐	☐
1.1.3	Surveillance des fichiers et programmes	●	☐	☐	☐
1.1.4	Protection contre les scripts malveillants	●	☐	☐	☐
1.1.5	Protection de l'intégrité du comportement	●	☐	☐	☐
1.2.1	Limite d'utilisation CPU pour l'analyse temps réel	●	☐	☐	☐
1.2.2	Analyse des processus nouveaux et modifiés	●	☐	☐	☐
1.2.3	Configuration des extensions de fichiers surveillées	●	☐	☐	☐
1.2.4	Analyse des archives et fichiers compressés	●	☐	☐	☐
1.2.5	Surveillance des lecteurs réseau	●	☐	☐	☐
1.3.1	Analyse des emails et pièces jointes	●	☐	☐	☐
1.3.2	Protection contre les rootkits	●	☐	☐	☐
1.3.3	Analyse des fichiers de démarrage	●	☐	☐	☐
1.3.4	Protection de l'intégrité des processus système	●	☐	☐	☐
1.3.5	Surveillance des connexions réseau suspectes	●	☐	☐	☐
1.4.1	Gestion des faux positifs en temps réel	●	☐	☐	☐
1.4.2	Notification des détections en temps réel	●	☐	☐	☐
1.4.3	Intégration avec SIEM pour temps réel	●	☐	☐	☐
1.4.4	Performance de la protection temps réel	●	☐	☐	☐
1.4.5	Audit de la protection temps réel	●	☐	☐	☐
1.5.1	Redémarrage automatique après détection	●	☐	☐	☐
1.5.2	Protection des fichiers de configuration Defender	●	☐	☐	☐
1.5.3	Surveillance de l'état des services Defender	●	☐	☐	☐
1.5.4	Protection contre la désactivation par malware	●	☐	☐	☐
1.5.5	Récupération automatique après corruption	●	☐	☐	☐
Section 2 — PROTECTION CLOUD (MAPS)					
2.1.1	Activation du service MAPS	●	☐	☐	☐
2.1.2	Configuration du niveau de rapport MAPS	●	☐	☐	☐
2.1.3	Block at First Sight (BAFS)	●	☐	☐	☐
2.1.4	Soumission automatique d'échantillons	●	☐	☐	☐
2.1.5	Délai d'attente cloud étendu	●	☐	☐	☐
2.2.1	Niveau de blocage cloud	●	☐	☐	☐
2.2.2	Protection renforcée contre les PUA	●	☐	☐	☐
2.2.3	Analyse comportementale cloud	●	☐	☐	☐
2.2.4	Classification des menaces en temps réel	●	☐	☐	☐
2.2.5	Réputation des fichiers et URLs	●	☐	☐	☐
2.3.1	Connectivité cloud sécurisée	●	☐	☐	☐
2.3.2	Configuration proxy pour MAPS	●	☐	☐	☐
2.3.3	Gestion des certificats cloud	●	☐	☐	☐
2.3.4	Surveillance des performances cloud	●	☐	☐	☐
2.3.5	Fallback en cas d'indisponibilité cloud	●	☐	☐	☐
2.4.1	Audit des soumissions cloud	●	☐	☐	☐
2.4.2	Protection des données sensibles	●	☐	☐	☐
2.4.3	Conformité réglementaire cloud	●	☐	☐	☐
2.4.4	Intégration SIEM pour événements cloud	●	☐	☐	☐
2.4.5	Optimisation continue de la protection cloud	●	☐	☐	☐
Section 3 — MISES À JOUR DES DÉFINITIONS					
3.1.1	Fréquence des mises à jour automatiques	●	☐	☐	☐
3.1.2	Source primaire de mise à jour	●	☐	☐	☐
3.1.3	Sources de fallback configurées	●	☐	☐	☐
3.1.4	Mise à jour au démarrage du système	●	☐	☐	☐
3.1.5	Mise à jour différentielle optimisée	●	☐	☐	☐
3.2.1	Mise à jour du moteur antivirus	●	☐	☐	☐
3.2.2	Mise à jour de la plateforme Defender	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
3.2.3	Synchronisation des signatures réseau	●	☐	☐	☐
3.2.4	Validation de l'intégrité des signatures	●	☐	☐	☐
3.2.5	Rollback des signatures défaillantes	●	☐	☐	☐
