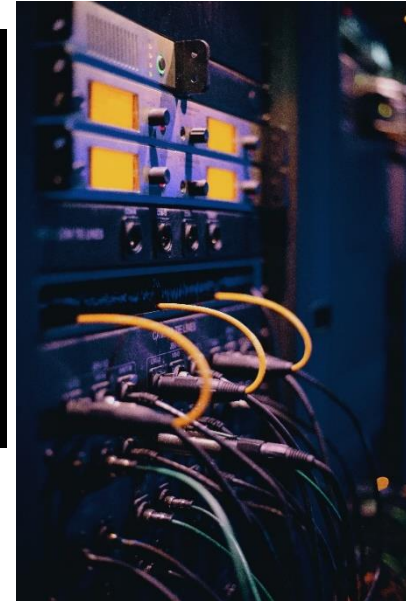
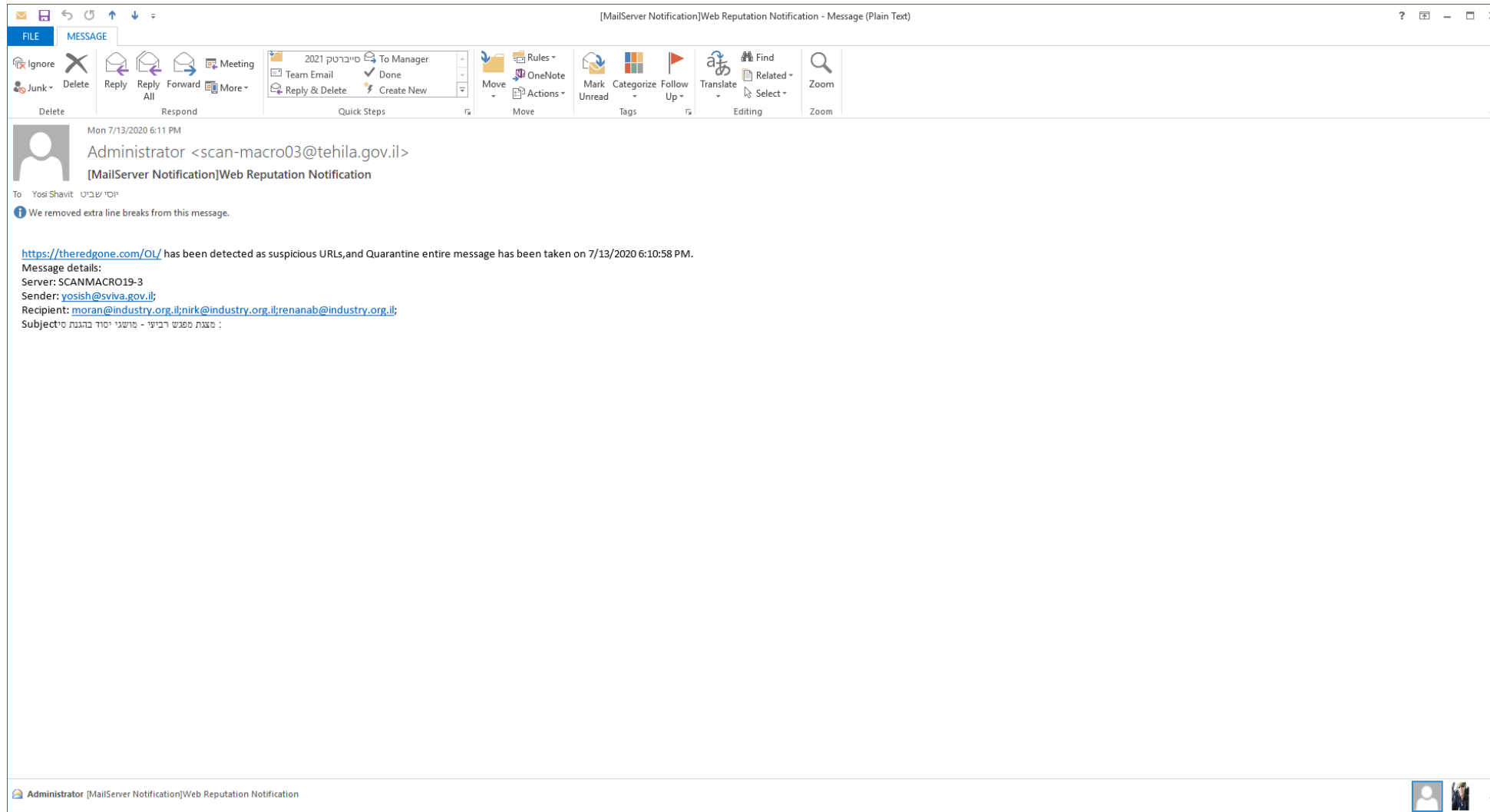


