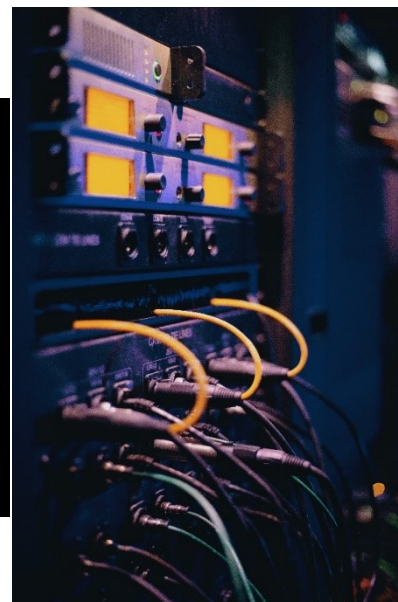


# קורס סייבר לתעשייה מחזור 3 נובמבר 2021



# מטרות הקורס

- ✓ הקניית ידע בנושאי סייבר עם דגש על סייבר בתעשייה, בדגש נוסף על תעשיית החומרים המסוכנים
- ✓ תמיכה בדרישות הרגולציה בסייבר במפעלי חומרים מסוכנים המקבלים היתר רעלים מהמשרד להגני"ס
- ✓ חשיפת אוכלוסיות נוספות במפעל (מעבר לאנשי IT, ואנשי סייבר) לאיומי הסייבר וסקירת פתרונות הגנה שונים
- ✓ מעבר והסבר על מדריך הסייבר של המשרד להגנת הסביבה גירסא 1.3
- ✓ חשיפת משתתפי הקורס לחברות סייבר שיכולות לסייע בפעילות העלאת החוסן בסייבר במפעלים (סקרים, הטמעת בקורות)



31 אוקטובר, 2021



המשרד להגנת הסביבה



המשרד להגנת הסביבה



המשרד להגנת הסביבה

מדינת ישראל  
המשרד להגנת הסביבה

המשרד להגנת הסביבה



الوزارة لحماية البيئة  
Israel Ministry of the Environmental Protection

## יוסי שביט (MBA, CISO, CISM, CDPSE)

ראש יחידת הסייבר בתעשייה

טל': 074-7675850

נייד: 058-6662242

E-mail: yosish@sviva.gov.il

רח' בנק ישראל 7, גנרי 2

ירושלים 9195021

www.sviva.gov.il

# קצת על עצמי

יוסי שביט – נשוי +3 מתגורר בהר אדר

## השכלה:

- מהנדס מכונות Bsc. הטכניון חיפה
- לימוד מדעי המחשב – אוניברסיטת מרילנד ארה"ב
- תואר שני MBA מינהל עסקים או"פ
- הסמכות בינלאומיות CISM, CSPSE מטעם ארגון ISACA העולמי

## נסיון מקצועי מעל 25 שנה בתחומי הסייבר:

- עבודת HANDS ON ברכיבי אבטחת מידע וסייבר בעולמות ה-IT
- כתיבת מתודולוגיות
- כתיבת רגולציה
- מרצה באקדמיה בקורסי סייבר במסלול תואר I במערכות מידע
- נסיון תעשייתי – ביצוע סקר סיכוני סייבר במערכות ICS



# נושאי הלימוד בקורס

● **מפגש 1:** חלק ראשון – הסבר על הרגולציה בסייבר לתעשיית החומרים המסוכנים, הצגת אירועי סייבר בתעשייה ובמערכות ICS

חלק שני – מבוא לחומרים מסוכנים – קבוצות חומרים מסוכנים, סווג חומרים מסוכנים, גיליון בטיחות, שילוט החומרים המסוכנים, קודי חירום, סיכונים סביבתיים ממתקני תעשייה ותשתית

● **מפגש 2:** זיהוי ומיפוי תהליכים מסוכנים, סיווג תהליכים מסוכנים, רשימת תרחישים לניתוח (תרחישי WCS) חברת אתוס – אדריכלות תכנון וסביבה בע"מ



● **מפגש 3:** מושגי יסוד בהגנת סייבר – חלק 1

● **מפגש 4:** מושגי יסוד בהגנת סייבר – חלק 2

● **מפגש 5:** מושגי יסוד בהגנת סייבר – חלק 3

● **מפגש 6:** מבוא להאקינג + שרשרת התקיפה

● **מפגש 7:** סייבר במערכות תעשייתיות

● **מפגש 8:** ניהול סיכונים במפעלי תעשיית המזון חומרים מסוכנים


● **מפגש 9:** מעבר משלים על מדריך הסייבר 1.3 וקובץ החישובים, השלמות, שאלות ותשובות, סיכום ומבחן סיום

