הגנת סייבר בתעשייה - מתודולוגיה חדשה לניהול סיכוני סייבר

Yosi Shavit MBA, CISO, CISM, CDPSE
Head of ICS Cyber Security Department
Ministry of Environmental Protection

+972-58-6662242

yosish@sviva.gov.il

www.sviva.gov.il

https://www.pexels.com/

יוסי שביט – ראש יחידת הסייבר בתעשייה המשרד להגנת הסביבה

- מוסמך CDPSE CISM– הסמכות בינלאומיות מארגון ISACA העולמי
- מרצה באקדמיה קורסי סייבר במגמת תואר ראשון במערכות מידע
- מנטור בתוכנית קידום סייבר באפריקה OCMP – Cyber In Africa
- הרצאות סייבר בעולמות תעשייתיים בפורומים בינלאומיים
- מעל 25 שנות ניסיון בנושאי אבטחת מידע וסייבר במערכות IT ומערכות OT (תעשייתיות)
  - פעילות HANDS ON – טכנולוגיות סייבר
  - כתיבת מתודולוגיות – כתיבת תקן סייבר לתעשייה
  - כתיבת רגולציה – מסמך RIA להחלת רגולציה במשק הישראלי

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

הגנת הסביבה וסייבר - מה הקשר?!

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

פגיעה בחיי אדם

- פיצוץ
- קרינת חום
- פיזור רעלים

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

אוגוסט 2020 - ביירות

אמוניום ניטראט 2750 טון

- **170 הרוגים**
- **6000 פצועים**
- **300,000 ללא קורת גג**
- **נזק למרחק של עשרות ק"מ**

מושל ביירות: נזקי הפיצוץ עלולים להגיע ל-15 מיליארד דולר

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

חומרים מסוכנים וסייבר

מערכות ייצור, שינוע ואחסון חומרים מסוכנים במקרים רבים מבוססות על מערכות מבוקרות מחשב

- **פריצה לבקר או למערכת HMI** (מערכת אדם-מכונה המנהלת את הבקר)
  - שינוי לחצים, טמפרטורות, ספיקות - גרימה לדליפת חומר מסוכן במכלים/ צנרת, או דליפת חומר בעיר / פציץ
  - שינוי ערכי PH– הזרמת חומר מסוכן לסביבה - גזים רעילים / זיהום מי תהום

- **פריצה למערכות ERP**
  - עלולות לשנות הרכבים של חומרים המגיעים לריאקטור ולגרום לריאקציות מסוכנות.
  - שינוי יעדי אחסון - החלפה בין חומרי תרופות לחומרי דשן למשל

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

תרחישים עקב אירוע סייבר

1. פיזור רעלים – נמדד ביחידות PPM (כמות חלקיקי רעל במיליון חלקיקי אוויר)

2. אפקט קרינת חום משריפה – נמדד ביחידות של קרינת חום ביחידות של קילוואט למ"ר למשך 60 שניות.

3. אפקט לחץ מפיצוץ – נמדד ביחידות של לחץ (PSI, BAR)

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

איך נראה מפעל תעשייתי?

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

OT NETWORK המשותף לכל המפעלים

HMI Station

commands

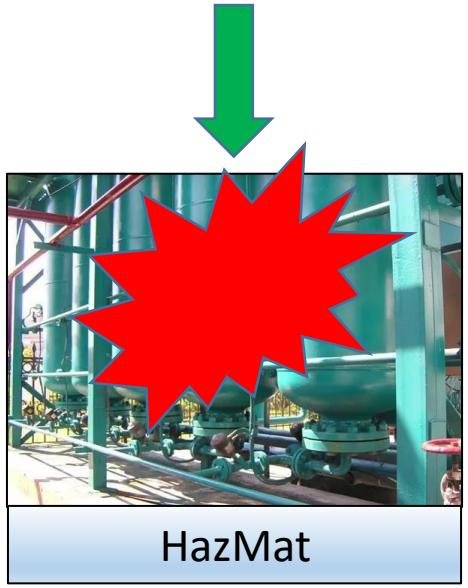
PLC Controller

commands

- Pressure regulators
- Electronic faucets
- Heaters

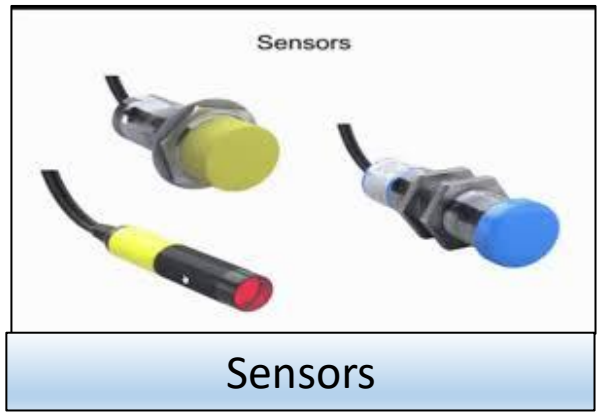
Field Devices (Actuators)

indication



HazMat

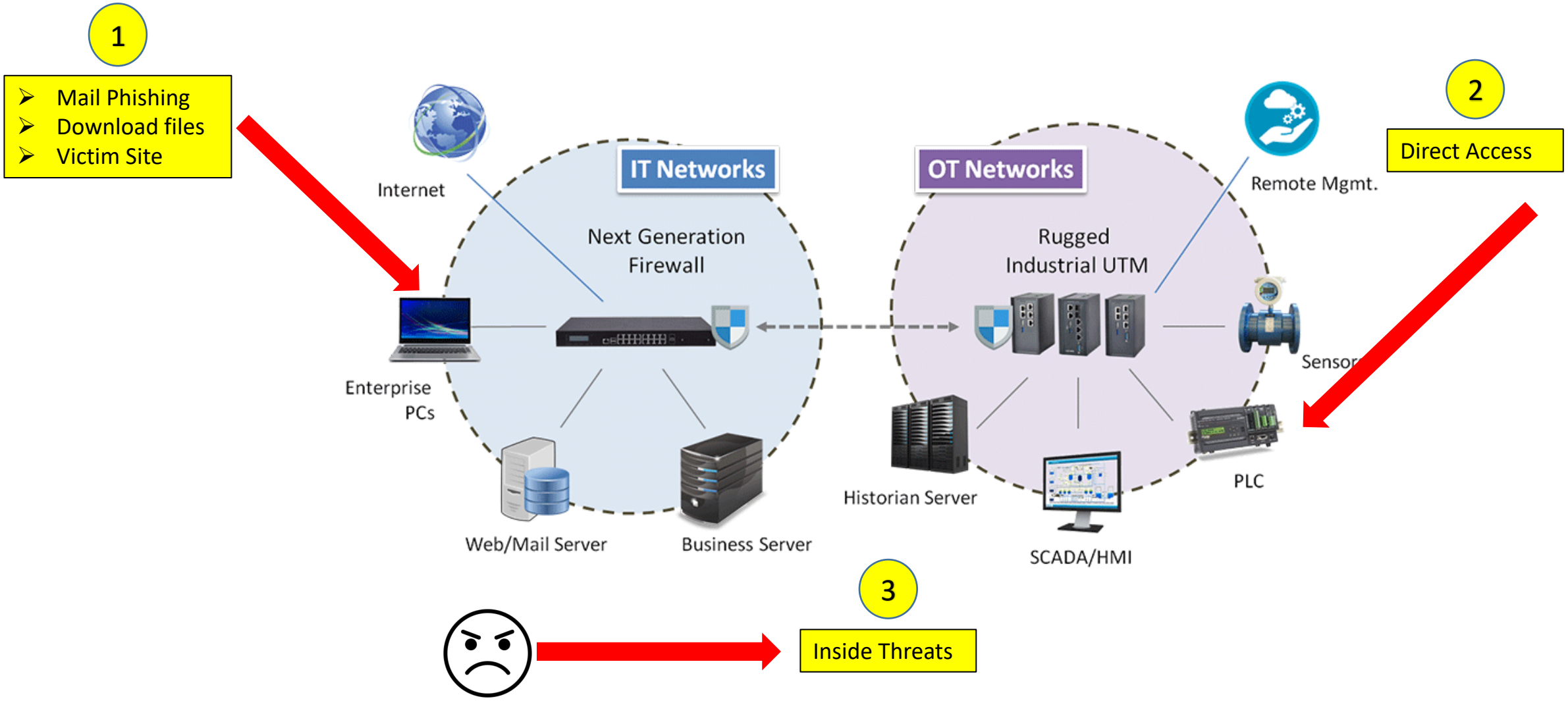
indication



Sensors

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

וקטורי התקיפה לעולם התעשייתי



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

תקיפת מתקני המים בישראל – מאי 2020

Iran cyberattack on Israel's water supply could have sickened hundreds – report

Western official says April hack aimed to raise chlorine to dangerous levels; Israeli official says attack began tit-for-tat on civilian targets

By TOI STAFF and AGENCIES
1 June 2020, 8:26 am |

The Eshkol water filtration plant in northern Israel, April 17, 2007. (Moshe Shai/FLASH90)

Iran tried to increase chlorine levels in the water flowing to residential areas during April's cyberattack against Israel's water systems, a Western intelligence official has told the Financial Times.

May 2020

Iran tried to **increase chlorine levels in the water flowing to residential areas** during cyberattack against Israel's water systems

https://www.shodan.io

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

פריצה למתקן מים בישראל מנקודת מבט של התוקף

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

ספטמבר 2020 – תקיפת מפעל טאואר סמיקונדקטור

במפעלי ייצור שבבים חומרים מסוכנים רבים בכללם גזים מאד רעילים

יצרנית השבבים הישראלית טאואר נמצאת עכשיו תחת מתקפת סייבר

אושרי אלקסלסי 06.09.2020 16 תגובות אבטחת מידע

Share

ציוץ

יצרנית השבבים הישראלית "זיהתה אירוע במערכות המידע והתקשורת שלה" וביצעה ניתוק יזום של המערכות כדי לבצע הערכת מצב. לא ברור כיצד המתקפה השפיעה על הייצור של החברה

יצרנית השבבים הישראלית טאואר (Tower Semiconductor) נמצאת תחת מתקפת סייבר המתמשכת החל מיום שישי. על פי הדיווחים ייתכן שמדובר במתקפה המבוססת על תוכנת כופר, בדומה לזו שתקפה את מערכות סאפיינס הישראלית בחודש יוני האחרון – והובילה על פי הדיווחים לתשלום של רבע מיליון דולר לתוקפים.

