

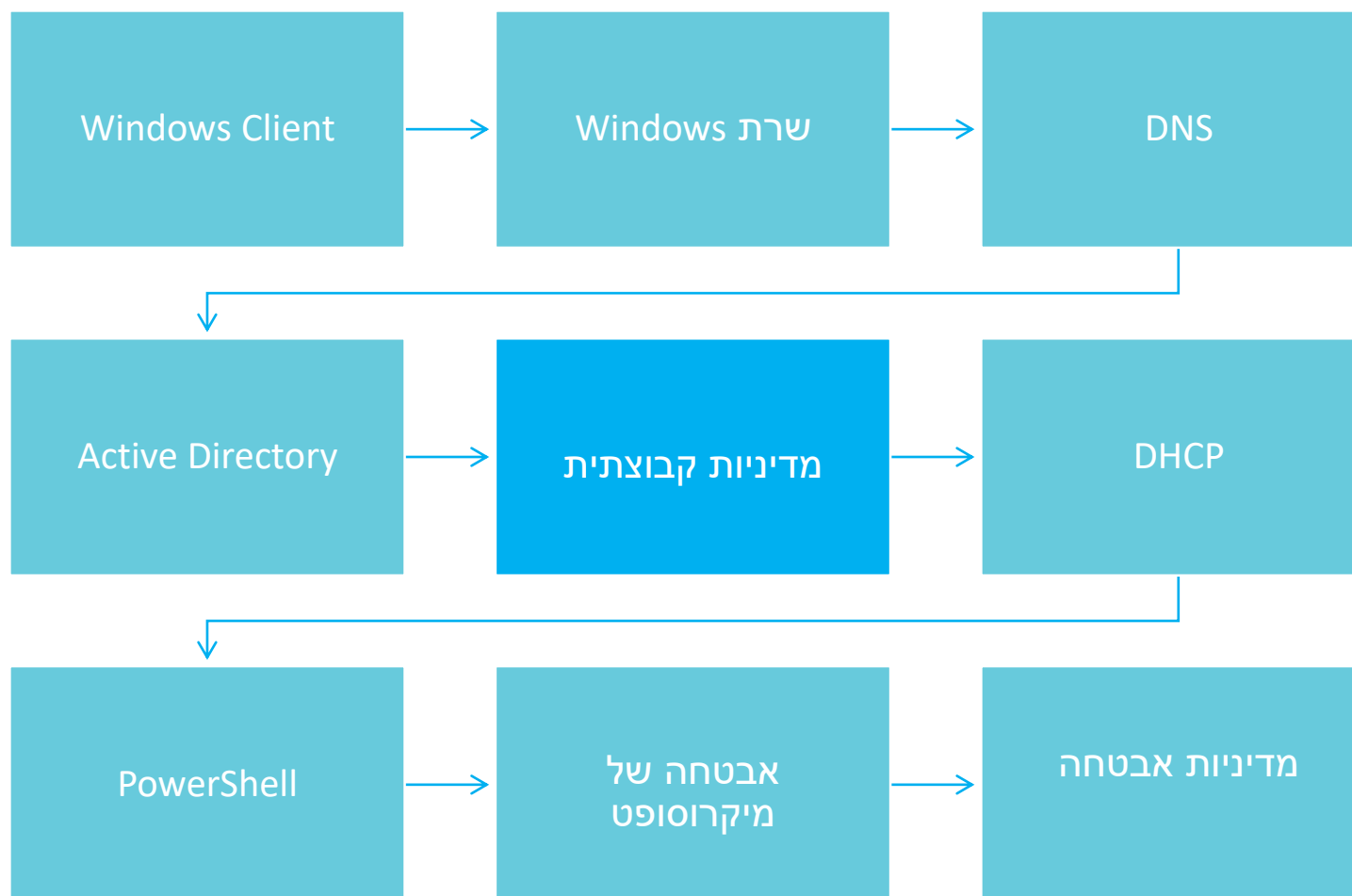
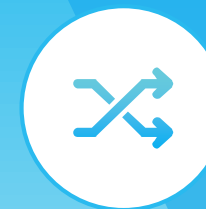
שיעור 5
אבטחת מערכות הפעלה

Group Policy



CYBER SCHOOL

מסלול הקורס





נלמד כיצד להשתמש בכלי ה-Group Policy Management בסביבת ה-Active Directory, כיצד להגדיר ואיך ליצור תפקידים ומדיניות.

- הקדמה ל-GPO
- ניהול GPO
- Group Policy Management Editor
- WMI Filters & Troubleshooting
- Additional GPO Extensions [אקסטרה]





CYBER SCHOOL

שיעור 5

אבטחת מערכות הפעלה

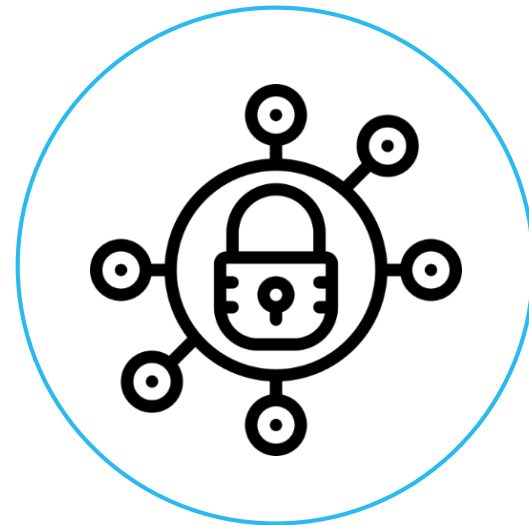
ניהול GPO

למה GPO משמשים?



