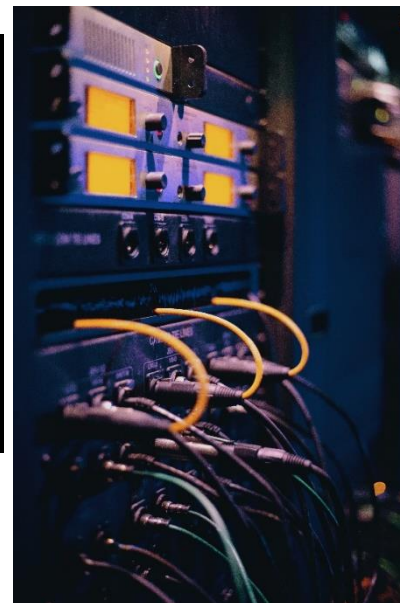


# מושגי ייסוד בהגנת סייבר – חלק ג



Yosi Shavit MBA, CISM - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: [yosish@gmail.com](mailto:yosish@gmail.com) , [yosish@sviva.gov.il](mailto:yosish@sviva.gov.il)



# נושאי הלימוד

בדיקת קוד זדוני / אתר זדוני VIRUS TOTAL

הלבנת קבצים – CDR

דיודה חד כוונית

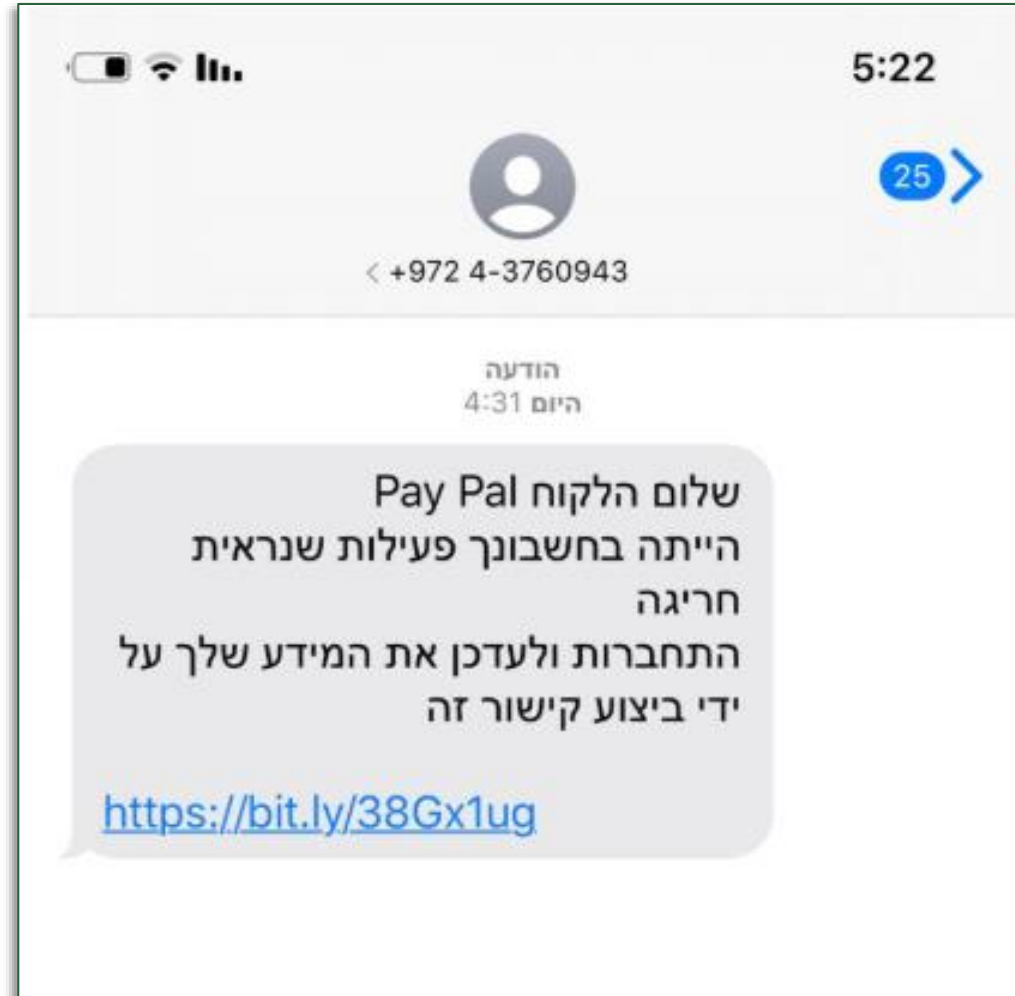
הגנה על בקרים


התחברות מרחוק

הגנה על מערכות – ERP

SIEM – SOC

# יום חמישי בבוקר 9.7.2020



 Dangerous | theredgone.com/OL/



## Deceptive site ahead

Attackers on **theredgone.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). [Learn more](#)

