ROMY

רומי דר | יועץ לפיתוח ארגוני

רשימת תיוג להקשחת Windows

תחנות עבודה Windows 11 ו-Windows 10 ושרתי Windows Server

גרסה 1.1 | עודכן ב-25 בנובמבר 2026

חשוב: לבדוק בסביבת בדיקה לפני סביבת הייצור

זו רשימה גנרית. היא אינה מותאמת לארגון מסוים, ליישומים שלו או לתשתית שלו.

יש לבדוק כל הגדרה קודם בסביבת בדיקה או בקבוצת פיילוט מייצגת, ורק אחר כך להעביר אותה לסביבת הייצור.

יש לבצע התאמות לפי הצורך. חלק מההגדרות עלולות לפגוע ביישומים ישנים, בהתקני NAS, במדפסות, בכלי ניהול ובחיבורים מרחוק.

לפני כל שינוי יש לבצע גיבוי ולהכין דרך לחזרה לאחור.

איך משתמשים ברשימה

- **עמודות W11, W10 ושרת:** V פירושו שהבדיקה רלוונטית, הסימן - פירושו שאינה רלוונטית, ו״לפי צורך״ פירושו שהיא תלויה בתפקיד המכשיר.
- **עמודת האימות:** פקודת PowerShell או בדיקה ידנית שמאמתת את המצב. מריצים את הפקודות בחלון PowerShell עם הרשאות מנהל. הפקודות קוראות מידע בלבד ואינן משנות הגדרות.
- **עמודת מצב:** V תקין, X לא תקין, ל״ח לא חל, ח חריגה מאושרת, ? לא נבדק או שגיאה. מצב שלא נבדק אינו תוצאה תקינה.
- **עמודת ראיה:** הפניה לראיה: צילום מסך, קובץ פלט, דוח או רשומה. רושמים בראש הרשימה את שם הבודק, התאריך והמכשירים שנבדקו.
- **פקודת אימות אחת לא תמיד מספיקה:** כשהבדיקה כוללת כמה רכיבים, כמו הגבלת משתמשים ומקורות, יש לבדוק כל רכיב ולתעד ראיה לכל אחד.
- **מקור:** הרשימה מבוססת על קווי הבסיס של Microsoft, על CIS Benchmarks ועל התיעוד של Microsoft Learn, נכון לנובמבר 2026. ברירות מחדל ותאריכי תמיכה משתנים, ולכן יש לבדוק מול המקור העדכני.

פרטי הבדיקה

שם הבודק	
תאריך	
מכשירים או קבוצה שנבדקו	
גרסת הרשימה	1.1

1 לפני שמתחילים

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
קיים מלאי עדכני של כל התחנות והשרתים: מערכת הפעלה, גרסה, מהדורה, ערוץ שירות, תאריך סיום תמיכה, תפקיד ובעלים	V	V	V	`Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' | Select-Object EditionID, DisplayVersion, CurrentBuild`		
הוגדרה סביבת בדיקה או קבוצת פיילוט מייצגת, וכל שינוי נבדק בה לפני הפצה לסביבת הייצור	V	V	V	תיעוד הפיילוט ותוצאותיו		
קיים גיבוי של הנתונים והמערכת, ונבדק שאפשר לשחזר ממנו	V	V	V	דוח בדיקת שחזור		
הגדרות האבטחה הקיימות יוצאו לקובץ לפני השינוי. הייצוא אינו מחליף גיבוי	V	V	V	`secedit /export /cfg C:\Hardening\before.inf`		
כל שינוי עובר ניהול שינויים ומתועד, כולל דרך חזרה לאחור	V	V	V	רשומת שינוי		
נפתחה רשימת חריגות: הגדרה שלא הוחלה, נימוק, בקרה מפצה, אחראי ותאריך בדיקה	V	V	V	רשימת חריגות		
קיים נוהל גישה ושחזור בחירום: מי מורשה, איך מגיעים לקונסולה, איפה מפתחות השחזור, ומה עושים כששינוי הקשחה חוסם גישה או ניהול	V	V	V	נוהל מאושר ותרגול		