Group Policy Objects (GPO) משמשים עבור
המטרות הבאות:

- הגדרות אבטחה
- ניהול שולחן עבודה
- שליטה מרחוק
- קביעת תצורת רשת
- שירותים



Policies לעומת Preferences



Preferences

מוגדר עבור תוכנות ב-Registries על מנת לבצע את בחירות המשתמש.

לא מבטל הגדרות בתוך התוכנות. במקום זאת, מאפשר למשתמשים לערוך, למחוק או לשנות הגדרות.

כברירת מחדל, מתרענן באותם הזמנים כמו הגדרות GPO.

Policies

אוכף מפתחות רישום וערכים.

מבטל את היכולת לשנות הגדרות ספציפיות.

מרענן את הגדרות המדיניות מידי פעם.

VS



פונקציונליות ה- Group Policy



- ל-GPO יש מדיניות מוגדרת מראש שאפשר להגדיר.
- זמן העידכון כברירת מחדל הוא 90 דקות או מוגדר ידנית.
- GPO משתמשים ב-CSE על מנת לבצע הגדרות אצל ה-Client.





CYBER SCHOOL

שיעור 5

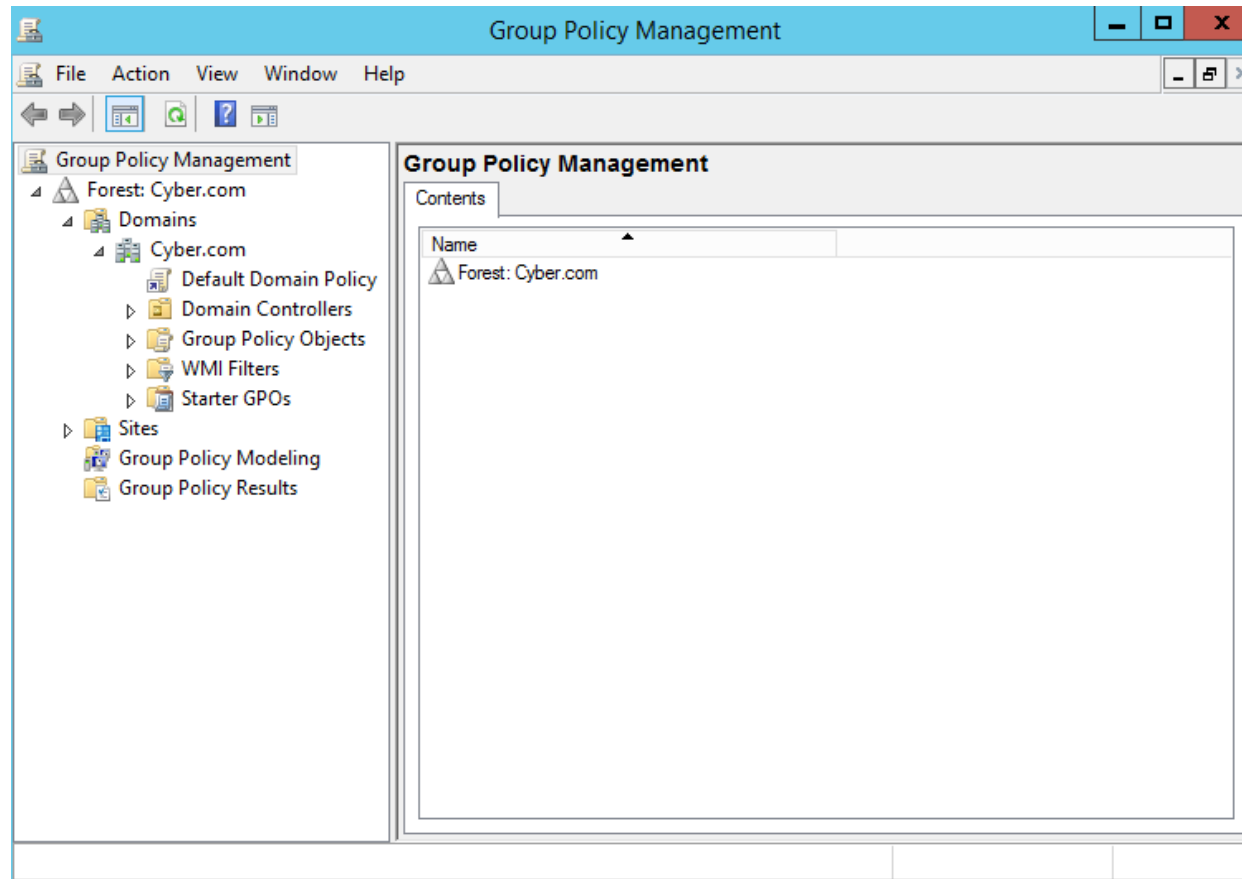
אבטחת מערכות הפעלה

מבוא ל-GPO

פאנל ה- Group Policy Management



למדיניות קבוצתית (Group Policies) יש מבנה היררכי.
Objects חדשים מקושרים ל-OU או לרמת ה-Domain.
כברירת המחדל ה-Domain Policy מקושר לרמת ה-Domain.



