Technologic Papers

Windows VS Linux - אוטומציית הקשחה ובקרה

מאת שרון וילנסקי

הקדמה

מאמר זה הינו המשך למאמר הקודם שלי בנושא "אוטומציה לתהליכי הקשחה לצמצום משטחי תקיפה". לאורך עבודתי בנושא הקשחת מערכות עסקתי בהקשחה של מערכות הפעלה מבוססות Windows. הבנתי כי הפתרון הקודם שהצגתי (OpenSCAP), המתאים לעולמות ה-Linux ונגזרותיו, הוא חלק מתוך פתרון כללי שיאפשר אוטומציה לתהליכי הקשחה עבור מערכות שונות, כגון: מערכות הפעלה, פלטפורמות ענן, תוכנות, דפדפנים וכד'.

בכדי לייצר תהליך הקשחה ובקרה אוטומטיים, נדרש להבין איך נוכל להשפיע על הגדרות בנושאי אבטחת-מידע. לשם כך, חשוב להכיר ולהבין מה הכלים הרלוונטים להתמודדות עם אוטומציה לאותן הגדרות בסביבות שונות.

במאמר זה אראה את הדרך להגדרת תקן הקשחה עבור משאבי Windows, בצורה המותאמת לארגונים שונים.

Windows Vs Linux

בחרתי לקרוא למאמר Windows Vs Linux בעקבות המידע שנחשפתי אליו לאורך עבודתי. **לא ניתן** לייצר אוטומציה לכלל המערכות באמצעות **כלי אחד** (לפחות לא OpenSource) אך, אם נבין מה מערכות ההפעלה\פלטפורמות שמשמשות אותנו, נוכל להבין מה סט הכלים המתאים למשימה.

אציין ואדייק את ההנחה המרכזית שהצגתי במאמר הקודם, בכדי להבהיר אילו מערכות יכולות לקבל מענה מהכלי שהצגתי (OpenSCAP) וכיצד נוכל לייצר תהליך דומה (הקשחה ובקרה אוטומטיים) בעבור סביבת מחשוב מבוססת Windows.

אסקור את היכולות שמגיעות מבית Microsoft והתמיכה שהיא מספקת באמצעות חבילות הכלים **SCT(Security Compliance ToolKit)** 1.0, שיאפשרו ניהול תהליך הקשחה בהתאם להמלצות Microsoft החל מ Windows 10 ועד ל Windows 11 (כולל גרסאות ביניים ושרתים). בנוסף, אדגים כיצד ניתן לייצר אוסף הגדרות מותאם בעזרת קבצים שונים הנתמכים ע"י יכולות SCT1.0. לפני שנמשיך אציג את ריכוז המערכות הן ב-SCT1.0 והן ב-OpenSCAP:

SCT1.0:

מערכות הפעלה	דפדפנים	שירותי Enterprise
Windows 10 & 11	Microsoft Edge	Office 2016
Windows Server 2012 & 2016 & 2019 & 2022		Microsoft 365 Apps For Enterprise

OpenSCAP:

- במאמר הקודם שלי ניתן למצוא הסברים מפורטים על אופן השימוש ב-OpenSCAP בכדי לייצר תקן הקשחה מותאם לצרכים אישיים - אוטומציה לתהליכי הקשחה לצמצום משטחי תקיפה.
- חלק מתקני ההקשחה מונגשים באמצעות תוסף לפלטופורמה אותה יש להקשיח - למשל RedHat OpenShift Container Platform דורש התקנה של תוסף בשם OpenShift Compliance אשר מנגיש את יכולות OpenSCAP לסביבה הנ"ל.

מערכות הפעלה	דפדפנים	שירותי Kubernetes	שירותי Enterprise	וירטואליזציה
Amazon Linux 2/3	Chromium	Amazon Elastic Kubernetes Service	RedHat Jboss Fuse	RedHat Virtualization 4
CentOS 7/8	FireFox	RedHat OpenShift Container Platform	Java Runtime Environment	
Debian 9/10/11		RedHat OpenStack Platform	McAfee VirusScan Enterprise	
Fedora				
MacOS				
Oracle Linux 7/8/9				
openSuse				
RedHat CoreOS 4				
RedHat Enterprise 7/8/9				
Suse Enterprise Linux 12 & 15				
Ubuntu 16.04/18.04/20.04/22.04				
UnionTech OS Server 20				

תקן הקשחה

כפי שהזכרתי, יש צורך להבדיל את הפתרון הקודם (OpenSCAP) שמתאים כמו כפפה ליד בעולמות ה-Linux מעולמות ה-Windows.כיוון שבעמוד הגיט-האב שלהם מצויין בבירור כי הם זונחים את התמיכה במשאבי Windows (מקור).

דבר זה מוביל אותי לשאלה: כיצד ניתן להקשיח ולבקר את משאבי ה-Linux **אך גם** משאבי Windows? לשם כך אחזור על מספר נקודות שפירטתי עלייהן יותר במאמר הקודם.

הזכרתי שבכדי להגיע לתקן הקשחה (Benchmark), מומלץ להשתמש בתקן ההקשחה של CIS (Central of Internet Security) מתוך ההנחה כי הגוף מתחזק תקני הקשחה (Benchmarks) למגוון רחב של מערכות, תוכנות ורכיבי רשת שונים. בנוסף, הזכרתי שניתן למצוא יכולות אוטומטיות להקשחה דרך מאגר של ארגון התקנים האמריקאי NIST - מאגר NCP (National Checklist Program).

הדיוק הרלוונטי להנחה שלי מהמאמר הקודם, היא כי מה שנמצא במאגר NCP יהווה בעיקר את התאוריה עבור תקני הקשחה של גופים שונים - ולא תמיד את האוטומציות לתהליך ההקשחה והבקרה.

אציין כי ניתן למצוא קבצי SCAP שיאפשרו בקרה עבור משאבי Windows דרך ממשק יעודי לעבודה עם קבצי SCAP - אותו תוכלו למצוא גם כן ב-NCP. אך, הפער עליו אני מצביע הוא דווקא ביכולות האוטומציה **להקשחה - אותם לא ניתן לקבל באמצעות OpenSCAP עבור סביבות Windows**.

אני אישית ממליץ לבחון מה ניתן למצוא במאגר NCP לפני תחילת תהליך מחקר בנושאי הקשחה לרכיבים שונים.

מוטביציה

במאמר הקודם הצגתי מצב בו תשתיות המחשוב השונות, בארגון קטן עד גדול, **חשופות** לחולשות חדשות\ישנות בעקבות ניהול הגדרות אבטחת-מידע לקוי.

לעיתים, התיקון הנדרש צריך להיות מוחל על מספר רב של משאבים ולא מאפשר טיפול נקודתי-ידני במסגרת הזמנים הנתונה.

בהמשך למאמר הקודם, בו הסברתי על יכולת אוטומטית להקשחה ובקרה בקרב משאבי ה-Linux, אסביר במאמר הנוכחי כיצד ניתן לייצר תהליך שכזה גם למשאבי ה-Windows שברשותנו.

המטרות העיקריות של התהליך הן:

- להגדיר פרופיל הקשחה - אוסף הגדרות בהבטי אבטחת-מידע שיחולו על מערכת.
- בקרה - תמונת מצב המאפשרת לקבל חיווי לעמידה בתקן ההקשחה.
- אכיפה - החלת הקשחה על מערכת.

מבוא

אנשי המחשוב נאלצים לדעת להתמודד עם גרסאות שונות של משאבי ארגון מבוססי Windows: עמדות עבודה (Desktops), שרתים (Servers), ניהול מערכות ומידע הארגוני (Data-Center) וכדו'. בסביבות 2022 (ע"פ אתר Microsoft) שוחררה גרסא 1.0 של SCT. SCT מיועד להפצות Windows שבאו לאחר Windows 10 1703. המערכות הנתמכות מתוארות בטבלה הבאה:

מערכות הפעלה	דפדפנים	שירותי Enterprise
Windows 10 & 11	Microsoft Edge	Office 2016
Windows Server 2012 & 2016 & 2019 & 2022		Microsoft 365 Apps For Enterprise

הקשחת Windows

תהליך ההקשחה ב-Windows מתרכז למספר ממשקים אשר דרכם ניתן להגדיר כל הקשור באבטחת-מידע: ערכי GPO והגדרות נוספות. ביניהן: Registry, Audit Policy ו-Security Templates.

אתחיל מסקירה קצרה של הממשקים הנ"ל ואתאר כיצד ניתן באמצעותם לייצר **תהליך הקשחה ובקרה** עבור משאבי ה-Windows שנרצה לנהל בהקשרי אבטחת-מידע. אפרט בהמשך המאמר כיצד אוסף ההגדרות השונות מרכיבות יחד תקן הקשחה למשאבי ה-Windows שברשותנו.

היכולת ב-Windows לייצא את אוסף ההגדרות, שנרצה כחלק מתקן ההקשחה שגובש, ולהשתמש בהן לצורך תהליך ההקשחה שלנו היא: **GPO Backup**, אותה נשיג באמצעות כלי המגיע יחד עם LGPO - SCT 1.0 (Local GPO).

באמצעות יכולת הגיבוי נוכל לייצא מצב הגדרות רצוי של משאב Windows ולטעונו בעמדת אחרת (הקשחה). בנוסף, ניתן יהיה גם לבקר את תאימות מצב המשאב להגדרות המוצגות בגיבוי.

בכדי להבין כיצד הכלי ישמש אותנו אסביר מה יהיו אוסף הקבצים אשר נקבל באמצעות LGPO - בפעולת GPO Backup.

במידה והקורא מכיר את המונחים הנגזרים מהנושא של GPO, אמליץ בכל זאת להתעכב על סוגי הקבצים המגיעים באמצעות תהליך GPO Backup - הכותרות: GptTmpl.inf, registry.pol ו-audit.csv.

GPO - Group Policy Objects

אובייקט GPO הוא אוסף וירטואלי של פוליסות המגדירות אוסף תכונות ברמת מערכת ההפעלה (Windows) והמשתמש(ים).