הווירוס שפגע בטאואר כבר תקף עיר שלמה באמריקה

בענף הסייבר מעריכים שהווירוס שפגע בחברה הוא RYUK, ששימש בעבר לתקיפת עיר במסצ'וסטס, תחנת הרדיו הגדולה בספרד וחברת ההייטק המקומית סאפיינס. לפי הערכות, חברות ישראליות נוספות נפלו קורבן למתקפת כופר שלו בסוף השבוע האחרון

מאיר אורבך 08.09.20 08:39

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

הרעלת מים בפלוריידה פברואר 2021

Hacker breaks into Florida water treatment facility, changes chemical levels

February 9, 2021

Maria Henriquez

Hackers broke into a water treatment facility in Florida, gained access to an internal ICS platform and changed chemical levels, making the water unsafe to consume.

February 9, 2021

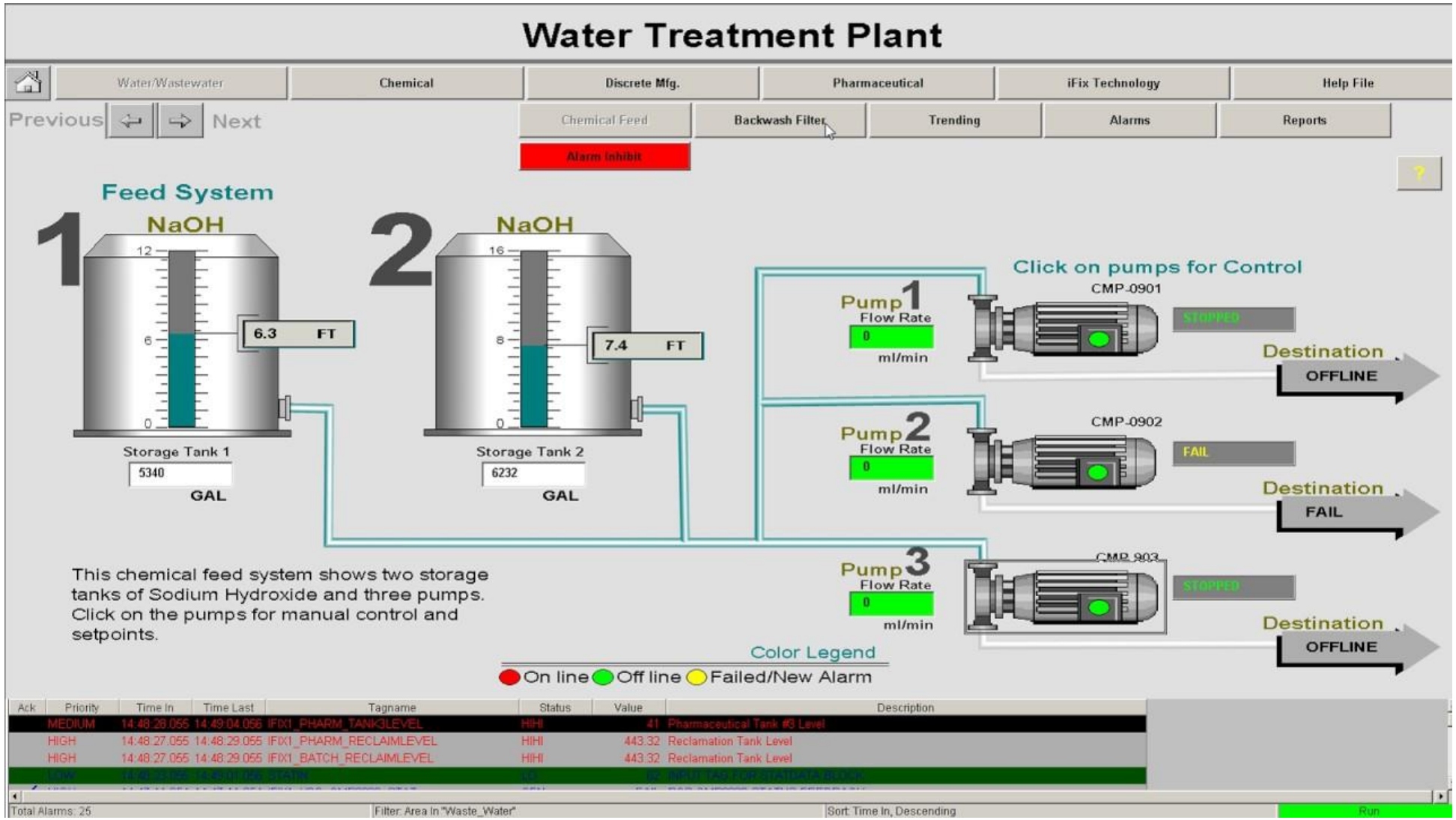
Hackers broke into a water treatment facility in Florida, gained access to an internal ICS platform and changed chemical levels, making the water unsafe to consume.

The hacker increased the amount of NaOH (Sodium Hydroxide) in the drinking water

100 times the required value

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

מתקן טיפול במים מנקודת מבט של המפעיל



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

Colonial Pipeline

May 7, 2021

Colonial Pipeline billing system was compromised while the operational technology systems were not affected. According to CNN sources in the company, the inability to bill the customers was the reason for halting the pipeline operation Colonial Pipeline reported that it shut down the pipeline as a precaution due to a concern that the hackers might have obtained information allowing them to carry out **further attacks** on vulnerable parts of the pipeline the day after the attack

Further attacks = Hazardous Material Attack: fires and explosions

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

סקר מערך הסייבר הלאומי והלמ"ס

המדגם כלל כ-2,500 עסקים

- שניים מכל חמישה עסקים גדולים חווה תקיפת סייבר (42%)
- בקרב תעשיית טכנולוגיית עילית (47%)
- בענפי ההיי-טק, אחד מכל שלוש חברות דיווחו על תקיפה (37%)
- כ-15% מהעסקים הקטנים חוו מתקפת סייבר

חדשות

אחד מחמישה עסקים בישראל חווה תקיפת סייבר

תאריך פרסום: 21.07.2021

אחד מכל חמישה עסקים בישראל (18%) חווה תקיפת סייבר – כך עולה מסקר חדש של הלמ"ס ומערך הסייבר הלאומי

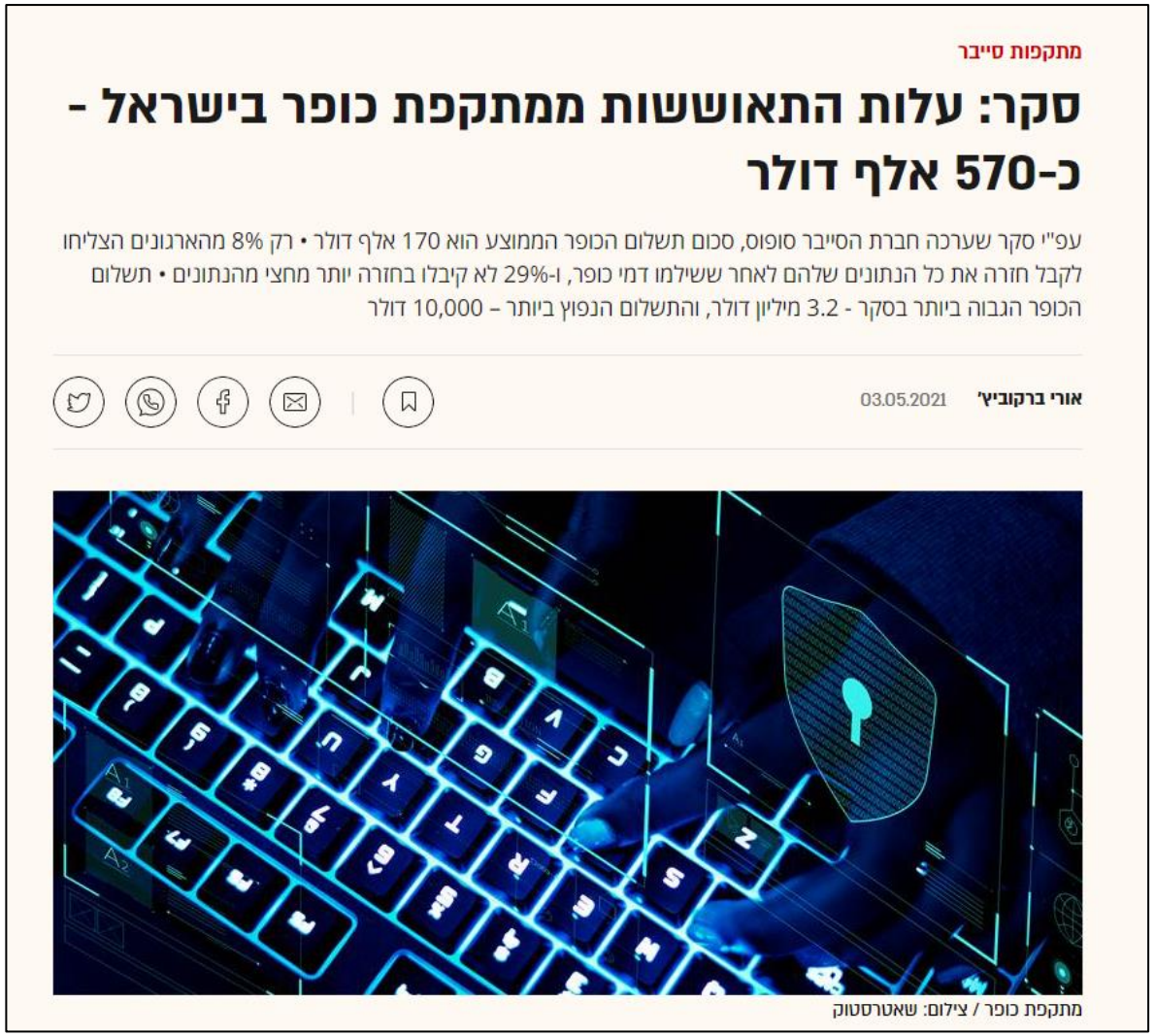
שתפו:

https://www.gov.il/he/departments/news/cyberweeknews

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

עלויות למשק

- צוות משא ומתן
- צוות תגובה ופורנזיקה
- ייעוץ משפטי
- נזק תדמיתי
- תביעות משפטיות הגנת פרטיות
- ניהול תקשורתי
- השבתת מערכות
- אובדן לקוחות
- תשלום כופרה !