ירושת (Inherited) Group Policy



GPO אשר מוכלים על Site , Domain או OU עוברים בירושה-
(Inherited) אל "הילד".

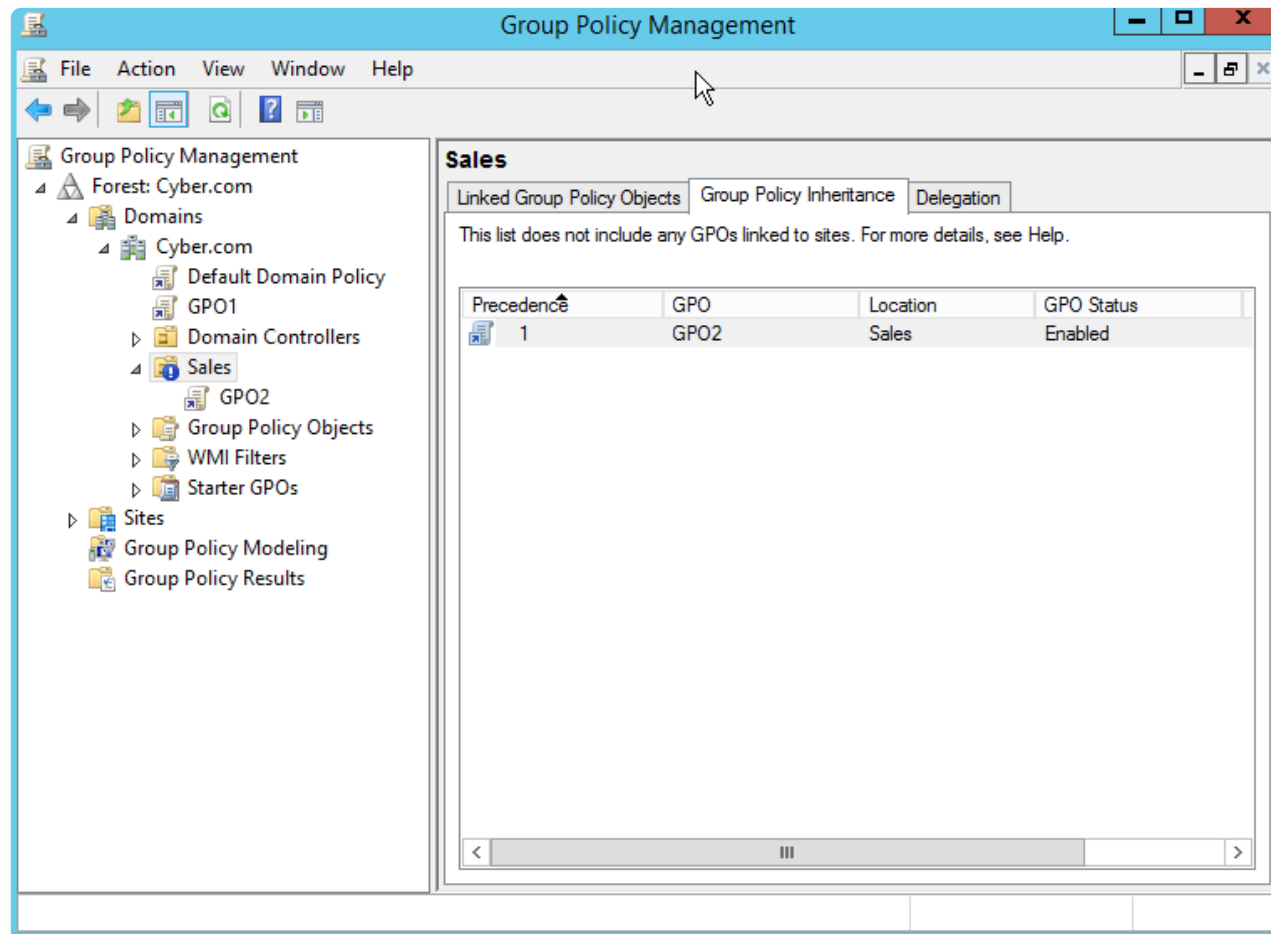
The screenshot shows the Group Policy Management console for the Forest: Cyber.com. The left pane shows the hierarchy: Forest: Cyber.com > Domains > Cyber.com > Sales. The right pane is titled 'Sales' and shows the 'Group Policy Inheritance' tab. A table lists the GPOs inherited by the Sales site:

Precedence	GPO	Location	GPO Status
1	GPO2	Sales	Enabled
2	Default Domain Policy	Cyber.com	Enabled
3	GPO1	Cyber.com	Enabled



חסימת Inheritance

ירושה- Inheritance יכולה להיחסם על ידי סמכות גבוהה יותר כמו Domain או OU "הורה".