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)


Details

Back to safety



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE      URL      SEARCH



By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Want to automate submissions? [Check our API](#), free quota grants available for new file uploads

## זהירות: ישראלים תחת מתקפת פשינג

משעות הבוקר נרשמו אלפי נסיונות להפיל ישראלים בפח באמצעות הודעות SMS שמדווחות על בעייה כביכול בחשבון הפייפאל שלהם. לפי בדיקת ynet המקור הוא ככל הנראה קבוצה ערבית שמבצעת את המתקפה מאתר בלוב. מה לעשות? כלום. פשוט לא ללחוץ על הקישור



טל שחף פורסם: 11.07.20, 12:27

קיבלתם הודעה על בעייה בחשבון הפייפאל (Paypal) שלכם? אל תלחצו על הקישור! אלפי משתמשי טלפון ישראלים קיבלו מאז שעות הבוקר המוקדמות הודעות SMS שמתריעות כביכול על בעייה בחשבון הפייפאל. מדובר בקמפיין דיג (פשינג), שנועד לגנוב את פרטי חשבונות הפייפאל במסווה של עדכון פרטים בשירות לקוחות. הנסיונות האלה נחסמו במהירות וככל הידוע בשלב זה כבר לא ניתן לגשת לדפים המסוכנים.

מבדיקה של ynet עולה כי מאחורי המתקפה מסתתרת ככל הנראה קבוצה ערבית או מישהו שמסווה את עצמו כקבוצה כזו. המתקפה כולה נעשית מתוך אתר של ארגון לובי שעוסק באיכות הסביבה, שייתכן שכלל לא יודע שהאתר שלו משמש לעקוץ ישראלים.

معرض صور

يحتوي هذا المعرض على العديد من صور أنشطة المركز  
يحتوي هذا المعرض على العديد من صور أنشطة المركز

شركائنا

يتعاون مع المركز العديد من الجهات المهنية بجانب بحوث وعلوم البيئة منها: جمعية علوم البيئة - المركز الليبي للبحوث

האתר שמשמש למתקפת הפשינג בישראל (צילום מסך)

התקפת פשינג דרך אתר  
איכות סביבה המשמש לעוקץ

# 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/>

# טכנולוגיית הלבנת קבצים מורכבת משלושה קווי הגנה

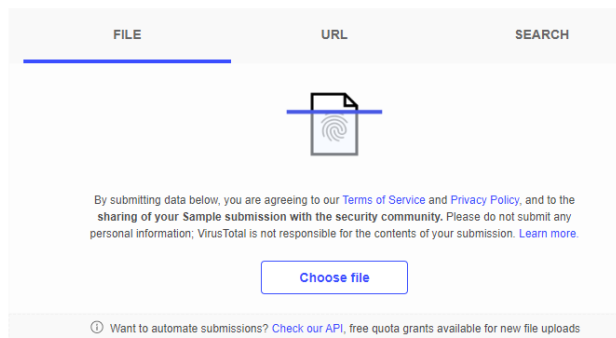
**קו הגנה ראשון** – סריקה ראשונית של מספר מנועי אנטי-וירוס\* לחסימת קבצים הנושאים נזקות ידועות