מתקפות סייבר

סקר: עלות התאוששות ממתקפת כופר בישראל - כ-570 אלף דולר

עפ"י סקר שערכה חברת הסייבר סופוס, סכום תשלום הכופר הממוצע הוא 170 אלף דולר • רק 8% מהארגונים הצליחו לקבל חזרה את כל הנתונים שלהם לאחר ששילמו דמי כופר, ו-29% לא קיבלו בחזרה יותר מחצי מהנתונים • תשלום הכופר הגבוה ביותר בסקר - 3.2 מיליון דולר, והתשלום הנפוץ ביותר – 10,000 דולר

אורי ברקוביץ' 03.05.2021

מתקפת כופר / צילום: שאטרסטוק

https://www.globes.co.il/news/article.aspx?did=1001369619

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

הנחיות סייבר ל 4262 מפעלים המקבלים היתר רעלים

- מפעלי ייצור חומרים מסוכנים
- תאגידי מים
- מתקני התפלה
- חברת החשמל הישראלית
- נתיבי גז לישראל
- בתי חולים
- נמלים
- שדה תעופה
- התעשייה הפרמצבטית
- תעשיית הדשנים
- מפעלים ביטחוניים
- מפעלי סמיקונדקטור
- שינוע חומרים מסוכנים
- יקבים
- בריכות שחיה

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

פעילות יחידת הסייבר

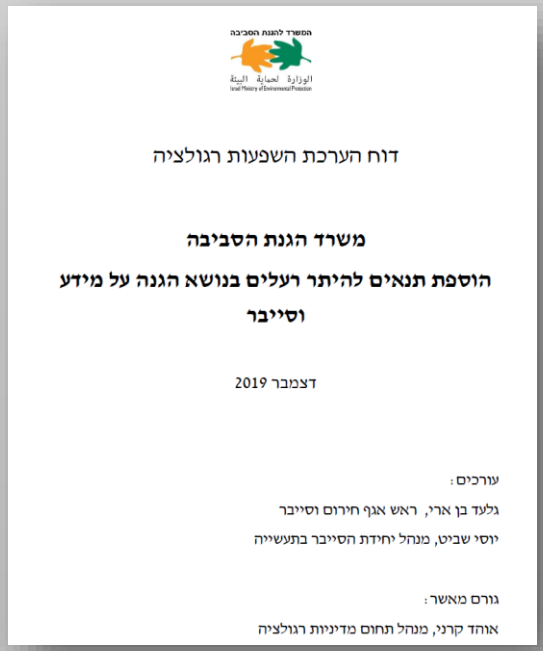
Yosi Shavit MBA, CISO, CISM, CDPSE - Information Security & Cyber Expert
Head of ICS Cyber Security Department
Cellular: 058-6662242 Mail: yosish@sviva.gov.il yosish@gmail.com

2 בשורות למשק בנושא הגנת סייבר

רגולציה חדשה בסייבר

לתעשיית החומרים המסוכנים

מסמך RIA



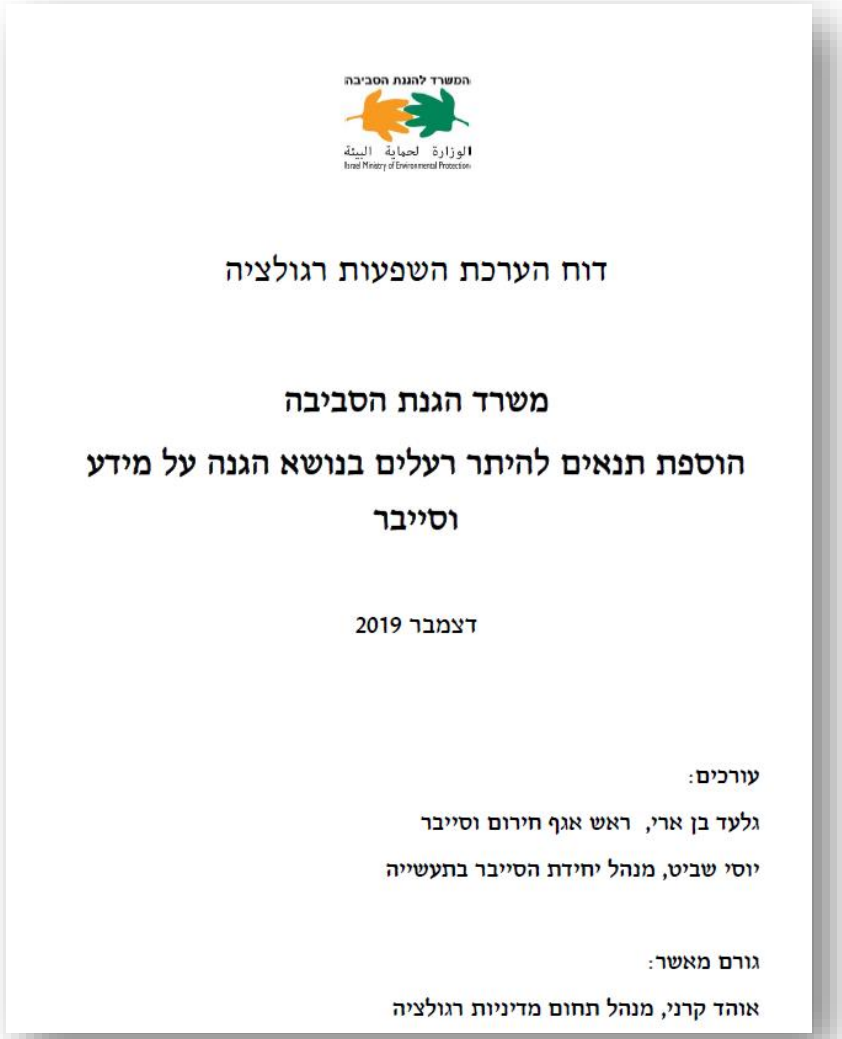
מתודולוגיה חדשה

לניהול סיכוני סייבר בתעשיית החומרים המסוכנים

מדריך סייבר לתעשייה

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

דו"ח RIA



המשרד להגנת הסביבה
الوزارة لحماية البيئة
Israel Ministry of Environmental Protection

דוח הערכת השפעות רגולציה

משרד הגנת הסביבה

הוספת תנאים להיתר רעלים בנושא הגנה על מידע וסייבר

דצמבר 2019

עורכים:

גלעד בן ארי, ראש אגף חירום וסייבר

יוסי שביט, מנהל יחידת הסייבר בתעשייה

גורם מאשר:

אוהד קרני, מנהל תחום מדיניות רגולציה

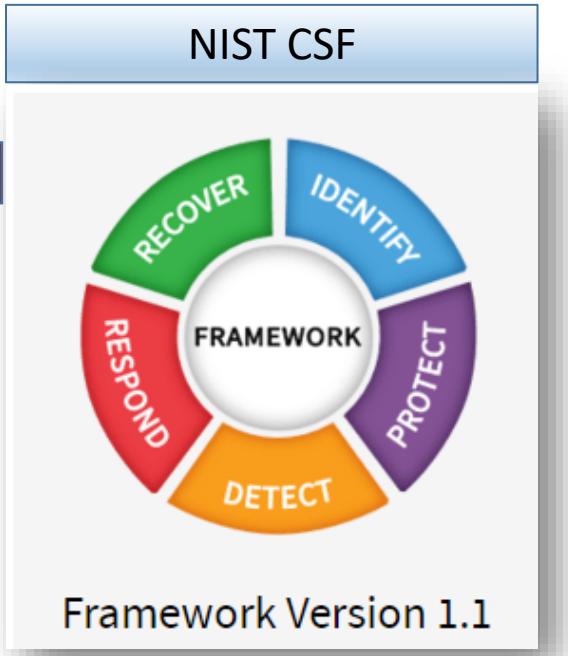
RIA = Regulatory Impact Assessment

- ✓ הגורם היוזם
- ✓ מהות היוזמה
- ✓ החלופות האפשריות
- ✓ רגולטורים משיקים
- ✓ מגבלות ביישום
- ✓ מיפוי בעלי ענין
- ✓ שיח עם בעלי עניין
- ✓ עלות תועלת למשק
- ✓ סקירה בינלאומית
- ✓ הערות הציבור

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

פיתוח מתודולוגיה – חדשה וייחודית בעולם

עבודת שטח - סקרי
סיכונים במפעלים



חורף 2022 – פרסום גרסה 2.0

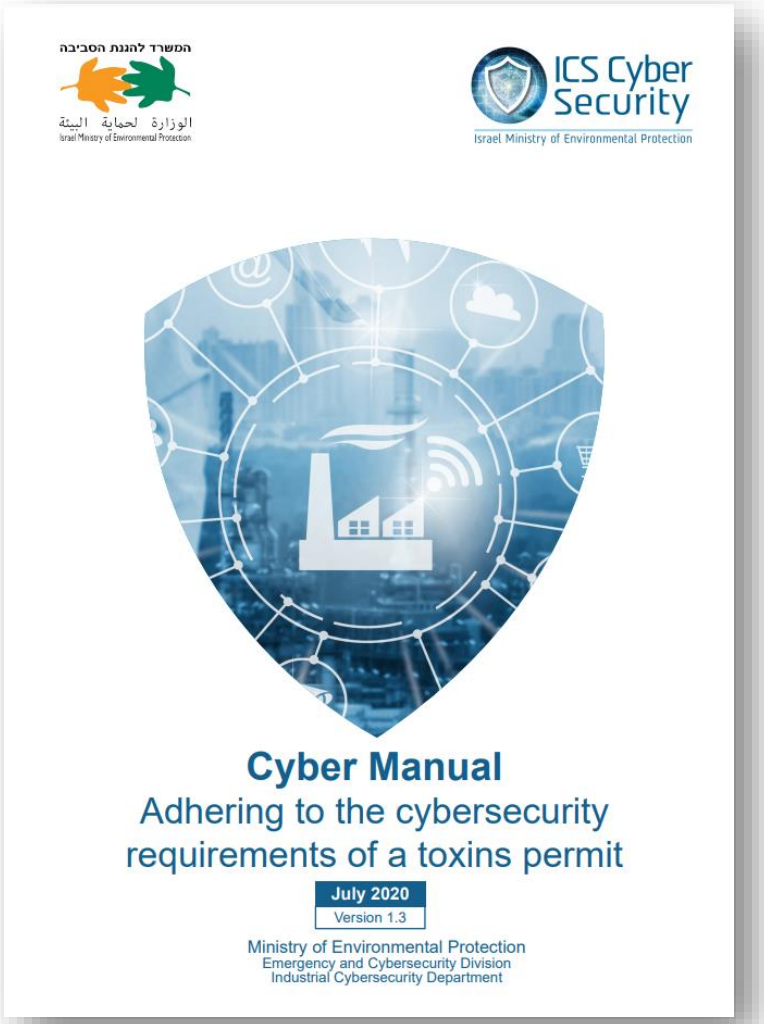
Yosi Shavit MBA, CISO, CISM, CDPSE - Information Security & Cyber Expert
Head of ICS Cyber Security Department
Cellular: 058-6662242 Mail: yosish@sviva.gov.il yosish@gmail.com