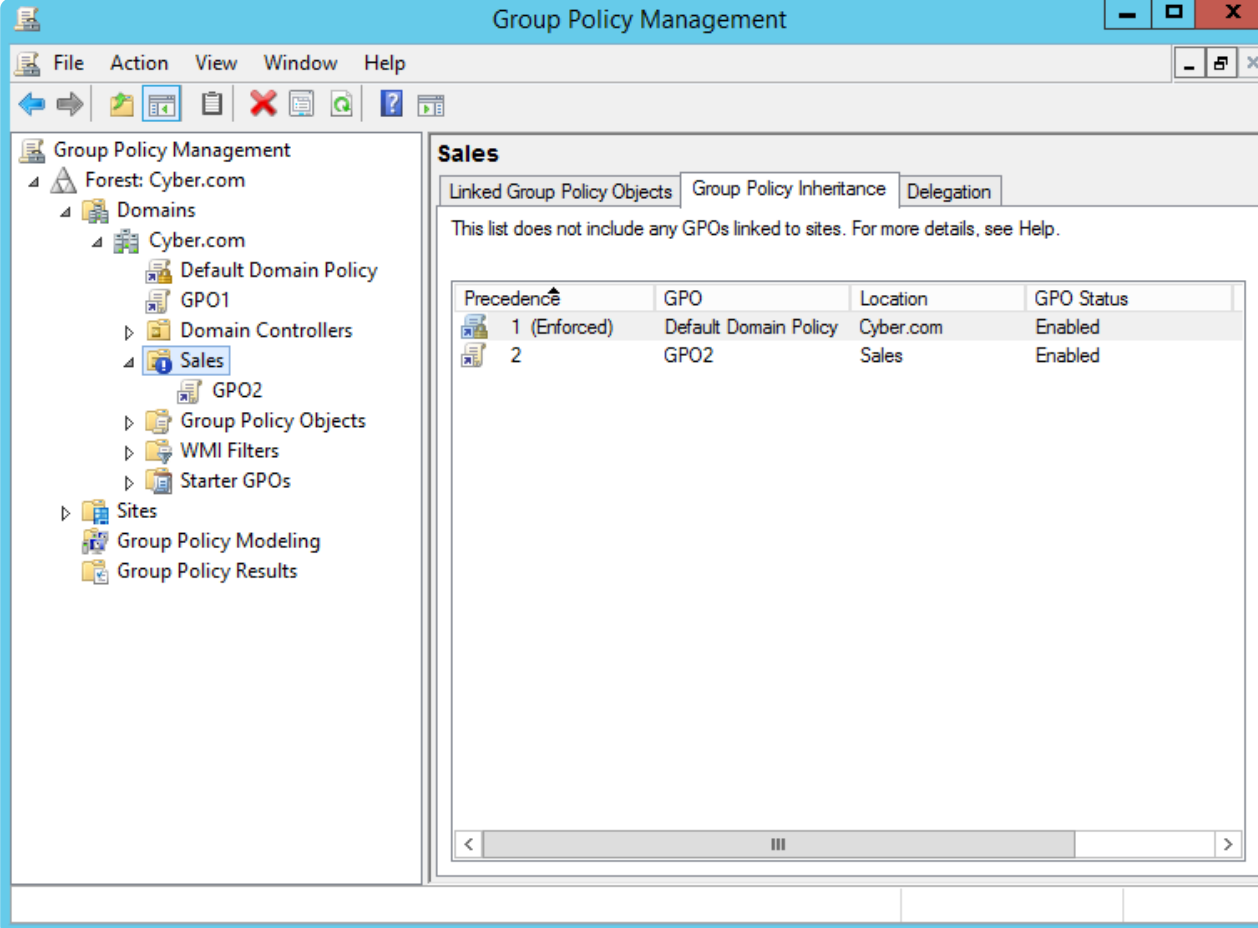
The screenshot shows the Group Policy Management console for the Forest: Cyber.com. The left pane shows the tree structure with 'Sales' selected under 'Group Policy Objects'. The right pane shows the 'Group Policy Inheritance' tab for the 'Sales' site. A table displays the inheritance information:

Precedence	GPO	Location	GPO Status
1	GPO2	Sales	Enabled



אכיפת GPO

GPO יכולים להיאכף על ידי קישור ל-GPO מרמה גבוהה יותר. לאכיפה מהרמה הגבוהה יותר תהיה עדיפות על פני GPO שמקושרים לרמות נמוכות יותר, אפילו אם ירושה חסומה (Block Inheritance) מופעלת.