קיימים 2 סוגים עיקריים של GPOs: מקומי (Local) ולא-מקומי (Non-Local).

מעבר להגדרת תכונות שונות למשאבי מערכת ההפעלה Windows קיימות הגדרות אשר מהוות פוליסת אבטחת-מידע. למשל ניתן:

- להגביל גישה ללוח-בקרה (Control Panel)
- לאסור הפעלת CMD או PowerShell (ממשקים להרצת סקריפטים וכו')
- לאסור התקנה של תוכנות
- לאכוף מדיניות שימוש בסיסמאות

אופן החלת הפוליסות נעשית בסדר קבוע, השייך בחלקו לניהול GPO בארגון (ע"י Active-Directory - מערכת שלא אפרט עליה ומיועדת לניהול מס' משאבי Windows כחלק מיכולות ניהול הארגון). לנו חשוב לזכור כי Local GPO הן ההגדרות הראשונות שיכולו על עמדה עלייה נחיל הקשחה. במידה והעמדה היא חלק מארגון יצטרפו הגדרות הנופלות לסוג השני - Non-Local GPO.

GPO Back-Up

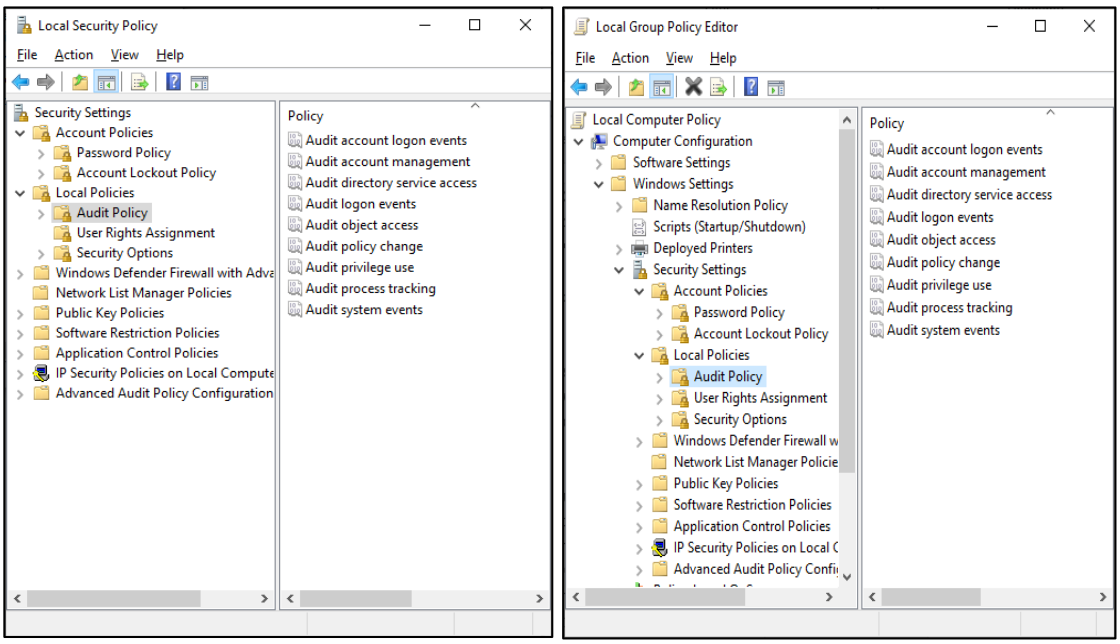
כאשר נרצה להחיל תקן הקשחה על משאב Windows נצטרך לזכור, כפי שתיארתי קודם לכן, כי קיימות הגדרות אבטחה הן לרמת מערכת ההפעלה והן לרמת המשתמש(ים). אלו ניתן להגדיר באמצעות אוסף של קבצים עלייהם ארחיב בחלקים הבאים: registry.pol, audit.csv ו GptTmpl.inf.

- בנוסף, קיים קובץ Backup.xml & Bkupinfo.xml אשר מכילים מידע נוסף על הגדרות המשאב. ההגדרות הנוספות נוגעות לתוספות למשאב Windows - בינהם BitLocker ונוספים.
- עלייהם לא אפרט במאמר זה, בעקבות הסיבה שהם ממשקים נוספים שניתן להגדיר בהקשרי אטבחת-מידע. מצד שני, התהליך שאתאר לאורך המאמר יוכל לאפשר לקוראים להבין כיצד להגדיר אותם **גם כן** - שכן גם הם מתרכזים להגדרות נוספות בקבצים שאתאר במאמר.

תקן ההקשחה, כפי שיגיע מ-Microsoft או גורם מאושר אחר (למשל *CIS*), יגיע עם מספר קבצים - אשר אחד מהם הוא ה-GPO-Backup, אשר יעזור לנו להקשיח ולבקר האם העמדה שלנו עומדת בהמלצות של Microsoft או בתקן ההקשחה שגובש בארגון.

מעבר להגדרות כלליות של משאב ה-Windows שלנו אשר נכללות בממשק ה-GPO של המשאב, קיים בתוך ה-GPO אזור המיועד לאבטחת-מידע - **Security Settings**.

בכדי להגיע לממשק ניהול הגדרות אבטחת-מידע נוכל לרשום ב"התחל" secpol.msc:



כעת, בהינתן העובדה כי יש סט הגדרות יעודיות לנושא אבטחת-מידע למשאבי Windows, כל שנותר הוא להבין כיצד לנצל זאת לטובתנו - ולייצר תקן הקשחה המתאים לדרישות הארגון שלנו.

Group Policy: Security Protocol Extension

פוליסות אבטחת-מידע מכילות הגדרות המאפשרות שימוש ביכולות אבטחה של Windows בכדי להבטיח אכיפה של מגוון קטגוריות:

- סמאות, נעילת משתמש ופרופיל Kerberos (מערכת הזדהות לארגון)
- הגדרות תיעוד ולוגים ברמת המערכת והמשתמש(ים) - תיעוד כללי
- הרשאות גישה לקבצים ותיקיות
- אבטחה לתוכנות, תהליכים
- שיוך פרופיל אבטחה לקבוצה

בכדי להשיג שליטה על קבוצת ההגדרות הנ"ל Microsoft מתעדת את השימוש בפרוטוקול שיאפשר לנו להגדיר את הקטגוריות השונות. לשם כך, הפרוטוקול מתאר את אוסף ההודעות שהוא תומך בהן. אוסף ההודעות מתורגם בפרוטוקול להגדרה נקודתית הקשורה לאבטחת-מידע.

- אוסף ההודעות וההגדרות השונות מפורטות ביתר פירוט במסמך MS-GPSB באתר של Microsoft - מקור
- בתוך המסמך המפורט של Microsoft ניתן לראות כי לחלק מההגדרות ישנם ערכים קבועים שהמסמך יודע להגדיר - ואותם נוכל לראות כבר במסמך.

בכדי לאגד את אוסף כל ההגדרות הנ"ל נתחיל להכיר את קובץ ה- GptTmpl.inf.

GptTmpl.inf

כאמור, נוכל להגדיר כל הגדרה הקשורה לאבטחת-מידע דרך הקובץ הנ"ל:

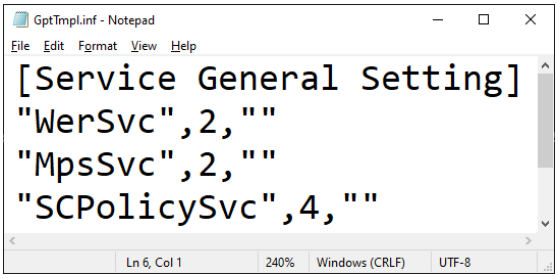
- חלק מסעיפי תקן הקשחה לא מוגדרים כחלק מאוסף הגדרות אבטחת-מידע של משאב Windows. אלו מוגדרים בהקשרים אחרים של ה-GPO ויקבלו מענה באמצעות הקובץ registry.pol (עליו אסביר בחלק הבא).

בכדי להכיר את הגדרות האבטחה השונות מומלץ להעזר בתקן הקשחה אשר ימליץ וילווה אותנו באוסף העצום של סעיפים שונים - שכל מטרתם היא **אבטחת-מידע**.

למשל, הגדרת אופן העלייה לשירותים (Services) הבאים:

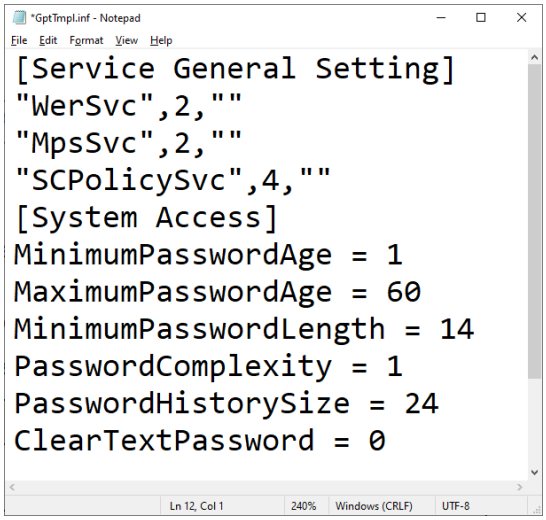
- עלייה אוטומטית לשירות WerSvc - Windows Error Reporting
- עלייה אוטומטית לשירות MpsSvc - FireWall
- ביטול שירות SCPolicySvc - Smart Card Removal

ניתנים לשליטה באמצעות קטע הטקסט הבא:

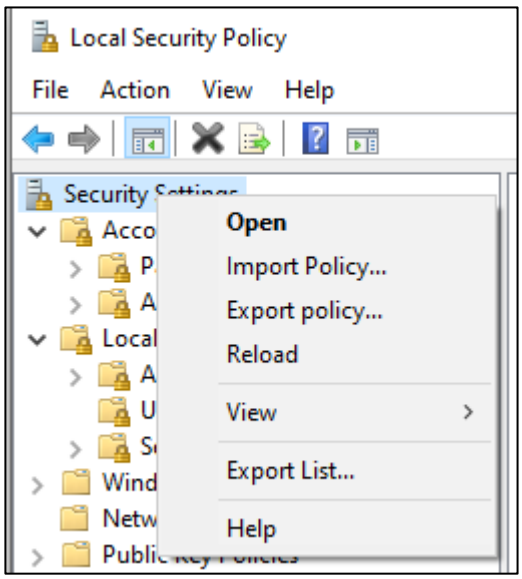


- הערך 2 מציין "עלייה אוטומטית" והערך 4 מציין "בטל שירות".
- ה "" (גרשיים ריקות) חייבות להמצא - לפירוט ניתן לפנות למקור [MS-GPSB].