המתודולוגיה הפכה לתקן מחייב למפעלים שמקבלים רגולציה

- תכנית עבודה סדורה למפעל
- מיפוי מערכות ממוחשבות בייצור
- סקר סיכונים מותאם לתעשייה
- בקרות לעולם התעשייתי

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

תורגם לאנגלית לבקשת ארגון ה-OECD



הוצג פיסית במדינות הבאות:

אירופה
כנס בנושא סייבר במערכות ICS
בלונדון

אסיה
כנס בנושא סייבר במערכות ICS
בסינגפור

אמירויות
כנס Cyber-Tech Global Dubai 2021
בדובאי

https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

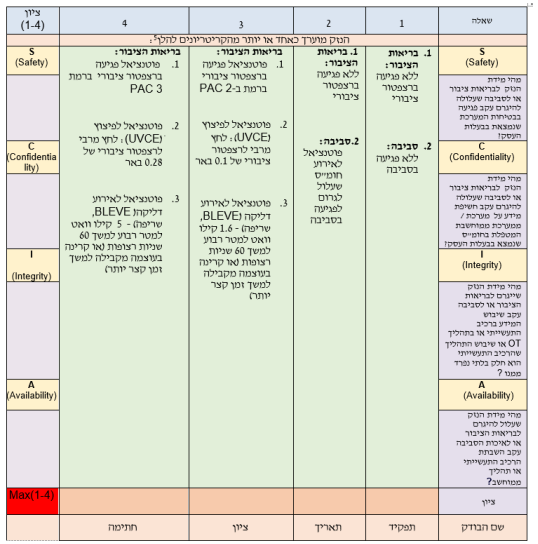
חישוב רמת הסיכון במערכת ממוחשבת המחוברת לחומ"ס

רמת נזק (I) / הסתברות (P)	4	3	2	1
4	16	13	10	7
3	15	12	9	6
2	14	11	8	5
1	13	10	7	4

I

$$Risk = P + 3*I$$

P

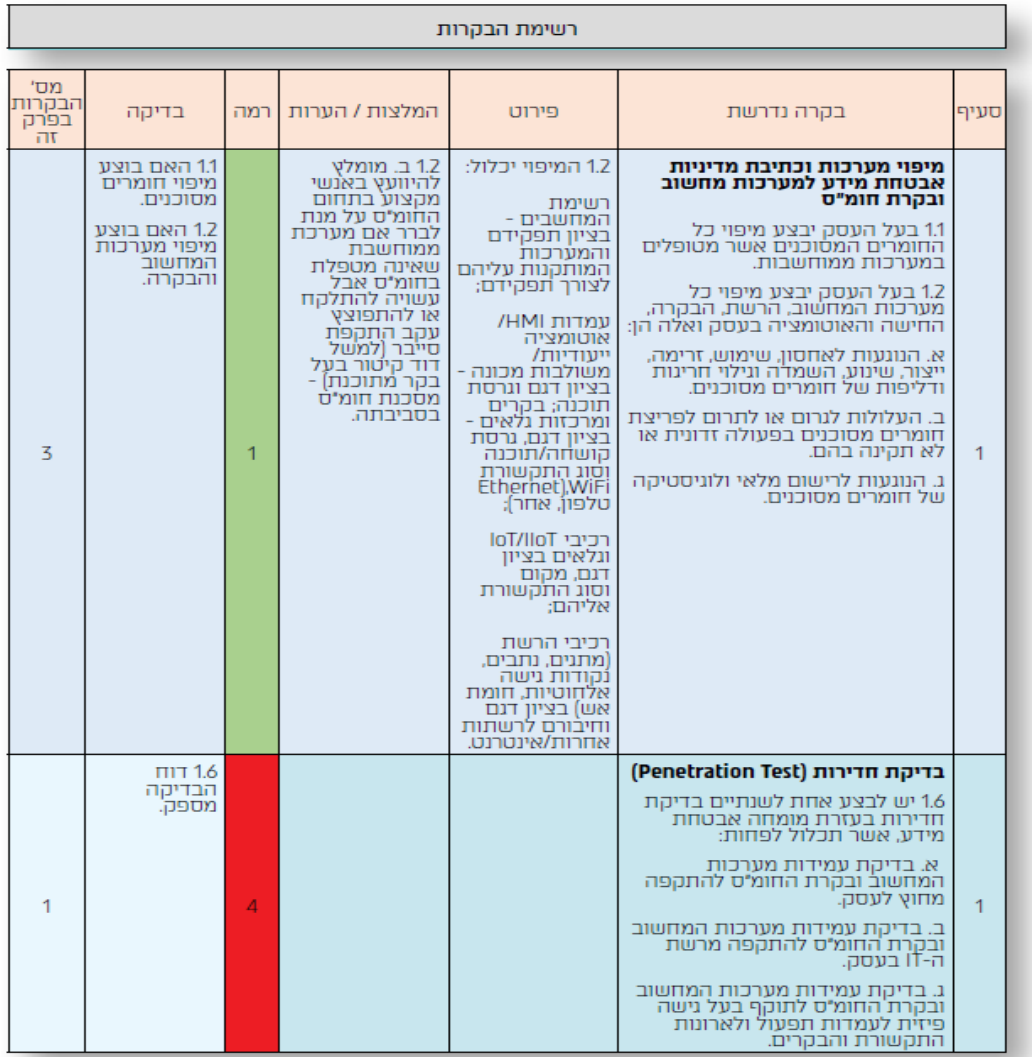


שאלה	1	2	3	4	ציון (1-4)
			הנזק מתערך כאחד או יותר מהקריטריונים להלן:		
S (Safety)	1. בריאות הציבור: ללא פגיעה ברצפטור ציבורי 2. סביבה: ללא פגיעה בסביבה	1. בריאות הציבור: ללא פגיעה ברצפטור ציבורי 2.סביבה: פוטנציאל לאירוע חומ"ס שעלול לגרום לפגיעה בסביבה	1. בריאות הציבור: פוטנציאל פגיעה ברצפטור ציבורי ברמת PAC 2 2. פוטנציאל לפיצוץ (UVCE), לחץ מרבי ברצפטור ציבורי של 0.1 באר 3. פוטנציאל לאירוע דליקה (BLEVE, שריפה) - 1.6 קילו וואט למטר רבוע למשך 60 שניות רצופות (או קרינה בעוצמה מקבילה למשך זמן קצר יותר)	בריאות הציבור: 1. פוטנציאל פגיעה ברצפטור ציבורי ברמת PAC 3 2. פוטנציאל לפיצוץ (UVCE), לחץ מרבי לרצפטור ציבורי של 0.28 באר 3. פוטנציאל לאירוע דליקה (BLEVE, שריפה) - 5 קילו וואט למטר רבוע למשך 60 שניות רצופות (או קרינה בעוצמה מקבילה למשך זמן קצר יותר)	
C (Confidentiality)					
I (Integrity)					
A (Availability)					
Max(1-4)					
	תפקיד	תאריך	ציון	חתימה	

רמת חשיפה > / פרמטר נבדק V	1	2	3	4	ציון (1-4)
1. מספר עובדים החשופים למערכות אדם-מכונה (HMI) הקשורות לחומ"ס	עד 5	6-10	11-50	מעל 50	
2. מספר עובדים בעלי גישה לבקרים המשפיעים על מערכת חומ"ס	עד 10	11-25	26-50	מעל 50	
3. אחריות הטיפול במערכות אדם-מכונה (HMI)	רק עובדים פנימיים	ספקים חיצוניים קבועים	ספקים חיצוניים מזדמנים	נגישות גם לגורמים נוספים	
4. אחריות הטיפול בבקרים המשפיעים על מערכת חומ"ס	רק עובדים פנימיים	ספקים חיצוניים קבועים	ספקים חיצוניים מזדמנים	נגישות גם לגורמים נוספים	
5. מספר עמדות אדם-מכונה (HMI) הקיימות במפעל	1	2-5	6-10	מעל 10	
6. מספר בקרים הקשורים לחומ"ס במפעל	עד 5	6-10	11-50	מעל 50	

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

הקצאת חבילת בקרות להטמעה



רשימת הבקרות

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות בפרק זה
1	**מיפוי מערכות וכתיבת מדיניות אבטחת מידע למערכות מחשוב ובקרת חומ"ס** 1.1 בעל העסק יבצע מיפוי כל החומרים המסוכנים אשר מטופלים במערכות ממוחשבות. 1.2 בעל העסק יבצע מיפוי כל מערכות המחשוב, הרשת, הבקרה, החישה והאוטומציה בעסק ואלה הן: א. הנוגעות לאחסון, שימוש, זרימה, ייצור, שינוע, השמדה וגילוי חריגות ודליפות של חומרים מסוכנים. ב. העלולות לגרום או לתרום לפריצת חומרים מסוכנים בפעולה זדונית או לא תקינה בהם. ג. הנוגעות לרישום מלאי ולוגיסטיקה של חומרים מסוכנים.	1.2 המיפוי יכלול: רשימת המחשבים - בציון תפקידם והמערכות המותקנות עליהם לצורך תפקידם; עמדות HMI/ אוטומציה ייעודיות/ משולבות מכונה - בציון דגם וגרסת תוכנה; בקרים ומרכזות נלאים - בציון דגם, גרסת קושחה/תוכנה וסוג התקשורת Ethernet),WiFi טלפון, אחר); רכיבי IoT/IIoT ונלאים בציון דגם, מקום וסוג התקשורת אליהם; רכיבי הרשת (מתגים, נתבים, נקודות גישה אלחוטיות, חומת אש) בציון דגם וחיבורם לרשתות אחרות/אינטרנט.	1.2 ב. מומלץ להיוועץ באנשי מקצוע בתחום החומ"ס על מנת לברר אם מערכת ממוחשבת שאינה מטפלת בחומ"ס אבל עשויה להתלקח או להתפוצץ עקב התקפת סייבר (למשל דוד קיטור בעל בקר מתוכנת) - מסכנת חומ"ס בסביבתה.	1	1.1 האם בוצע מיפוי חומרים מסוכנים. 1.2 האם בוצע מיפוי מערכות המחשוב והבקרה.	3
1	**בדיקת חדירות (Penetration Test)** 1.6 יש לבצע אחת לשנתיים בדיקת חדירות בעזרת מומחה אבטחת מידע, אשר תכלול לפחות: א. בדיקת עמידות מערכות המחשוב ובקרת החומ"ס להתקפה מחוץ לעסק. ב. בדיקת עמידות מערכות המחשוב ובקרת החומ"ס להתקפה מרשת ה-IT בעסק. ג. בדיקת עמידות מערכות המחשוב ובקרת החומ"ס לתוקף בעל גישה פיזית לעמדות תפעול ולארונות התקשורת והבקרים.			4	1.6 דוח הבדיקה מספק.	1

