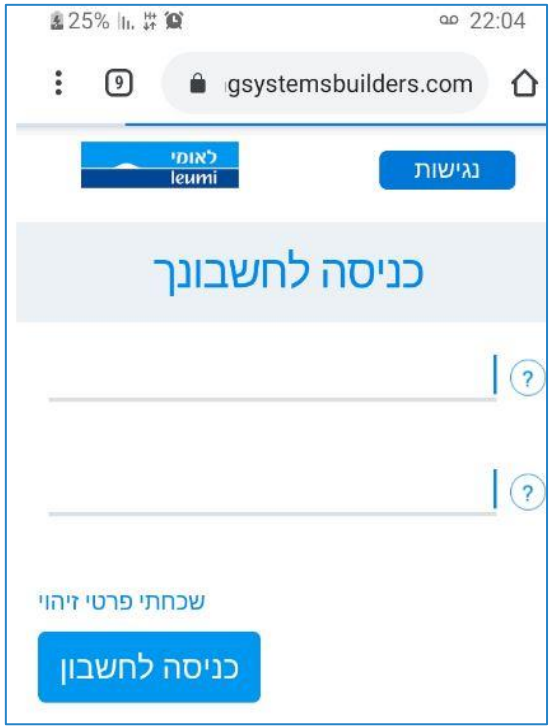
# מושגי ייסוד בסייבר – חלק ג

Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# איך יוצרים תקיפת פישינג?

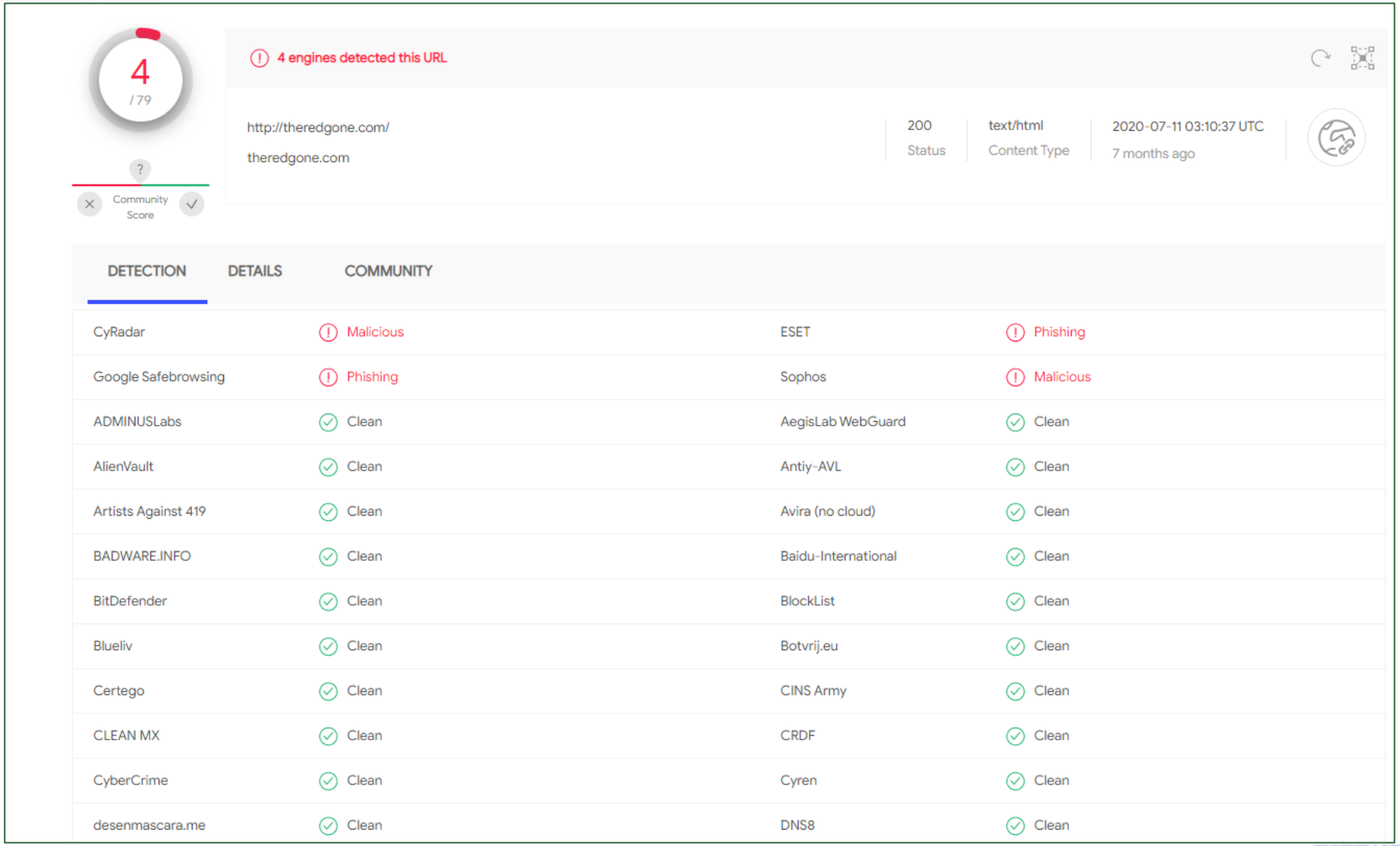



- ✓ הפעלת כלי: SE-TOOL (כחלק מחבילת כלים שניתן להוריד חינם)
- ✓ מעתיקים אליו לינק אליו מבקשים הזדהות למשל אתר בנק לאומי
- ✓ הכלי לוקח את דף ההזדהות של האתר + את דף האתר ויוצר לינק מוכן שמדמה את דף האתר.
- ✓ שולחים את הלינק ל"תפוצת נאטו" – תפוצה רחבה ככל האפשר בהנחה ש- 1% מהקורבנות מכניס פרטי משתמש וסיסמא
- ✓ פרטי ההזדהות (שם משתמש וסיסמא) מועברים לכתובת התוקף


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

https://www.virustotal.com/gui/

Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il



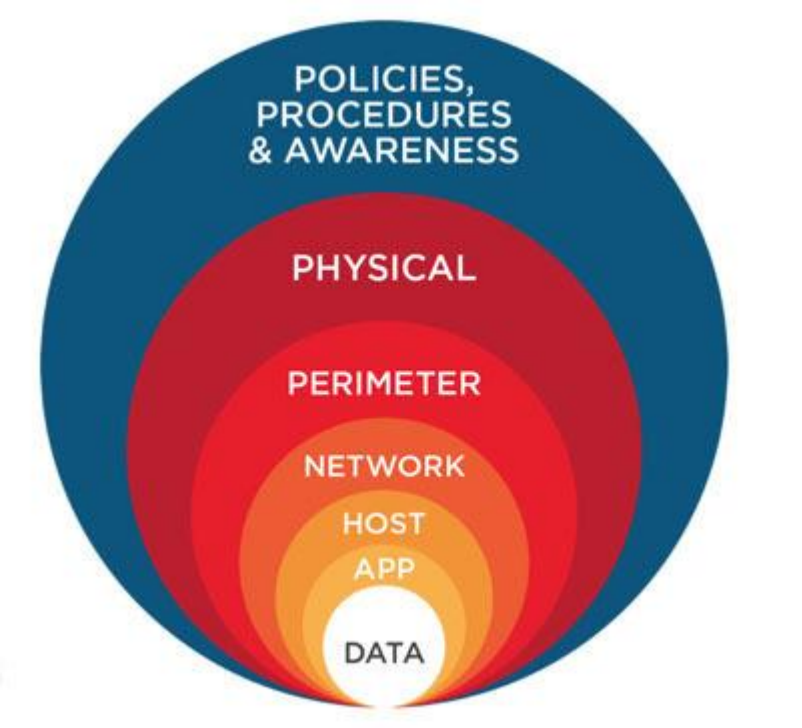



Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# הגנות סייבר

Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# עקרון DEFENSE-IN-DEPTH




## העיקרון אומר: הגנה על כל רכיב כאילו הוא לבד.

- ✓ הגנה על בסיס הנתונים
- ✓ הגנה על האפליקציות
- ✓ הגנה על המחשבים
- ✓ הגנה על הרשת
- ✓ הגנה פיסית על חדרי השרתים
- ✓ בקרות גישה בתוך הארגון
- ✓ הגנה היקפית של הארגון (גדרות, מצלמות, שומרים)
- ✓ מודעות עובדים
- ✓ נהלים ופרוצדורות עבודה