2 עדכונים וגרסאות נתמכות

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
הגרסה והמהדורה נתמכות. התמיכה תלויה במהדורה: Windows 11 24H2 Home ו-Pro יצאו מתמיכה ב-13.10.2026, ו-Enterprise ו-Education נתמכות עד 12.10.2027	V	-	V	השוואת המלאי לטבלת הגרסאות הנתמכות של Microsoft		
Windows 10 22H2 מכוסה ב-ESU בתוקף לשנה הנוכחית. למהדורות LTSC ו-IoT יש מחזור תמיכה נפרד	-	V	-	`slmgr /dlv`		
עדכוני האבטחה החודשיים מותקנים בתוך היעד הארגוני, למשל 14 יום	V	V	V	`Get-HotFix | Sort-Object InstalledOn -Descending`		
תוכנות צד שלישי מעודכנות: דפדפנים, קוראי PDF, כלי דחיסה וכלי שיחות	V	V	V	`winget upgrade`		
קושחה, BIOS או UEFI ומנהלי התקנים מעודכנים לפי פרסומי היצרן	V	V	V	כלי העדכון של היצרן		
עדכון אישורי Secure Boot של 2023 הושלם: UEFICA2023Status שווה Updated ו-UEFICA2023Error שווה 0. אישורי 2011 פגו במהלך 2026	V	V	V	`Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing' | Select-Object UEFICA2023Status, UEFICA2023Error`		

3 קו בסיס

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
הוחל קו הבסיס של Microsoft לגרסה המתאימה, דרך GPO, Intune או OSConfig ב-Windows Server 2025	V	V	V	PolicyAnalyzer, דוח Intune או OSConfig		
ההגדרות הושוו ל- CIS Benchmark ברמה Level 1, והפערים טופלו או נרשמו כחריגות	V	V	V	דוח השוואה		
חריגות מוחלות ב-GPO נפרד, בלי לערוך את אובייקט קו הבסיס עצמו	V	V	V	`gpresult /h C:\Hardening\gp.html`		

4 חשבונות והרשאות

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
משתמשים רגילים עובדים ללא הרשאת מנהל מקומי	V	V	V	`Get-LocalGroupMember -Group Administrators`		
לאנשי IT יש חשבון ניהול נפרד שאינו משמש לדואר ולגלישה	V	V	V	סקירת חשבונות		
חברות בקבוצות מיוחסות מצומצמת ונסקרת פעם ברבעון	V	V	V	`Get-ADGroupMember 'Domain Admins' -Recursive`		
Windows LAPS מנהל סיסמה ייחודית למנהל המקומי בכל מכשיר. ב-Windows Server 2016 נדרש Legacy LAPS	V	V	V	`Get-LapsADPassword -Identity <PC>`		
הוגדר מי רשאי לפענח סיסמאות LAPS מוצפנות, ונבדק שאיש תמיכה מורשה מצליח לאחזר ומשתמש לא מורשה נכשל. הצפנה ב-AD דורשת רמת תפקוד תחום 2016 ומעלה	-	-	V	ADPasswordEncryptionPrincipal וניסיון אחזור		
חשבון Guest מושבת	V	V	V	`Get-LocalUser -Name Guest`		
חשבונות מנהל מקומיים חסומים לכניסה מהרשת ול-RDP, דרך הקבוצה Local account and member of Administrators group	V	V	V	User Rights Assignment ב-GPO		
מדיניות סיסמאות ונעילת חשבון הוגדרו לפי קו הבסיס	V	V	V	`net accounts`		
UAC מופעל	V	V	V	`(Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).EnableLUA`		
מצב Administrator protection נבדק ותועד. הוא מופעל כברירת מחדל מעדכון אוקטובר 2026, ו-Microsoft ממליצה שלא להפעילו במכשירים המנוהלים ב-LAPS, במכשירים שנדרש בהם Hyper-V ובאפליקציות שמשתפות קבצים בין פרופילים	V	-	-	Windows Security, Account protection ותיעוד ההחלטה		
אימות רב-שלבי לכל גישה מרחוק ולכל חשבון ניהול	V	V	V	הגדרות ספק הזהות		
חשבונות מנהלי התחום חברים בקבוצה Protected Users	-	-	V	`Get-ADGroupMember 'Protected Users'`		