● **מפגש 10:** מפגש ספקים מטעם התאחדות התעשיינים

קבלת תעודה סיום משתתף  
קבלת תעודה סיום משתתף ועבר מבחן מסכם

# מפגש 1 – מבוא + מבוא לחומרים מסוכנים



הסבר כללי ממעוף הציפור על הרגולציה בסייבר לתעשיית החומרים המסוכנים   
**לא לדאוג:** בהמשך הקורס תהיה העמקה

הצגת אירועי סייבר בתעשייה 



# החלטות ממשלה 2443, 2444 מ-15.2.2015

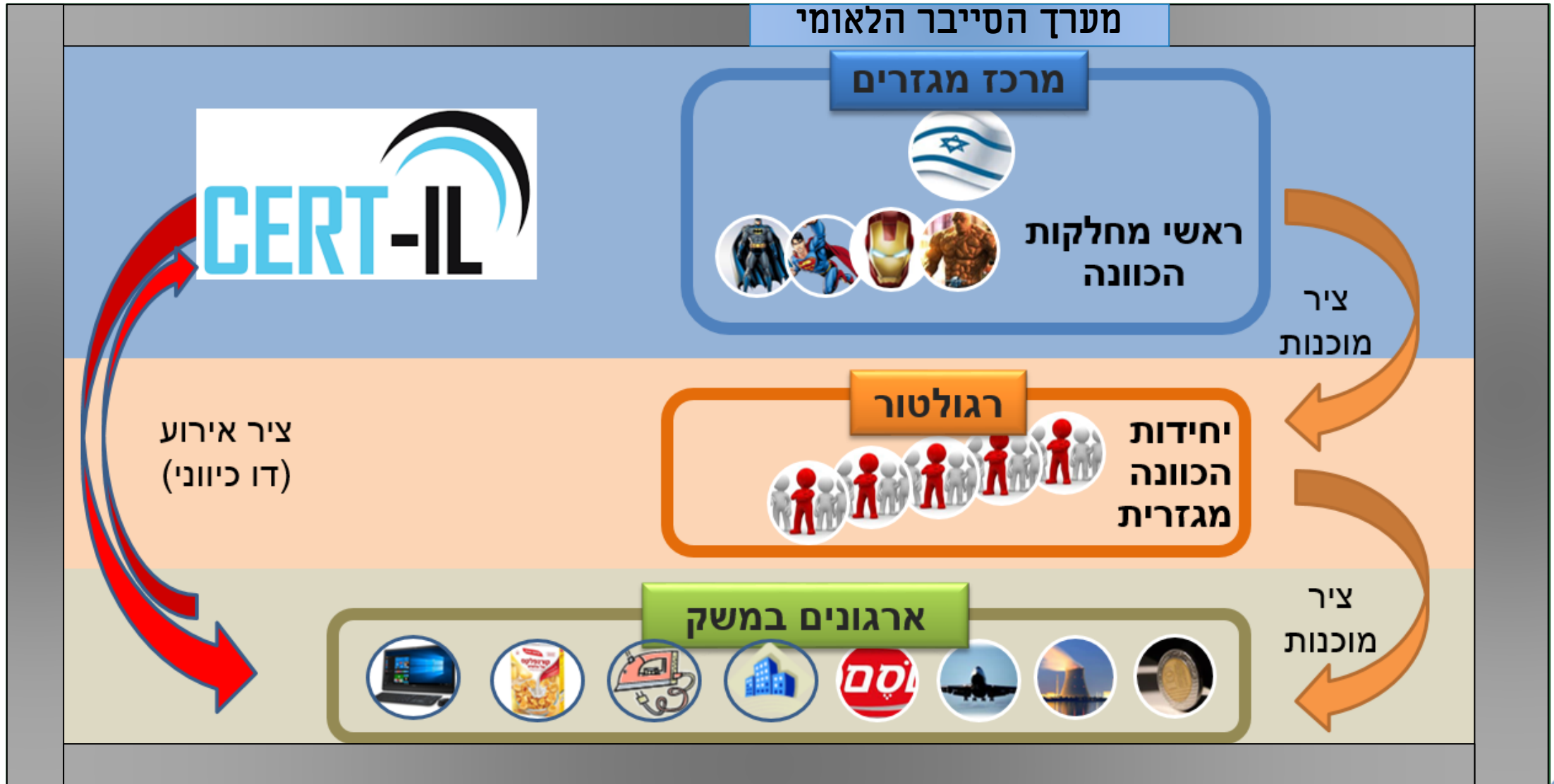
1. החלטת ממשלה 2443 בנושא - קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר - **הקמת יה"ב (יחידת הגנה בסייבר של משרדי הממשלה)**

2. החלטת ממשלה 2444 בנושא קידום ההיערכות הלאומית להגנת הסייבר - **הקמת מערך הסייבר הלאומי - אחריות הגנה בסייבר על כל המשק הישראלי.**