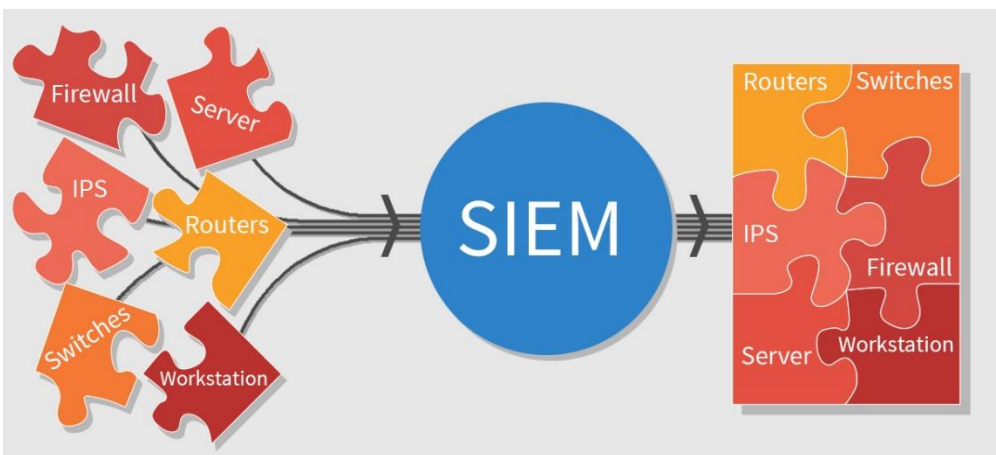
# מושגי ייסוד בהגנת סייבר – חלק ג – המשך



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)



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



**ALERTS FROM:**

- Security Intelligence Platform
- Help Desk
- Other IT departments

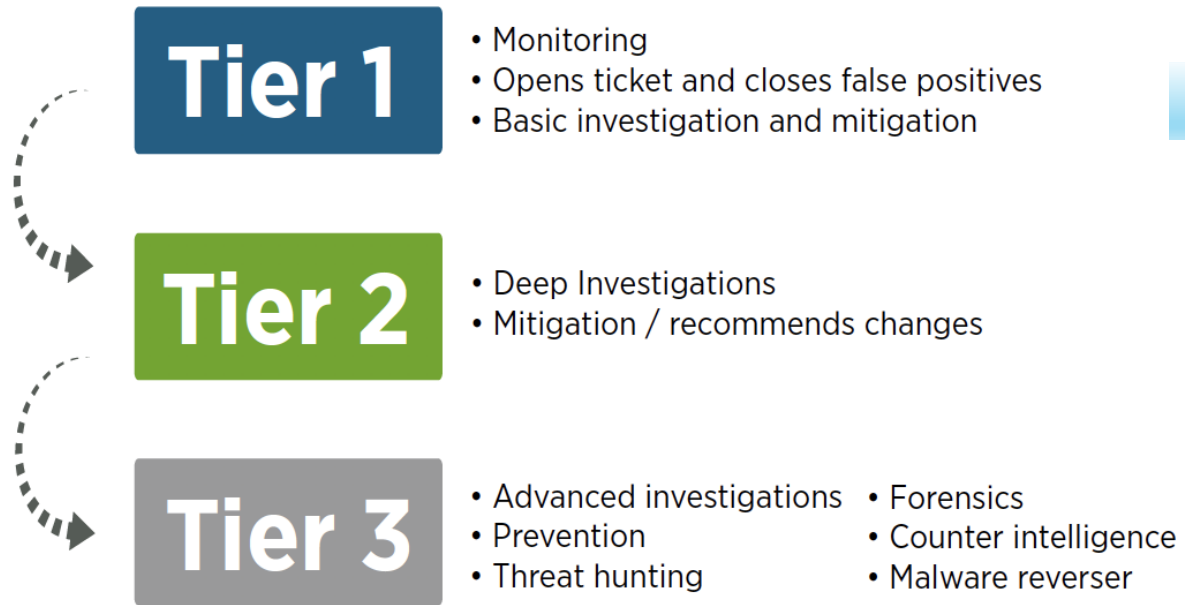


Figure 2: Example of a three-tier SOC and related responsibilities.