פוטנציאל הסיכון	חבילת הבקרות בהתאם לפוטנציאל הסיכון	כמות הבקרות לחבילה זו
4-7	1	41
8-11	2	59
12-14	3	81
15-16	4	92

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

תכנית עבודה להעלאת חוסן במפעלים

12 Months

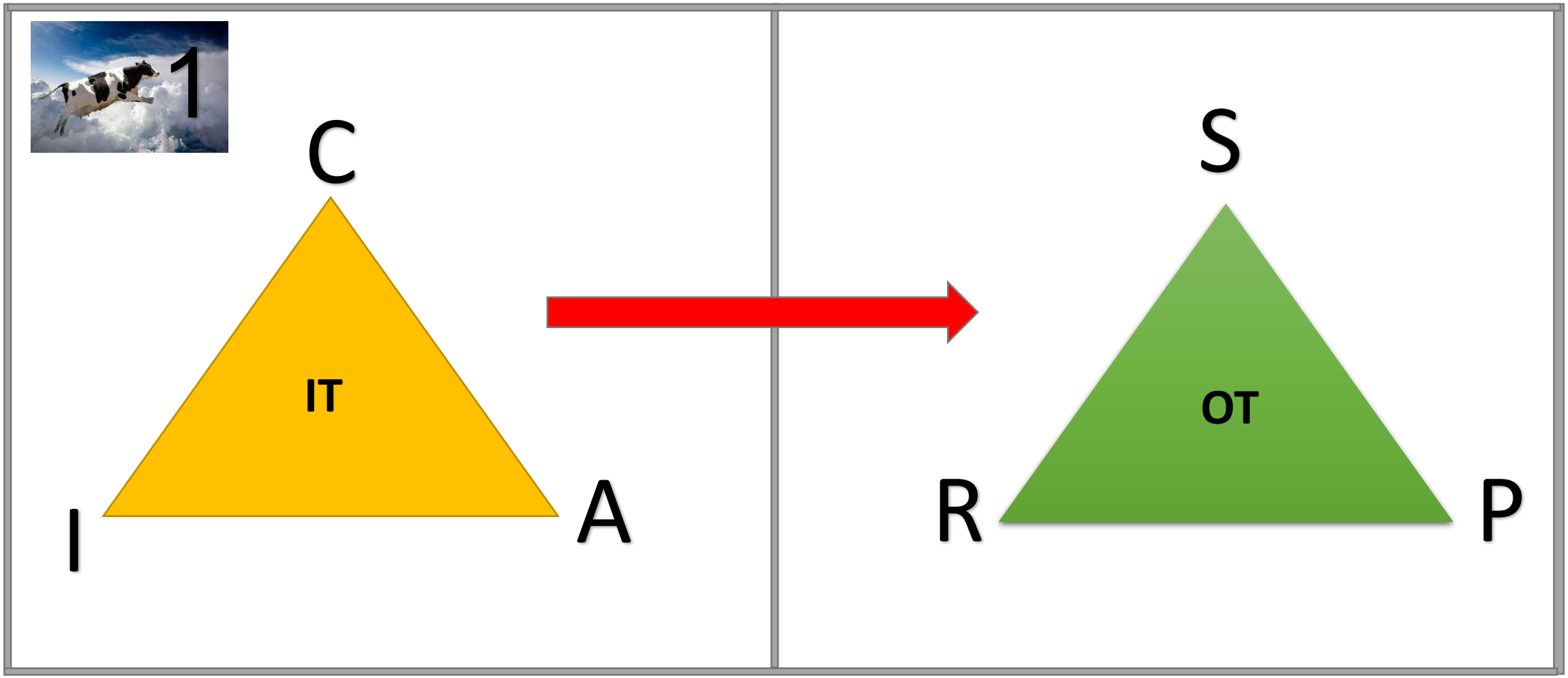
24 months

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

פרות קדושות (נשחטות) בתעשייה

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

SAFETY!!!



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

UPDATES?!

Y

N

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

סיסמא לבקר

PassWord? Or Pass – Word!

מקרה א' – אין סיסמא לבקר כי הוא לא מאפשר (בקר ישן)
מקרה ב' – אין סיסמא כי "אנחנו צריכים להגיב מהר"
מקרה ג' – יש משתמש וסיסמא דיפולטיבים מיום התקנת הבקר
מקרה ד' – יש משתמש וסיסמא גנרים הידועים לכל אנשי המפעל כולל ספקים

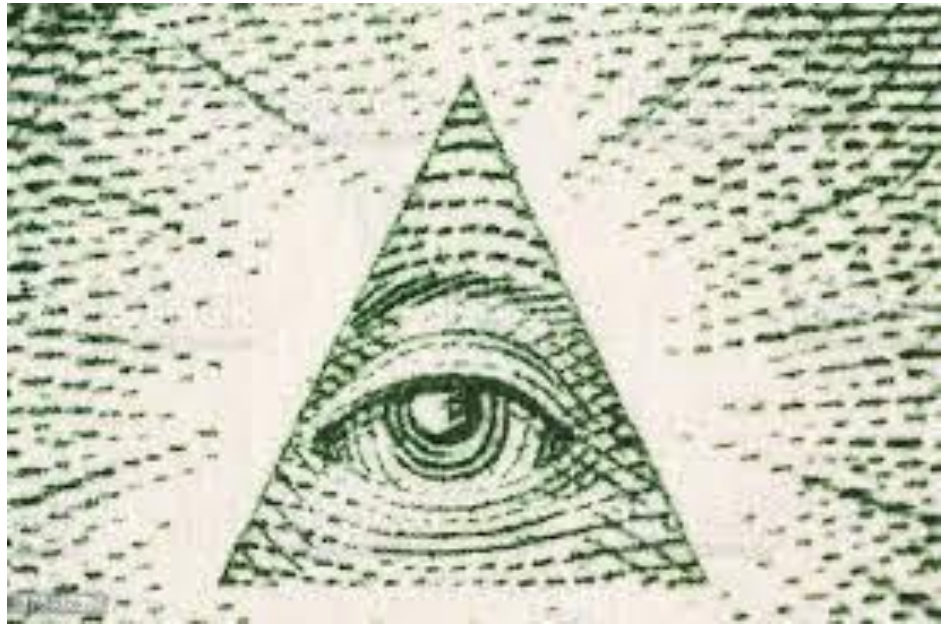
נדרש: משתמש וסיסמא ייחודיים ומורכבים בליווי 2FA

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

השבתת מערכת ייצור עקב שדרוג?
בעולמות ה-OT זמן תחזוקה: אחת לשנה

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

Eyes

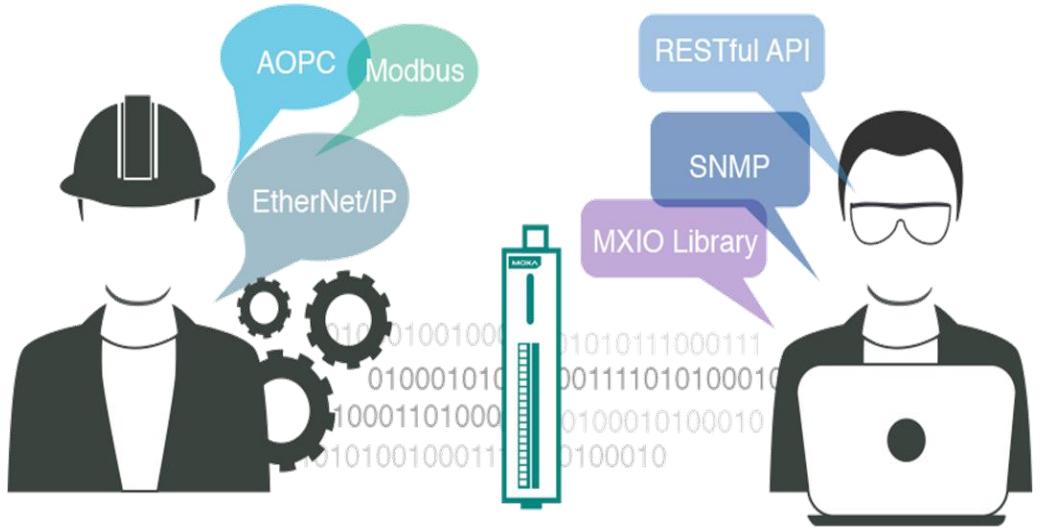


IT
• Fw • IDS, IPS • Anti-virus • CDR

OT
• ? • ? • ? • ?

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

מי אחראי על הגנת סייבר ב רשת ה-OT ?!