<http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2443.aspx>

**על בסיס שתי ההחלטות, יחזקן במדינת ישראל חוק הסייבר.**

# תהליכי עבודה במשק – על פי החלטות הממשלה



# פעילות יחידת הסייבר





# הקמת "מרכז הגנה ארצי לתעשייה"

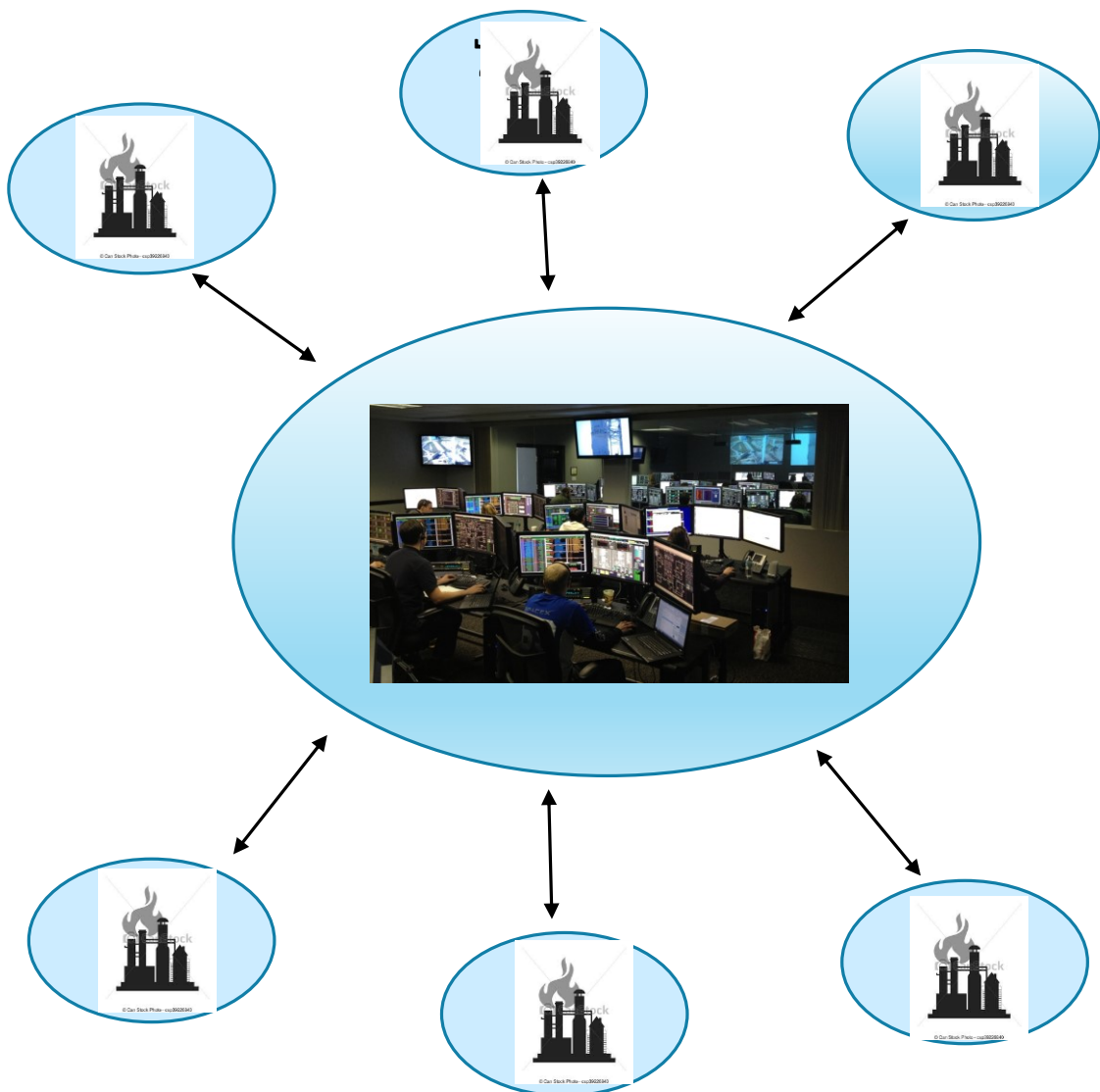
החל מדצמבר 2020 מרכז הגנה ארצי לתעשייה מופעל במתחם הסייבר בבאר שבע תחת ה-CERT הלאומי במערך הסייבר הלאומי

המטרה: פעילות פרו-אקטיבית לניטור מידע על חולשות ופערי הגנת סייבר של מפעלים מסוכנים



**CERT: Cyber Emergency Response Team**

# הקמת מק"מ תעשייתי (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

# רגולציה: הוספת תנאי סייבר בהיתר הרעלים

החלטות ממשלה 2443, 2444 מיום 15.2.2015

”... הכוונה והנחיה מקצועית בתחום הגנת הסייבר בהתאם **לסמכויות הרגולציה** המופעלות על ידי המשרד הממשלתי או במסגרתו....”