3.3.1	Programmation des vérifications de mise à jour	●	☐	☐	☐
3.3.2	Gestion de la bande passante pour les mises à jour	●	☐	☐	☐
3.3.3	Notification des échecs de mise à jour	●	☐	☐	☐
3.3.4	Mise à jour prioritaire en cas de menace émergente	●	☐	☐	☐
3.3.5	Historique des versions de signatures	●	☐	☐	☐
3.4.1	Cache local des signatures	●	☐	☐	☐
3.4.2	Nettoyage automatique des anciennes signatures	●	☐	☐	☐
3.4.3	Surveillance de l'espace disque pour signatures	●	☐	☐	☐
3.4.4	Intégration avec la gestion des correctifs	●	☐	☐	☐
3.4.5	Métriques de performance des mises à jour	●	☐	☐	☐
Section 6 — RÈGLES DE RÉDUCTION DE SURFACE D'ATTAQUE (ASR)					
6.1.1	Règle ASR: Bloquer l'exécutable créé par commandes Office	●	☐	☐	☐
6.1.2	Règle ASR: Bloquer Office créant des processus enfants	●	☐	☐	☐
6.1.3	Règle ASR: Bloquer injection dans processus Office	●	☐	☐	☐
6.1.4	Règle ASR: Bloquer JavaScript/VBScript dans Office	●	☐	☐	☐
6.1.5	Règle ASR: Bloquer macros Office avec contenu Web	●	☐	☐	☐
6.2.1	Règle ASR: Bloquer exécutables suspects d'email	●	☐	☐	☐
6.2.2	Règle ASR: Bloquer vol de credentials Windows LSASS	●	☐	☐	☐
6.2.3	Règle ASR: Bloquer création processus via WMI	●	☐	☐	☐
6.2.4	Règle ASR: Bloquer processus non signés via USB	●	☐	☐	☐
6.2.5	Règle ASR: Bloquer scripts obfusqués suspects	●	☐	☐	☐
6.3.1	Règle ASR: Bloquer injection dans processus système	●	☐	☐	☐
6.3.2	Règle ASR: Bloquer téléchargements depuis navigateurs	●	☐	☐	☐
6.3.3	Règle ASR: Bloquer communications avec ransomware	●	☐	☐	☐
6.3.4	Règle ASR: Bloquer Adobe Reader processus enfants	●	☐	☐	☐
6.3.5	Règle ASR: Bloquer persistance via WMI	●	☐	☐	☐
6.4.1	Configuration mode Audit vs Block	●	☐	☐	☐
6.4.2	Exclusions ASR documentées et justifiées	●	☐	☐	☐
6.4.3	Surveillance des déclenchements ASR	●	☐	☐	☐
6.4.4	Intégration ASR avec SIEM	●	☐	☐	☐
6.4.5	Règle ASR: Bloquer exécution depuis dossiers système	●	☐	☐	☐
6.5.1	Performance et impact des règles ASR	●	☐	☐	☐
6.5.2	Tests de régression ASR	●	☐	☐	☐
6.5.3	Déploiement progressif des règles ASR	●	☐	☐	☐
6.5.4	Formation utilisateurs sur ASR	●	☐	☐	☐
6.5.5	Métriques et reporting ASR	●	☐	☐	☐
Section 4 — ANALYSES PROGRAMMÉES					
4.1.1	Configuration de l'analyse complète hebdomadaire	●	☐	☐	☐
4.1.2	Analyse rapide quotidienne	●	☐	☐	☐
4.1.3	Limitation CPU pour analyses programmées	●	☐	☐	☐
4.1.4	Analyse de rattrapage pour systèmes hors ligne	●	☐	☐	☐
4.1.5	Analyse uniquement si inactif	●	☐	☐	☐
4.2.1	Analyse des lecteurs réseau dans les scans programmés	●	☐	☐	☐
4.2.2	Analyse des archives dans les scans programmés	●	☐	☐	☐
4.2.3	Profondeur maximale d'analyse des archives	●	☐	☐	☐
4.2.4	Analyse des emails dans les scans programmés	●	☐	☐	☐
4.2.5	Analyse des supports amovibles	●	☐	☐	☐
4.3.1	Mise à jour des signatures avant analyse	●	☐	☐	☐
4.3.2	Timeout pour analyses longues	●	☐	☐	☐
4.3.3	Exclusions spécifiques aux analyses programmées	●	☐	☐	☐
4.3.4	Priorité des processus d'analyse	●	☐	☐	☐
4.3.5	Planification intelligente des analyses	●	☐	☐	☐
