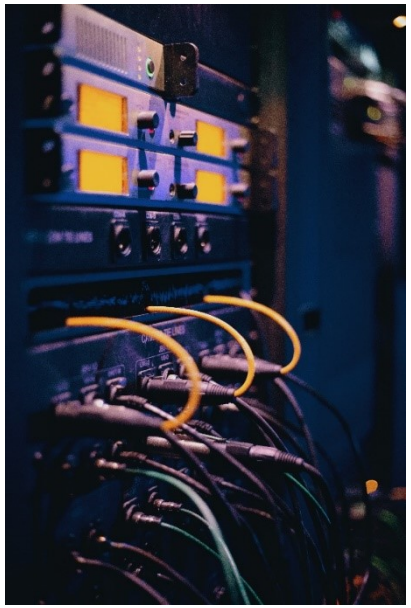
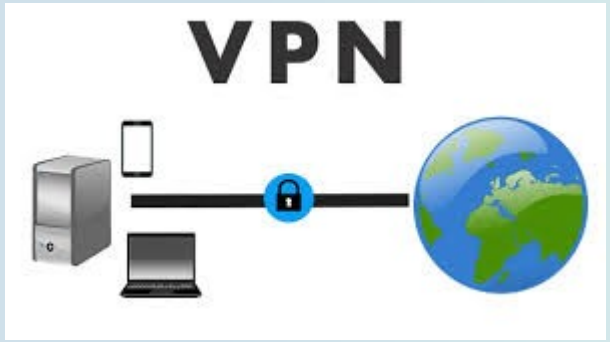
מושגי ייסוד בסייבר – חלק אחרון