The screenshot shows the Group Policy Management console for the Forest: Cyber.com. The left pane shows the hierarchy: Forest: Cyber.com > Domains > Cyber.com > Sales. The right pane shows the 'Group Policy Inheritance' tab for the Sales site. A table lists the linked GPOs:

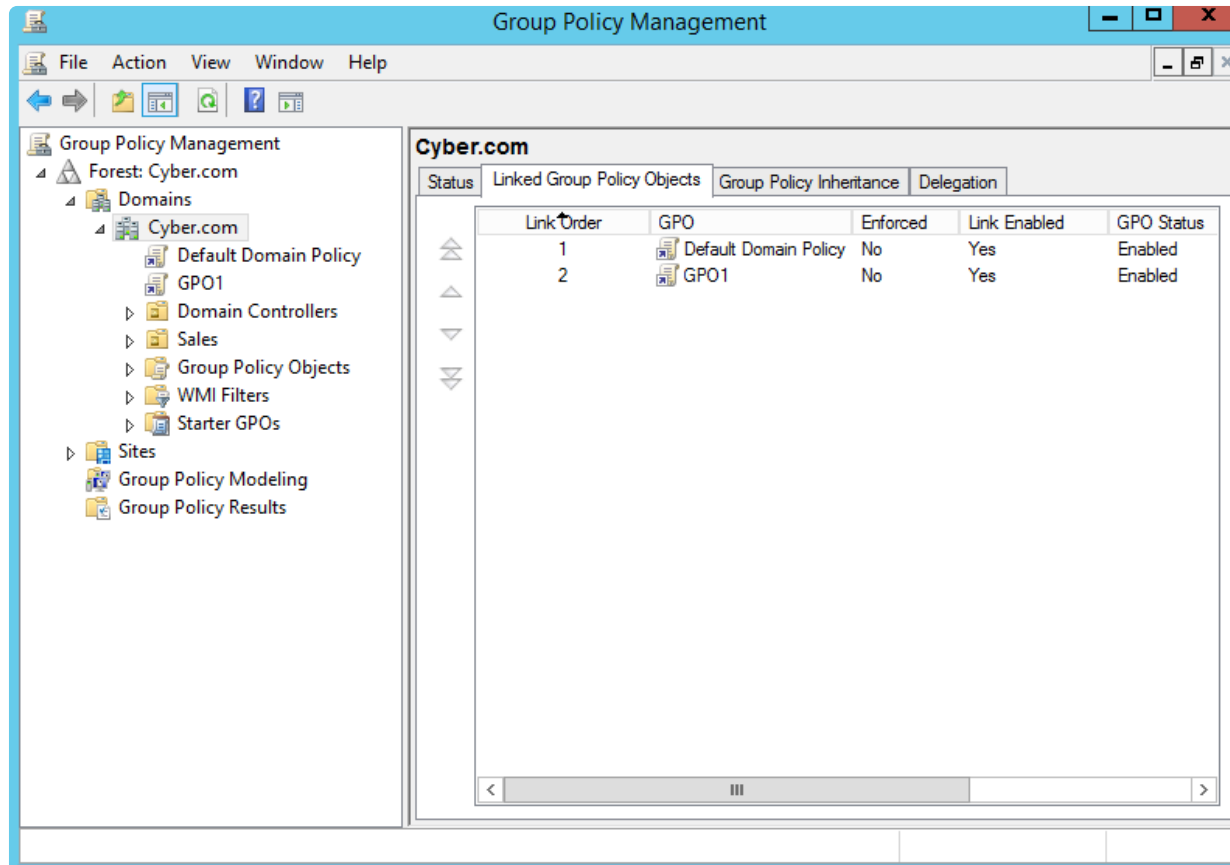
Precedence	GPO	Location	GPO Status
1 (Enforced)	Default Domain Policy	Cyber.com	Enabled
2	GPO2	Sales	Enabled



Group Policy Link Order



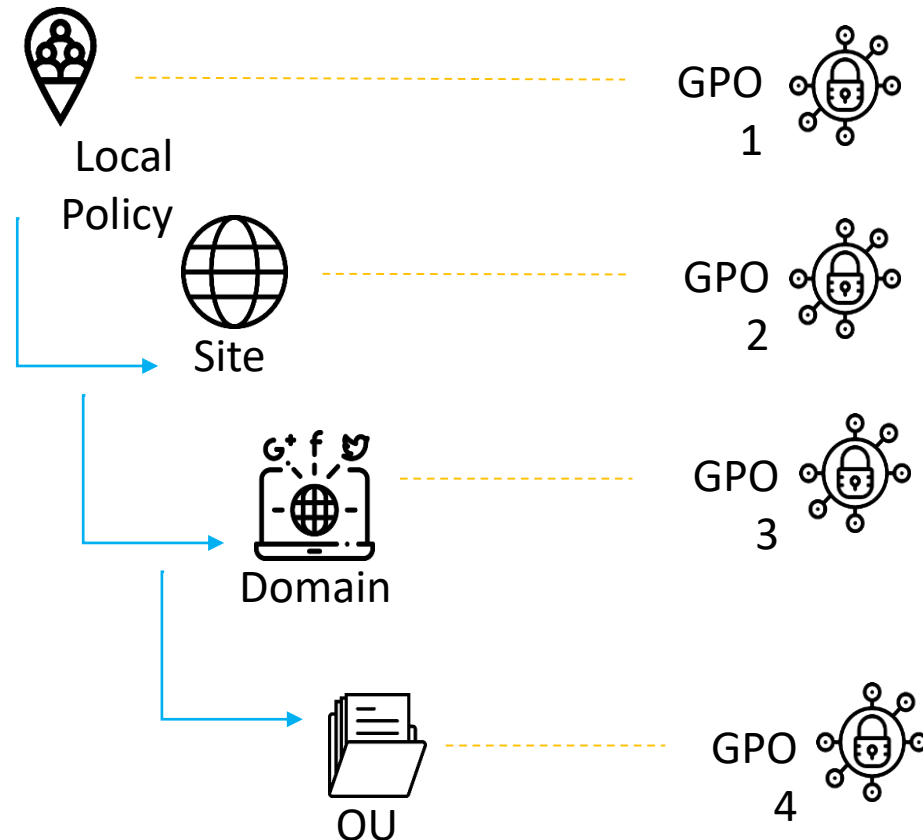
כשיש מספר GPO בתוך OU, סדר העבודה נקבע על ידי סדר הקישורים.