4.4.1	Reporting des résultats d'analyses programmées	●	☐	☐	☐
4.4.2	Surveillance des échecs d'analyses programmées	●	☐	☐	☐
4.4.3	Métriques de performance des analyses	●	☐	☐	☐
4.4.4	Intégration avec outils de monitoring	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
4.4.5	Archivage des historiques d'analyse	●	☐	☐	☐
Section 5 — GESTION DES EXCLUSIONS					
5.1.1	Inventaire documenté des exclusions	●	☐	☐	☐
5.1.2	Exclusions de chemins avec wildcards sécurisés	●	☐	☐	☐
5.1.3	Exclusions d'extensions strictement limitées	●	☐	☐	☐
5.1.4	Exclusions de processus avec validation sécurité	●	☐	☐	☐
5.1.5	Exclusions temporaires avec échéance	●	☐	☐	☐
5.2.1	Exclusions pour applications métier critiques	●	☐	☐	☐
5.2.2	Exclusions pour bases de données	●	☐	☐	☐
5.2.3	Exclusions pour systèmes de sauvegarde	●	☐	☐	☐
5.2.4	Exclusions pour outils de développement	●	☐	☐	☐
5.2.5	Exclusions pour services système critiques	●	☐	☐	☐
5.3.1	Processus d'approbation des exclusions	●	☐	☐	☐
5.3.2	Tests d'impact avant exclusion	●	☐	☐	☐
5.3.3	Surveillance renforcée des zones exclues	●	☐	☐	☐
5.3.4	Révision périodique des exclusions	●	☐	☐	☐
5.3.5	Métriques et reporting des exclusions	●	☐	☐	☐
Section 7 — PROTECTION RÉSEAU					
7.1.1	Activation de la protection réseau	●	☐	☐	☐
7.1.2	Configuration SmartScreen pour Microsoft Edge	●	☐	☐	☐
7.1.3	SmartScreen pour applications et fichiers	●	☐	☐	☐
7.1.4	Protection contre les applications potentiellement indésirables (PUA)	●	☐	☐	☐
7.1.5	Filtrage DNS avec protection contre le DNS poisoning	●	☐	☐	☐
7.2.1	Blocage des connexions sortantes suspectes	●	☐	☐	☐
7.2.2	Protection contre l'exfiltration de données	●	☐	☐	☐
7.2.3	Blocage des communications C&C (Command and Control)	●	☐	☐	☐
7.2.4	Protection contre les attaques par déni de service	●	☐	☐	☐
7.2.5	Inspection SSL/TLS et détection de certificats malveillants	●	☐	☐	☐
7.3.1	Intégration avec Windows Firewall	●	☐	☐	☐
7.3.2	Configuration proxy et inspection du trafic	●	☐	☐	☐
7.3.3	Surveillance des connexions P2P et BitTorrent	●	☐	☐	☐
7.3.4	Protection contre les attaques de réseaux sans fil	●	☐	☐	☐
7.3.5	Reporting et métriques de protection réseau	●	☐	☐	☐
Section 10 — MICROSOFT DEFENDER FOR ENDPOINT					
10.1.1	Déploiement et onboarding MDE	●	☐	☐	☐
10.1.2	Configuration des politiques de détection EDR	●	☐	☐	☐
10.1.3	Configuration de l'investigation automatisée (AIR)	●	☐	☐	☐
10.1.4	Configuration Advanced Hunting	●	☐	☐	☐
10.1.5	Intégration avec Microsoft Sentinel	●	☐	☐	☐
10.2.1	Gestion des indicateurs de compromission (IOCs)	●	☐	☐	☐
10.2.2	Configuration des groupes d'appareils	●	☐	☐	☐
10.2.3	Configuration des notifications et alertes	●	☐	☐	☐
10.2.4	Configuration du live response	●	☐	☐	☐
10.2.5	Configuration de l'analyse comportementale	●	☐	☐	☐
10.3.1	Threat and Vulnerability Management (TVM)	●	☐	☐	☐
10.3.2	Microsoft Secure Score intégration	●	☐	☐	☐
10.3.3	Configuration des simulations d'attaque	●	☐	☐	☐