Source: [https://www.splunk.com/en\\_us/cyber-security/security-operations-automation/building-a-soc-with-splunk.html](https://www.splunk.com/en_us/cyber-security/security-operations-automation/building-a-soc-with-splunk.html)

# 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

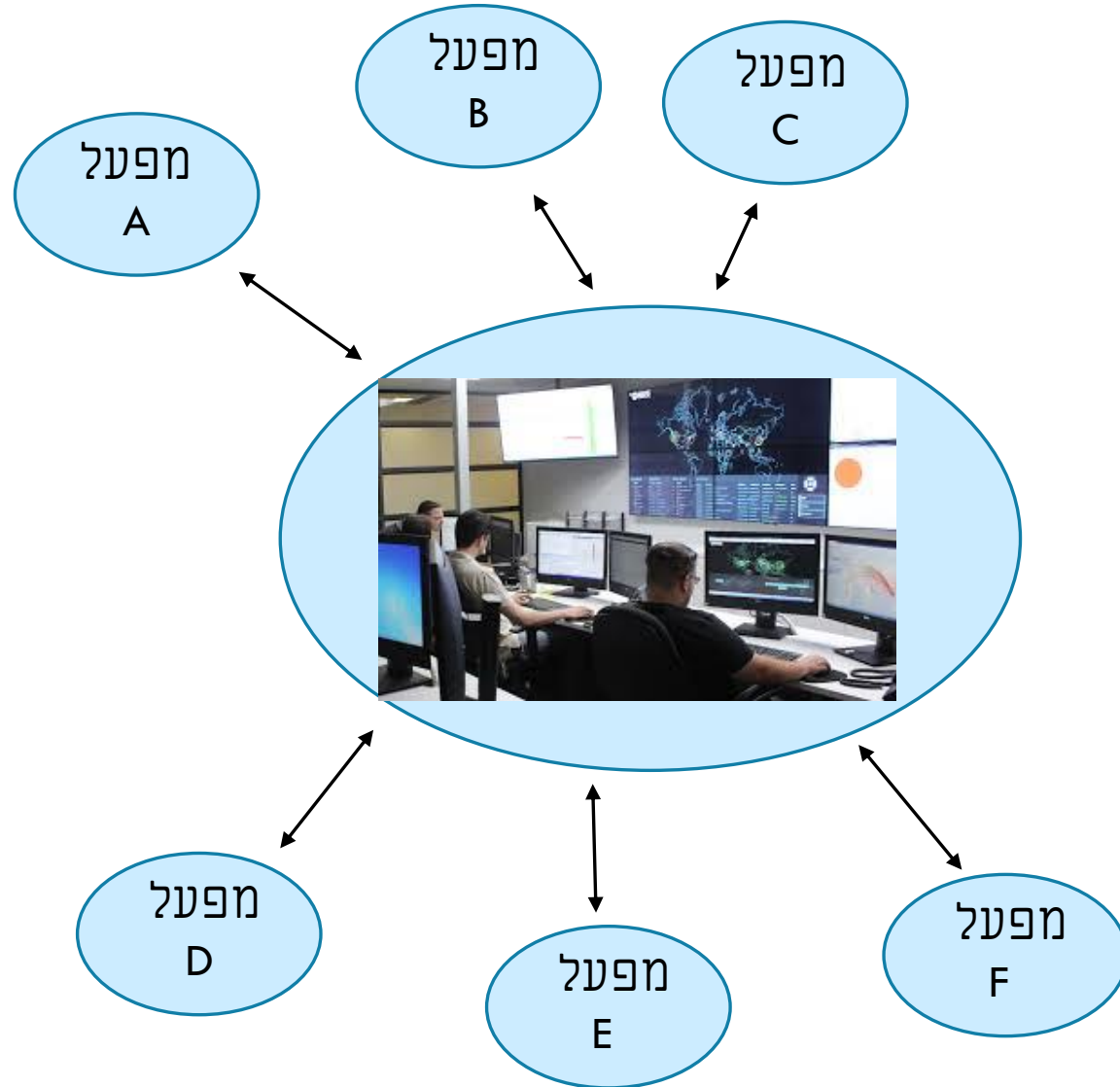
✓ רתימת גופים להעלאת רמת החוסן באמצעות הצפת סיכונים ואיומים קונקרטיים אשר המרכז יזהה אל מול גופים שונים במגזר

✓ 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)



# מערך הסייבר הלאומי מרכז הסייבר בבאר שבע