סדר העיבוד במדיניות הקבוצה



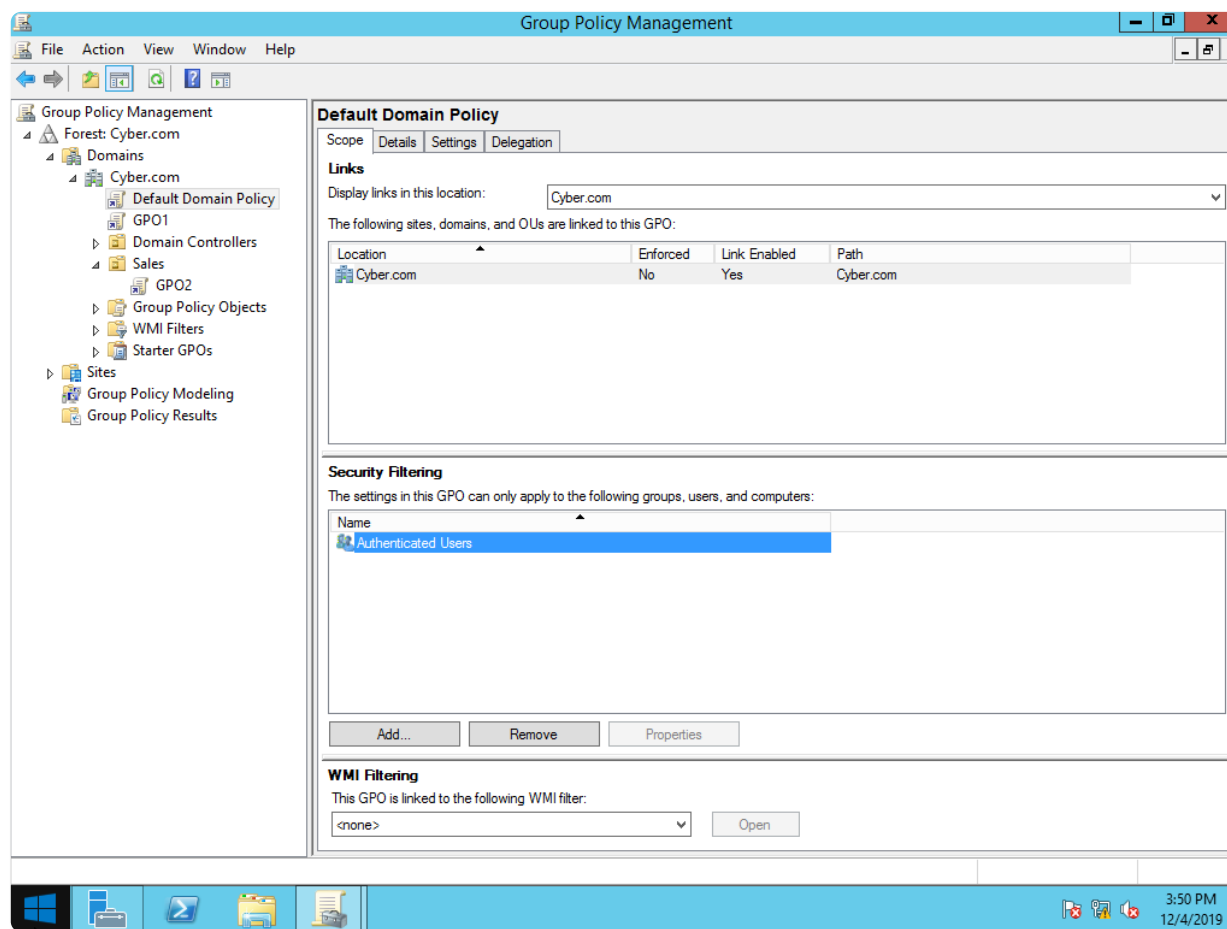
בעת קביעת הגדרות המדיניות שרוצים להכיל, צריך להתייחס למדיניות המקומית שנמצאת על המכונה, לאחר מכן למדיניות של ה-Site, אחריהם מדיניות ה-Domain ולבסוף המדיניות של כל ה-OU שמכילים בהם Object מופעלים שמתחילים עם ה-Domain Root.