בנוסף, ניתן להגדיר מדיניות ניהול ססמאות בצורה הבאה:



ניתן לייצא ולייבא את קובץ פוליסת אבטחת-מידע באמצעות ממשק ה-Security Settings:



האפשרות **לגבות ולבחון** את ההגדרות שלנו עבור תהליך ההקשחה הוא חשוב, שכן נרצה לבחון את השינויים שלנו בצורה נקודתית לפני שנריץ אוטומציות המכילות מס' רב של שינויי הגדרות.

מעתה, נוכל להגדיר עבור משאב ה-Windows שלנו אוסף הגדרות המתאים לתקן ההקשחה שגובש בארגון - **ולהבטיח עמידה של אוסף המשאבים המתאימים** בהגדרות אבטחת-המידע השונות.

אם כך, ברור שיש לנו קובץ אחד שניתן דרכו להגדיר את כל קטגוריות אבטחת-המידע ב-Windows. ראינו דוגמא להגדרת Services ו-Policy לסמאות. בהתייחס לניהול Registry נכיר כי קיימת דרך ברורה ואוטומטית לניהול ערכים ברמת מערכת ההפעלה וברמת משתמשים בהרשאות שונות.

registry.pol

הקובץ הנ"ל הינו קובץ בינארי אשר מאפשר למשאב Windows להגדיר הגדרות שונות ברמת מערכת ההפעלה והמשתמשים השונים (**לא רק בהקשרי אבטחת-מידע**). בכל כיבוי של המשאב ההגדרות נשמרות ונטענות מחדש בעת עליית המשאב.

כאשר נבצע פעולת GPOBack-Up נקבל את הקובץ המתאים הן להגדרות מערכת ההפעלה והן להגדרות משתמש - אלו ימצאו בתיקיות מתאימות בגיבוי.

- בכדי שנוכל לקבל דינאמיות על אופי הגדרת קובץ pol. נקבל החל מ-Windows 10 תמיכה של LGPO3.0 עבור פעולה ליצירת קובץ pol. מקובץ טקסט בפורמט הבא:

```
; Removes all “allowed remote assistance helpers”
Computer
Software\Policies\Microsoft\Windows NT\Terminal Services\RAUnsolicit
*
DELETEALLVALUES
```

את קובץ ה-registry.pol נוכל לטעון (בהתאם ליעודו) לאחת מהקבוצות הבאות:

Computer	Computer Configuration.
User	System-wide User Configuration.
User:Administrators	MLGPO User Configuration for Administrators.
User:Non-Administrators	MLGPO User Configuration for Non-Administrators.
User:*username*	MLGPO User Configuration for the named local account.

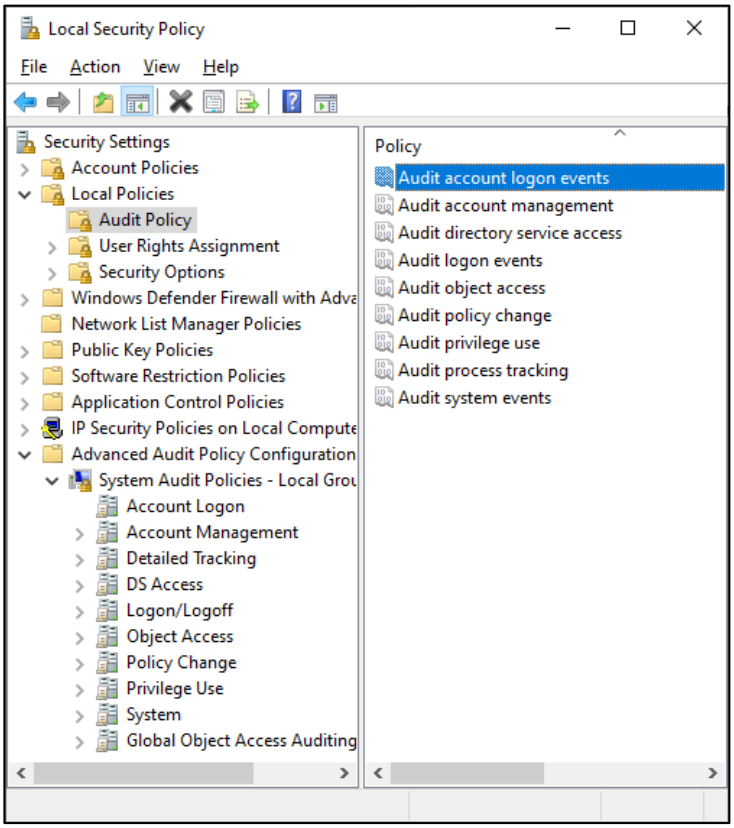
כך שלאחר שנחליט אילו ערכי Registry נרצה להוסיף להגדרות משאב ה-Windows שברשותנו, נוכל להשתמש ב-LGPO בכדי לייצר קובץ pol.*. זאת נעשה באמצעות GPOBack-Up שהזכרתי קודם לכן.

- Registry.pol המשויך למשתמש (User) מהווה את אוסף ההגדרות **המוחל על המשתמש שיזם** את פעולת הגיבוי.
- כפי שהזכרתי בפסקה הקודמת - נוכל לטעון אותו למשתמש(ים) ספציפי(ם).

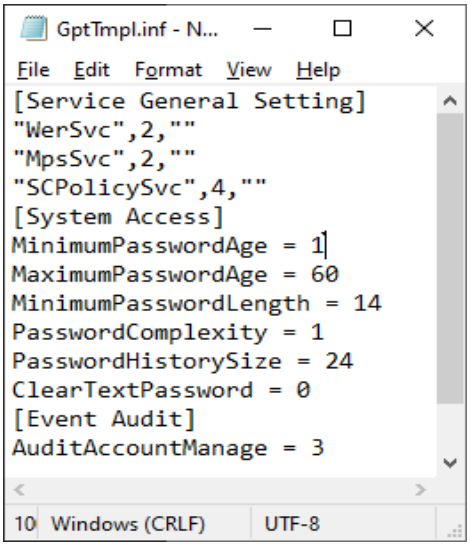
audit.csv

מנגנון התיעוד לפעולות במשאבי Windows מאפשר לנו שליטה ברמה כללית ופרטנית. כאשר נתבונן במסך Security Settings נבחין כי יש 2 מקבצי הגדרות לתיעוד:

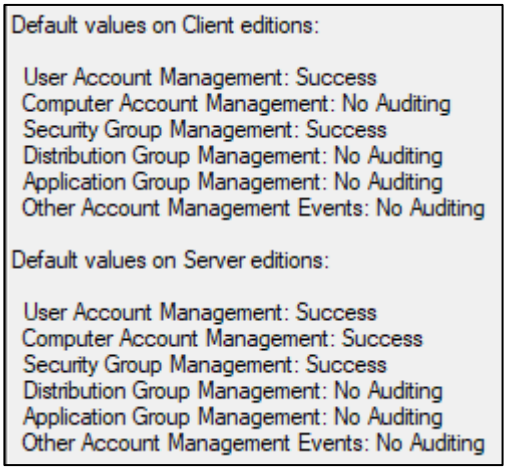
- Audit Policy - סט הגדרות תיעוד כלליות (מכיל את כלל ההגדריות הפרטניות)
- Advenced Audit Policy - סט הגדרות תיעוד פרטניות המאפשרות הגדרה נקודתית לתיעוד פעולות שונות (מאפשר לחסוך מידע שאינו נחוץ - המגיע בהגדרה הכללית)



בעבור ההגדרות הכלליות, נוכל להגדירן כבר בקובץ GptTmpl.inf שהצגנו קודם לכן. במידה ונוסיף את התוכן הבא ב-[Event Audit]:



נוכל להבין כי הפעלנו אפשרות "3" המסמנת תיעוד במקרה של הצלחה\כשלון עבור אוסף הארועים הבאים:

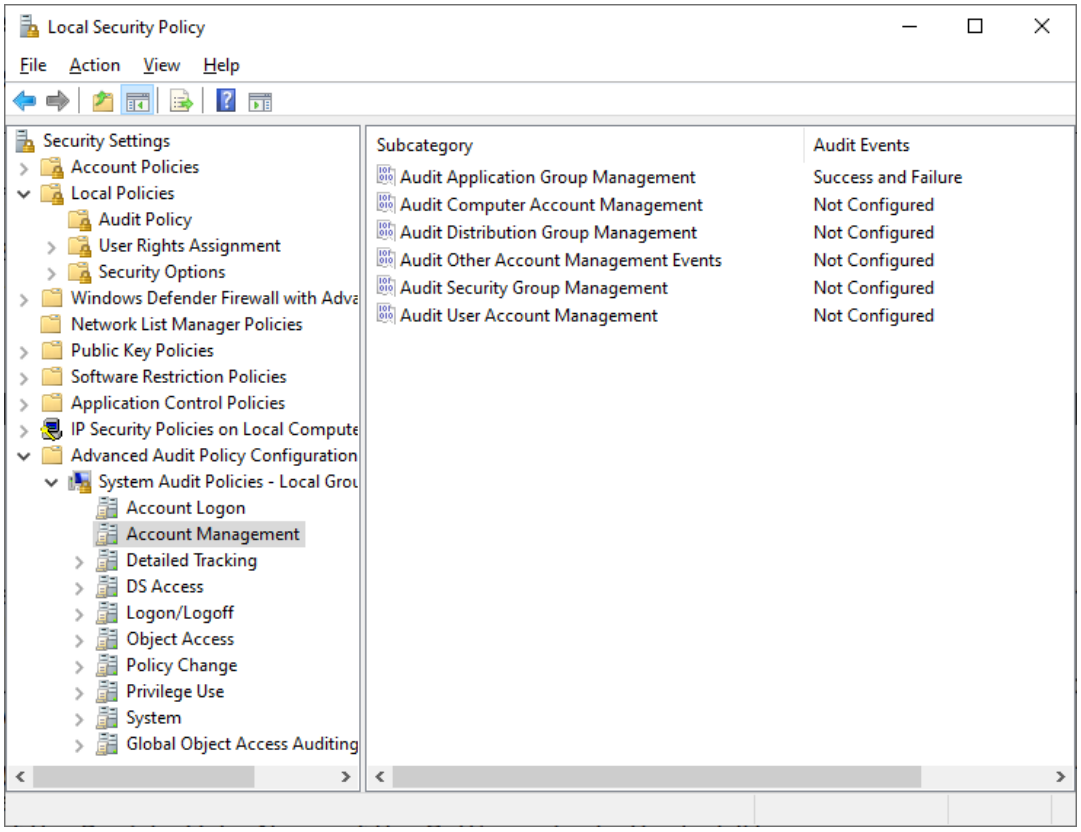


מה שאנו רואים כי יוגדר בצורה כללית מקבל פירוט אשר עוזר לנו להבין מה רמת התיעוד שניתן לקבל בצורה מפורטת יותר. במידה ונגדיר משהו על ה-Audit Policy הכללית, ההגדרה תוכל על כל תת ההגדרות שמפורטות ב Advenced Audit Policy - זאת נוכל לראות גם בקבצי audit.csv המתקבל ב-GPOBack-Up:

- System	MPSSVC Rule-Level Policy Change	{0CCE9232	No Auditing	0
- System	Other Account Management Events	{0CCE923A	Success and Failure	3
- System	Application Group Management	{0CCE9239	Success and Failure	3
- System	Distribution Group Management	{0CCE9238	Success and Failure	3
- System	Security Group Management	{0CCE9237	Success and Failure	3
- System	Computer Account Management	{0CCE9236	Success and Failure	3
- System	User Account Management	{0CCE9235	Success and Failure	3
- System	Directory Service Replication	{0CCE923D	No Auditing	0

במידה ולא נרצה התנהגות סטנדרטית של תיעוד עבור סעיפי התיעוד המפורט, ניתן יהיה להגדיר אותו בחלק המתאים ב-Advenced Audit Policy. ניתן לראות את אותן ההגדרות, אך בקובץ האקסל יש לנו אפשרות לשלוט עלייהן בצורה ברורה:

- יש לשים לב שהגדרה דרך Advenced Audit Policy דורסת את ההגדרות שהוחלו לאותה קטגוריה ע"י הגדרות ה-Audit Policy.



במידה ונבחן את קובץ ה-audit.csv שנקבל ב-GPOBack-Up נבחין כי יהיה תוכן רק במידה ויצרנו שינוי בהגדרות התיעוד הפרטניות (שכן אם צריך לכסות הגדרות כלליות נעשה זאת דרך קובץ ה inf.)

- בגלל ההגדרה הפרטנית שביצענו, ההגדרות הקודמות שנבעו מ-Audit Policy "נזנחו" והוגדרו ע"י Advenced Audit Policy.

3	System	Authorization Policy Change	{0CCE9231-	No Auditing		0
3	System	MPSSVC Rule-Level Policy Change	{0CCE9232-	No Auditing		0
3	System	Other Account Management Events	{0CCE923A-	No Auditing		0
3	System	Application Group Management	{0CCE9239-	Success and Failure		3
3	System	Distribution Group Management	{0CCE9238-	No Auditing		0
3	System	Security Group Management	{0CCE9237-	No Auditing		0
3	System	Computer Account Management	{0CCE9236-	No Auditing		0

LGPO.exe - Local GPO Utility

לאחר שהכרנו את קבצי ההגדרות הרלוונטים להגדרת תקן-הקשחה למשאב Windows, אפרט על אופן השימוש ב-LGPO. במאמר זה אדאג לפרט על יכולות LGPO 3.0 אשר מגיע בחבילת SCT 1.0. הזכרתי את הכלי מספר פעמים לפניכן וציינתי כי מטרתו של הכלי היא לאפשר GPOBack-Up. פעולות עיקריות:

- יצירת GPOBack-Up (פעולת Export) המכיל את כלל ההגדרות של משאב ה-Windows והמשתמשים - הן מקבצי registry.pol, audit.csv ו-GptTmpl.inf.
- ביצוע פעולת Import להגדרות הנ"ל במשאב Windows.
- החלת ערכי Registry על מערכת ההפעלה או קבוצות משתמשים.
- יצירת קבצי Registry.pol ע"י קבצתי טקסט בפורמט מתועד.

כעת, אתאר כיצד נוכל להשיגו ואת אופן השימוש בו.

LGPO 3.0

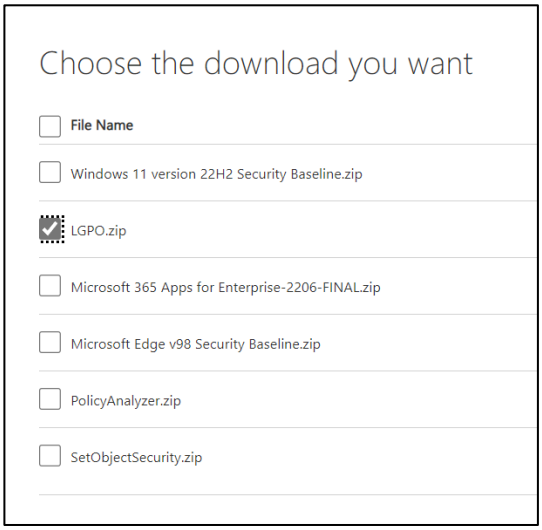
ב-LGPO3.0 ניתן למצוא מגוון רחב של פעולות:

```
LGPO.exe - Local Group Policy Object Utility
Version 3.0.2004.13001
Copyright (C) 2015-2020 Microsoft Corporation
Security Compliance Toolkit - https://www.microsoft.com/download/details.aspx?id=55319

LGPO.exe has four modes:
  * Import and apply policy settings;
  * Export local policy to a GPO backup;
  * Parse a registry.pol file to "LGPO text" format;
  * Build a registry.pol file from "LGPO text".
To apply policy settings:
    LGPO.exe command [...]
    where "command" is one or more of the following (each of which can be repeated):
    /g path                 import settings from one or more GPO backups under "path"
    /p path\lgpo.PolicyRules  import settings from a Policy Analyzer .PolicyRules file
    /m path\registry.pol    import settings from registry.pol into machine config
    /u path\registry.pol    import settings from registry.pol into user config
    /ua path\registry.pol   import settings from registry.pol into user config for Administrators
    /un path\registry.pol   import settings from registry.pol into user config for Non-Administrators
    /u:username path\registry.pol
                            import settings from registry.pol into user config for local user
                            specified by "username"
    /s path\GptTmpl.inf     apply security template
    /a[c] path\Audit.csv    apply advanced auditing settings; /ac to clear policy first
    /t path\lgpo.txt        apply registry commands from LGPO text
    /e <name>|<guid>        enable GP extension for local policy processing; specify a
                            GUID, or one of these names:
                            * "zone" for IE zone mapping extension
                            * "mitigation" for mitigation options, including font blocking
                            * "audit" for advanced audit policy configuration
                            * "LAPS" for Local Administrator Password Solution
                            * "DGVBS" for Device Guard virtualization-based security
                            * "DGCI" for Device Guard code integrity policy
    /ef path\backup.xml     enable GP extensions referenced in backup.xml from a GPO backup
    /boot                   reboot after applying policies
    /v                      verbose output
    /q                      quiet output (no headers)
To create a GPO backup from local policy:
    LGPO.exe /b path [/n GPO-name]
    /b path             Create GPO backup in "path"
    /n GPO-name         Optional GPO display name (use quotes if it contains spaces)
To parse a Registry.pol file to LGPO text (stdout):
    LGPO.exe /parse [/q] {/m|/u|/ua|/un|/u:username} path\registry.pol
    /m path\registry.pol   parse registry.pol as machine config commands
    /u path\registry.pol   parse registry.pol as user config commands
    /ua path\registry.pol  parse registry.pol as user config for Administrators
    /un path\registry.pol  parse registry.pol as user config for Non-Administrators
    /u:username path\registry.pol
                           parse registry.pol as user config for local user
                           specified by "username"
    /q                     quiet output (no headers)
```

הורדה

ניתן להוריד בצורה עדכנית מהאתר של Microsoft. יש לשים לב שהוא חלק מחבילת SCT1.0:



פעולות

אציג את הפעולות העיקריות שהגדרתי כחלק מביצוע הקשחה. פעולת גיבוי (Export) לכלל ההגדרות:

```
C:\[redacted]\OS Hardening Docs>LGPO.exe /b "C:\GPOBackups"

LGPO.exe - Local Group Policy Object Utility
Version 3.0.2004.13001
Copyright (C) 2015-2020 Microsoft Corporation
Security Compliance Toolkit - https://www.microsoft.com/download/details.aspx?id=55319

Creating LGPO backup in "C:\GPOBackups\{032C7664-1C21-4BEE-9A14-B414EAF11B13}"

C:\GPOBACKUPS
└───{032C7664-1C21-4BEE-9A14-B414EAF11B13}
    │   Backup.xml
    │   Bkupinfo.xml
    │
    └───DomainSysvol
        └───GPO
            ├───Machine
            │       registry.pol
            │
            │   └───microsoft
            │       └───windows nt
            │           ├───Audit
            │                   audit.csv
            │
            │           └───SecEdit
            │                   GptTmpl.inf
            │
            └───User
                    registry.pol
```

ניתן לי לראות כי השוני בין קבצי הגיבוי ל-Machine ו-User מתבטאים רק ב-registry.pol.