**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 נזקות.



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community



\* הפניה ל-VIRUS TOTAL – <https://www.virustotal.com/gui/home/upload>



# עמדת Kiosk

עמדת הלבנה פיסיית, 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

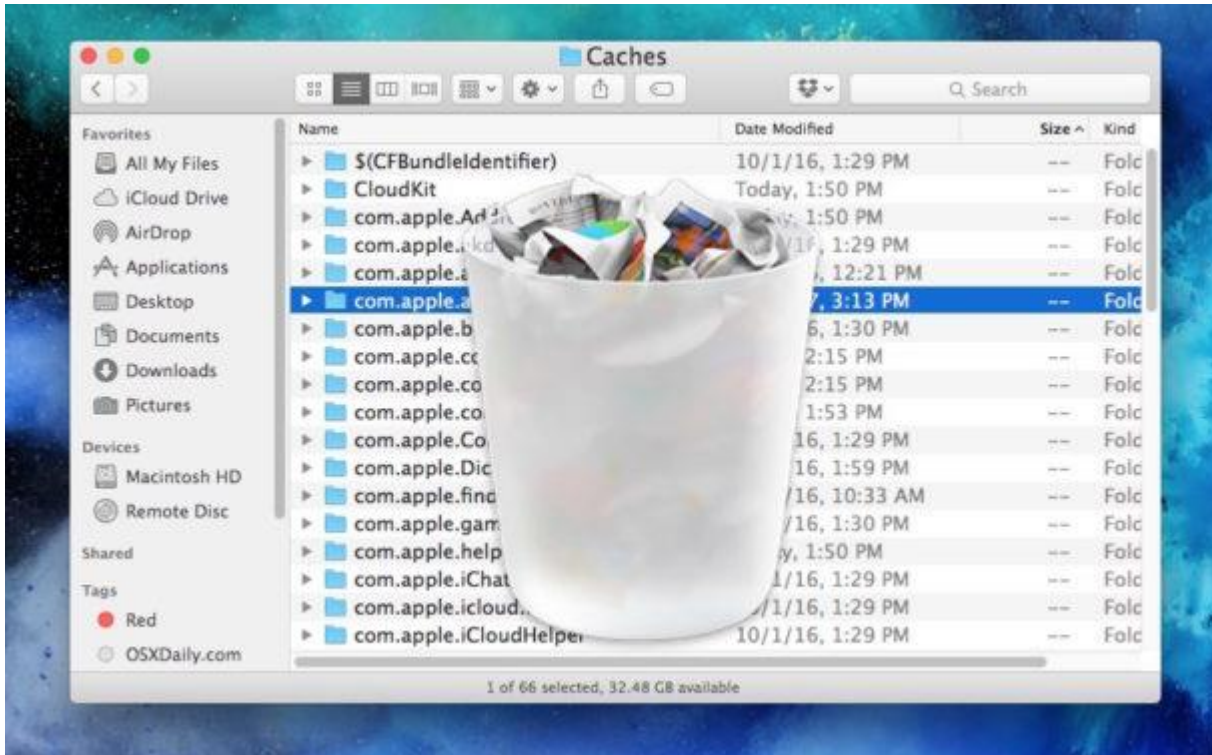
✓ תוכנת ההפעלה מוצפנת



Source [https://www.sasa-software.com/wp-content/uploads/2019/02/GateScanner\\_Kiosk.pdf](https://www.sasa-software.com/wp-content/uploads/2019/02/GateScanner_Kiosk.pdf)