כל הזכויות שמורות - המשרד להגנת הסביבה ©

חוק החומרים המסוכנים, התשנ"ג-1993<sup>1</sup>

הגדרות  
(תיקונים:  
התשנ"ז, התשס"ה,  
התשע"ג)

1. בחוק זה -  
"חומר מסוכן" - רעל או כימיקל מזיק;  
"אירוע חומרים מסוכנים" - התרחשות בלתי מבוקרת או תאונה, שמעורב בה  
חומר מסוכן, הגורמת או העלולה לגרום סיכון לאדם ולסביבה, לרבות  
שפך, דליפה, פיזור, פיצוץ, התאיידות, דליקה;  
"גוף הצלה" - (נמחקה);  
"כימיקל מזיק" - כל חומר מן החמרים המפורטים בתוספת הראשונה, בין  
בצורתו המשוערת ובנו מעורב או ממוזג בחמרים אחרים.



חוק החומרים  
המסוכנים התשנ"ג  
1993

# תוספת תנאים בהיתר – חוק חומרים מסוכנים

2. כל מקום למכירת חומרים מסוכנים טעון רישוי לפי חוק רישוי עסקים, התשכ"ח-1968.	חובת רישוי
3. (א) לא יעסוק אדם ברעלים אלא אם כן יש בידו היתר רעלים מאת הממונה; הוראה זו לא תחול על רוקח מורשה העוסק ברעלים רפואיים לצרכי רפואה בבית מרקחת או בעסק שעיקרו עיסוקו סמי מרפא או רעלים רפואיים או על עסק המוכר תכשירים בלא מרשם, כהגדרתם בפקודת הרוקחים, אף אם המכירה נעשית שלא בבית מרקחת. (ב) בהיתר רעלים יפורטו מסחרו של בעל ההיתר, הרעלים שהוא רשאי לסחור בהם ומטרת השימוש בהם, אין בהיתר כדי להחיר סחר או יבוא של סם מסוכן כמשמעותו בפקודת הסמים המסוכנים (נוסח חדש), התשל"ג-1973. (ג) היתר רעלים יינתן רק למבקש שידוע כאדם הנון ולאחר שהוכיח להנחת דעתו של נוהן ההיתר שהוא יודע קרוא וכתוב שהוא מודע היטב לתכונות המסוכנות של אותם רעלים. (ד) תוקפו של היתר רעלים יהיה לשנה אחת, לשנתיים, לשלוש או לתקופה המחזתה משנה או העולה על שלוש שנים, בהתאם לאמות מידה, ובכללן סוג המטלה, חומרי הרעל, כמות הרעל, והכל כפי שקבע הממונה. (ה) הממונה רשאי להתנות את מתן היתר הרעלים בתנאים מיוחדים שיש לקיימם לפני מתן ההיתר, כן רשאי הוא לקבוע בהיתר תנאים מיוחדים, ורשאי הוא, בכל עת, להוסיף או לגרוע מהם, הכל על מנת להגן על הסביבה או על בריאות הציבור. (ו) הממונה רשאי לנסות בכל עת להיטות רעלים, מהטעמים המנויים בסעיף קטן (ה), לא יבטל הממונה היתר רעלים אלא לאחר שנתן לבעל ההיתר הזדמנות להשמיע את טענותיו.	חיתר רעלים (תיקונים והסכ"מ)
4. לא ימסור המכס רעלים המוכנסים לישראל אלא לאחד מאלה בלבד - (1) לבעל היתר רעלים; (2) למי שיש לו הרשאה בכתב מאת הממונה.	רעלים מיוצאים
5. (א) בעל היתר רעלים ינהל מנקסי רעלים לפי הנוסח שבתוספת השלישית ובהם יירשמו כל קניות ומכירות של רעלים. (ב) בנקס הקניות יפורטו תאריכה של כל קניה, החמרים שנקטו, כמויות וכן שמו של האדם שממנו נתקבלו. (ג) בנקס המכירות יפורטו תאריכה של כל מכירה, תיאורו של הרעל שנמסר וכמותו, השימוש לו הוא מיועד ושמו ומענו של הקונה.	מנסי רעלים



חוק חומרים מסוכנים

3. (ה) הממונה רשאי להתנות את מתן היתר הרעלים בתנאים מיוחדים שיש לקיימם לפני מתן ההיתר, **כן רשאי הוא לקבוע בהיתר תנאים מיוחדים ורשאי הוא בכל עת להוסיף או לגרוע מהם**, הכל על מנת להגן על הסביבה או על בריאות הציבור



# היתר רעלים

**לעיסוק ברעלים** כמפורט בתוספת הראשונה לבקשה להיתר רעלים מיום 03/03/2020 המאושרת והחתומה בידי הממונה, המצורפת להיתר זה והמהווה חלק בלתי נפרד ממנו (להלן - הבקשה).