השוני נובע מהעובדה שרוב הגדרות אבטחת-מידע מוחלות על מערכת ההפעלה. דברים נוספים יוגדרו ב-registry.pol מתאים למשתמש:

```
C:\[redacted]\OS Hardening Docs>LGPO.exe /g "C:\GPOBackups\{032C7664-1C21-4BEE-9A14-B414EAF11B13}"

LGPO.exe - Local Group Policy Object Utility
Version 3.0.2004.13001
Copyright (C) 2015-2020 Microsoft Corporation
Security Compliance Toolkit - https://www.microsoft.com/download/details.aspx?id=55319

Registering Machine CSE: Audit, {F3CCC681-B74C-4060-9F26-CD84525DCA2A}
Registering User CSE: Registry Policy, {35378EAC-683F-11D2-A89A-00C04FBBCFA2}
Clearing existing audit policy
Apply Audit policy from C:\GPOBackups\{032C7664-1C21-4BEE-9A14-B414EAF11B13}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
Apply security template: C:\GPOBackups\{032C7664-1C21-4BEE-9A14-B414EAF11B13}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\GPOBackups\{032C7664-1C21-4BEE-9A14-B414EAF11B13}\DomainSysvol\GPO\Machine\registry.pol
Import User settings from registry.pol: C:\GPOBackups\{032C7664-1C21-4BEE-9A14-B414EAF11B13}\DomainSysvol\GPO\User\registry.pol
```

- פעולת ייבוא (Import) להגדרות (אוסף הקבצים) הנמצאים בגיבוי הנתון. ניתן לראות שקיבלנו חיווי מתאים לטעינת הקבצים הרלוונטים.
  - כמוכן, ניתן לראות כי נטענו קבצי CSE - קבצים אלו מוגדרים ב-manifest.xml שמגיע ב-GPOBack Up כאשר הגדרות אבטחת-מידע נוספות הוחלו עלייה.
  - הצורך בקובץ manifest.xml נדרש בכדי לאפשר לתוכנת Microsoft להכיר את סוגי ההגדרות השונות ושיוכן המתאים ליכולות נוספות במשאבי Windows (מעבר להגדרות מערכת הפעלה ומשתמשים).
  - למשל, עבור Windows11 נמצא ברשימה את:

Policy Name	Policy Type	File name
MSFT Windows 11 - BitLocker	Computer	registry.pol
MSFT Windows 11 - Defender Antivirus	Computer	registry.pol
MSFT Windows 11 - Credential Guard	Computer	registry.pol
MSFT Windows 11 - User	User	registry.pol
MSFT Windows 11 - Computer	Computer	registry.pol
MSFT Internet Explorer 11 - User	User	registry.pol
MSFT Internet Explorer 11 - Computer	Computer	registry.pol
MSFT Windows 11 - Domain Security	Sec Template	GptTmpl.inf
MSFT Windows 11 - BitLocker	Sec Template	GptTmpl.inf
MSFT Windows 11 - Computer	Sec Template	GptTmpl.inf
MSFT Internet Explorer 11 - Computer	Sec Template	GptTmpl.inf
MSFT Windows 11 - Computer	Audit Policy	audit.csv
*** Group policy client-side extension: Group Policy Mitigation Options	CSE-Machine	{2A8FDC61-2347-4C87-92F6-B05EB91A201A}
*** Group policy client-side extension: Registry Policy	CSE-Machine	{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
*** Group policy client-side extension: Security	CSE-Machine	{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
*** Group policy client-side extension: Local Administrator Password Solution (LAPS)	CSE-Machine	{D76B9641-3288-4F75-942D-087DE603E3EA}
*** Group policy client-side extension: Device Guard	CSE-Machine	{F312195E-3D9D-447A-A3F5-08DFFA24735E}
*** Group policy client-side extension: Audit Policy Configuration	CSE-Machine	{F3CCC681-B74C-4060-9F26-CD84525DCA2A}
*** Group policy client-side extension: Registry Policy	CSE-User	{35378EAC-683F-11D2-A89A-00C04FBBCFA2}

- פעולה ליצירת Registry.pol באמצעות קובץ טקסט בפורמט מתאים:

```
To build a Registry.pol file from LGPO text:

    LGPO.exe /r path\lgpo.txt /w path\registry.pol [/v]

    /r path\lgpo.txt      Read input from LGPO text file
    /w path\registry.pol  Write new registry.pol file

    /m path\registry.pol      import settings from registry.pol into machine config
    /u path\registry.pol      import settings from registry.pol into user config
    /ua path\registry.pol     import settings from registry.pol into user config for Administrators
    /un path\registry.pol     import settings from registry.pol into user config for Non-Administrators
    /u:username path\registry.pol
                              import settings from registry.pol into user config for local user
                              specified by "username"
```

1. ישנן פעולות נוספות כגון פעולות לטעינת Registry.pol ל-Machine או User (ניתן גם לטעון לקבוצות שצוינו מקודם) או פעולה לטעינת קובץ טקסט בפורמט מתאים ל-Registry.

דוגמאות שימוש

כפי שראינו בתיעוד הכלי, נוכל לקבל דינאמיות להחיל ולהגדיר קבצים אשר מהווים את אוסף הגדרות אבטחת-המידע שנרצה:

- LGPO /g <path> - יחיל את אוסף ההגדרות שנמצא בתיקיית ה-GPO Backup - הכוללת את הקבצים: GptTmpl.inf, Registry.pol, audit.csv.
  - ניתן להחיל את הקבצים בצורה עצמאית ע"י הפקודות /s, /a, /t המפורטות ב-LGPO.

- LGPO /p <path> - יחיל את אוסף ההגדרות הנמצא בפורמט PolicyRules.
  - זהה למצב המערכת בביצוע /g רק על קובץ PolicyRules.

- LGPO /m <path> - יחיל קובץ registry.pol בעל הגדרות מערכת הפעלה.

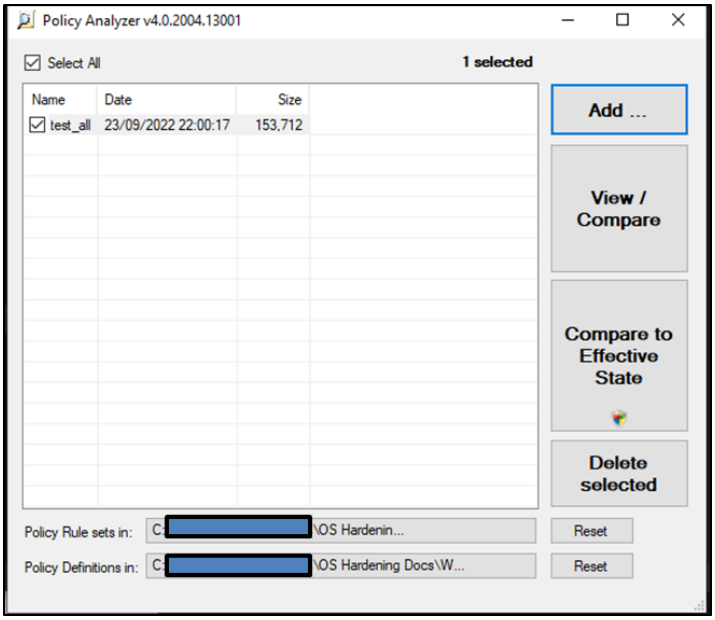
- LGPO /u < path> - יחיל קובץ registry.pol בעל הגדרות על משתמש.
  - ניתן לייחס לקבוצות משתמשים שונות.

- ל-LGPO יש גם יכולות לייצר קובץ registry.pol מתוך קובץ טקסט המתואר לפי פורמט קבוע
  - ניתן למצוא אותו בתיאור של LGPO המגיע בהורדה בחבילת SCT1.0.

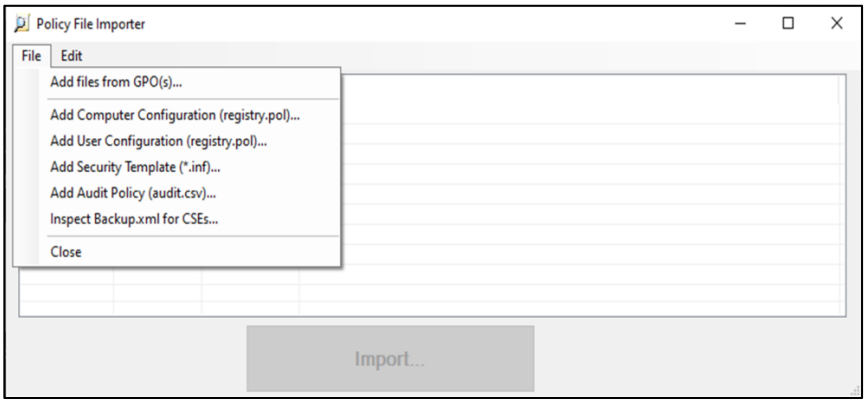
SCT 1.0

לאחר שהכרנו את השימושים השונים שנעשה עם LGPO נרצה לראות כיצד נוכל לראות את ההגדרות שלנו מבקורות ע"י הכלים של Microsoft. לשם כך ארחיב על הכלים הנוספים בחבילת SCT 1.0.

