**CyScore**

אפיון פרויקט גמר

שמות הסטודנטים: (ת.ז. אימייל וטלפון):

1. אלמוג שמעון – 207921149, 0502800038, [almogsh98@gmail.com](mailto:almogsh98@gmail.com)
2. עמית קסטל – 208108365, 0545358441, amitkastel3@gmail.com

התמחות: סייבר

מאשר הפרויקט: יניב ברקאי

קישור לגיט: -

# תוכן עניינים

Contents

[תוכן עניינים 2](#_Toc99663966)

[תיאור הפרויקט 3](#_Toc99663967)

[ארכיטקטורה 4](#_Toc99663968)

[פירוט טכני 5](#_Toc99663969)

# תיאור הפרויקט

מערכת אשר מאפיינת, מנטרת ומנתחת את חוסן העמדות ברשת מקומית ומציגה תמונה כוללת של מצב העמדה בפרט ומצב הרשת בכלל באמצעות dashboards נוחים להבנה עבור המשתמש.

על כל עמדה יותקן Agent שתפקידו לדווח נתונים שהוגדרו לו מראש לשרת מרכזי שינתח, יבצע חיתוכים ואנליזות על המידע ויציג ב- dashboard למשתמש את הציון שהמערכת ניתחה והפיקה בנוגע לרמת האבטחה בתחנה. כמו כן, המערכת תציג המלצות לשיפור רמת האבטחה בהתאם לנתונים שנחקרו.

המערכת תשכלל את כלל הנתונים ותציג רמת אבטחה כוללת של הרשת בהתבסס על המידע ומסקנות שיפור רמת האבטחה בעמדות הקצה.

סוכן המערכת מבצע בדיקות מקומיות על עמדות הקצה בלבד ללא בדיקות בשרתים ורכיבים נוספים ברשת.

# ארכיטקטורה

Diagram

Description automatically generated

המערכת שלנו בנויה מעמדות קצה, שרת ריכוז נתונים, מסד נתונים וצד Front.

**עמדות קצה -**  בעמדות הקצה יותקן Agent שיאסוף נתונים, יבצע המרה לפורמט Json אחיד ולבסוף יבצע שליחה לשרת ריכוז הנתונים לניתוח והפקת תובנות.  
הAgent ייכתב בשפת C# וישתמש ביכולות של .NET כדי למשוך את הנתונים מן העמדה.   
לאחר איסוף המידע מהתחנה הAgent ישלח את המידע לשרת על גבי פרוטוקול HTTP בכדי לבצע אנליזות וחיתוכים.

**מסד נתונים** – מסד הנתונים יהיה על גבי SQL Server – בו ירוכז כלל המידע שהועבר מהתחנות.

**שרת –** השרת ייכתב בשפת C# וישתמש בטכנולוגיות הבאות:

1. **.Net Core** – Framework קוד פתוח מודולרי, אשר חוצה פלטפורמות ומשמש לבניית יישומי Web, Windows ונייד עבור מ"ה Windows, Linux וOS. Framework זה תשמש אותנו לצורך כתיבת ה-API , כתיבת ה-Agent ובגישה נוחה למשאבים של מערכת ההפעלה ה-windows-ית. .Net מספקת אבסטרקציה מעל מספר APIs של windows שבהן נוכל להשתמש לגישה לערכי Registry או לFilesystem לדוגמה.
2. **Web API** – Framework שרץ מעל .Net ובו נשתמש על מנת לתכנת את התקשורת של הAgent אל מול שרת ריכוז הנתונים והמשתמש אל מול צד הFront.
3. **Entity framework/ADO.NET** – מכיל מחלקות ופונקציות לביצוע אינטראקציה מול מסדי נתונים. ספרייה זו מאפשרת לנו למפות טבלאות SQL לתוך Enumerables ואובייקטים בC#. כך נוכל לעבוד עם הטבלאות והרשומות המצויות בSQL Server ישירות מתוך הקוד.

**צד לקוח –** ייכתב ב-React ויפעל כ-Single page application. React - ספריית קוד פתוח בשפת JavaScript המשמשת לבניית ממשקי משתמש. בעזרת React ובספריות המתאימות לו נוכל ליצור ממשק משתמש נוח ושמיש בקלות ובמהירות.

# 

# פירוט טכני

**אפליקציית המערכת מורכבת מדפי הFront הבאים:**

* 1. **דף Login** – הדף יכלול תיבות להכנסת שם משתמש וסיסמא.  
     הפרטים שהוכנסו ייבדקו אל מול פרטי המשתמשים ששמורים במסד הנתונים.

ראשית, נבדוק האם קיים משתמש בשם שהוכנס בדף ה-Login אל מול מסד הנתונים ובמידה וכן, האם הסיסמא שהוכנסה תואמת את הסיסמה ששמורה.  
סיסמת המשתמש תשמר כ-hash במסד הנתונים.

* 1. **דף סטטוס (תמונת מצב) כללי על הרשת** – רשימת עמדות מנוטרות בארגון, עמדות בעל ציון שלילי גבוה, וכן ציון כולל לרשת שיתבסס ויחושב על סמך כלל העמדות בהם מותקן הסוכן.

דף זה נותן למשתמש אינדיקציה לתשובה לשאלה - האם יש צורך במבט מעמיק על העמדה?