# 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

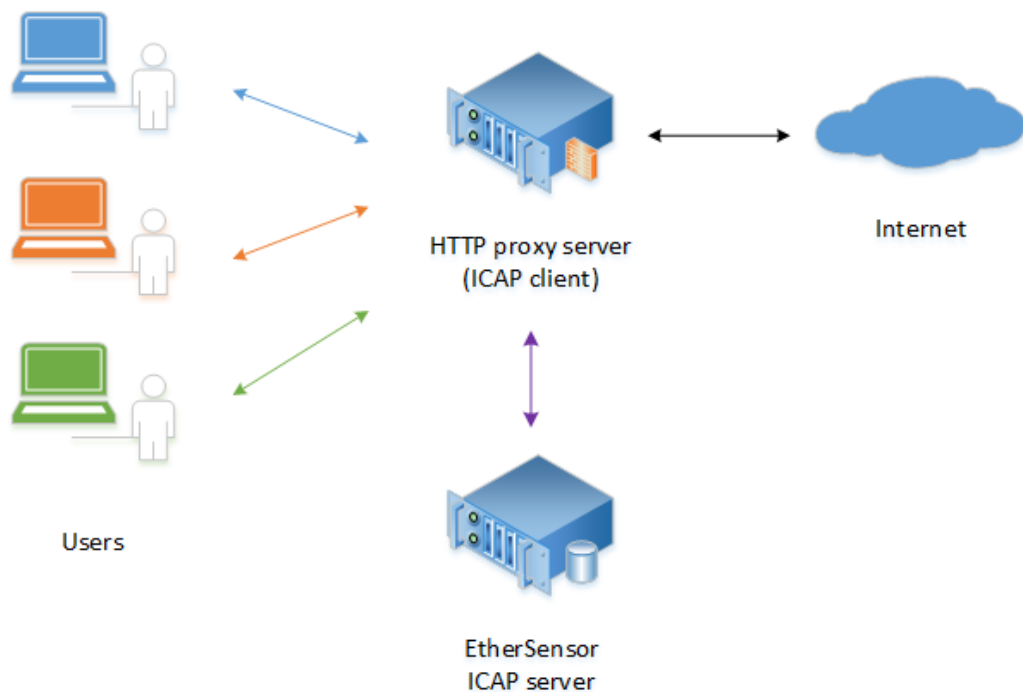


Source: <https://osxdaily.com/2017/04/18/clean-caches-temporary-files-mac/>

# 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

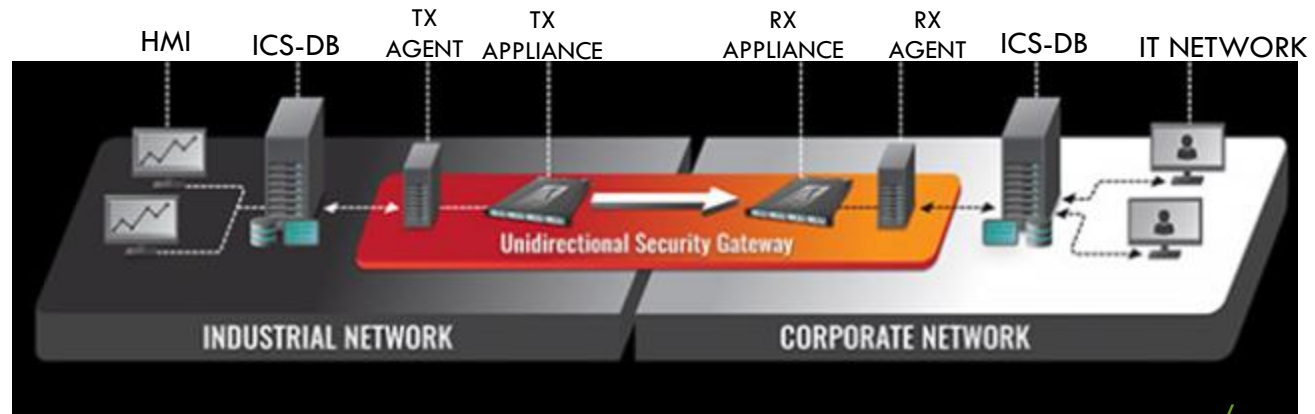
○ הקובץ נבדק ב-ICAP SERVER

○ במידה ותקין – הקובץ נטען בהצלחה לשרתי החברה

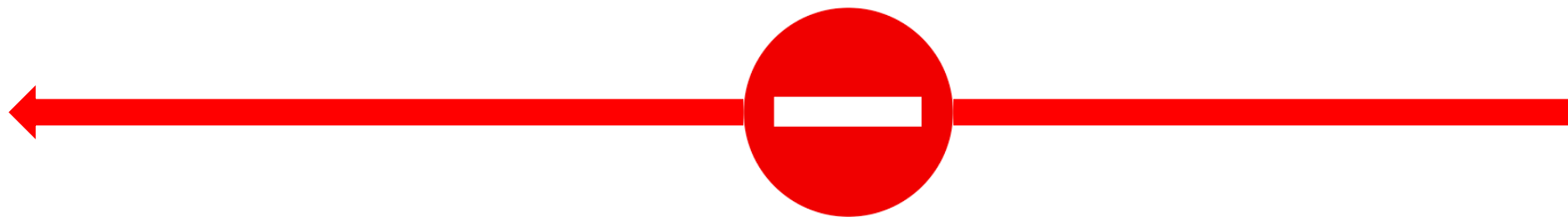
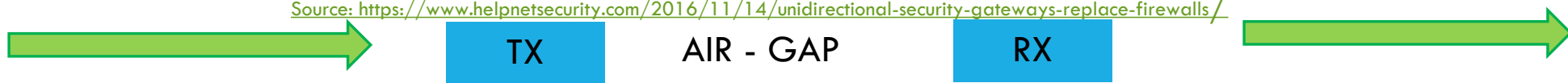
○ במידה ולא תקין – נשלחת הודעה ללקוח כי הקובץ נגוע