Operation Manager

CISO

× <u>תשובה א:</u> אין אחראי

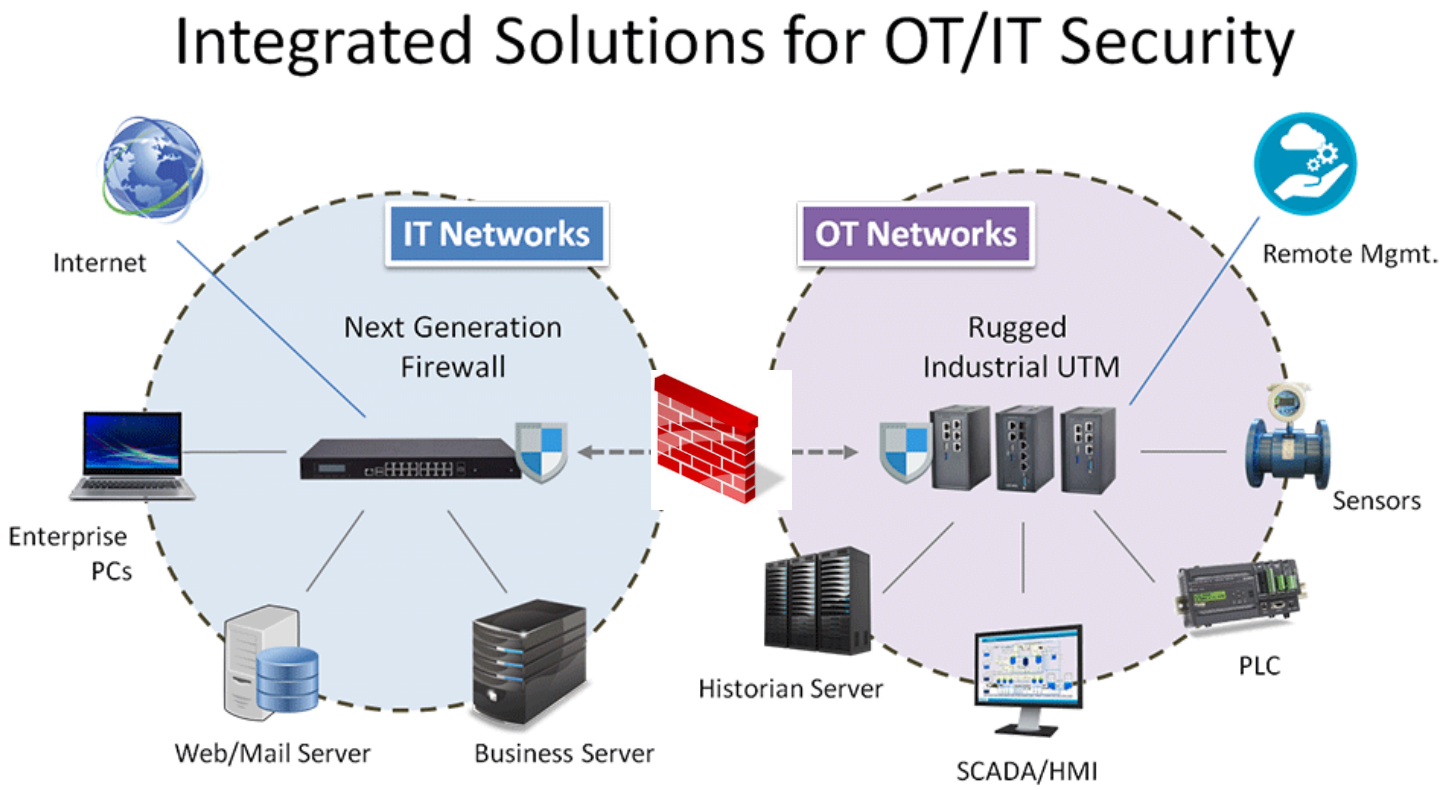
× <u>תשובה ב:</u> כל אחד אחראי על תחומו

✓ <u>תשובה ג:</u> HSE אחראי

HSE – Health, Safety, Environment

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

הפרדת רשתות



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

איומים

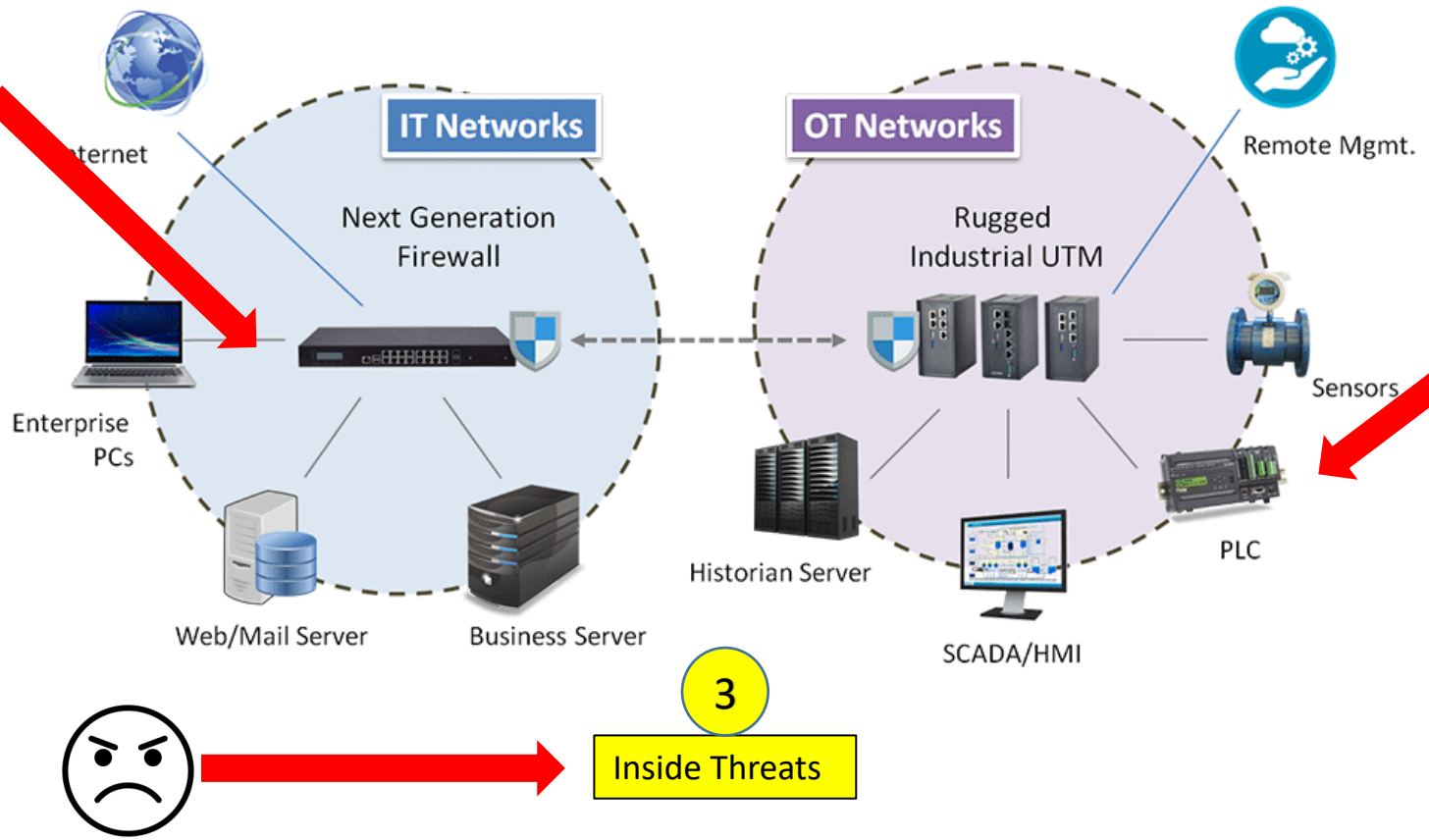
Attack Surface

Systems : WinXP, Win 7
Access to HMI
Supply Chain

Attack Vector

1

- Mail Phishing
- Download files
- Victim Site



2

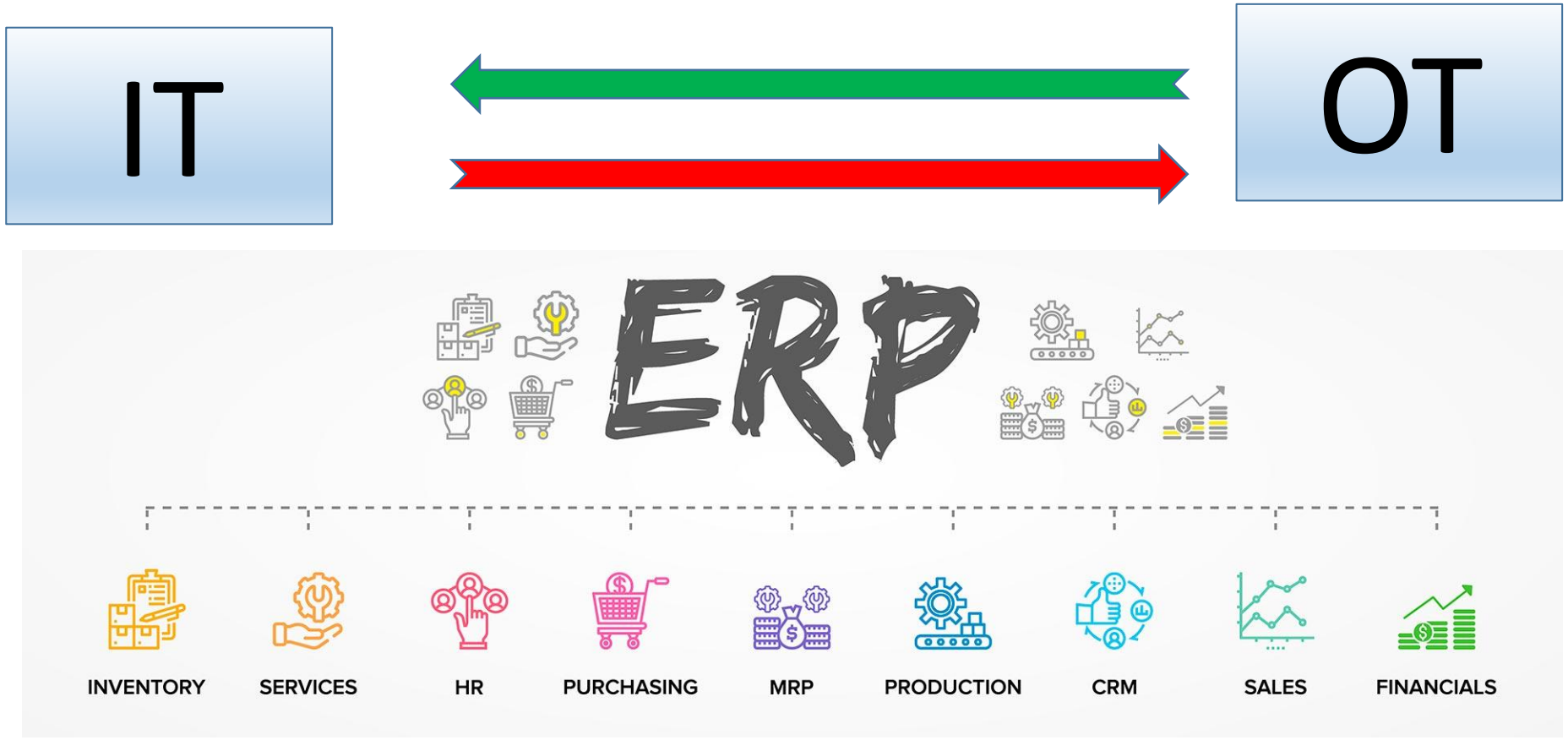
Direct Access

3