5 הגנה על פרטי הזדהות

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
Credential Guard פעיל. נתמך במהדורות Enterprise ו-Education ובשרתים, ולא בבקרי תחום	V	V	V	(Get-CimInstance Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning		
הגנת LSA פעילה. מפעילים קודם במצב ביקורת	V	V	V	(Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa).RunAsPPL		
WDigest אינו שומר סיסמאות בזיכרון: UseLogonCredential שווה 0 או לא מוגדר	V	V	V	Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest		
LAN Manager authentication level מוגדר ל-NTLMv2 בלבד, ערך 5	V	V	V	(Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa).LmCompatibilityLevel		
השימוש ב-NTLM נבדק ביומני הביקורת, ותוכנית לצמצום שלו קיימת	V	V	V	יומני NTLM ב-Event Viewer		

6 רשת ופרוטוקולים

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
חומת האש פעילה בכל הפרופילים, תעבורה נכנסת חסומה כברירת מחדל ורישום חבילות שנחסמו מופעל. נבדקה המדיניות שחלה בפועל, כולל האם כללים מקומיים מתמזגים	V	V	V	Get-NetFirewallProfile -PolicyStore ActiveStore | Format-Table Name, Enabled, DefaultInboundAction, LogBlocked, AllowLocalFirewallRules		
רכיבי SMBv1 מוסרים, בצד הלקוח ובצד השרת	V	V	V	Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol		
חתימת SMB נדרשת בצד השרת ובצד הלקוח	V	V	V	(Get-SmbServerConfiguration).RequireSecuritySignature ; (Get-SmbClientConfiguration).RequireSecuritySignature		
התחברות SMB כאורח חסומה	V	V	V	(Get-SmbClientConfiguration).EnableInsecureGuestLogons		
LLMNR מבוטל	V	V	V	(Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient').EnableMulticast		
NetBIOS over TCP/IP מבוטל, ערך 2	V	V	V	Get-CimInstance Win32_NetworkAdapterConfiguration -Filter 'IPEnabled=TRUE' | Select-Object Description, TcpipNetbiosOptions		
RDP מושבת במכשירים שאינם צריכים אותו, ואינו חשוף לאינטרנט	V	V	V	(Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server').fDenyTSConnections		
ב-RDP נדרש NLA: UserAuthentication שווה 1	V	V	V	(Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp').UserAuthentication		
הגישה ב-RDP מוגבלת לקבוצה ייעודית ולכתובות מקור מוגדרות, ונבדק חיבור ממקור מורשה וממקור שאמור להיחסם	V	V	V	Get-LocalGroupMember 'Remote Desktop Users' ; Get-NetFirewallRule -DisplayGroup 'Remote Desktop' | Get-NetFirewallAddressFilter		
WinRM מוגבל לרשת הניהול, ללא Basic authentication וללא תעבורה לא מוצפנת	לפי צורך	לפי צורך	V	Get-Item WSMan:\localhost\Service\Auth\Basic ; Get-Item WSMan:\localhost\Service\AllowUnencrypted ; Get-ChildItem WSMan:\localhost\Listener		

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
OpenSSH Server מותקן רק כשנדרש, עם הזדהות במפתחות בלבד	לפי צורך	לפי צורך	לפי צורך	`C:\ProgramData\ssh\sshd_config`		
TLS 1.0 ו-TLS 1.1 מבוטלים	V	V	V	`HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`		