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

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

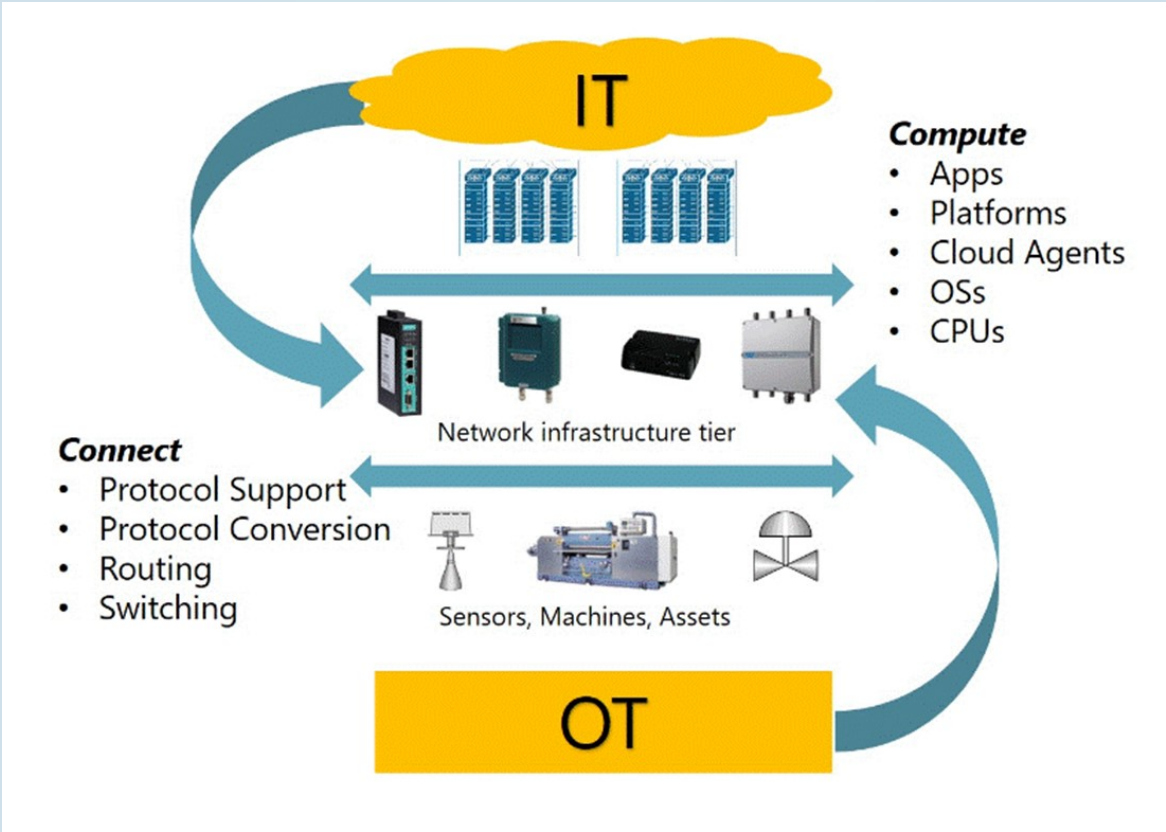
User_Name: Malam

User_Name: YosiSh

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

הגנה על מערכת ERP

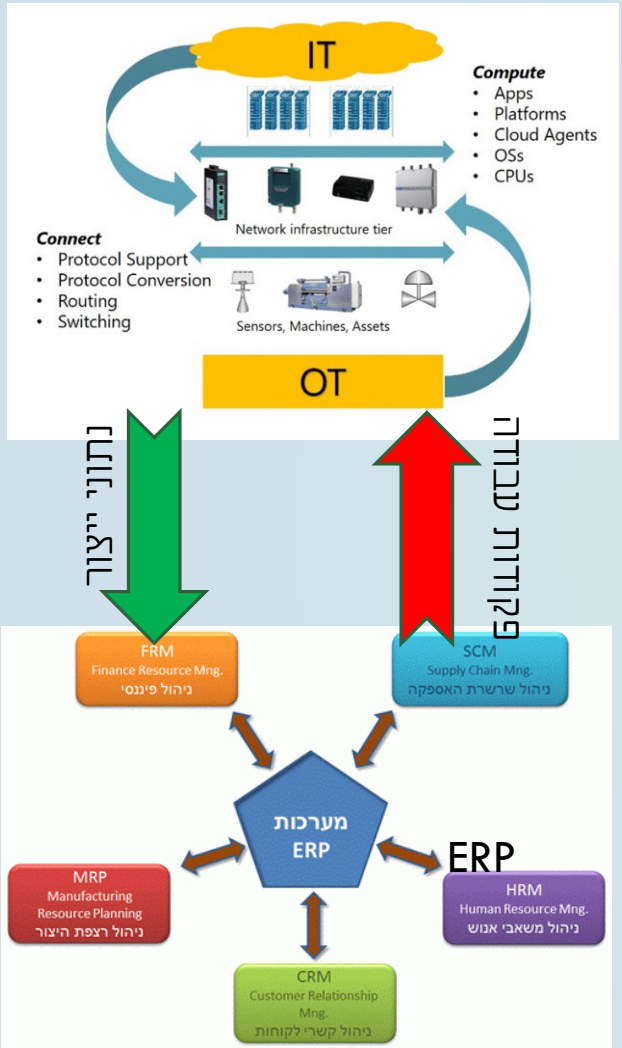
פקודות עבודה



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-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

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

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)

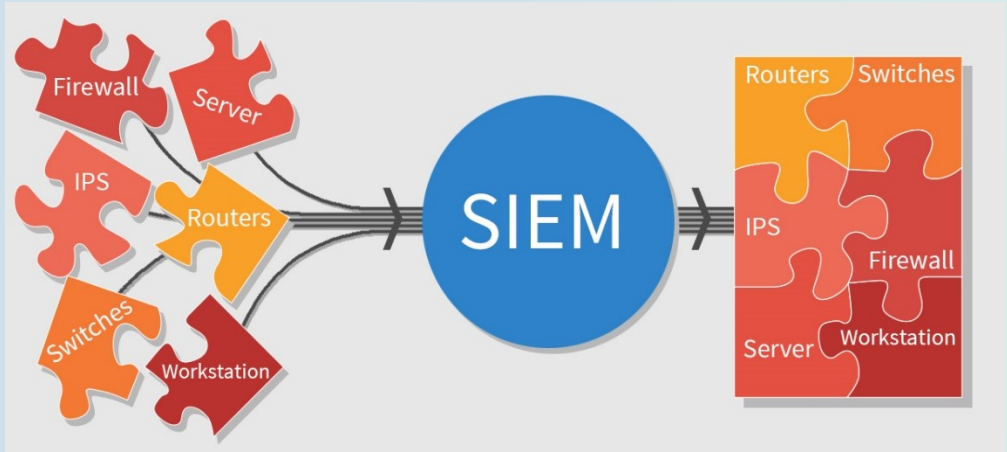
SIEM
- טכנולוגיה שמספקת "עיניים" למה שקורה ברשת בהיבטי סייבר
- מציפה ארועים של תקשורת "חשודה" , או התנהגות "לא לגיטימית" ברשת
- בונים סט של חוקים כדי לקבל ארועים שמעניינים אותנו