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# WAF – הגנה על האפליקציה

WAF = WEB APPLICATION FIREWALL

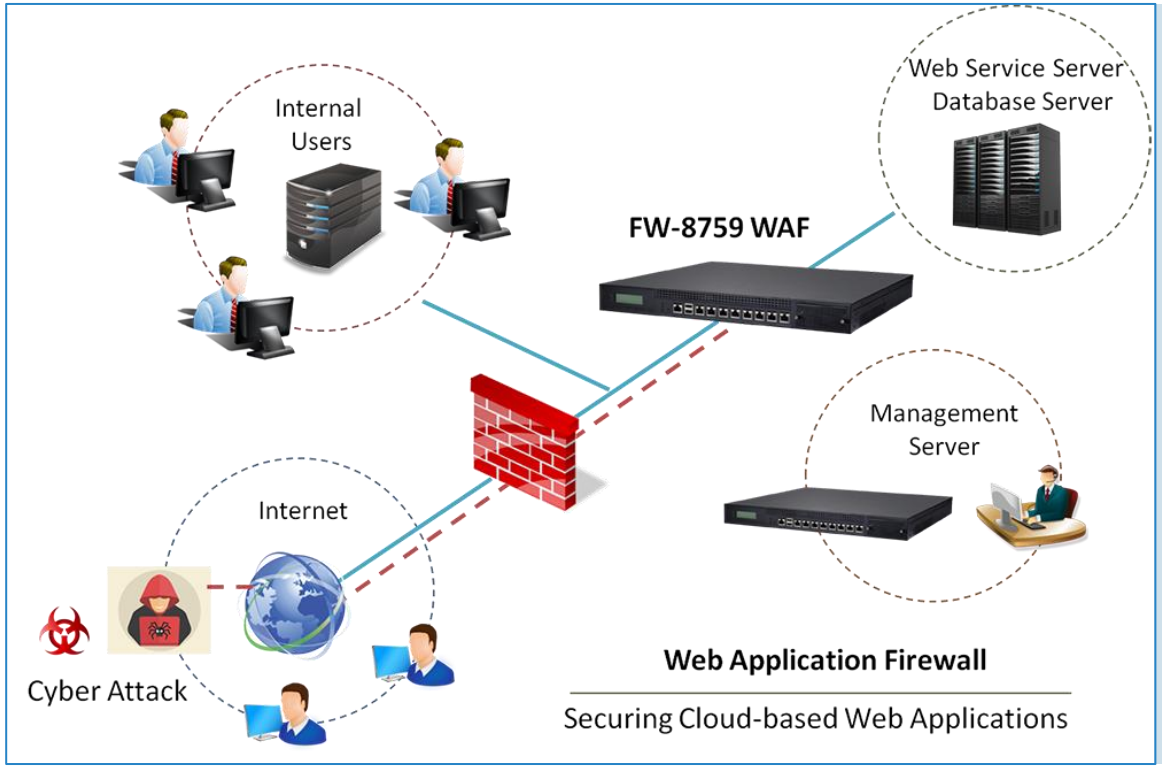
ההתקפות על האפליקציה נובעות מחולשה באפליקציית האתר שאליה מחדיר ההאקר נוזקה

הבעיה: חומת אש מעבירה כל בקשה לשירות WEB ולא מזהה התקפות אפליקטיביות

הפתרון:

Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# שלבים ביישום WAF




**שלב 1:** המוצר לומד את התנהגות המשתמשים (מצב Learning Mode)

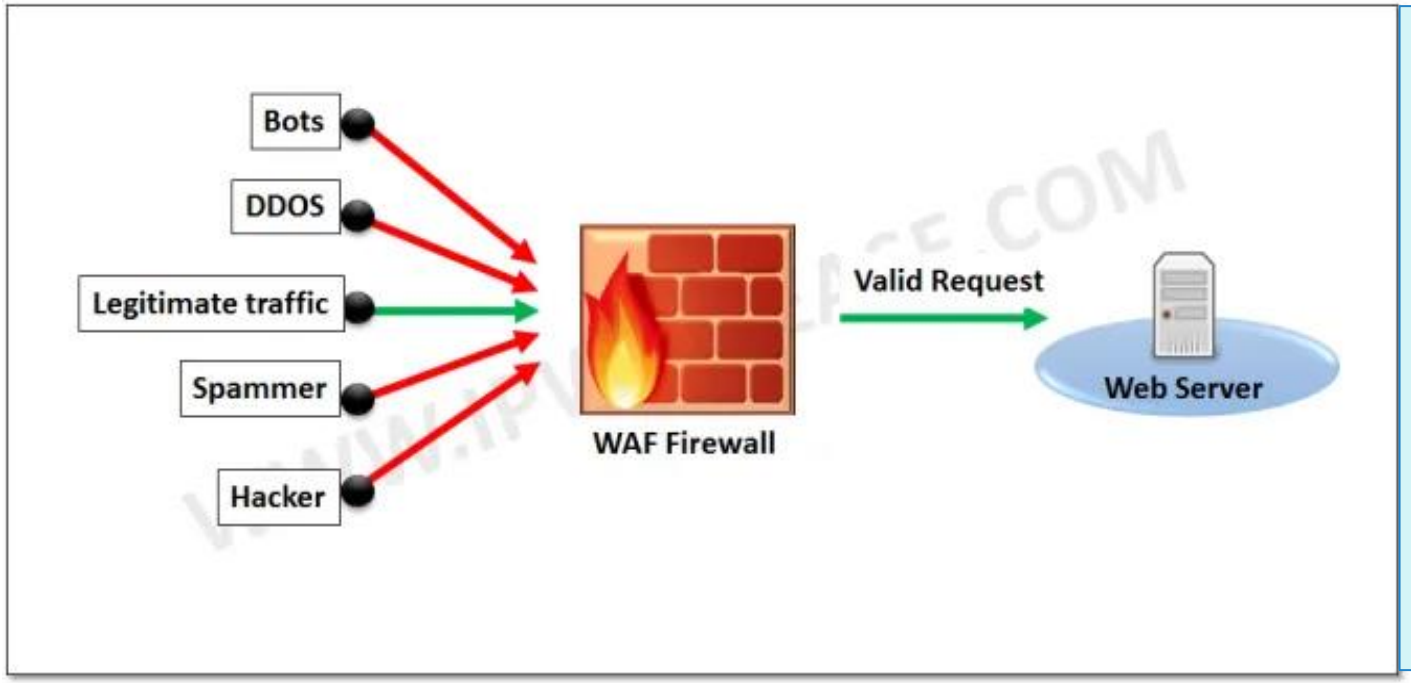
**שלב 2:** חוסם פעילות חריגה

**שלב 3:** טיוב ידני של המוצר

**שלב 4:** תחזוקה שוטפת- איש הסייבר מול איש מערכות מידע . כל אתר שנוסף יש להכליל

SOURCE: https://www.lanner-america.com/network-computing/securing-cloud-based-web-applications-next-generation-waf/