10.3.4	Intégration avec Microsoft 365 Defender	●	☐	☐	☐
10.3.5	Configuration du machine learning et IA	●	☐	☐	☐
10.4.1	Collecte et analyse des données télémétrie	●	☐	☐	☐
10.4.2	Configuration des playbooks de réponse	●	☐	☐	☐
10.4.3	Gestion des permissions et RBAC	●	☐	☐	☐
10.4.4	Monitoring et métriques de performance MDE	●	☐	☐	☐
10.4.5	Processus de mise à jour et maintenance MDE	●	☐	☐	☐
10.5.1	Formation et certification des équipes	●	☐	☐	☐
10.5.2	Documentation et procédures opérationnelles	●	☐	☐	☐
10.5.3	Tests et validation des capacités MDE	●	☐	☐	☐
10.5.4	Intégration avec processus ITSM	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
10.5.5	Métriques business et ROI de MDE	●	☐	☐	☐
Section 8 — ACCÈS CONTRÔLÉ AUX DOSSIERS					
8.1.1	Activation de l'accès contrôlé aux dossiers	●	☐	☐	☐
8.1.2	Configuration des dossiers protégés	●	☐	☐	☐
8.1.3	Applications autorisées pour accès contrôlé	●	☐	☐	☐
8.2.1	Protection des dossiers de sauvegarde	●	☐	☐	☐
8.2.2	Surveillance des tentatives d'accès bloquées	●	☐	☐	☐
Section 9 — PROTECTION CONTRE L'EXPLOITATION					
9.1.1	Activation de l'ASLR système	●	☐	☐	☐
9.1.2	Configuration du DEP (Data Execution Prevention)	●	☐	☐	☐
9.1.3	Protection SEHOP (Structured Exception Handler Overwrite Protection)	●	☐	☐	☐
9.2.1	Mitigations par application	●	☐	☐	☐
9.2.2	Protection Control Flow Guard (CFG)	●	☐	☐	☐
Section 11 — PROTECTION CONTRE LA FALSIFICATION (TAMPER PROTECTION)					
11.1.1	Activation de la protection contre la falsification	●	☐	☐	☐
11.1.2	Protection des services Windows Defender	●	☐	☐	☐
11.1.3	Protection des clés de registre Defender	●	☐	☐	☐
11.2.1	Gestion centralisée de Tamper Protection	●	☐	☐	☐
Section 12 — INTÉGRATION INTUNE/MEM					
12.1.1	Déploiement des politiques Defender via Intune	●	☐	☐	☐
12.1.2	Configuration des règles de conformité	●	☐	☐	☐
12.1.3	Accès conditionnel basé sur la sécurité Defender	●	☐	☐	☐
12.2.1	Automatisation des déploiements Defender	●	☐	☐	☐
12.2.2	Rapports et dashboards Intune-Defender	●	☐	☐	☐
Section 13 — QUARANTAINE ET RÉPONSE					
13.1.1	Configuration de la quarantaine automatique	●	☐	☐	☐
13.1.2	Gestion des faux positifs en quarantaine	●	☐	☐	☐
Section 14 — GESTION DES INDICATEURS DE COMPROMISSION (IOC)					
14.1.1	Intégration des feeds de threat intelligence	●	☐	☐	☐
14.1.2	Création d'IOCs personnalisés	●	☐	☐	☐
Section 15 — REPORTING ET DASHBOARDS					
15.1.1	Dashboards de supervision opérationnelle	●	☐	☐	☐
15.1.2	Rapports exécutifs mensuels	●	☐	☐	☐
Section 16 — SCÉNARIOS SERVEURS					
16.1.1	Optimisation Defender pour serveurs	●	☐	☐	☐
16.1.2	Defender pour serveurs critiques	●	☐	☐	☐
Section 17 — RÉPONSE AUX INCIDENTS					
17.1.1	Playbooks de réponse automatisée	●	☐	☐	☐
17.1.2	Collecte forensique avec Live Response	●	☐	☐	☐
Section 18 — GOUVERNANCE ET CONFORMITÉ					
18.1.1	Politiques de gouvernance Defender	●	☐	☐	☐
18.1.2	Conformité réglementaire (RGPD, SOX, etc.)	●	☐	☐	☐