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

אין SOC בלי SIEM אך יכול להתקיים SIEM בלי SOC

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

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

ALERTS FROM:
- Security Intelligence Platform
- Help Desk
- Other IT departments

Tier 1
- Monitoring
- Opens ticket and closes false positives
- Basic investigation and mitigation

Tier 2
- Deep Investigations
- Mitigation / recommends changes

Tier 3
- Advanced investigations
- Prevention
- Threat hunting
- Forensics
- Counter intelligence
- Malware reverser

Figure 2: Example of a three-tier SOC and related responsibilities.

Source: https://www.splunk.com/en_us/cyber-security/security-operations-automation/building-a-soc-with-splunk.html

מתכנת SOC

בקרי SOC

אנליסט

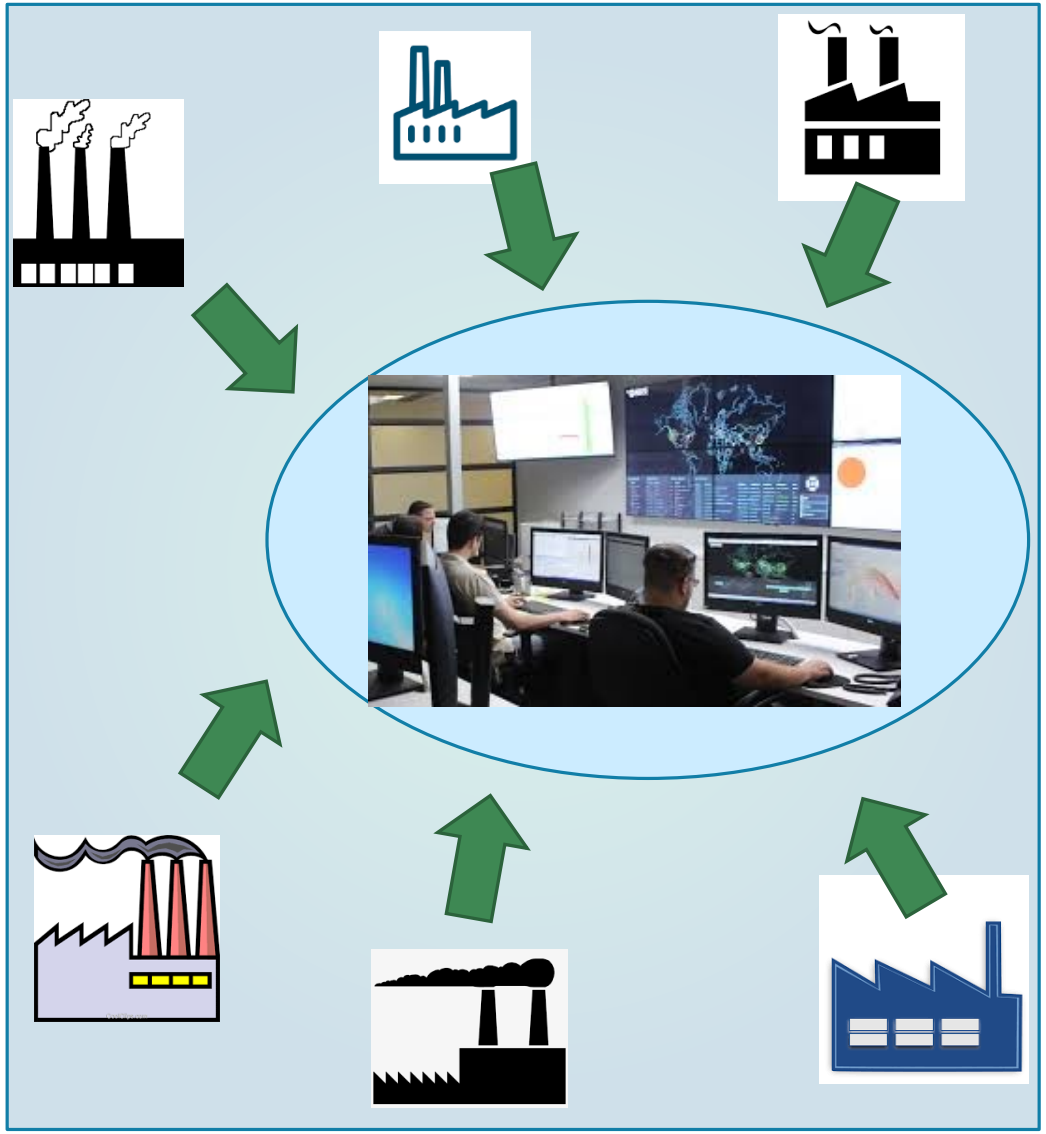
צוותי תגובה

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

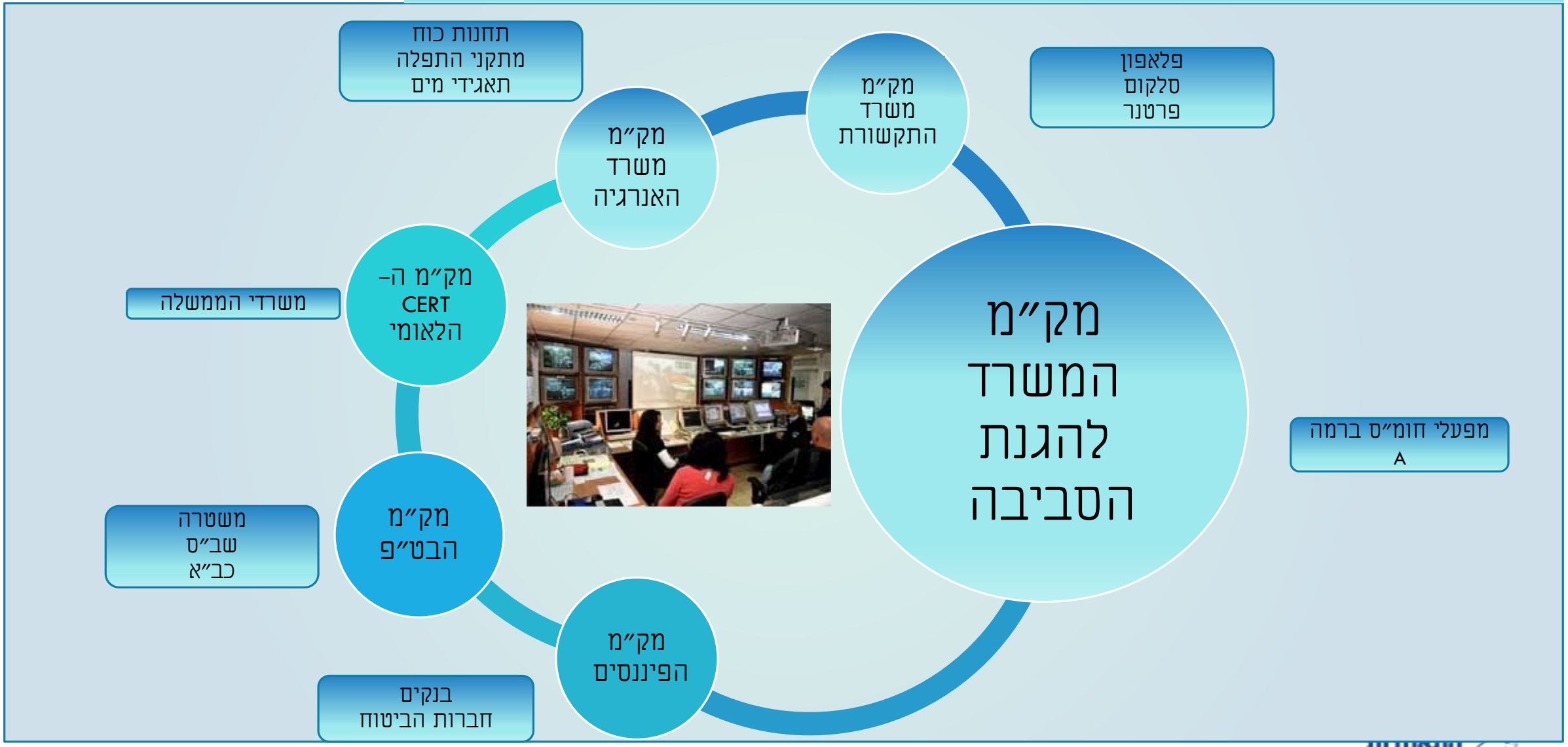
מק"מ = מרכז קיברנטי מגזרי

- ✓ 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