## עסקד מסווג לסיווג A.

**בתנאים מיוחדים** כמפורט בתוספת השנייה המצורפת להיתר זה והמהווה חלק בלתי נפרד ממנו.

### **מודגש בזה כי :**

1. היתר זה ניתן אך ורק לסוגי העיסוק, זהות העוסק, מיקום העיסוק, שם הבעלים/מנהל, שם אחראי הרעלים וסוגי וכמויות הרעלים שפורטו בו. יש להודיע מיד לממונה על כל שינוי בנתונים האמורים, לשם בדיקת הצורך לשנות את ההיתר, לבטלו או להחליפו.
2. עיסוק ברעלים ללא היתר רעלים ובכלל זה עיסוק שלא לפי הנתונים להם ניתן ההיתר או בניגוד לתנאיו **מהווה עבירה פלילית** שהעונש המרבי עליה הוא מאסר עד שלוש שנים או קנס **מ- 404,000 ש"ח עד 808,000 ש"ח למנהל ועד 1,616,000 ש"ח** לתאגיד או עסק, כמפורט בחוק.

תאריך

חתימת הממונה וחותמת

כל האמור בלשון זכר אמור גם בלשון נקבה.

עבור :

מר ישראל ישראלי  
חברת ישראל

ישראלי 1, הרצליה

שלום רב,

הנדון : היתר רעלים

מצי"ב היתר רעלים שמספרו 123456.

לאחר סיווג עסקד בקטגוריה A תוקף ההיתר

הוא ל 1 שנים.

מיום 03/03/2020 עד ליום 02/03/2021.

הנך מתבקש להתחיל בהליך חידוש ההיתר הבא

3 חודשים לפני מועד פקיעת היתר זה.

בכבוד רב

הממונה



# 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
- מפעלי סמיקונדקטור
- תעשיות ביטחוניות
- תעשיית הדשנים
- יקבים
- בריכות שחיה
- מכבסות חכמות
- בתי דפוס

# דרישות רגולטוריות להגנה בסייבר

מה מפיק המפעל:

העלאת החוסן בסייבר



שמירה על רציפות עסקית



גופי תמ"ק  
שמירה על רציפות תפקודית

מנדט המשרד להגנת הסביבה :

בריאות הציבור



הגנה על הסביבה



# גופי תמ"ק – תשתיות מידע קריטיות

תמ"ק = תשתית מדינה קריטית

"גופים הנדרשים לעמוד ברגולציית סייבר של מערך הסייבר הלאומי על פי התוספת החמישית בחוק להסדרת הביטחון בגופים ציבוריים התשנ"ח 1998"

רגולטור בסייבר:

מערך הסייבר הלאומי – אגף תמ"ק  
חוק להסדרת הביטחון בגופים  
ציבוריים התשנ"ח 1998  
התוספת החמישית

רגולטור בסייבר:

המשרד להגנת הסביבה  
החלטת ממשלה 2443  
חוק חומרים מסוכנים התשנ"ג 1993

מטרה:

רציפות תפקודית למשק

מטרה:

בריאות הציבור הגנת  
הסביבה





# גופי תמ"ק

מתווה עבודה משותף : המשרד להגנת הסביבה – מערך הסייבר הלאומי

אכיפה	פיקוח	הנחיה
על פי סמכות	משותף	תוספת תנאים ספציפיים

## המטרה

קיום רגולציה משלימה



מניעת כפל רגולציה



# גופי מלמ"ב – תעשיות בטחוניות



הממונה על הביטחון במשרד הביטחון

על פי המתווה שסוכם בשלב הראשון:

1. הוקצה איש קשר במלמ"ב לצורך אסדרת פעילות הסייבר בגופים משותפים
2. מלמ"ב יעביר ליחידת הסייבר רשימה של גופים מונחים שלו בסייבר, אנו נבצע סינון על פי היתר רעלים.
3. תבוצע פעילות משותפת של איתור 2-3 גופים בשרשרת האספקה של מלמ"ב אשר מקבלים היתר רעלים מהמשרד
4. יבוצע מיפוי משותף של הממשקים באותם גופים
5. העברת מדריך הסייבר לתעשייה אל מלמ"ב על מנת שיוכלו להשוות למול התקינה שלהם ולהבין חפיפות והבדלים.