# ארכיטקטורת WAF



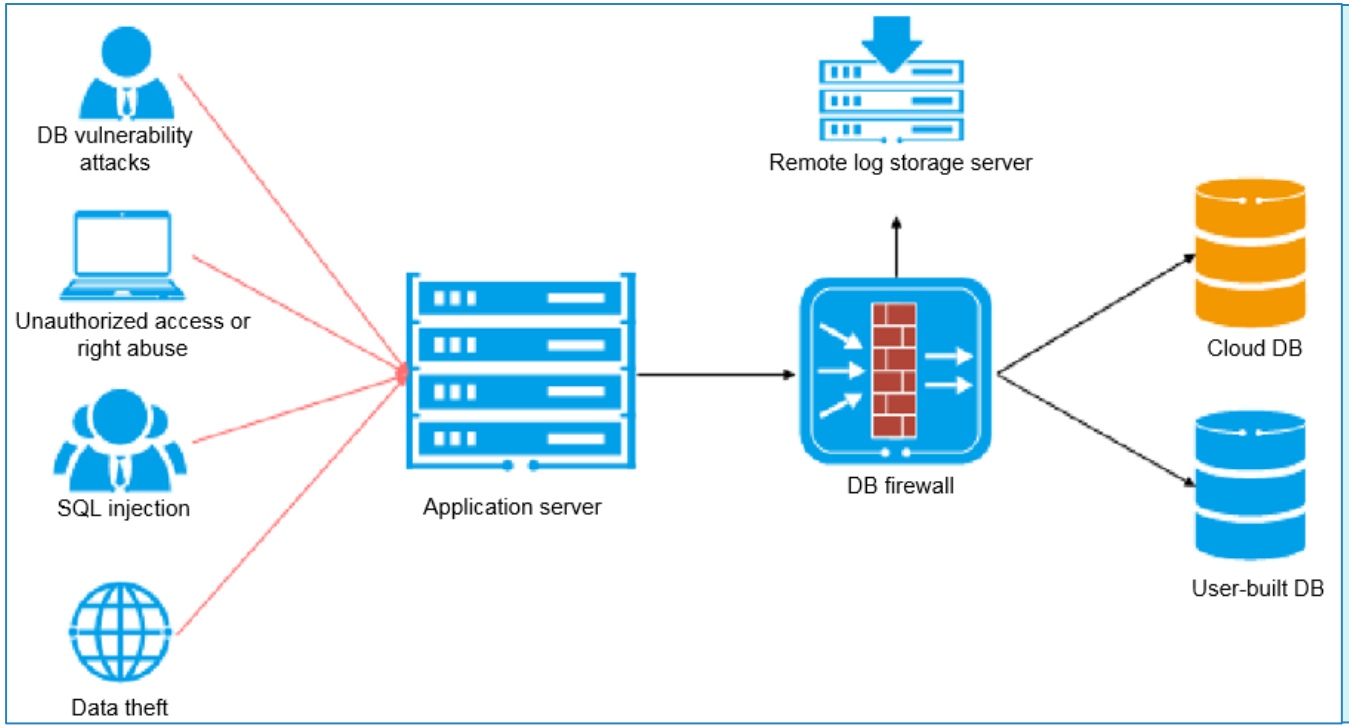

עלינו להיות ערים:

- יתכנו פניות לגיטימיות שיחסמו
- יתכנו פניות לא לגיטימיות שיעברו
- ככל שיעבור זמן, כמות הטעויות תלך ותקטן עקב עקומת למידה של המוצר

SOURCE : https://ipwithease.com/introduction-to-waf-web-application-firewall/

# DAF –הגנה על בסיס הנתונים

## DAF = DATABASE FIREWALL

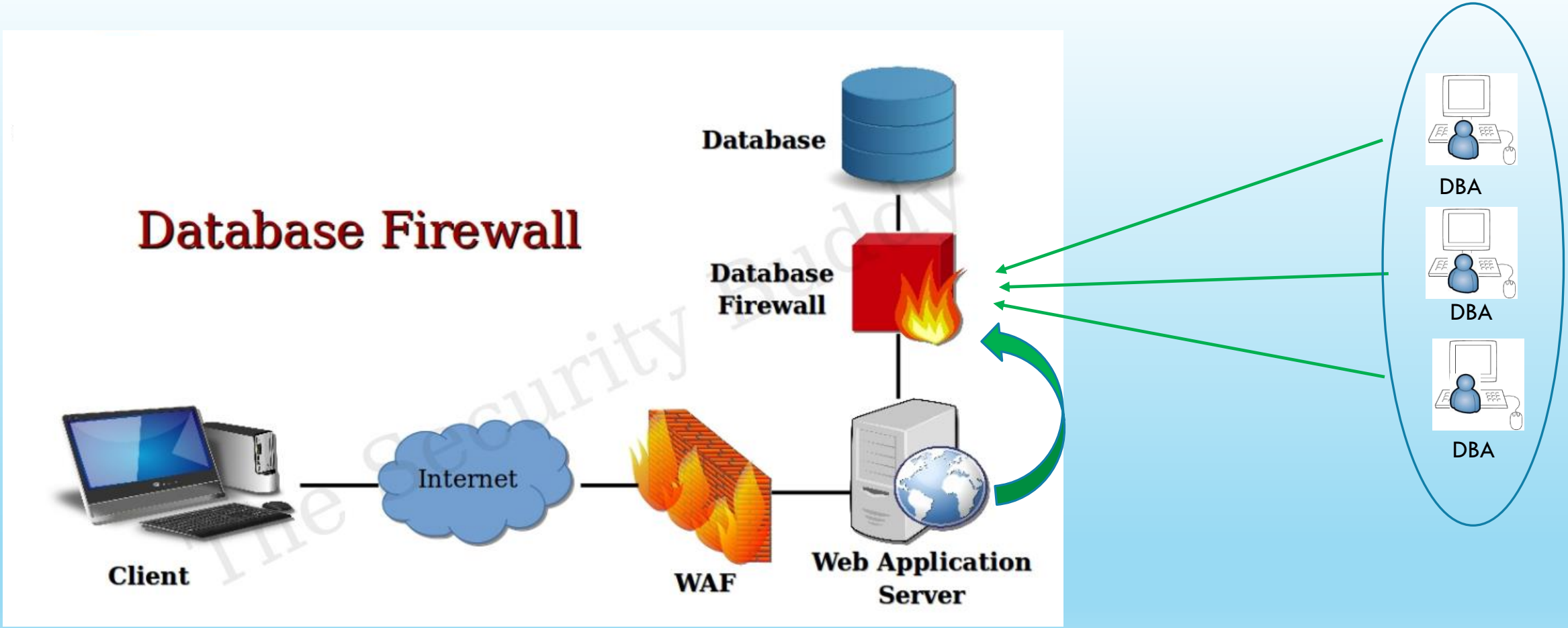



**האתגרים:**

- ✓ מניעת חיבור ישיר של משתמשים לגיטימיים בארגון אל בסיס הנתונים (למשל ה–DBA )
- ✓ שימוש נרחב של אנשי הארגון ב–TOAD (לניהול בסיסי נתונים של SQL ו–ORACLE) מתחנות עבודה מקומיות
- ✓ ניהול מרכזי ומאובטח
- ✓ מניעת התקפות על בסיס הנתונים: גניבת מידע, שינוי מידע