7 הגנה מפני נוזקות ובקרת יישומים

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
Microsoft Defender או מוצר חלופי פעיל, עם הגנה בזמן אמת וחתימות עדכניות. ב- Windows Server מוצר חלופי אינו מעביר את Defender למצב פסיבי אוטומטית. עם מוצר חלופי, הראיות נאספות מהמוצר עצמו	V	V	V	`Get-MpComputerStatus | Select-Object AMRunningMode, RealTimeProtectionEnabled, AntivirusSignatureLastUpdated`		
Tamper Protection מופעל	V	V	V	`(Get-MpComputerStatus).IsTamperProtected`		
הגנת ענן, חסימת PUA ו-Network Protection מופעלות	V	V	V	`Get-MpPreference | Select-Object MAPSReporting, PUAProtection, EnableNetworkProtection`		
שלושת כללי ASR של ההגנה הבסיסית במצב חסימה. שאר הכללים עוברים מביקורת לחסימה אחרי בדיקה. כללי ASR דורשים ש-Defender יהיה מנוע ההגנה הפעיל	V	V	V	`Get-MpPreference | Select-Object AttackSurfaceReductionRules_Ids, AttackSurfaceReductionRules_Actions`		
נבחנה הפעלת Controlled Folder Access	V	V	לפי צורך	`(Get-MpPreference).EnableControlledFolderAccess`		
בקרת יישומים פעילה: App Control for Business או AppLocker, ולפחות חסימת הרצה מתיקיות המשתמש. האכיפה נבדקת לכל טכנולוגיה	V	V	V	`Get-AppLockerPolicy -Effective ; CiTool.exe -lp`		
פקודות מאקרו בקבצי Office שהגיעו מהאינטרנט חסומות	V	V	לפי צורך	קו הבסיס של Microsoft 365 Apps		
הוחל קו הבסיס של Microsoft Edge, ו-SmartScreen מופעל	V	V	לפי צורך	`edge://policy`		

8 הצפנה וחומרה

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
BitLocker מצפין את כונן מערכת ההפעלה. במחשבים ניידים המגן הוא TPM יחד עם PIN, ולא TPM בלבד	V	V	לפי צורך	`(Get-BitLockerVolume -MountPoint C:).KeyProtector | Select-Object KeyProtectorType`		
מפתחות השחזור של BitLocker נשמרים ב-Active Directory או ב-Microsoft Entra ID, ונבדק שאיש תמיכה מורשה מצליח לאחזר מפתח בבדיקה מבוקרת	V	V	לפי צורך	בדיקה ב-AD או ב-Entra וניסיון אחזור מבוקר		
Secure Boot מופעל	V	V	V	`Confirm-SecureBootUEFI`		
TPM 2.0 קיים ומוכן	V	V	V	`Get-Tpm`		
Memory integrity, או HVCI, מופעל	V	V	V	`(Get-CimInstance Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning`		

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
הכתיבה לכוננים נשלפים חסומה או מבוקרת, ונבדקה בניסיון כתיבה	V	V	V	(Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}').Deny_Write		
AutoPlay מבוטל	V	V	V	(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer').NoDriveTypeAutoRun		
סיסמת קושחה מוגדרת, והאתחול מהתקנים חיצוניים חסום	V	V	V	הגדרות BIOS או UEFI		

9 מערכת ההפעלה ושירותים

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
PowerShell 2.0 מוסר. ב-Windows 11 24H2 ומעלה וב-Windows Server 2025 הוא כבר הוסר	V	V	V	Get-WindowsOptionalFeature -Online | Where-Object FeatureName -like '*PowerShellV2*'		
Script Block Logging מופעל ב-Windows PowerShell, וגם ב-PowerShell 7 אם הוא מותקן	V	V	V	(Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging').EnableScriptBlockLogging ; (Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\PowerShellCore\ScriptBlockLogging').EnableScriptBlockLogging		
Print Spooler מושבת בכל שרת שאינו שרת הדפסה, ובכל בקרי התחום	לפי צורך	לפי צורך	V	Get-Service Spooler | Select-Object Status, StartType		
הוסרו רכיבים, תפקידים ושירותים שאינם בשימוש	V	V	V	Get-WindowsOptionalFeature -Online | Where-Object State -eq 'Enabled'		
המסך ננעל אחרי 15 דקות של חוסר פעילות לכל היותר	V	V	V	(Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).InactivityTimeoutSecs		
השעון מסונכרן מול מקור זמן אמין	V	V	V	w32tm /query /status		