Security Filtering



אפשר להכיל Security Filtering על משתמשים ספציפיים, מחשבים וקבוצות.



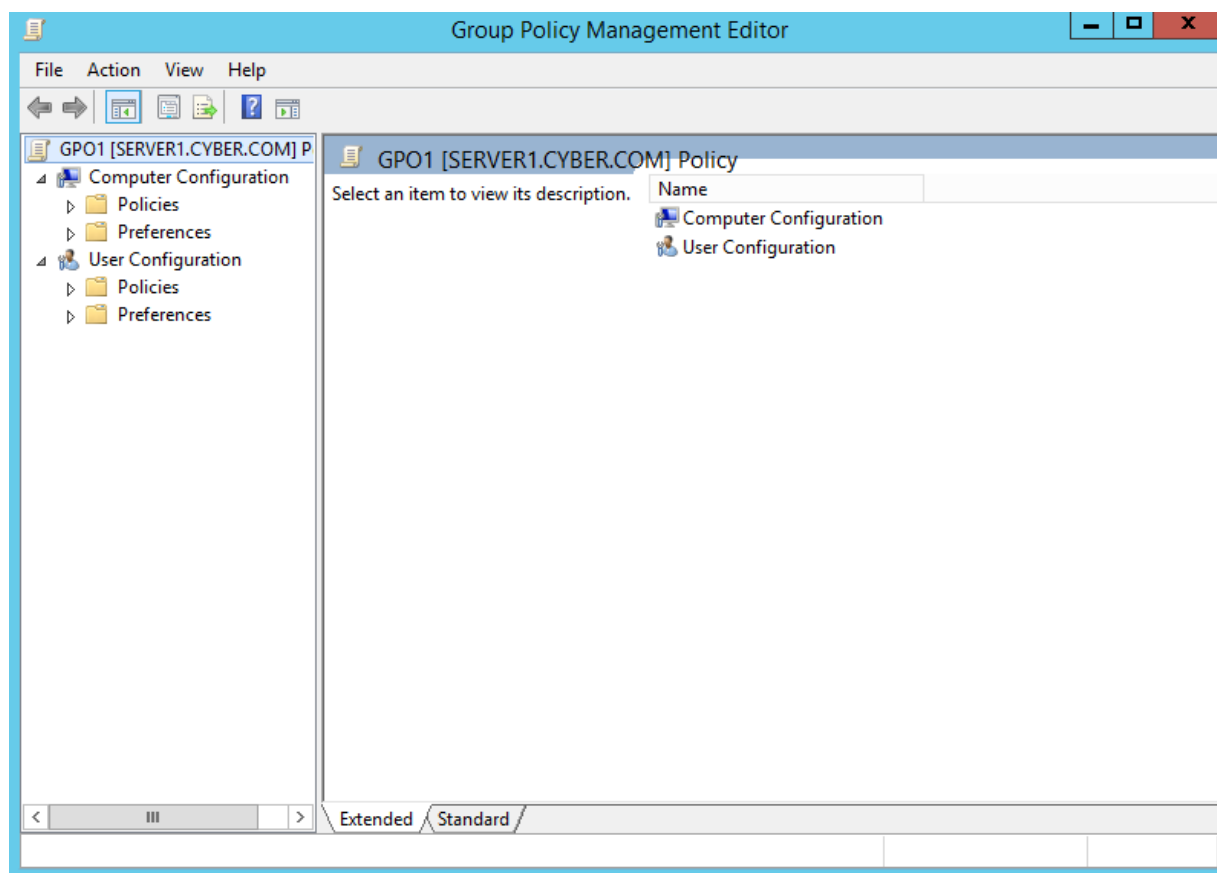


שיעור 5

אבטחת מערכות הפעלה

עורך ה- GroupPolicy Management

אפשר לבצע עריכה של GPO ב- Group Policy Management Editor.
ישנן שתי דרגות של קביעת תצורה: Computer Configuration ו-User Configuration.



עריכת GPO



אפשרויות עריכה



התקנת תוכנה ברמת המשתמש או המחשב.



הגדרת קוד להרצה בזמנים מוגדרים.



אכיפת מדיניות סיסמאות.



Event Viewer



מספק מידע מפורט על Group policy events.
נכללות בו כל סביבות מערכת ההפעלה של Windows.



מעבדה 1

קביעת תצורת
GPO בסיסית



20 – 40 דקות

המשימה

החל מדיניות כללית על מחשבים בתוך ה-Domain.

השלבים

- קבע תצורת הגדרות
- וודא GPO שהוחלו

קבצים קשורים

Lab document

כלים

Windows Client
Windows Server 2012 R2



CYBER SCHOOL

מעבדה 2

קביעת התצורה של
מדיניות סימא



20 – 30 דקות

המשימה

הגדר מדיניות שאוכפת כללים הקשורים לסימאות ב-Domain.

השלבים

- הגדר אורך סימא.
- הגדר מורכבות סימא.
- הגדר כללים מגבילים עבור ניסיונות התחברות.