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# ארכיטקטורת DAF

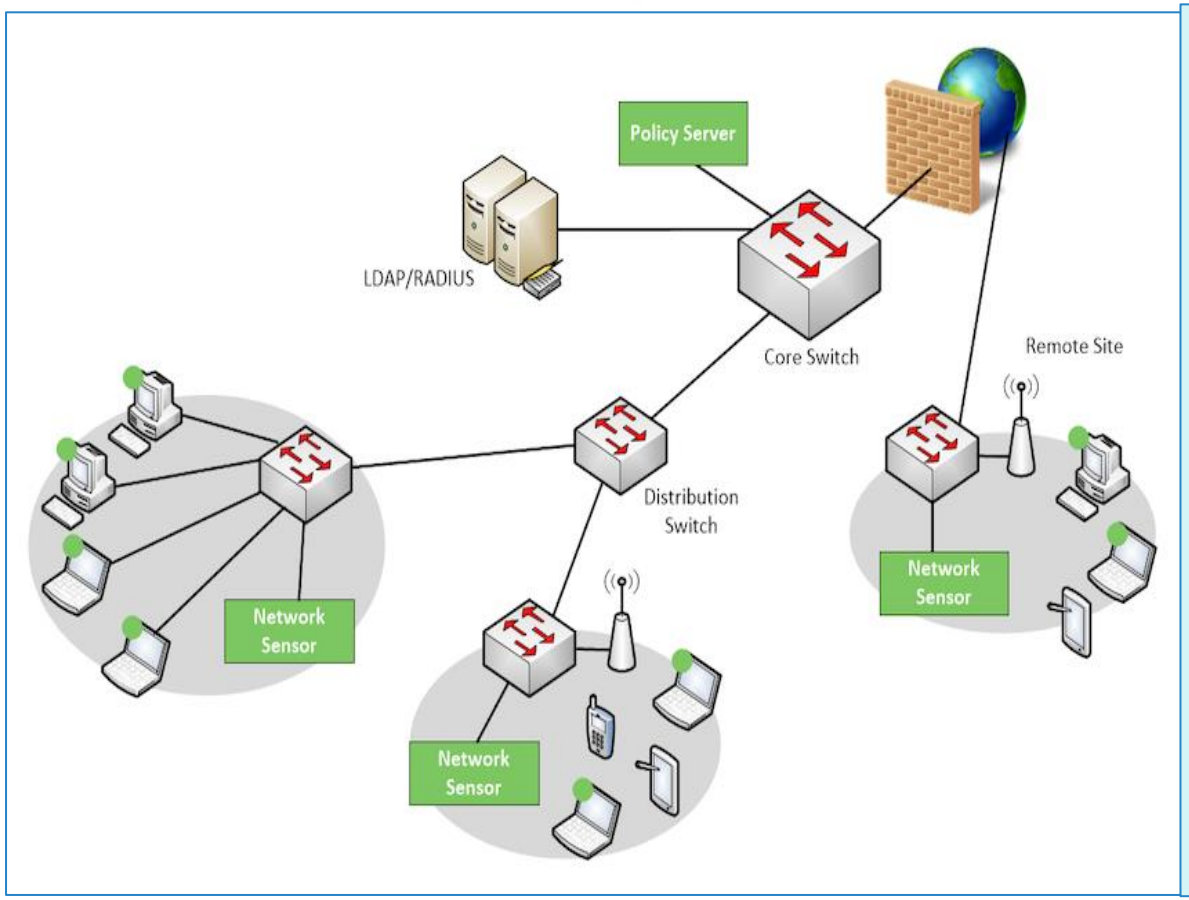



source: https://www.thesecuritybuddy.com/database-security/what-is-database-firewall/


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# NAC – הגנה על הכנסת רכיבים זרים לרשת

## NAC = NETWORK ACCESS CONTROL




**האתגר: מניעת חיבור רכיבים זרים לרשת הארגון**

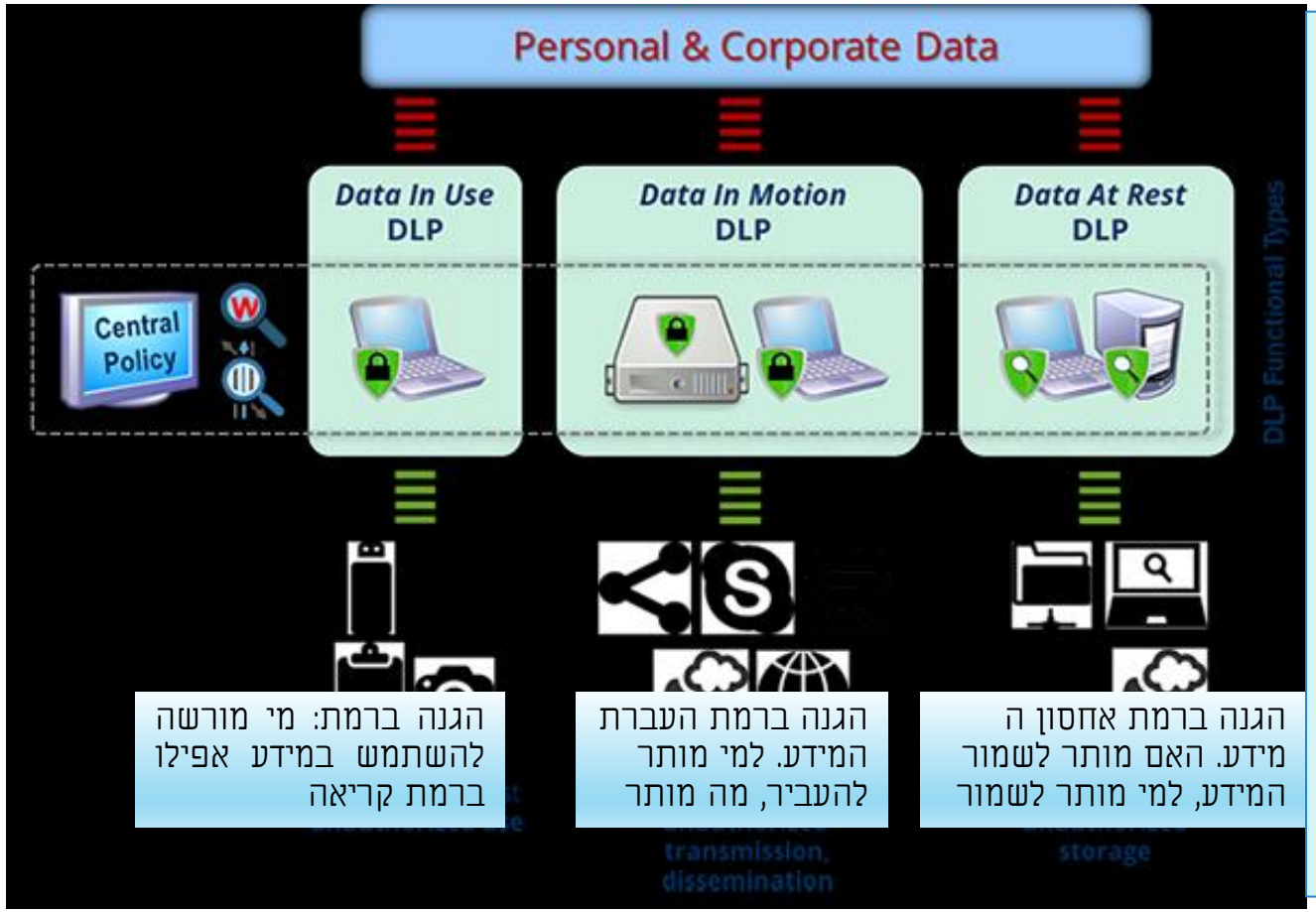
- ✓ **מחשב לא מורשה**
  מניעת גישה – זיהוי על פי MAC ADDRESS או מזהה חד חד ערכי של הארגון . גם משתמש חוקי של הארגון לא יוכל להכנס.
- ✓ **משתמש לא מורשה**
  מניעת גישה גם אם המחשב המתחבר מזוהה ושייך לארגון
- ✓ **מחשב מורשה ולא מוגן**
  הכנסה לבידוד, אפשרות ל"טפל" בו וכשהוא נקי לאפשר לו גישה לרשת , אפשר לתת לו עבודה מצומצמת באתר הבידוד

**יש בקרה מפצה?**


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# DLP – הגנה על זליגת מידע מהרשת

## DLP = DATA LOSS PREVENTION




DLP = DATA LOSS PROTECTION

DLP = DATA LEAK PREVENTION

**אתגרי הטמעה** – ארגון צריך לדעת לקטלג את המידע

**<u>דוגמאות:</u>**

- למי מותר לראות מה?
- איזה מידע אי אפשר לשמור היכן שרוצים ?
- איזה מידע אי אפשר להדפיס?
- איזה מידע לא ניתן לשלוח במייל ?
- לאיזה מידע לא ניתן לבצע COPY ?