# הפרדת רשתות פיסית

## דיודה חד כוונית – UNIDIRECTIONAL SECURITY GATEWAY



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



# הגנה על הבקר

ערכי סף בקוד הבקר (טמפ, לחץ, רמת PH)

יישום משתמש וסיסמא ייעודיים בבקר

בידוד הבקר מרשת ה-IZ (אתר SHODAN)

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](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

- מצב הבקר –
  - RUN – מצב ריצה
  - Program – מצב תכנות
  - Remote – ניתן מרחוק לשנות את המצב

התקנת עדכוני SOFTWARE

התקנת עדכוני FIRMWARE



## VPN



User\_Name: Malam



User\_Name: YosiSh



# התחברות מרחוק

○ זיהוי חד – חד ערכי של הספק

○ זיהוי לא גנרי של הספק

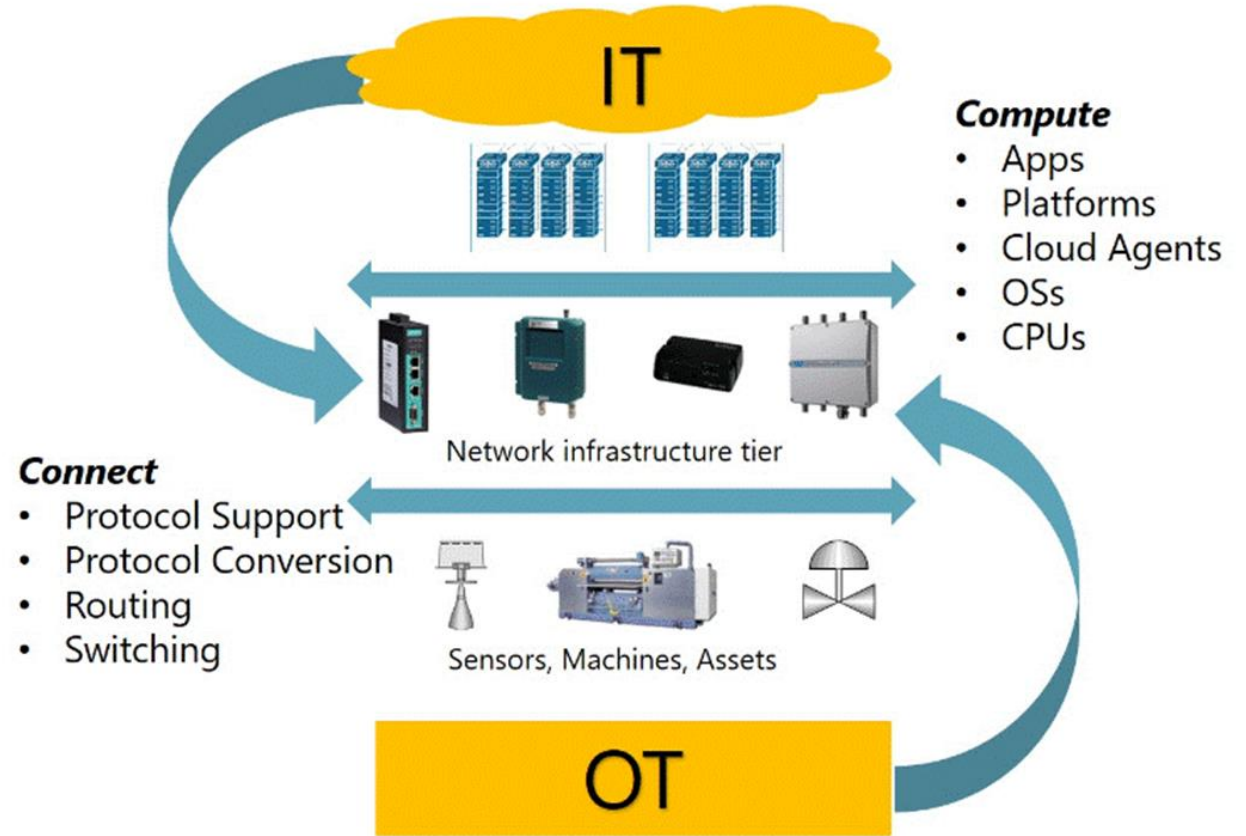