Inside Threats

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

איומים



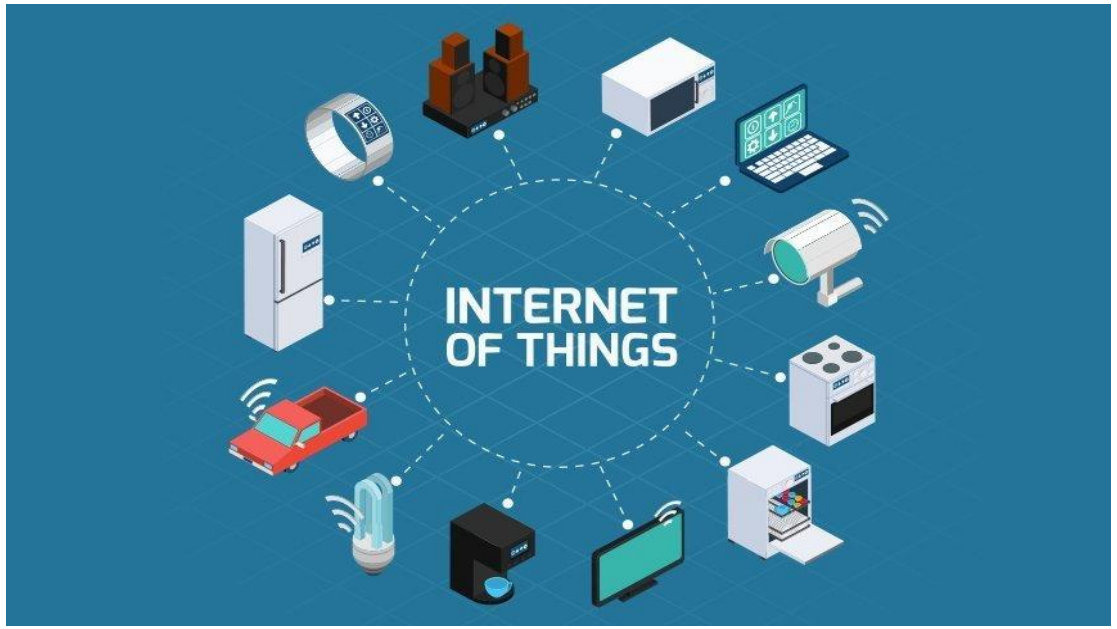
Material Requirements Planning

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

איומים

Industry 4.0

IOT

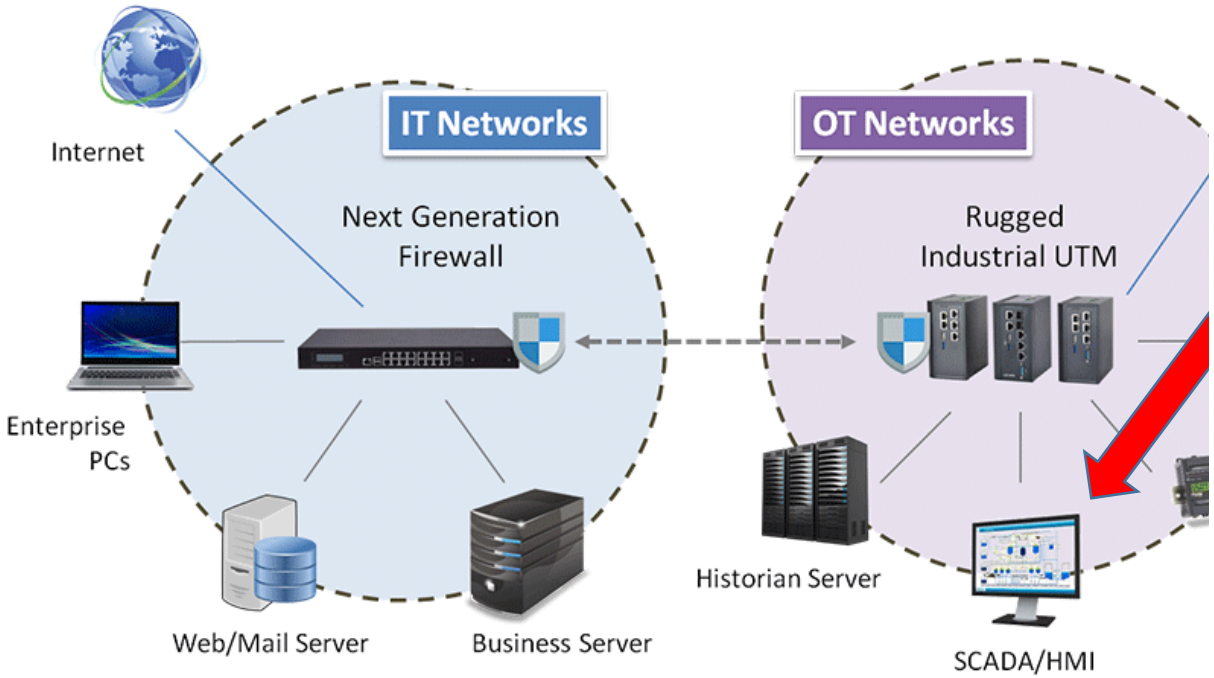


IIOT

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

Remote Access

איומים

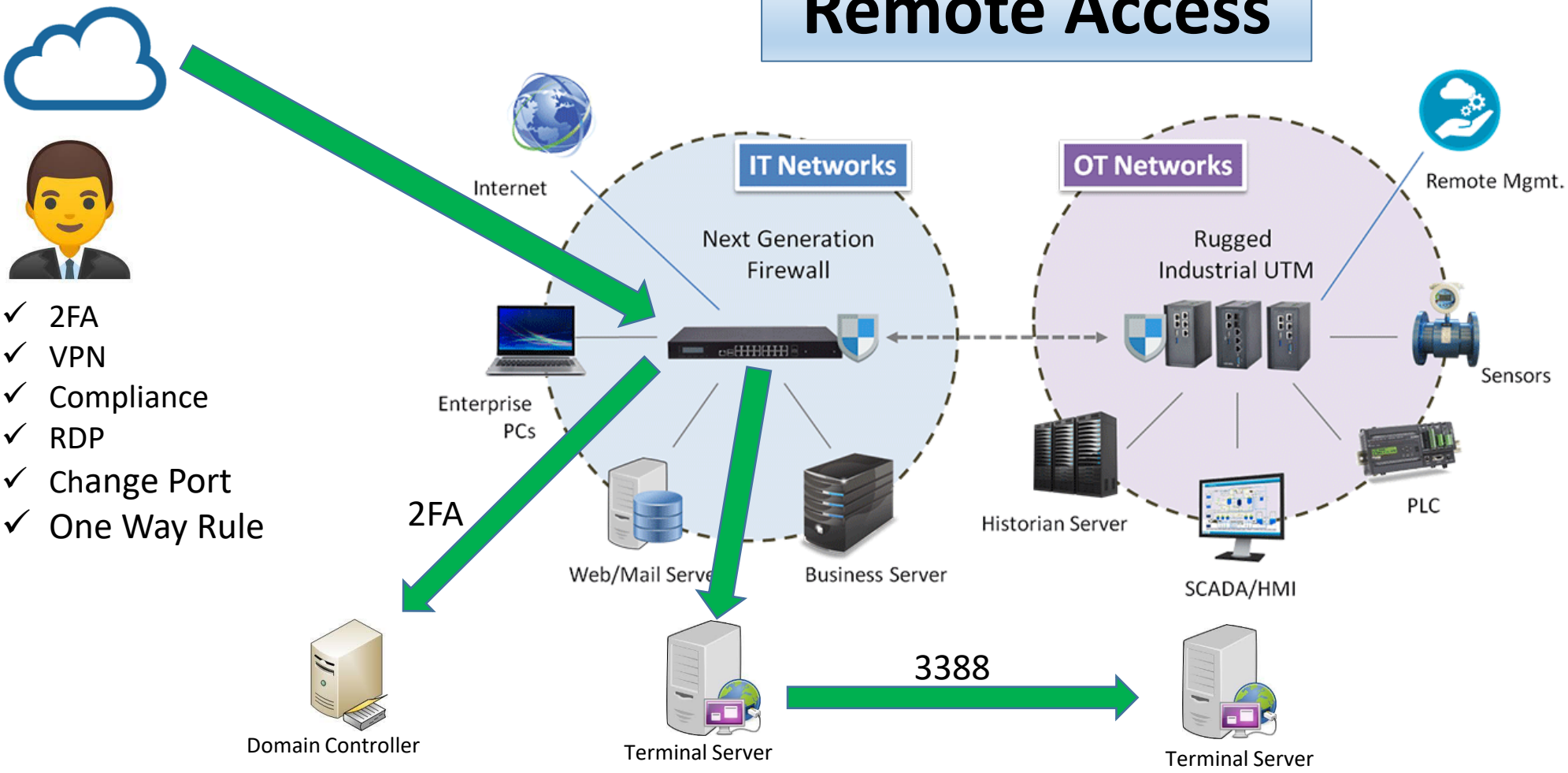


Yosi Shavit MBA, CISO, CISM, CDPSE - Information Security & Cyber Expert
Head of ICS Cyber Security Department
Cellular: 058-6662242 Mail: yosish@sviva.gov.il yosish@gmail.com