**איך ניתן לעקוף את ההגנה הזו?**

# הלבנת קבצים – CDR

## CDR = Content Disarm and Reconstruction

מערכת הלבנת הקבצים בוחנת את סוגי הקבצים המועברים בעסק מסויים ועוקבת אחריהם:

- קבצים בעל סיומת חשודה
- חסימת קבצים המכילים מרכיבים אסורים כגון: Macro, Virus
- קבצים בעלי מבנה לא נכון לפי סטנדרטים.

דרכים ליישום הלבנת קבצים בארגון

- ✓ הלבנה ברמת קיוסק
- ✓ הלבנה ברמת סוכן
- ✓ ICAP SERVER

Source: https://odi-x.com/hebrew/

# הצורך בהלבנה

כדי למנוע הכנסת וירוסים דרך יציאת ה-USB של המחשב ישנן מספר אפשרויות

העיקריות שבהן:

אפשרות א' – חסימת יציאות USB ושאר התקנים כך שלא ניתן להכניס כלל קבצים למחשב

אפשרות ב' – שימוש בהתקנים של הארגון שמזוהים ע"י המחשב

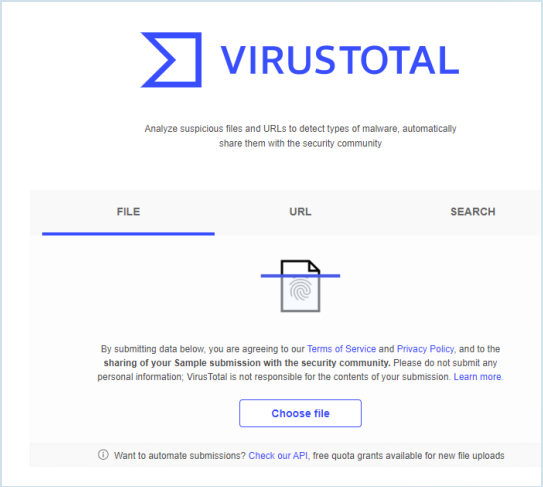
אפשרות ג' – לאפשר הכנסת קבצים דרך המדיות השונות אך לבדוק מה מכניסים:
- ✓ ברמה גבוהה יותר מאנטי-וירוס
- ✓ מטפל גם בהתקנים נוספים ( CDROM , דיסקטים)

# טכנולוגיית הלבנת קבצים מורכבת משלושה קווי הגנה

**קו הגנה ראשון** – סריקה ראשונית של מספר מנועי אנטי-וירוס* לחסימת קבצים הנושאים נוזקות ידועות

**קו הגנה שני** – אימות בין סוג הקובץ, מבנה הקובץ, הסיומת שלו ופרמטרים נוספים על מנת לוודא כי הקובץ חוקי

**קו הגנה שלישי** – הפעלת אלגוריתם ייחודי לכל סוג קובץ המנטרל נוזקות.





Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# עמדת Kiosk

עמדת הלבנה פיסית, מוקשחת ומוגנת בפני התקפת סייבר (יכולה לשמש כקו ראשון)

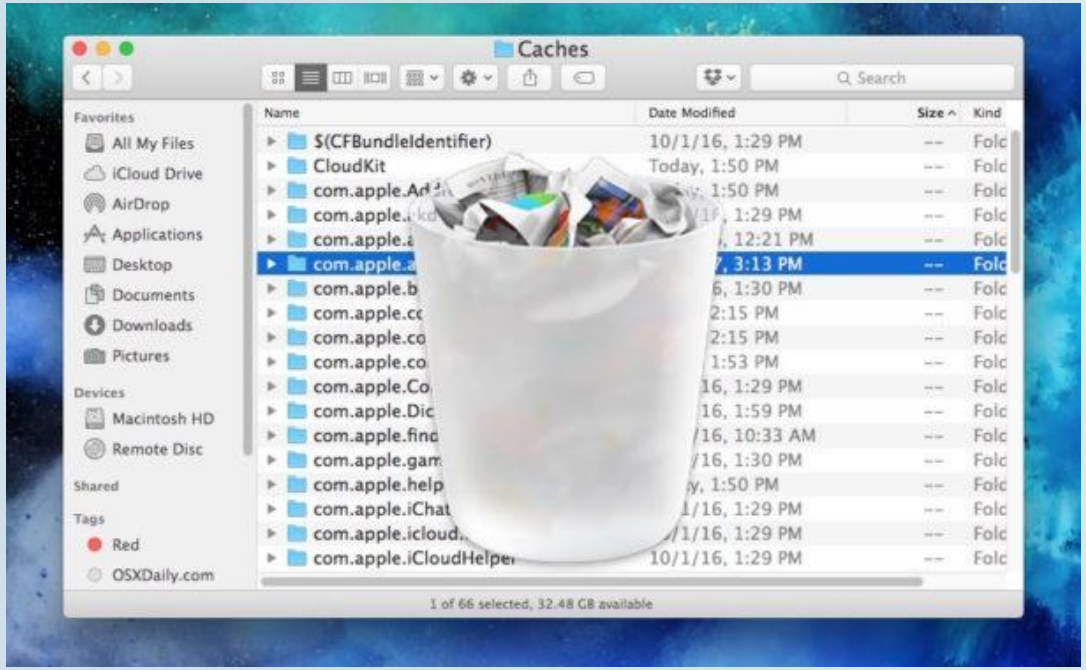
- ✓ מומלץ שתהיה ללא דיסק קשיח
- ✓ מיועדת לסריקת מדיות זיכרון נתיקות כגון:
  Disk on Key (DOK), CD, DVD, Smart Phone, Camera
- ✓ מערכת ההפעלה (רצוי שתבוסס לינוקס) והתוכנה של העמדה עולים מכרטיס מוקשח
- ✓ תוכנת ההפעלה מוצפנת

Source https://www.sasa-software.com/wp-content/uploads/2019/02/GateScanner_Kiosk.pdf


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# הלבנה ברמת סוכן

- התקנת סוכן על כל המחשבים בארגון / המחשבים המורשים להכניס DOK
- מאפשר סריקה של תהליכים רצים בכל מחשב ומחשב תוך כדי עבודה רגילה של המחשב
- יכול לבצע סריקה מלאה או במקומות מסויימים שקבענו מראש (תיקיות, קבצים, כונני רשת)
- ניהול הסוכן מעמדת מרכזית  או מהענן




Source:https://osxdaily.com/2017/04/18/clean-caches-temporary-files-mac/



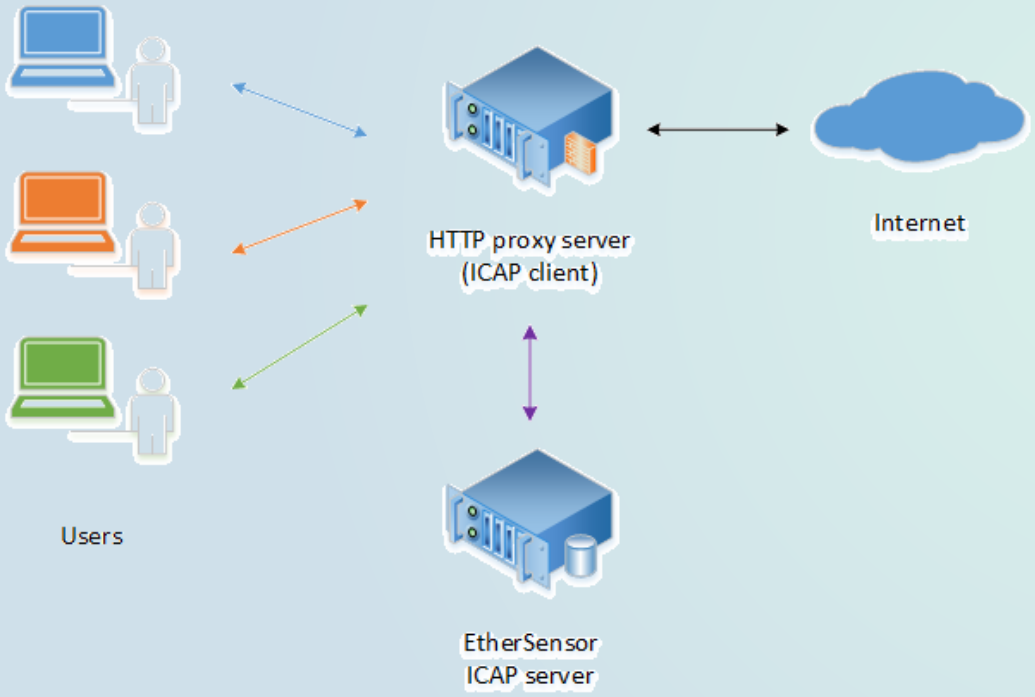
Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# עמדת ICAP SERVER