Policy Analyzer



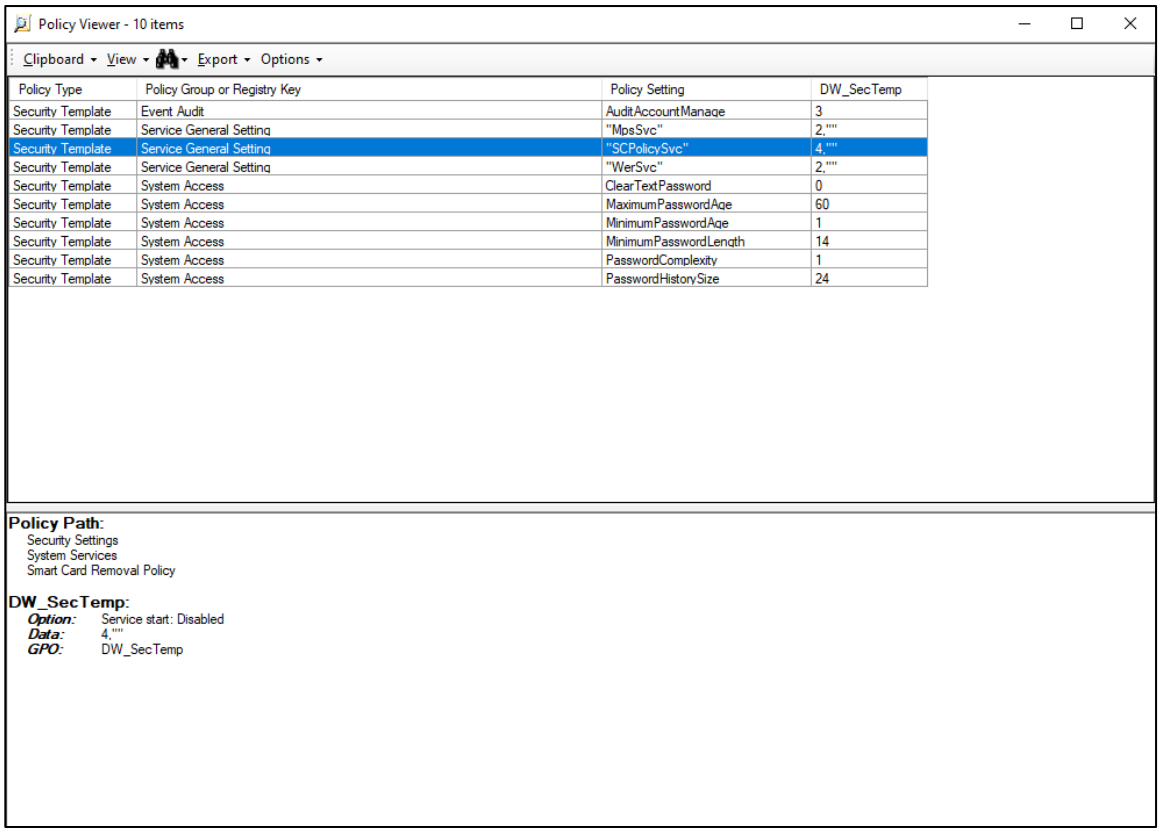
הכלי הנ"ל יאפשר טעינת הגדרות ע"י טעינה של GPOBackUp או ע"י קבצים נפרדים. לשם כך, בחלון הראשי נלחץ על כפתור "Add":



נטען לדוגמא את קובץ ה-GptTmpl.inf שיצרנו בחלק של הסבר ונראה כיצד נוכל **לבקר** את הסעיפים לדוגמה שסקרנו.

- שימו לב שהתווסף לנו קובץ לרשימה ב-Policy Analyzer ע"פ השם שספקנו בתהליך טעינת הקובץ. הקובץ שהצטרף הוא מסוג PolicyRules ומהווה את כלל הגדרות שנטענו מקובץ הגדרות.
- קבצי PolicyRules יכולים לשמש להקשחה ובקרה עבור משאבי Windows הנתמכים ב-SCT.
  - ניתן להשתמש ב-LGPO3.0 בכדי להחילם על משאב Windows (**פעולת הקשחה**)

נוכל לשים לב כי הכלי מזהה את הקבצים שהגדרנו בצורה מתאימה ויודע לשייך את ההגדרות לנושא המתאים:

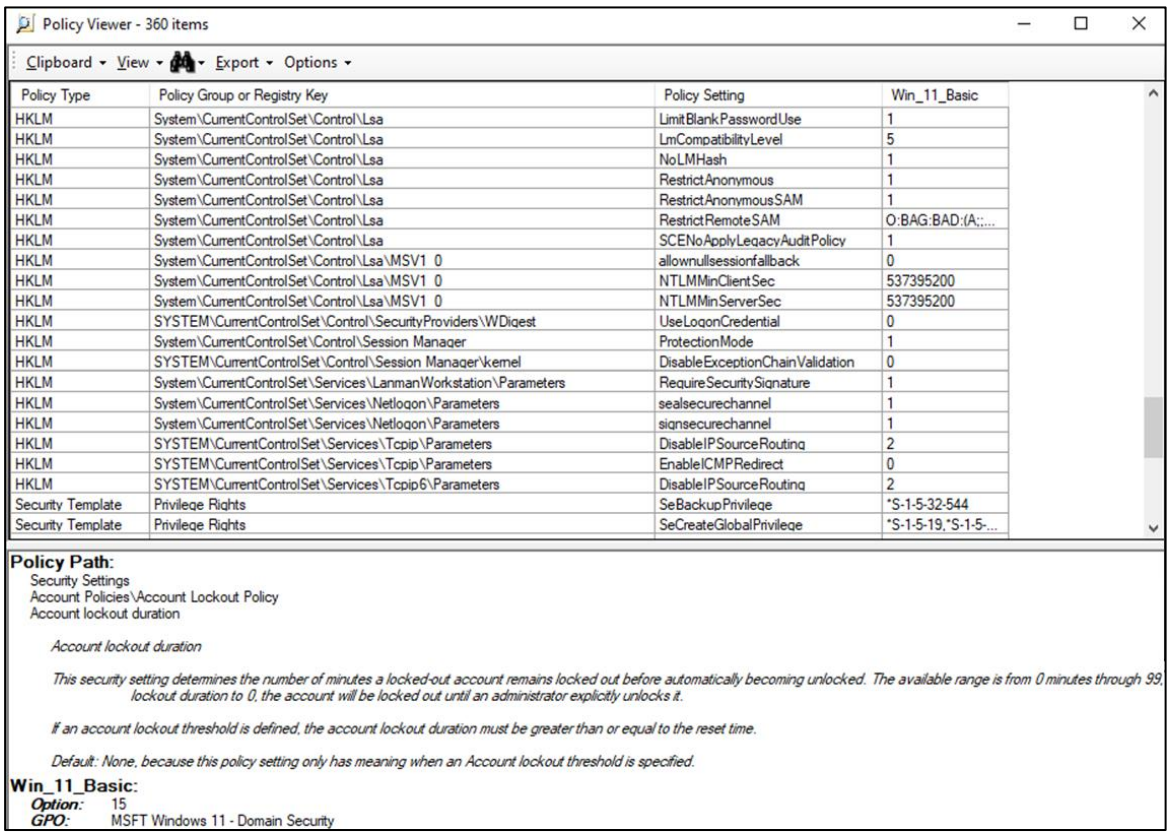


בנוסף, שימו לב שניתן לראות פירוט על הסעיפים (בחלק התחתון של התמונה) ברמה ברורה יותר מרק להגדיר קבועים המסמלים הגדרות במשאבי Windows.

Policy Name	Policy Type	File name
MSFT Windows 11 - BitLocker	Computer	registry.pol
MSFT Windows 11 - Defender Antivirus	Computer	registry.pol
MSFT Windows 11 - Credential Guard	Computer	registry.pol
MSFT Windows 11 - User	User	registry.pol
MSFT Windows 11 - Computer	Computer	registry.pol
MSFT Internet Explorer 11 - User	User	registry.pol
MSFT Internet Explorer 11 - Computer	Computer	registry.pol
MSFT Windows 11 - Domain Security	Sec Template	GptTmpl.inf
MSFT Windows 11 - BitLocker	Sec Template	GptTmpl.inf
MSFT Windows 11 - Computer	Sec Template	GptTmpl.inf
MSFT Internet Explorer 11 - Computer	Sec Template	GptTmpl.inf
MSFT Windows 11 - Computer	Audit Policy	audit.csv

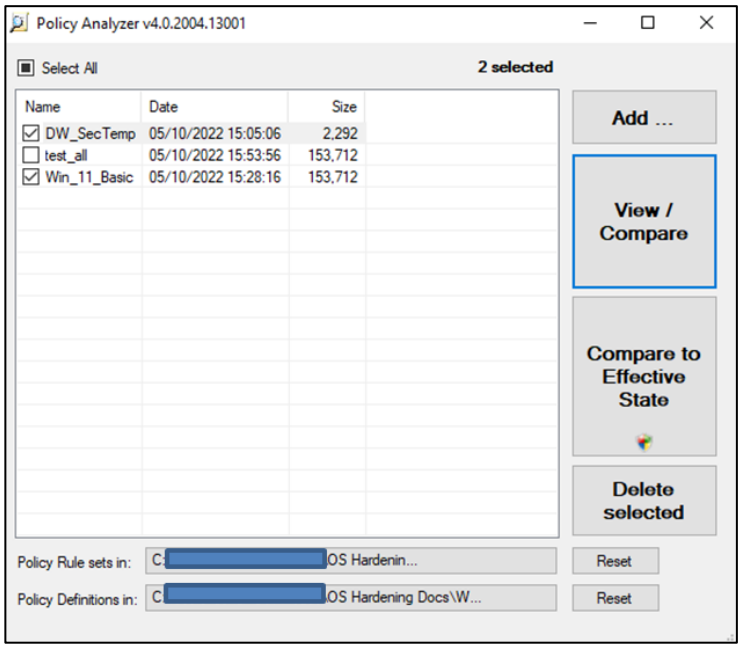
במידה ונטען GPOBackUp מתאימים של Microsoft ל-PolicyAnalyzer (לא נטען את כל ההגדרות אלא רק מה ששקול למשאב Windows 11 בסיסי).

