מגישים:
נתנאל לוי
שקד בנו
רונן ועלני

מנחה:
רועי זימון

SIEM
מערכת ניטור קורלציות לאירועי אבטחת מידע

שנה"ל תשפ"ב, סמסטר אביב – 2022

מכון טכנולוגי חולון
Holon Institute of Technology

תקציר-מהי מערכת SIEM ?

SIEM היינה מערכת ניהול אבטחת מידע ואירועים

המערכת מקבלת נתונים ולוגים מ- Clients שמפוזרים ברחבי הרשת הארגונית, במקביל לקבלת הנתונים מה- Clients בזמן אמת המערכת מבצעת ניתוח של המידע המתקבל ומאפשרת בקרה על תהליכים ואירועים שמתרחשים בזמן אמת , יחד עם תהלכים של הפקת דוחות המערכת גם אחראית על זיהוי פרצות אבטחה ותגובה למתקפות המתרחשות בזמנים שונים.

המטרה העיקרית של המערכת היא לספק אינפורמציה, התראות וניתוחים בזמן אמת ולזהות פעילויות חשודות ואנומליות ברשת ,בהתאם לחוקים מוגדרים מראש בשילוב של למידת מכונה.

מערכת ה-SIEM שבנינו ☺

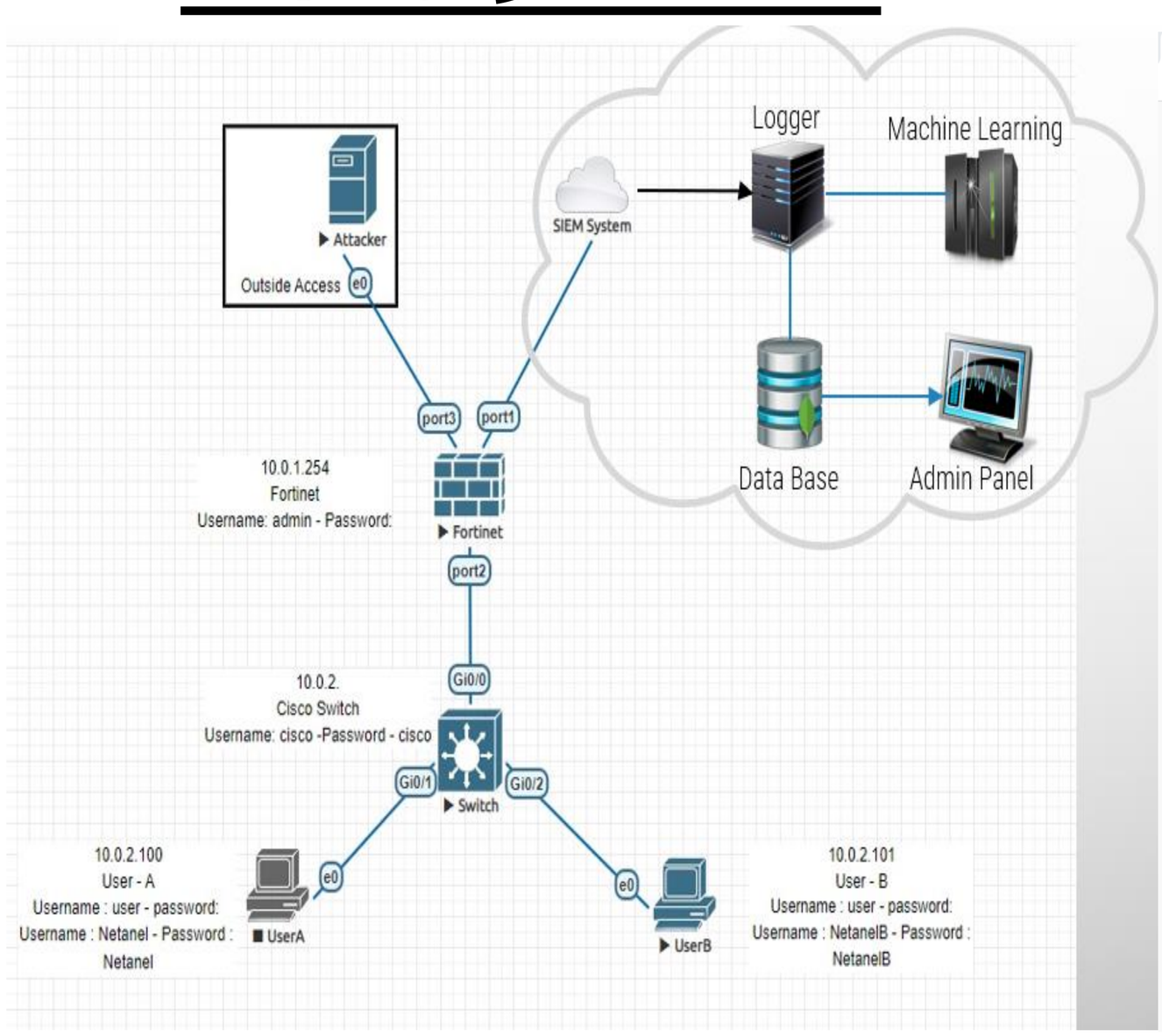
המערכת מתבססת על מחשב ניהול מרכזי (SIEM System) אשר מקבל את ה-Logים מה-Clients השונים (על כל Client מוגדר Agentששולח את הלוגים לשרת ה-Logger) :