קבצים המועלים לפורטל החברה ע"י צרכנים, ספקים או כל משתמש אחר

שלבים:

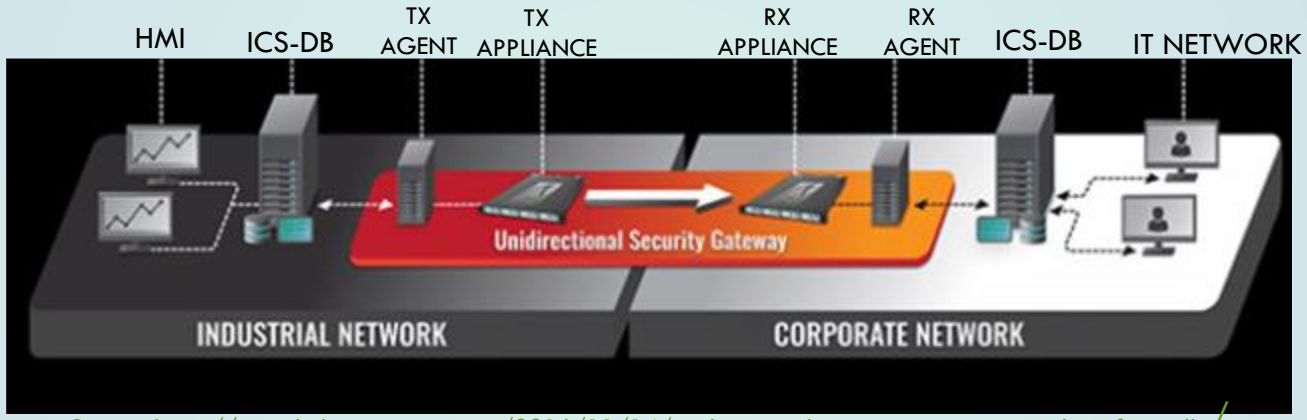
- הלקוח מעלה קובץ אל הפורטל
- הקובץ מועבר דרך ICAP CLIENT אל ICAP SERVER
- הקובץ נבדק ב-ICAP SERVER
- במידה ותקין – הקובץ נטען בהצלחה לשרתי החברה
- במידה ולא תקין – נשלחת הודעה ללקוח כי הקובץ נגוע





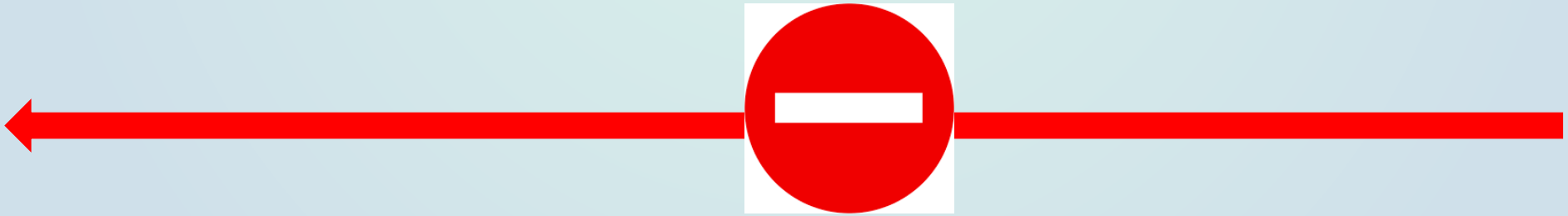
Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# דיודה חד כוונית – UNIDIRECTIONAL SECURITY GATEWAY



Source: https://www.helpnetsecurity.com/2016/11/14/unidirectional-security-gateways-replace-firewalls/

TX AIR - GAP RX



# הגנה על הבקר

- ערכי סף בקוד הבקר (טמפ, לחץ, רמת PH )
- יישום משתמש וסיסמא ייעודיים בבקר
- בידוד הבקר מרשת ה-IT
- גישה ישירה לבקר עם LAPTOP ייעודי ומוקשח
- החלת הגנות מובנות בבקר

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=STN+-+How+can+I+reduce+vulnerability+to+cyberattacks+v3+Feb2019.pdf&p_Doc_Ref=STN+v2

# הגנה על הבקר הישן

- מצב הבקר –
  - RUN – מצב ריצה (המצב הרצוי!)
  - Program – מצב תכנות
  - Remote – ניתן מרחוק לשנות את המצב