# פעילויות נוספות מתוכננות לזמן המידי



נמלים – חיפה (בוצע), אשדוד, אילת  
נמלים חדשים: נמל המפרץ, נמל אשדוד



לולים – לולים מבוקרים (בוצע)



משאיות חומ"ס – מיפוי הסיכונים הקיימים ברכב  
מקושר ורכב אוטונומי

# אימוץ דירקטיבת III SEVESO

## נספח י"א – כמויות סף לחומרים מסוכנים

טבלת החומרים המסוכנים הנכללים בביצוע סקר סיכוני סייבר

סך עליון כמות השווה על העולה על (טון)	סך תחתון כמות השווה או העולה על (טון)	מספר CAS \ משפטי סיכון (H) (הערה 0)	חומר
			עם תכונות סיכון לבריאות (H), מקטגוריות הסיכון הבאות:
20	5	H300, H310, H330	H1 ACUTE TOXIC - Category 1, all exposure routes
200	50	H300, H310, H330, H331	H2 ACUTE TOXIC - Category 2, all exposure routes - Category 3, inhalation exposure route (הערה 7)
200	50	H370	H3 STOT SPECIFIC TARGET ORGAN TOXICITY – SINGLE EXPOSURE STOT SE Category 1
			עם תכונות סיכון פיזיקאליות (P), מקטגוריות הסיכון הבאות:
50	10	H200, H201, H202, H203, H205	P1a EXPLOSIVES (הערה 8) - Unstable explosives or - Explosives, Division 1.1, 1.2, 1.3, 1.5 or 1.6, or - Substances or mixtures having explosive properties and do not belong to the hazard classes Organic peroxides or Self-reactive substances and mixtures, Type C, D, E or F or organic peroxides, Type C, D, E, or F
200	50	H204	P1b EXPLOSIVES (הערה 8) Explosives, Division 1.4
50	10	H220, H221	P2 FLAMMABLE GASES

הרגולציה תחול תחילה על מפעלי סבסו תחתון קריטריון כניסה לרשימת סבסו על פי נתוני טבלאות שיפורסמו במדריך הסייבר 1.3 – נספח י"א



<sup>10</sup> הטבלה מבוססת על טבלת כמויות סף לחומרים מסוכנים הקיימת במדריך ניהול הסיכונים של אגף חומ"ס

# תנאים לכניסה לרגולציה בסייבר 2020



עמידה בכמויות סף של דירקטיבת SEVESO



עמידה ב"תהליך מסוכן"



התהליך המסוכן מחובר למערכות בקרה ומיחשוב

מבוסס על חוק  
חומרים  
מסוכנים 1993



# רגולציה בסייבר שנת 2020

רגולציה בסייבר החלה בפועל מ-8.6.2020

- 21 מפעלי סבסו תחתון – תוספת תנאי סייבר בהיתר רעלים
- 7 מפעלי סבסו עליון – רגולציה משולבת: ניהול סיכונים (חומ"ס), סייבר, רע"ד



# רגולציה בסייבר שנת 2021

○ 32 מפעלי סבסו תחתון – תוספת תנאי סייבר בהיתר רעלים

○ 25 מפעלי סבסו עליון – רגולציה משולבת: ניהול סיכונים (חומ"ס), סייבר, רע"ד

○ ביצוע פיקוח ל-21 מפעלים שקיבלו רגולצית סייבר בשנה החולפת.