* 1. **מבט עומק על עמדה** – יוצגו הפרטים הבאים:
     1. פרטים מזהים עבור כל עמדה – כמו : IP,MAC,Hostname.
     2. כלל הפוליסות והסטטוס שלהן כאשר בראש העמוד יוצגו הפוליסות שבהם העמדה לא עומדת וציון העמדה. כל מנתח ומעריך סיכונים יוכל להבין מתמונת מצב זו על העמדה כיצד לתעדף את הטיפול בכלל הרשת לאחר שכלול הנתונים עבור כל עמדה בנפרד.
  2. דף שמכיל את **כלל הפוליסות שנבדקות במערכת** – על ידי פירוט זה יוכל להבין משתמש המערכת האם נדרש לבצע עדכון ושדרוג של הפוליסות למתקפות ואיומים חדשים שאינם קיימים בפוליסות הנוכחיות או שיקבל תמונת מצב שהפוליסות מכסות את מרבית האיומים הפוטנציאליים.
  3. **דף סטטיסטיקות** – דף זה יספק תמונת מצב מהירה ואפקטיבית של הנתונים לדרגי הנהלה על ידי הצגת סטטיסטיקות בנוגע לפוליסות שלא עומדות ביעדים במחשבים בהם מותקן הAgent. לדוגמה:
     1. כמות עמדות קצה שעומדות/לא עומדות בכל פוליסה.
     2. שלושת הפוליסות הנפוצות שבהן הכי הרבה עמדות קצה לא עומדות.
     3. חיתוכים של עמדות קצה לפי גרסת מע"ה – כמה עמדות windows7? כמה windows10? וכו'..

**עמדות – Agents:**

* 1. **הפצת הAgent**:
     1. הפצת הסוכן תתבצע באופן ידני. קובץ הAgent הינו קובץ הרצה אשר ירוץ ברקע ללא הפרעה למשתמש.
     2. בהרצתו הראשונה, יצור הAgent- משימה מתוזמנת (בtask scheduler) שתריץ אותו באופן אוטומטי אחת לשעה.
  2. **תפקידי ה-Agent:**
     1. **יצירת תעודת זהות לעמדת הקצה.**בעת ריצתו, יאסוף הסוכן פרטיי מידע כדוגמת כתובת IP,כתובת MAC,hostname, ,username, גרסת מ"ה וכו' על מנת ליצור תעודת זהות לעמדה, אשר תוצג בדף העומק על העמדה.

בנוסף, יוצגו פורטים פתוחים על כל עמדה שבסבירות יכולים לשמש לLateral Movement, הזלגת מידע והסלמת הרשאות (SSH, SMB, RDP).

* + 1. **איסוף נתונים עבור פוליסות האבטחה והחיתוכים שינותחו בשרת ריכוז הנתונים ויוצגו בדפי הFront:** 
       1. בדיקת הימצאות של תוכנות אנטי וירוס המותקנות על העמדה – במידה ומותקנות, נציג בעמוד העמדה את שמות התוכנות.
       2. בדיקת סטטוס ההפעלה של הwindows defender – נצפה לראות שהתוכנה פעילה. את סטטוס ההפעלה נציג בעמוד העמדה.
       3. האם למשתמש Guest בעמדה יש הרשאות Administrator?
       4. האם העמדה מכילה hotfix משלושת החודשים האחרונים?   
          hotfix הינו עדכון תוכנה/אבטחה אשר בא לפתור בעיה ספציפית.
       5. האם ישנם נתיבי services אשר פגיעים לניצול על ידי חולשת  
          "unquoted service"?
       6. האם בוטל מנגנון הUAC במחשב? מנגנון זה מחייב הכנסת פרטי משתמש עם הרשאות Admin בעת ניסיון הרצת תוכנות שדורשות הרשאות אלו. כך מונע המנגנון ממשתמשים רגילים להריץ תוכנות בהרשאות Admin.
       7. האם מוגדר הLevel protection של תהליך ה-Lsass ברמה הנדרשת?
       8. האם קיימים סקריפטים -vbs/bat בנתיבים בהם תוקפים ישתמשו לרוב למטרת שרידות? למשל:
          1. תיקיית startup – תיקייה שבה ירוצו קבצים באופן אוטומטי בעת הפעלת המחשב.
          2. ערכי registry כדוגמת "Run"\”RunOnce” אשר גם בהם יוגדרו נתיבים לקבצים שירוצו בעת התחברות המשתמש למחשב.  
             Run – יריץ את התוכנה בכל פעם שהמשתמש יתחבר למחשב.  
             RunOnce – יריץ את התוכנה בפעם הראשונה שבה יתחבר המשתמש למחשב ולאחר מכן הערך ימחק. את הערכים הנ"ל ניתן להגדיר עבור משתמש או מכונה.  
             \* נשים לב כי ישנן תוכנות לגיטימיות שירוצו תחת נתיבים אלו ולכן נבצע הערכה לתקינות הקבצים בהתאם לכמות הסקריפטים.
       9. האם קיימים נתיבים או תוכנות הנמצאות המוגדרות תחת ההחרגות של ה-windows defender? (windows defender excludes).
    2. **איסוף המידע** – הסוכן יאסוף את המידע עבור הפוליסות ממקורות המידע הבאים:
       1. ערכי Registry.
       2. File System.
       3. Process List.
       4. הסתכלות על פורטים פתוחים בעמדה.
    3. **אופן שליחת הנתונים** – תוך כדי ריצתו של ה-Agent הוא ישלח את הנתונים הנאספים לשרת ריכוז הנתונים בזמן אמת (הנתונים לא יישמרו על דיסק עמדת הקצה והאיסוף יתבצע בזיכרון).