- מחשבי Windows
- Firewall FortiGate

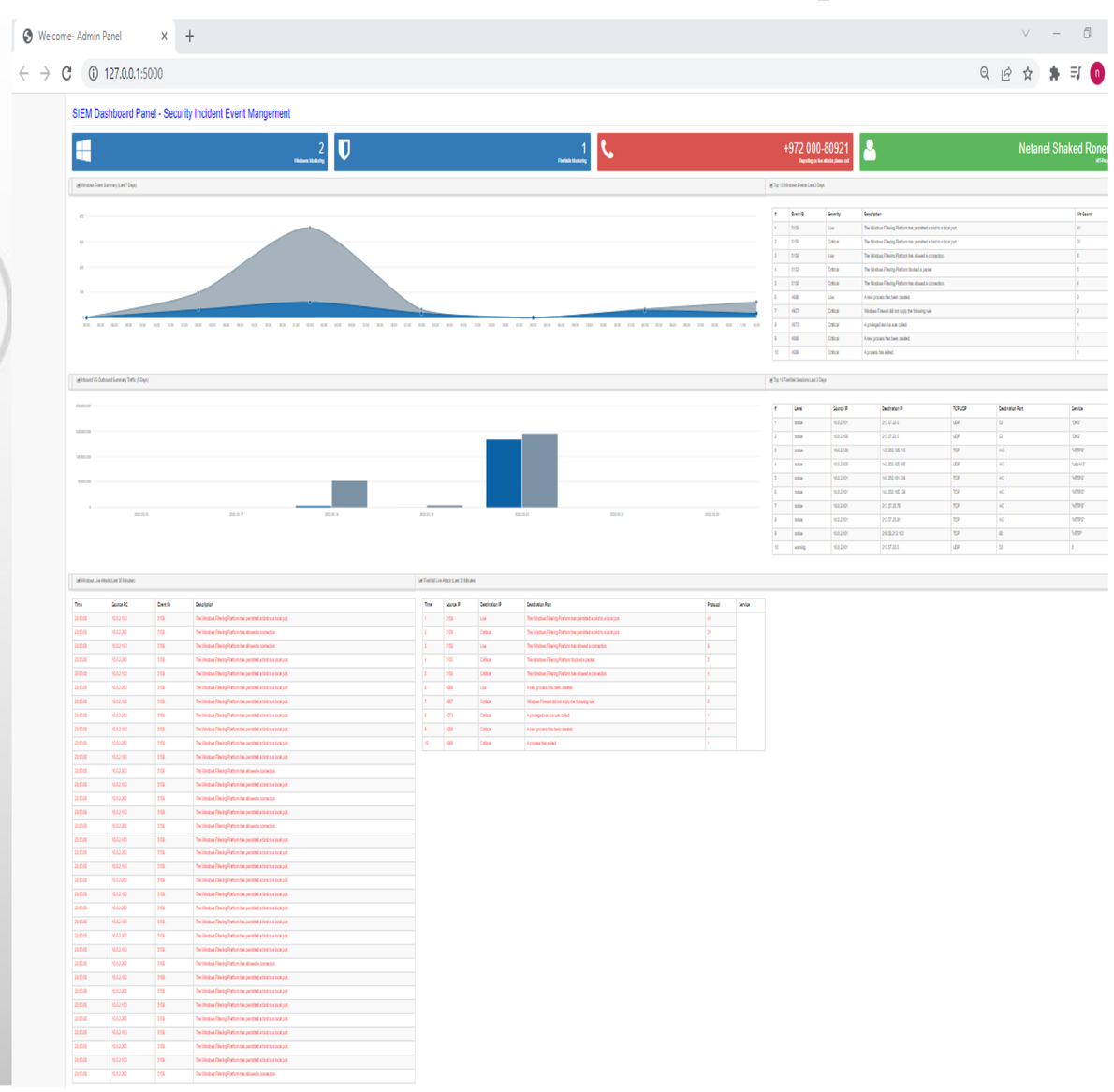
המערכת מחפשת קורלציות מתוך חיוויים שונים וזאת בהתאם לקורלציות אשר נכתבו על ידנו באופן ידני (Windows Event ID Dictionary of) וגם באופן אוטומטי על ידי יישום של מערכת מבוססת בינה מלאכותית מסוג PCA.

במידה והמערכת מזהה קורלציה/חיווי על מתקפה או התנהגות מוזרה המערכת תתריע על גבי מסך ה- SIEM Dashboard Panel.

תצורת המערכת שלנו



מסך Admin Panel



מסקנות:

המטרה המרכזית שלנו הייתה לאפשר לארגונים קטנים לפרוס מערכת SIEM שיודעת לזהות חריגות ואנומליות ברשת עם מימוש של בינה מלאכותית ויחד עם ממשק משתמש ידידותי , אנחנו שמחים שהמערכת שלנו פועלה בצורה מושלמת כאב טיפוס

YouTube Link

GitHub link

דיונים:

מערכת SIEM זה עולם מורכב בפני עצמו, היינו שמחים לממשק את המערכת SIEM שלנו לעוד סוגי Clients כמו:Active Directory,F5, EDR,NAC כדי לקבל סקירה גדולה יותר של הרשת וככה לבצע זיהוי בצורה מדויקת יותר