✓התקנת עדכוני SOFTWARE

✓התקנת עדכוני FIRMWARE

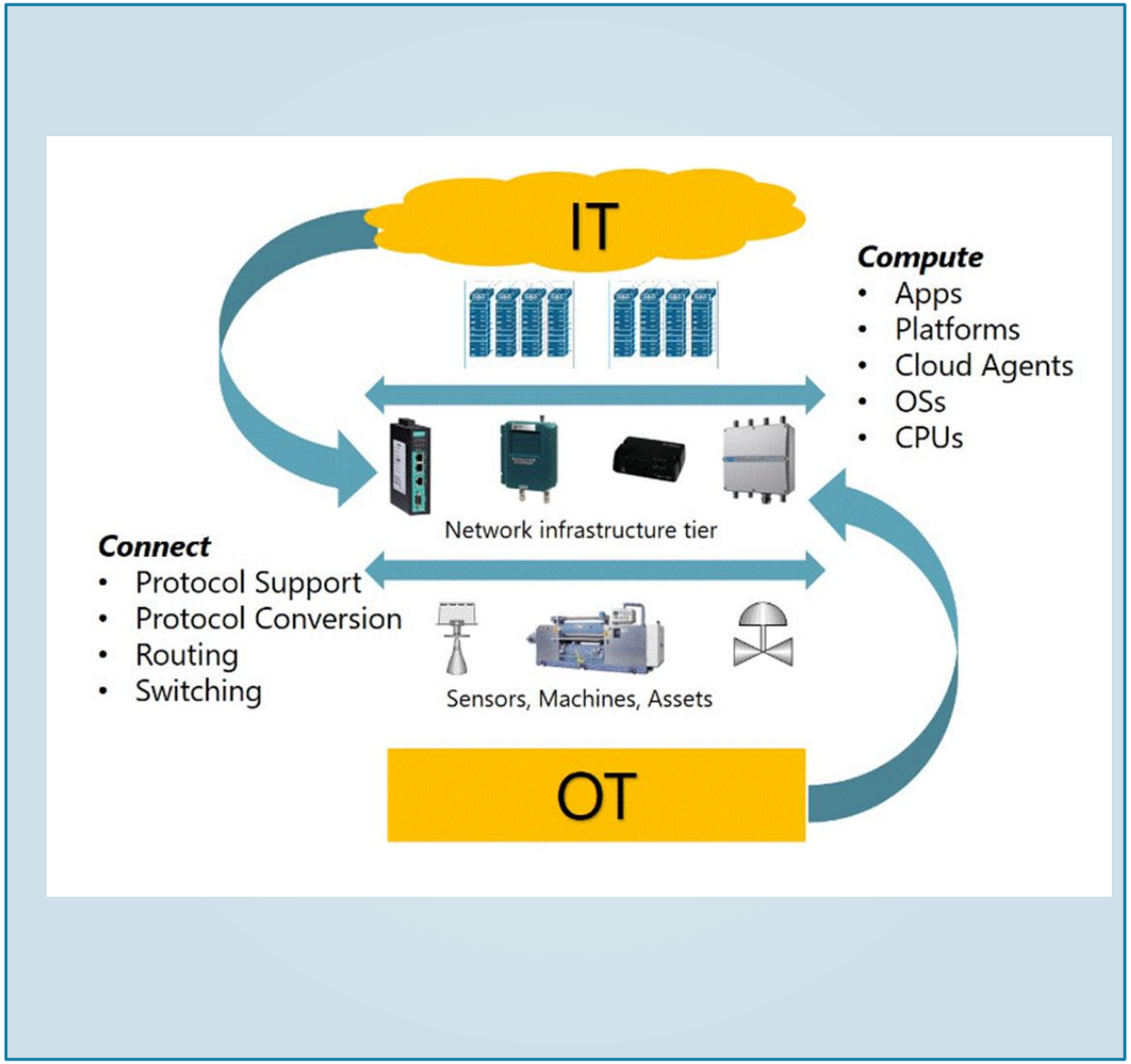

Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# מערכת ERP

פקודות עבודה

אל רצפת הייצור

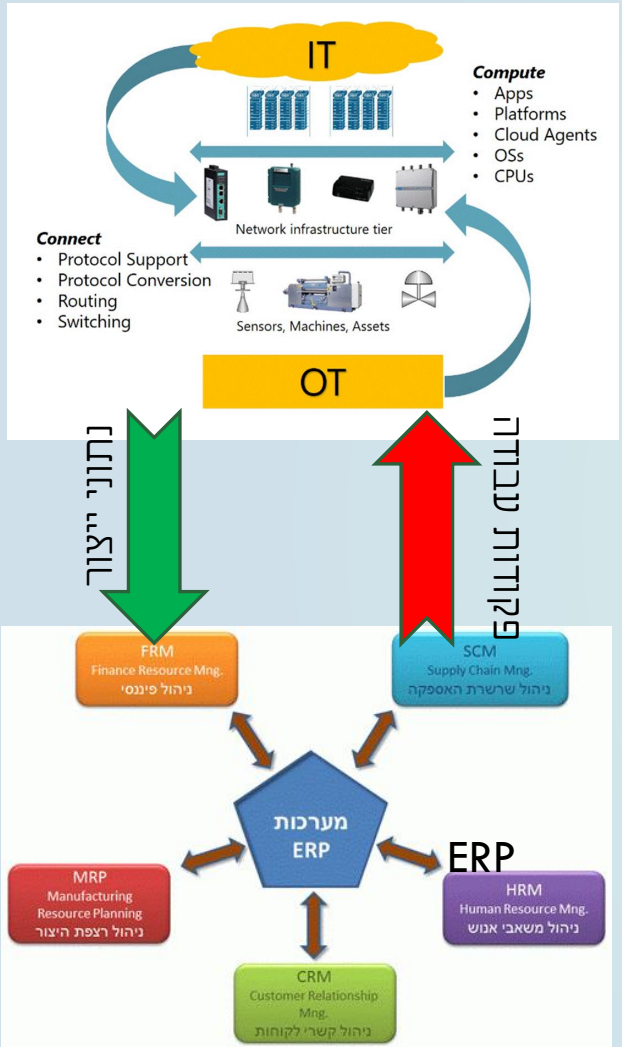

Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il




נתוני ייצור


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# איומים על מערכת ERP




- פירצה מרשת ה-זו אל רשת ה-זס (רצפת הייצור) – השתלטות על בקר ברשת ה- OT
- שינוי מינוני חומרים לראקציה כימית בריאקטור - ייצור מוצר אחר, אפשרות לפיצוץ
- שינוי וערבוב בין יעדים שונים של חומרים שונים
- מימשקים עם ספקים חיצוניים – חשיפת הארגון לספק לא בטוח
- השתלטות על סודות מסחריים

# הגנה על מערכת ERP

- ✓ בידוד ברמת סגמנטציה
- ✓ הקשחת ברמת מערכת הפעלה
- ✓ הקשחת ברמת מערכת (SAP ,PRIORITY)
- ✓ נהלים בהזרמת מידע למערכת (מי ראשי? , מה ניתן?)

# MES vs ERP

## ERP Enterprise Resource Planning

- ניהול שרשרת אספקה
- ניהול פיננסי
- ניהול משאבי אנוש
- ניהול לקוחות
- ניהול רצפת הייצור

## MES Manufacturing Execution Systems

- הפעלות פעולות ייצור ודווח בזמן אמת
- התמקדות בעולם הייצור
- התממשקות למערכת ERP

# מערכת ניטור אירועים – SIEM SOC

SIEM (Security Information and Event Management)

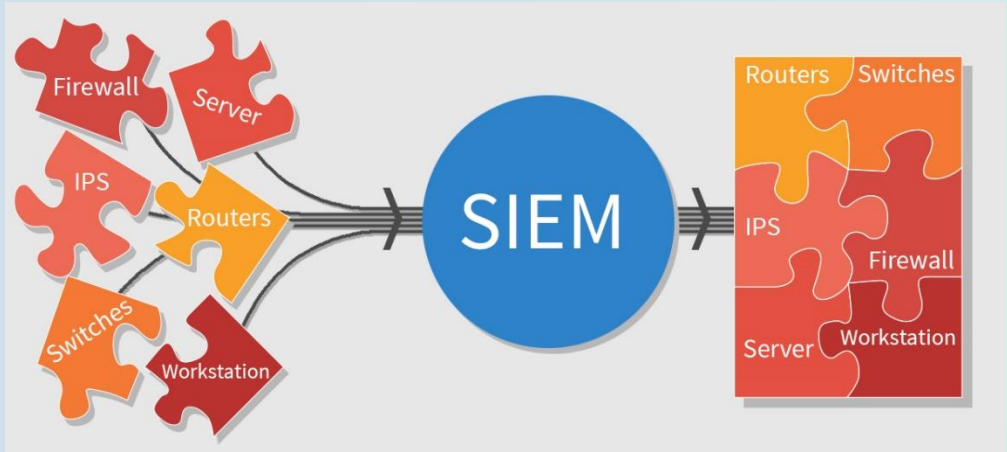
SOC (Security Operations Center)

SIEM
- טכנולוגיה שמספקת "עיניים" למה שקורה ברשת בהיבטי סייבר
- מציפה ארועים של תקשורת "חשודה" , או התנהגות "לא לגיטימית" ברשת
- בונים סט של חוקים כדי לקבל ארועים שמעניינים אותנו

SOC
- ניתוח המידע
- קבלת מודיעין
- תגובה לארועים
- תחקור איומים ידועים ולא ידועים