○ תקשורת מוצפנת

○ בדיקת **compliance** (ציות) של הספק

○ שמירת לוגים של ההתחברות

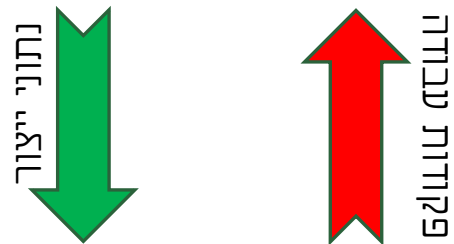
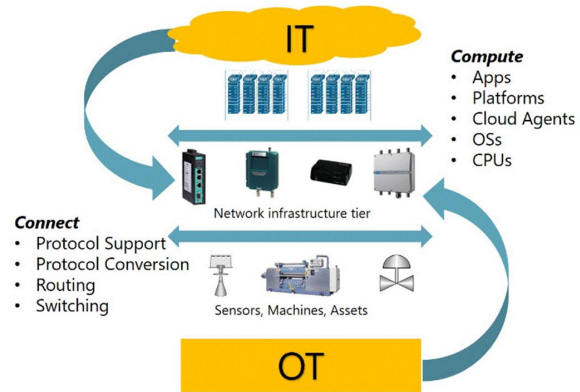
○ החתמת הספק על הצהרת סודיות בטרם כניסה

# הגנה על מערכת ERP





# איומים על מערכת ERP



- פירצה מרשת ה-IT אל רשת ה-OT (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



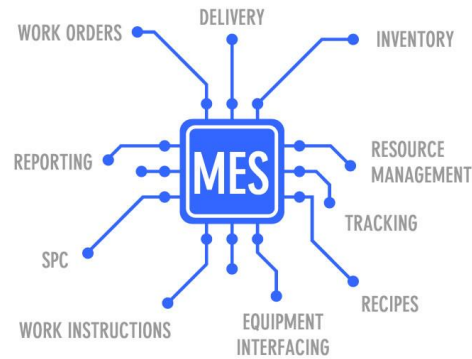
✓ בידוד ברמת סגמנטציה

✓ הקשחת ברמת מערכת הפעלה

✓ הקשחת ברמת מערכת (SAP ,PRIORITY)

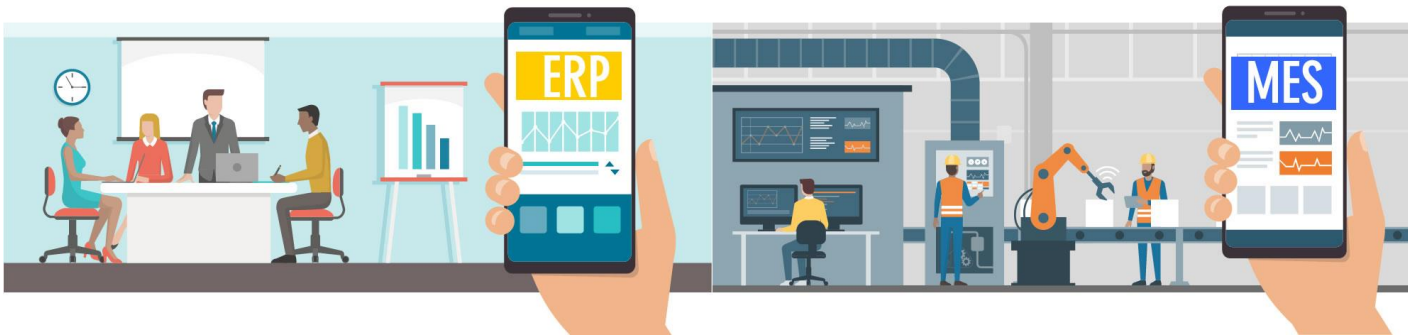
✓ נהלים בהזרמת מידע למערכת (מי ראשי? , מה ניתן?)

# 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 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