10 רישום וניטור

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
מדיניות ביקורת מתקדמת הוגדרה לפי המלצות Microsoft לתפקיד המכשיר: תחנת עבודה, שרת חבר או בקר תחום. נבדק שהאירועים הצפויים נוצרים בפועל	V	V	V	auditpol /get /category:*		
שורת הפקודה נרשמת באירועי יצירת תהליך, אירוע 4688	V	V	V	(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit').ProcessCreationIncludeCmdLine_Enabled		
גודל יומן Security הוא 196608 KB לפחות	V	V	V	wevtutil gl Security		
Sysmon מותקן עם קובץ הגדרות. ב-Windows 11 וב-Windows Server 2025 כרכיב מובנה, ובשאר כגרסה עצמאית	V	V	V	Get-Service *sysmon*		
היומנים מועברים לשרת מרכזי, ב-WEF או ב-SIEM. נבדק שמכל מכשיר מגיע אירוע עדכני, ושאירוע בדיקה מגיע ליעדו	V	V	V	השוואת המלאי למכשירים המדווחים ואירוע בדיקה		

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
קיימת התראה על מכשיר או מקור שהפסיק לדווח, על שירות איסוף שנעצר ועל יומן שמתמלא	V	V	V	כללי ההתראה ב-SIEM ואירוע בדיקה		
הוגדרו התראות לאירועים קריטיים, ובהם 1102, 4720, 4732, 4740, 7045 ו-4104. לכל התראה יש אחראי, זמן תגובה ותנאי הסלמה	V	V	V	כללי ההתראה ב-SIEM ונוהל הטיפול		

11 שרתים ובקרי תחום

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
התקנה מינימלית, Server Core כשאפשר, ורק התפקידים הנדרשים	-	-	V	`Get-WindowsFeature | Where-Object Installed`		
הניהול מתבצע מתחנת ניהול ייעודית, ואין גלישה או שימוש בדואר מהשרת	-	-	V	מדיניות ובדיקה ידנית		
מודל שכבות: חשבונות שמנהלים בקרי תחום אינם מתחברים לשרתים ולתחנות אחרים	-	-	V	User Rights Assignment ב-GPO		
בבקרי תחום נאכפות חתימת LDAP ו-LDAP Channel Binding	-	-	V	`Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters | Select-Object LDAPServerIntegrity, LdapEnforceChannelBinding`		
הסיסמה של חשבון krbtgt מוחלפת פעמיים, אחרי בדיקת תקינות השכפול, עם המתנה של 10 שעות לפחות בין ההחלפות, או יותר אם תוקף כרטיסי Kerberos שונה. תדירות מומלצת: פעם בשנה, לפי מדיניות הארגון	-	-	V	`Get-ADUser krbtgt -Properties PasswordLastSet ; repadmin /replsummary`		
Active Directory Recycle Bin מופעל	-	-	V	`Get-ADOptionalFeature -Filter 'Name -like "Recycle Bin Feature"' | Select-Object EnabledScopes`		
ב-Windows Server 2025 חתימת SMB נדרשת גם בחיבורים נכנסים, ולא רק ביוצאים	-	-	V	`(Get-SmbServerConfiguration).RequireSecuritySignature`		
גיבוי לפי כלל 3-2-1, עם עותק מנותק או בלתי ניתן לשינוי, ובדיקת שחזור פעם ברבעון	-	-	V	דוח בדיקת שחזור		
שרתי Windows Server 2016 מוחלפים עד סוף התמיכה ב-12.1.2027, או מכוסים ב-ESU	-	-	V	`Get-ComputerInfo | Select-Object OsName`		