אין SOC בלי SIEM אך יכול להתקיים SIEM בלי SOC

# SIEM vs SOC

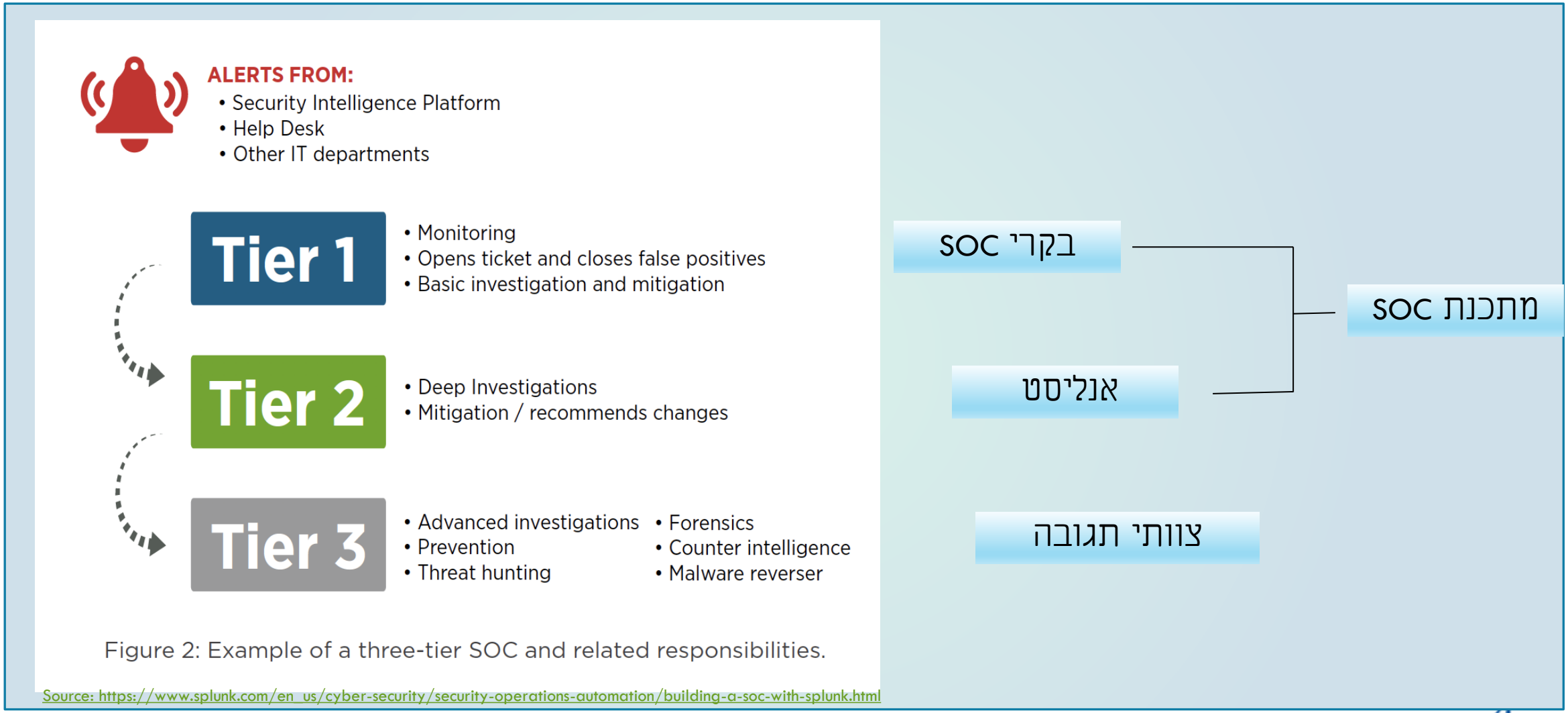



Source: https://gbhackers.com/soc-indicator/

Source: https://www.cloudsec.com/wp-content/uploads/2016/09/au_Disruption-in-Cloud_Sumo-Logic-by-Layer-8-Security.pdf


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# מבנה מערכת SIEM - SOC



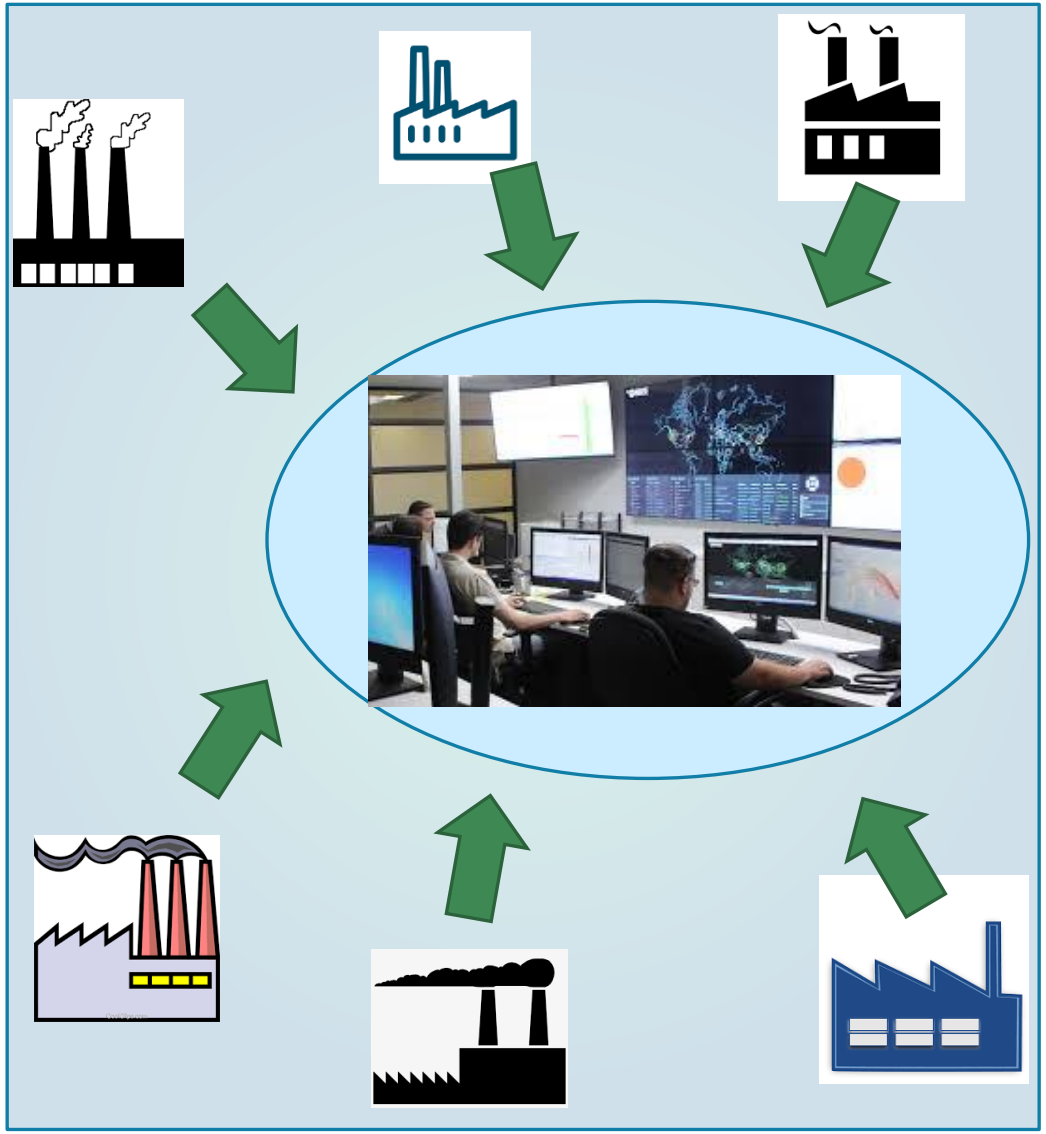


Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# הקמת מק"מ המשרד להגנת הסביבה

## מק"מ = מרכז קיברנטי מגזרי

- ✓ שיתוף ידע ומידע בין מפעלים, כולל מודיעיני ועל מתקפות קיימות למניעת התפשטות מתקפה
- ✓ שיתוף ניסיון ותובנות להתמודדות עם אירוע קיים
- ✓ בניית מאגר ידע מקצועי של טיפול באירועים מורכבים באמצעות העמדת מומחי תוכן לעולם התוכן של המגזר
- ✓ רתימת גופים להעלאת רמת החוסן באמצעות הצפת סיכונים ואיומים קונקרטיים אשר המרכז יזהה אל מול גופים שונים במגזר
- ✓ בניית תמונת מצב מגזרית למקבלי החלטות בשגרה
- ✓ שיתוף פעולה עם מק"מים נוספים: משרד האנרגיה, התקשורת, הבט"פ, הפיננסיים, הסוק הממשלתי בנושא התקפות סייבר במערכות דומות / משיקות / משותפות.
- ✓ מידע מודיעיני
- ✓ צוותי תגובה - מענה להתקפות על מערכות תעשייתיות (בהמשך להתקפות על מתקני מים בישראל)




Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

# מערך הסייבר הלאומי מרכז הסייבר בבאר שבע

Yosi Shavit MBA, CISO, CISM, CDPSE- Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

שאלות ותשובות