Remote Access

בקרות

- ✓ 2FA
- ✓ VPN
- ✓ Compliance
- ✓ RDP
- ✓ Change Port
- ✓ One Way Rule



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

בקרות

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

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

בקרות

הגנה על הבקר

מצב הבקר –

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

✓התקנת עדכוני SOFTWARE

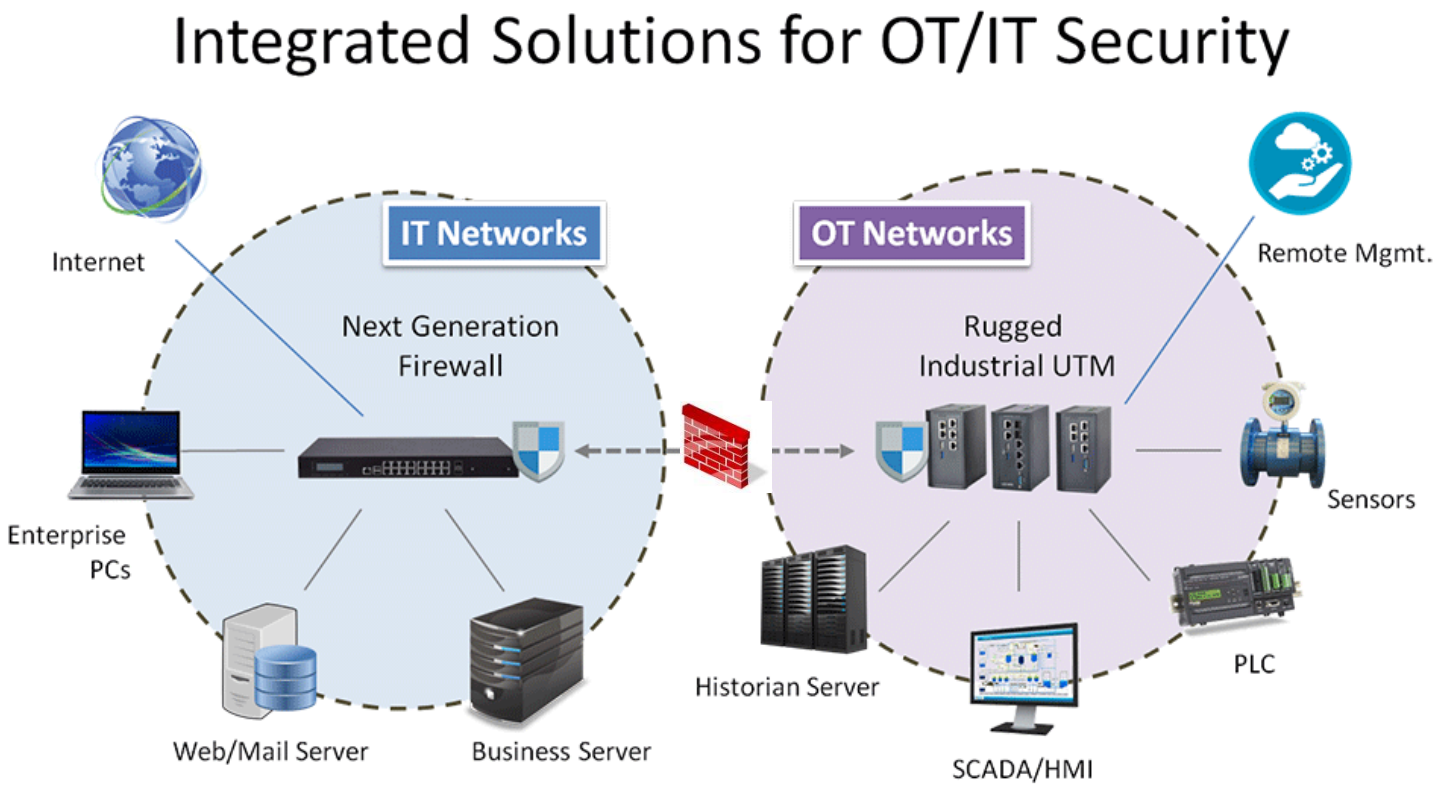
✓התקנת עדכוני FIRMWARE

Head of ICS Cyber Security Department
Cellular: 058-6662242 Mail: yosish@sviva.gov.il yosish@gmail.com

הפרדת רשתות

בקרות

- ✓ דיודה חד כיוונית – UNIDIRECTIONAL SECURITY GATEWAY
- ✓ חומת אש
- ✓ הפרדה פיסית בכבילה נפרדת
- ✓ בקרת גישה פיזית לארון תקשורת
- ✓ ככל הניתן מניעת גישת ספקים מרחוק
- ✓ חברות הסייבר – פתרונות יצירתיים



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

בקרות

התמודדות עם סוגיית העדכונים

Windows HMI

PLC

Virtual Patching

Digital Twin

Digital Shadow

Simulation

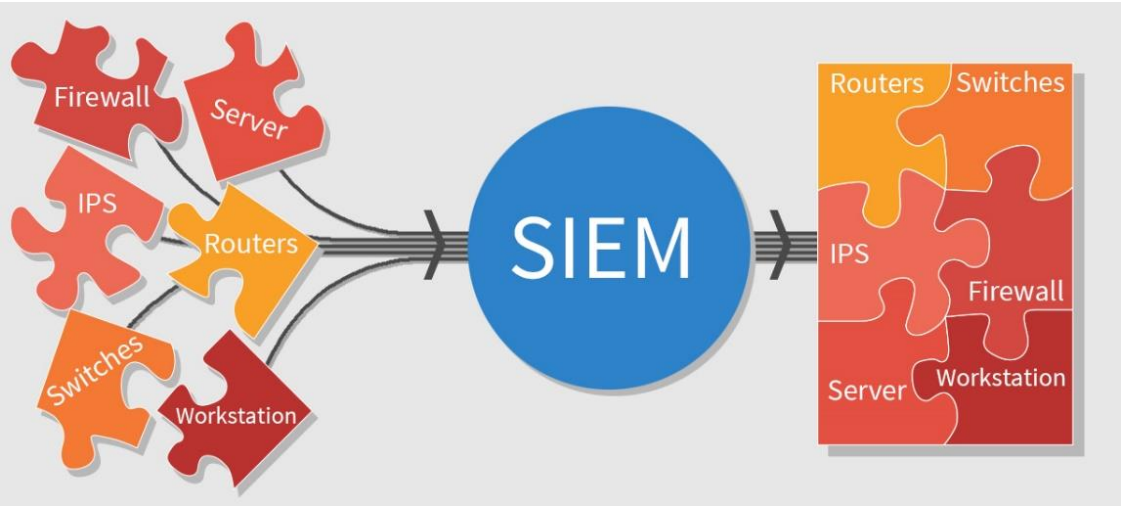
Laboratory environment

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

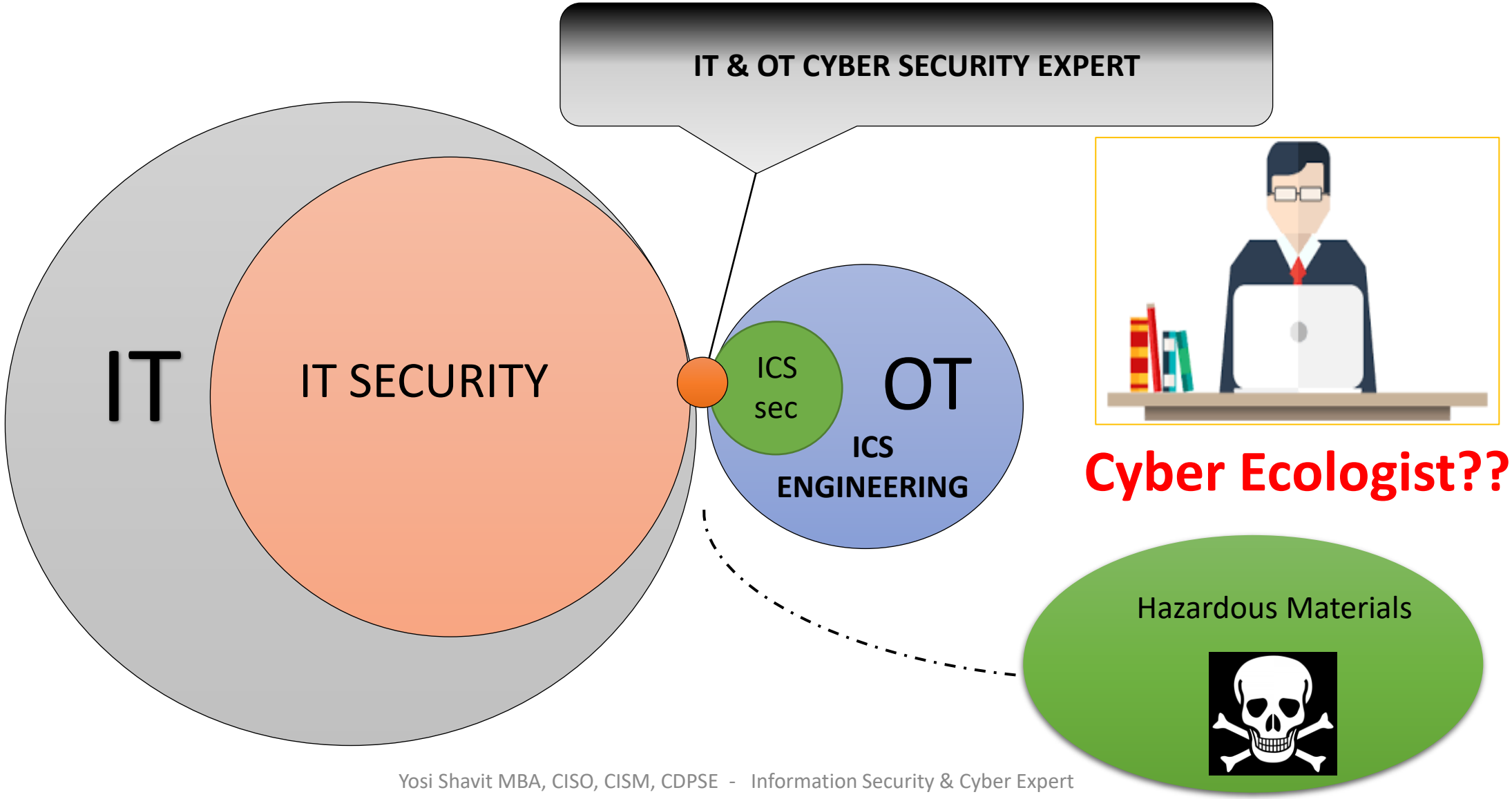
בקרות

"עיניים"

- ✓ IDS , IPS תעשייתי
- ✓ רישום וצבירת לוגים (Collector)
- ✓ מיפוי רכיבים תעשייתיים – בקרים, עמדות HMI ,פאנלים לוקאליים, סנסורים, גלאים , מצלמות
- ✓ SIEM -SOC - SOC לעולמות ה-OT



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



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

תודה על ההקשבה!