12 תחזוקה שוטפת

בדיקה	W11	W10	שרת	אימות	מצב	ראיה
חודשי: עדכוני אבטחה, דוחות עמידה וסקירה תקופתית של ההתראות שטופלו	V	V	V	יומן תחזוקה		
רבעוני: סקירת קבוצות מיוחסות, החרגות ב-Defender ובחומת האש, ובדיקת שחזור	V	V	V	יומן תחזוקה		
עם כל גרסת Windows חדשה: קו בסיס חדש, השוואה, פיילוט והפצה	V	V	V	PolicyAnalyzer		
שנתי: סקירה מלאה מול רשימה זו ותרגיל תגובה לאירוע	V	V	V	דוח סקירה		

הגבלת אחריות

הרשימה מוגשת כפי שהיא, ללא אחריות מכל סוג. היא אינה מחליפה ייעוץ מקצועי, בדיקה של הסביבה הספציפית או הנחיות היצרן.

האחריות ליישום ההגדרות ולתוצאותיו חלה על מי שמיישם אותן.

רישיון שימוש פתוח

הרשימה מופצת ברישיון Creative Commons ייחוס 4.0 בינלאומי, CC BY 4.0.

מותר להעתיק, להפיץ, להתאים ולהשתמש בה, גם למטרות מסחריות, בתנאי שמציינים את המקור: רומי דר, ROMY, romy.co.il.

https://creativecommons.org/licenses/by/4.0/

מקורות

קישורים לתיעוד הרשמי, לבדיקה ולעדכון ההגדרות. לחיצה על שם המקור פותחת אותו.

Microsoft Security Compliance Toolkit
קווי הבסיס של Microsoft וכלי ההשוואה PolicyAnalyzer

CIS Benchmarks
קווי בסיס של CIS לתחנות ולשרתים

Microsoft Learn - Supported versions of Windows client
גרסאות, מהדורות ותאריכי סיום תמיכה

Microsoft Support - Secure Boot registry key updates, KB5068202
בדיקת מצב עדכון אישורי Secure Boot

Microsoft Support - Secure Boot certificate expiration, KB5062710
פקיעת אישורי 2011 ועדכון לאישורי 2023

Microsoft Learn - Windows LAPS with Active Directory
הצפנת סיסמאות והרשאות קריאה ופענוח

Microsoft Learn - Administrator protection
מצבים שבהם לא מומלץ להפעיל את המנגנון

Microsoft Learn - Windows Firewall rules
כללים אפקטיביים ומיזוג כללים מקומיים

Microsoft Learn - Detect, enable and disable SMBv1, SMBv2 and SMBv3
בדיקה והסרה של רכיבי SMBv1

Microsoft Learn - Installation and configuration for WinRM
שיטות אימות, הצפנה ומאזינים

Microsoft Learn - Microsoft Defender Antivirus compatibility
עבודה לצד מוצר אבטחה אחר ומצב פסיבי

Microsoft Learn - Attack surface reduction rules
כללי ASR ומצבי ביקורת וחסימה

Microsoft Learn - Get-AppLockerPolicy
תחולת פקודת האימות של AppLocker

Microsoft Learn - Enable-BitLocker
הפעלת הצפנה וסוגי מגנים

Microsoft Learn - Audit policy recommendations
המלצות ביקורת לתחנות, לשרתים ולבקרי תחום

Microsoft Learn - PowerShell logging on Windows
רישום ב-Windows PowerShell וב-PowerShell 7

Microsoft Learn - Sysmon configuration files
לוגיקת הסינון וכללי האיסוף

Microsoft Learn - Reset the krbtgt password
שתי החלפות והמתנה לפי תוקף כרטיסי Kerberos

NCSC - Logging and monitoring
תקינות האיסוף ובדיקות מקצה לקצה

לשאלות ולליווי בהקשחה ובאבטחת מידע: romy@romy.co.il | 052-3375029 | romy.co.il