נוכל לראות את אוסף כלל ההגדרות ש-Microsoft ממליצה להחיל למשאב Windows 11 בסיסי:

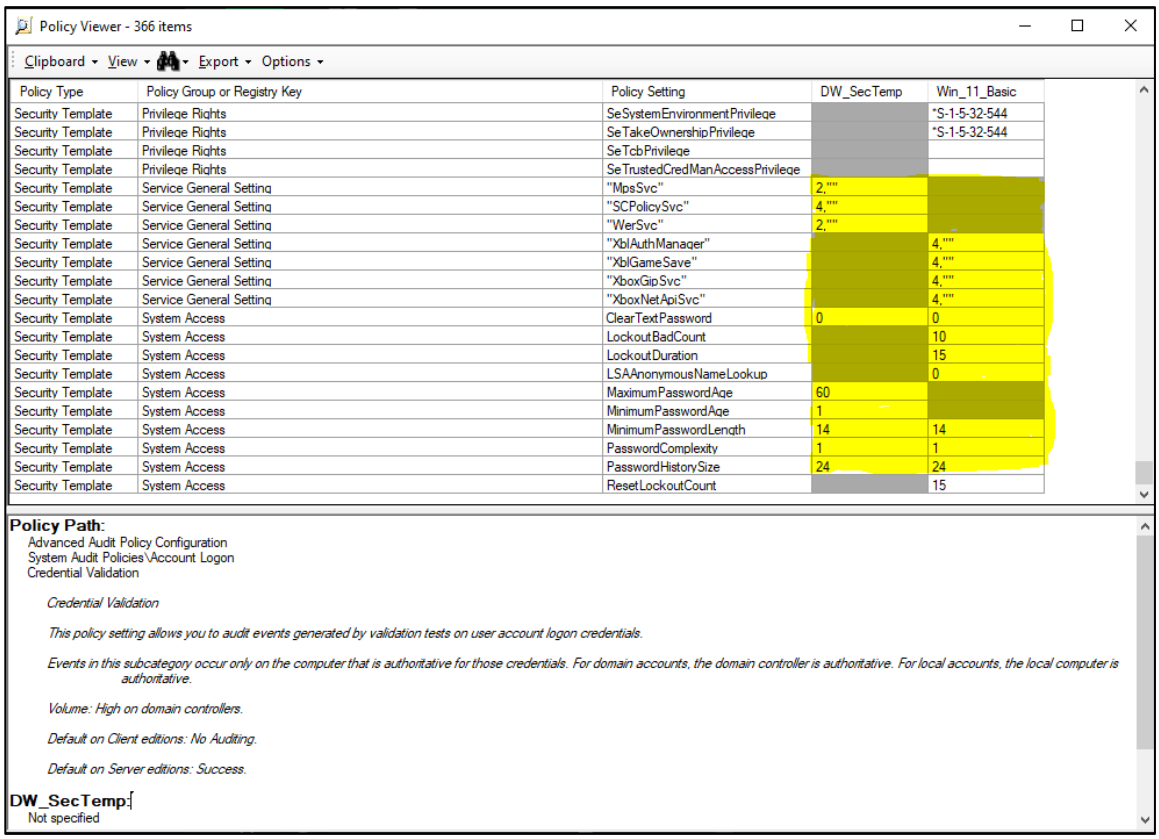


Compare/View

נוכל להשוות בין 2 קלטים (או יותר) על מנת להעזר ב-PolicyAnalyzer בכדי לראות את ההבדלים המהותיים בין 2 סוגי הגדרות שטענו:



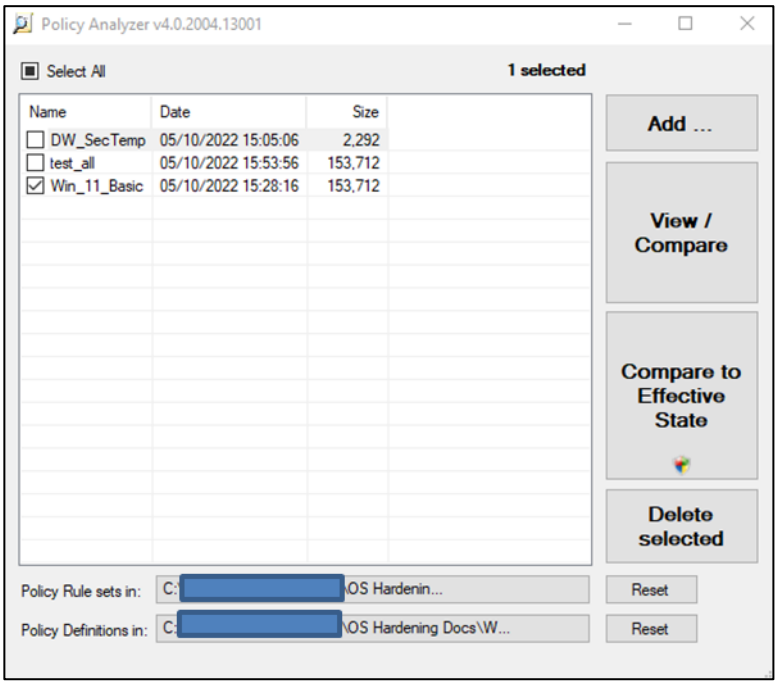
למשל נבחן את אוסף ההגדרות שבחנו בפרקים הקודמים אל מול אוסף ההגדרות המומלצות ע"י Microsoft להקשחה בסיסית ל-Windows 11. לאחר מכן נוכל לראות את כל מה ששונה בין 2 הקבצים:



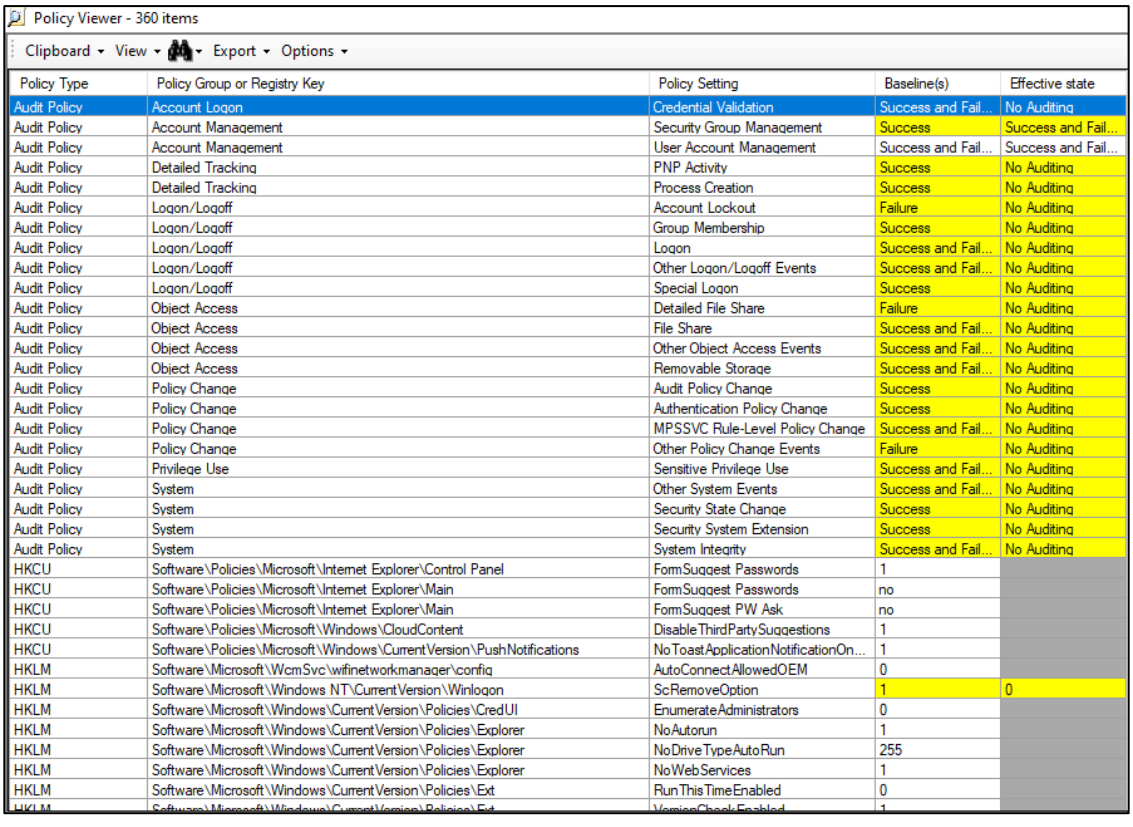
- ניתן לראות את השירותים שהגדרנו וחלק מהגדרות הסמא שהוצגו במאמר.
- שדה אפור מראה כי יש חוסר בהגדרה של השדה המוצג באחד מאוספי ההגדרות (תקן הקשחה / בקרה)
- בהמשך המאמר אציג כיצד נוכל להעזר ביכולות של PolicyAnalyzer בכדי להתמקד בשוני הקיים בין 2 אוספי הגדרות.

Compare to Effective State

באמצעות הפעולה הנ"ל (לעיתים דורשת הרשאות מנהל בהתאם לקבצי הסריקה) נוכל להשוות את מצב משאב ה-Windows דרכו אנחנו מריצים את PolicyAnalyzer לאוסף הגדרות שבחרנו מתוך מה שנטען ל-PolicyAnalyzer.