# רגולציה בסייבר 2022

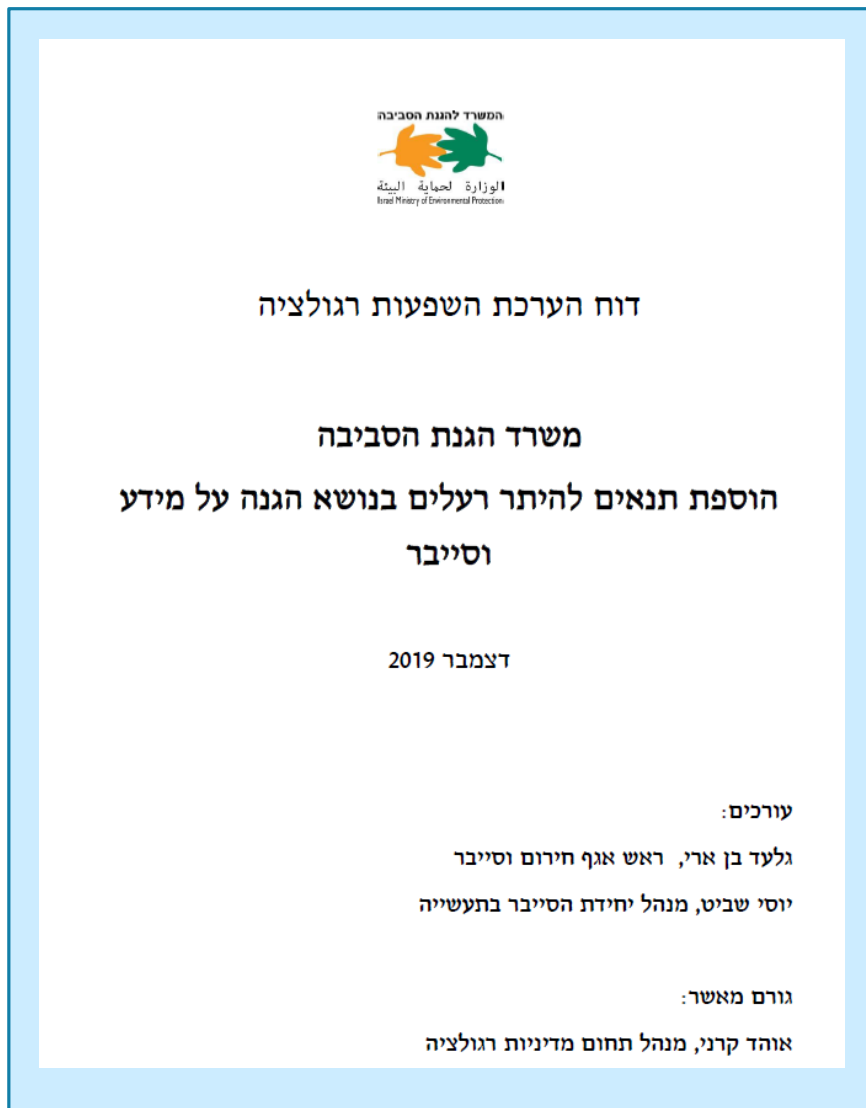
## תכנית חומש

אישור להחלת רגולציה ל-1000 מפעלים נוספים ברמות היתר A ו-B

פריסת הגנת סייבר במפעלים לאורך השנים 2022 – 2027



# 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

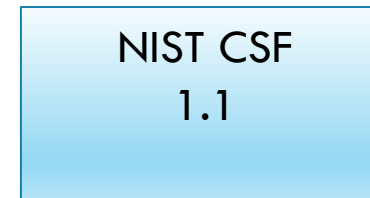
עורכים:  
גלעד בן ארי, ראש אגף חירום וסייבר  
יוסי שביט, מנהל יחידת הסייבר בתעשייה

גורם מאשר:  
אוהד קרני, מנהל תחום מדיניות רגולציה

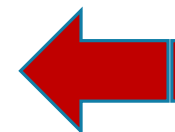
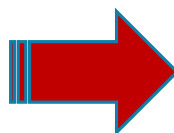
## RIA = Regulatory Impact Assessment

- ✓ הגורם היוזם
- ✓ החלופות
- האפשרויות
- ✓ רגולטורים משיקים
- ✓ מגבלות ביישום
- ✓ מיפוי בעלי עניין
- ✓ שיח עם בעלי עניין
- ✓ סקירה בינלאומית
- ✓ הערות הציבור

# מדריך הסייבר לתעשייה גירסא 1.3



עבודת שטח מסיבית  
סקרי סיכונים במפעלים



**מדריך סייבר**  
 עמידה בתנאים של  
 היתר רעלים בתחום  
 הסייבר בתעשייה

יולי 2020  
 נדסה 13

[https://www.gov.il/he/departments/publications/reports/cyber\\_industry\\_toxins\\_permit](https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit)



## Cyber Manual

Adhering to the cybersecurity  
requirements of a toxins permit

July 2020  
Version 1.3

Ministry of Environmental Protection  
Emergency and Cybersecurity Division  
Industrial Cybersecurity Department

[https://www.gov.il/he/departments/publications/reports/cyber\\_industry\\_toxins\\_permit](https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit)

תורגם לאנגלית לבקשת ארגון ה-OECD

- חישוב רמת הנזק - I
- חישוב רמת החשיפה - P
- חישוב רמת הסיכון = R

- רשימת בקורות לרמת סיכון 1
- רשימת בקורות לרמת סיכון 2
- רשימת בקורות לרמת סיכון 3
- רשימת בקורות לרמת סיכון 4



המשרד להגנת הסביבה



המשרד להגנת הסביבה  
الوزارة لحماية البيئة  
Israel Ministry of Environmental Protection

## מדריך סייבר לעמידה בתנאים של היתר רעלים בתחום הסייבר בתעשייה

### הנחיות לחישוב רמת סיכון

הערכת הסיכון מבוססת על שקלול רמת הנזק הצפויה לנוכח הסיכוי שהנזק יתרחש.

יש לחשב תחילה את רמת הנזק ואת רמת החשיפה ולאחר מכן תחשוב רמת הסיכון לפי הנוסחה:  
 $P+3 \cdot I = \text{סיכון}$  (הסיכון שווה לרמת החשיפה ועוד 3 פעמים רמת הנזק).