קבצים קשורים

➤ Lab document

כלים

Windows Client
Windows Server 2012 R2



CYBER SCHOOL



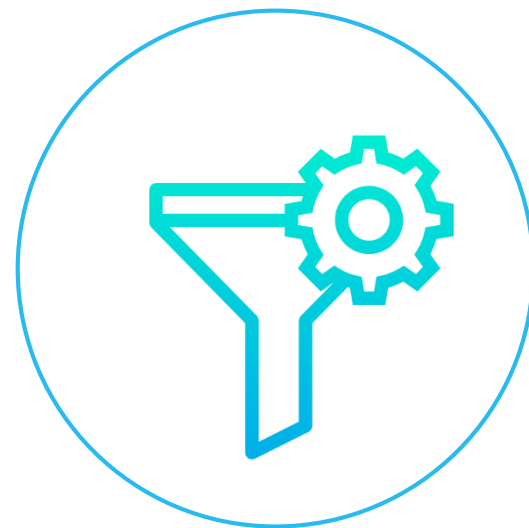
CYBER SCHOOL

שיעור 5

אבטחת מערכות הפעלה

WMI Filters & Troubleshooting

Windows Management Instrumental Filters



מאפיין אשר עובד עם חומרת ה-OU ומערכת ההפעלה.
אפשר להכיל מדיניות על בסיס פרמטרים ספציפיים
שקשורים למכונה.
WMI filter מצריכים קוד מיוחד שמבצעי שאלתה, אפשר
להוריד אותו דרך הקישור הבא:
<https://www.microsoft.com/en-us/download/details.aspx?id=8572>



דוגמא ל-WMI



לדוגמא, בצד ימין אפשר לראות את הקוד עבור ה-WMI שבודק את גרסאת מערכת ההפעלה והארכיטקטורה שלה.

Target Windows 7 or 8 64 bit

Name:
Target Windows 7 or 8 64 bit

Description:
|

Queries:

Namespace	Query
root\CIMv2	select Version from Win32_OperatingSystem WHERE (Version like "6.1%" OR Version like "6.2%" OR Version like "6.3%") AND ProductType="1" AND OSArchitecture = "64-bit"

Add
Remove ...
Edit ...

Save ... Cancel ...

Group Policy Modeling



כלי שמובנה במערכת ההפעלה ומשמש ל-Troubleshooting וצפיה בפרטי שימוש במדיניות.
הוא מצריך את שם ה-Domain ואת שם ה-DC.

Group Policy Modeling Wizard

Domain Controller Selection
You must specify a domain controller to use for performing the simulation.

The simulation performed by Group Policy Modeling must be processed on a domain controller running Windows Server 2003 or later.

Show domain controllers in this domain:
Cyber.com

Process the simulation on this domain controller:

Any available domain controller running Windows Server 2003 or later

This domain controller:

Name	Site
Server1.Cyber.com	Default-First-Site-Name
Server2.Cyber.com	Default-First-Site-Name

< Back Next > Cancel



מכיל מדניות אשר ניתנות לאימות אצל ה-Client.
פקודת /R gpresult מראה את המדיניות אשר מוכלות על המשתמש והמחשב.

```
C:\Users\Administrator>gpresult /R

RSOP data for CYBER\Administrator on DC1 : Logging Mode
-----
OS Configuration:           Primary Domain Controller
OS Version:                  6.3.9600
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No
```

Troubleshooting



כך זה ניראה בהמשך

COMPUTER SETTINGS

CN=DC1,OU=Domain Controllers,DC=Cyber,DC=com

Last time Group Policy was applied: 1/26/2020 at 3:58:30
AM

Group Policy was applied from: DC1.Cyber.local

Group Policy slow link threshold: 500 kbps

Domain Name: CYBER

Domain Type: Windows 2008 or
later

Troubleshooting



וכך סוף התוצאה של הפקודה מוצגת.

```
Applied Group Policy Objects
```

```
-----
```

```
Default Domain Controllers Policy
```

```
Default Domain Policy
```

```
Enable Remote Desktop
```

```
Unused TPM
```

Troubleshooting





שיעור 5

אבטחת מערכות הפעלה

Additional GPO Extensions

[אקסטרה]

שימוש מורחב ב-GPO



➤ אפשר להוסיף הרחבות נוספות למדיניות הקבוצה.

➤ Google Chrome יכול להשתלב עם GPO.

➤ GPO מקושרים למערכת ההפעלה של Windows באמצעות קבצי ADM ו-ADMX.



מעבדה 3

צור מדיניות קבוצה
עבור דפדפן Chrome



40 – 60 דקות

המשימה

הוסף תבניות חיצונית של Google וקבע את תצורת ה-GPO עבור דפדפן Chrome לכל אורך ה-Domain.

השלבים

- התקן Chrome.
- הוסף תבנית ADM.
- שנה את המדיניות של דפדפן Chrome.
- וודא את ההגדרות המדיניות החדשה.
- בחן את המדיניות החדשה אצל ה-Client.

קבצים קשורים

➤ Lab document

כלים

Windows Client
Windows Server 2012 R2



CYBER SCHOOL

קורס CSRP

שיעור 5

אבטחת מערכות הפעלה



שאלות?