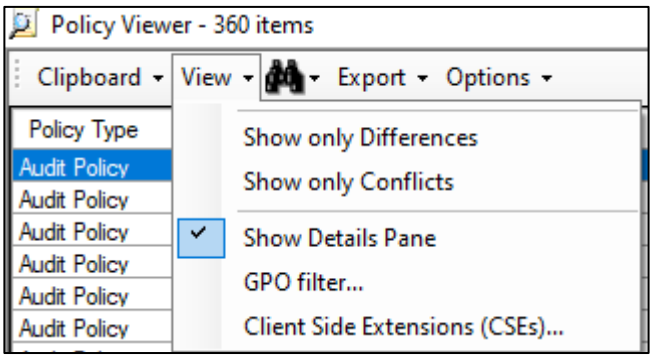
לצורך הדוגמה נריץ השוואה של הגדרות Windows 10 ל-Windows 11. ונקבל:



Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	No Auditing
Audit Policy	Account Management	Security Group Management	Success	Success and Fail...
Audit Policy	Account Management	User Account Management	Success and Fail...	Success and Fail...
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	No Auditing
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Logon	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Special Logon	Success	No Auditing
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	Audit Policy Change	Success	No Auditing
Audit Policy	Policy Change	Authentication Policy Change	Success	No Auditing
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Audit Policy	Policy Change	Other Policy Change Events	Failure	No Auditing
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	No Auditing
Audit Policy	System	Other System Events	Success and Fail...	No Auditing
Audit Policy	System	Security State Change	Success	No Auditing
Audit Policy	System	Security System Extension	Success	No Auditing
Audit Policy	System	System Integrity	Success and Fail...	No Auditing
HKCU	Software\Policies\Microsoft\Internet Explorer\Control Panel	FormSuggest Passwords	1	
HKCU	Software\Policies\Microsoft\Internet Explorer\Main	FormSuggest Passwords	no	
HKCU	Software\Policies\Microsoft\Internet Explorer\Main	FormSuggest PW Ask	no	
HKCU	Software\Policies\Microsoft\Windows\CloudContent	DisableThirdPartySuggestions	1	
HKCU	Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications	NoToastApplicationNotificationOn...	1	
HKLM	Software\Microsoft\WcmSvc\wifinetworkmanager\config	AutoConnectAllowedOEM	0	
HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ScRemoveOption	1	0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\CredUI	EnumerateAdministrators	0	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoAutorun	1	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoDriveTypeAutoRun	255	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoWebServices	1	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Ext	RunThisTimeEnabled	0	

ניתן להבחין כי קיימים המון שדות המודגשים בצהוב - שדות אלו מדגישים Conflict (התנגשות) בין הערך בעמודת ה-Baseline ל-Effective state (עמודה שנוצרה בגלל רצוננו לבצע Compare to effective state).

נוכל בהתאם לייצא דו"ח רק של הפערים באמצעות תפריט View:



או, לייצא דו"ח רק של השוני באמצעות Show only Differences:

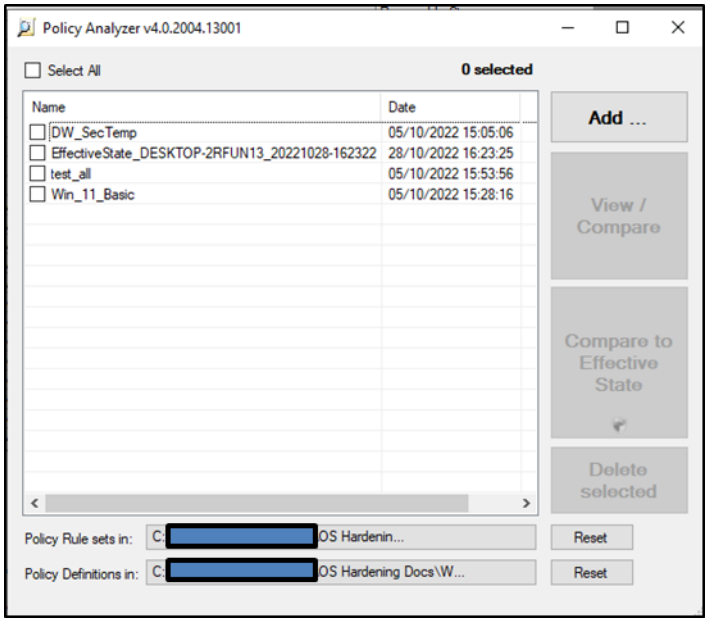
Policy Viewer - 319 items

Clipboard ▾ View ▾ Export ▾ Options ▾

Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	No Auditing
Audit Policy	Account Management	Security Group Management	Success	Success and Fail...
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	No Auditing
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Logon	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Special Logon	Success	No Auditing
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	Audit Policy Change	Success	No Auditing
Audit Policy	Policy Change	Authentication Policy Change	Success	No Auditing
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Audit Policy	Policy Change	Other Policy Change Events	Failure	No Auditing
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	No Auditing
Audit Policy	System	Other System Events	Success and Fail...	No Auditing
Audit Policy	System	Security State Change	Success	No Auditing
Audit Policy	System	Security System Extension	Success	No Auditing
Audit Policy	System	System Integrity	Success and Fail...	No Auditing
HKCU	Software\Policies\Microsoft\Internet Explorer\Control Panel	FormSuggest Passwords	1	
HKCU	Software\Policies\Microsoft\Internet Explorer\Main	FormSuggest Passwords	no	
HKCU	Software\Policies\Microsoft\Internet Explorer\Main	FormSuggest PW Ask	no	
HKCU	Software\Policies\Microsoft\Windows\CloudContent	DisableThirdPartySuggestions	1	
HKCU	Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications	NoToastApplicationNotificationOn...	1	
HKLM	Software\Microsoft\WcmSvc\wifinetworkmanager\config	AutoConnectAllowedOEM	0	
HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ScRemoveOption	1	0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\CredUI	EnumerateAdministrators	0	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoAutorun	1	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoDriveTypeAutoRun	255	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoWebServices	1	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Ext	RunThisTimeEnabled	0	
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Ext	VersionCheckEnabled	1	

- שימו לב כי יש 319 סעיפים שונים (או שלא הוגדרו או שיש Conflict).
- מכאן, ניתן להבין כי כ-40 חוקים היו זהים (באוסף הגדרות מומלצות ל-Windows 11 יש כ-360 חוקים).

שימו לב שבעת לחיצה על Compare to Effective State יצטרף לממשק PolicyAnalyzer קובץ המכיל את כל ההגדרות המוצגות לאחר פעולת ההשוואה.



בעת שנגיע למצב הרצוי מבחינת אוסף החוקים שהכלנו באמצעות SCT, נוכל להשתמש בקובץ PolicyRules (אשר ימצא בתיקייה המצויינת בשדה Policy Rule sets in: בממשק PolicyAnalyzer) בכדי להחיל את כלל ההגדרות באמצעות קובץ בודד ופקודת LGPO מתאימה (/p).

Policy Viewer - 79 items

Clipboard ▾ View ▾ Export ▾ Options ▾

Policy Type	Policy Group or Registry Key	Policy Setting	EffectiveState_DE
Audit Policy	Account Logon	Credential Validation	No Auditing
Audit Policy	Account Management	Security Group Management	Success and Fail...
Audit Policy	Account Management	User Account Management	Success and Fail...
Audit Policy	Detailed Tracking	PNP Activity	No Auditing
Audit Policy	Detailed Tracking	Process Creation	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	No Auditing
Audit Policy	Logon/Logoff	Group Membership	No Auditing
Audit Policy	Logon/Logoff	Logon	No Auditing
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	No Auditing
Audit Policy	Logon/Logoff	Special Logon	No Auditing
Audit Policy	Object Access	Detailed File Share	No Auditing
Audit Policy	Object Access	File Share	No Auditing
Audit Policy	Object Access	Other Object Access Events	No Auditing
Audit Policy	Object Access	Removable Storage	No Auditing
Audit Policy	Policy Change	Audit Policy Change	No Auditing
Audit Policy	Policy Change	Authentication Policy Change	No Auditing
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	No Auditing
Audit Policy	Policy Change	Other Policy Change Events	No Auditing
Audit Policy	Privilege Use	Sensitive Privilege Use	No Auditing
Audit Policy	System	Other System Events	No Auditing
Audit Policy	System	Security State Change	No Auditing
Audit Policy	System	Security System Extension	No Auditing
Audit Policy	System	System Integrity	No Auditing
HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ScRemoveOption	0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorAdmin	5
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorUser	3
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableInstallerDetection	1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableLUA	1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableSecureUIAPaths	1

במידה ונבחן את אוסף החוקים הנמצאים בקובץ ה-EffectiveState נראה כי הוא מכיל 79 חוקים שנמצאו בחפיפה מול ההגדרות המומלצות ל-Windows 11. (רק הגדרות אבטחה שהוגדרו יוצגו)

סיכום

הגדרת תקן הקשחה

בחלק הראשון של המאמר למדנו על קבצי ההגדרות של Windows אשר יאפשרו לנו שליטה על הגדרות שונות שנרצה להחיל במשאב Windows. הגדרות האבטחה המומלצות ניתן למצוא גם ב-Microsoft (כחלק מחבילת SCT1.0) וגם ב-NCP (National Checklist Program).

בנוסף, אם נבחן את תקן CIS נראה הוראות ברורות לאילו ערכים צריך לעדכן בכדי לקבל את מענה האבטחה ההולם לצרכינו. בהינתן אוסף הקבצים אשר מכיל את הגדרות האבטחה המומלצות נוכל להמשיך לתהליך ההקשחה והבקרה.

תהליך הקשחה

בהנחה ויש לנו את קבצי ההגדרות באחת מן התצורות הבאות:

- GptTmpl.inf, Registry.pol, audit.csv
- Registry_formatted.txt
- HardenGuide.PolicyRules

נוכל להשתמש בפקודות של תוסף ה-LGPO (המגיע כחלק מ-SCT1.0) בכדי להחיל את הקבצים על ממשקי ההגדרות השונים במשאב Windows. שלב זה מבטיח שינוי הגדרות במשאב ה-Windows בהתאם למפורט בקבצים.

תהליך בקרה

כלי ה-PolicyAnalyzer מאפשר טעינה של קבצי הגדרות (בדומה לאוסף שתואר ב"תהליך הקשחה"). כאשר אוספי הגדרות טעונים בו נוכל לבצע השוואה שטחית בין האוספים הטעונים (Compare/View). במידה ונרצה לבצע בקרה המתאימה לאוסף הגדרות שטענו (תקן ההקשחה) נוכל לבצע השוואה אל מול אוסף ההגדרות הקיימות בעמדה (Compare to Effective State).

על המחבר

בעל תואר ראשון בהנדסת תכנה, עוסק כמהנדס פתרונות אבטחת-מידע. חוקר ומיישם יכולות לאוטומצית תהליכי הקשחה ובקרה ארגוניים. מתעניין ובוחן איומי סייבר שונים לצורכי מחקר ומענה.