בגיליונות "חישוב רמת הנזק" ו"חישוב רמת החשיפה" יש להשיב על השאלות ע"י הזנת מספר. בתחתית הגיליון יחושבו הרמות באופן אוטומטי.

לאחר חישוב רמת הנזק והחשיפה, יש להיכנס לגיליון "חישוב רמת הסיכון" ולצפות ברמת הסיכון שהתקבלה (חושבה אוטומטית לפי המספרים שהוזנו), בהתאם לתשובותיכם. יש להטמיע את הבקורות הדרושות על פי ערך הסיכון המתקבל (בין 4 ל-16).

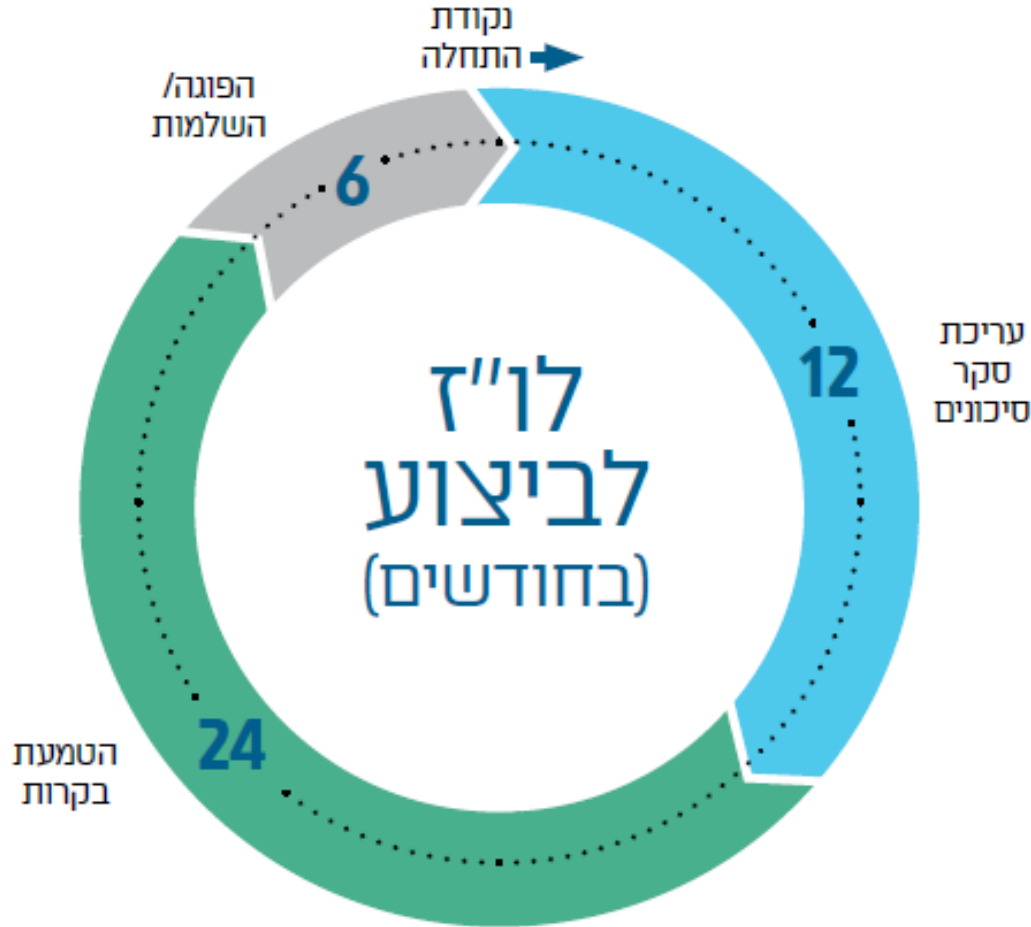
קובץ זה מכיל 7 גיליונות נוספים:

1. חישוב רמת הנזק - I
2. חישוב רמת החשיפה - P
3. חישוב רמת הסיכון = R
4. רשימת בקורות לרמת סיכון 1
5. רשימת בקורות לרמת סיכון 2
6. רשימת בקורות לרמת סיכון 3
7. רשימת בקורות לרמת סיכון 4

לשאלות ומידע נוסף ניתן ליצור קשר עם יחידת הסייבר בתעשייה במייל:  
[cyber\\_industry@sviva.gov.il](mailto:cyber_industry@sviva.gov.il)



# לו"ז לביצוע



1. החלת תנאים נוספים בהיתר
2. פעילות סקר סיכונים
3. הטמעת בקורות
4. חצי שנה הפוגה
5. פיקוח ואכיפה



## מינוי ממונה הגנת סייבר במפעל



## מסמך מדיניות המגדיר מחויבות ההנהלה לפעילות סייבר

# פעולות המשך לאחר קבלת תנאי סייבר בהיתר הרעלים



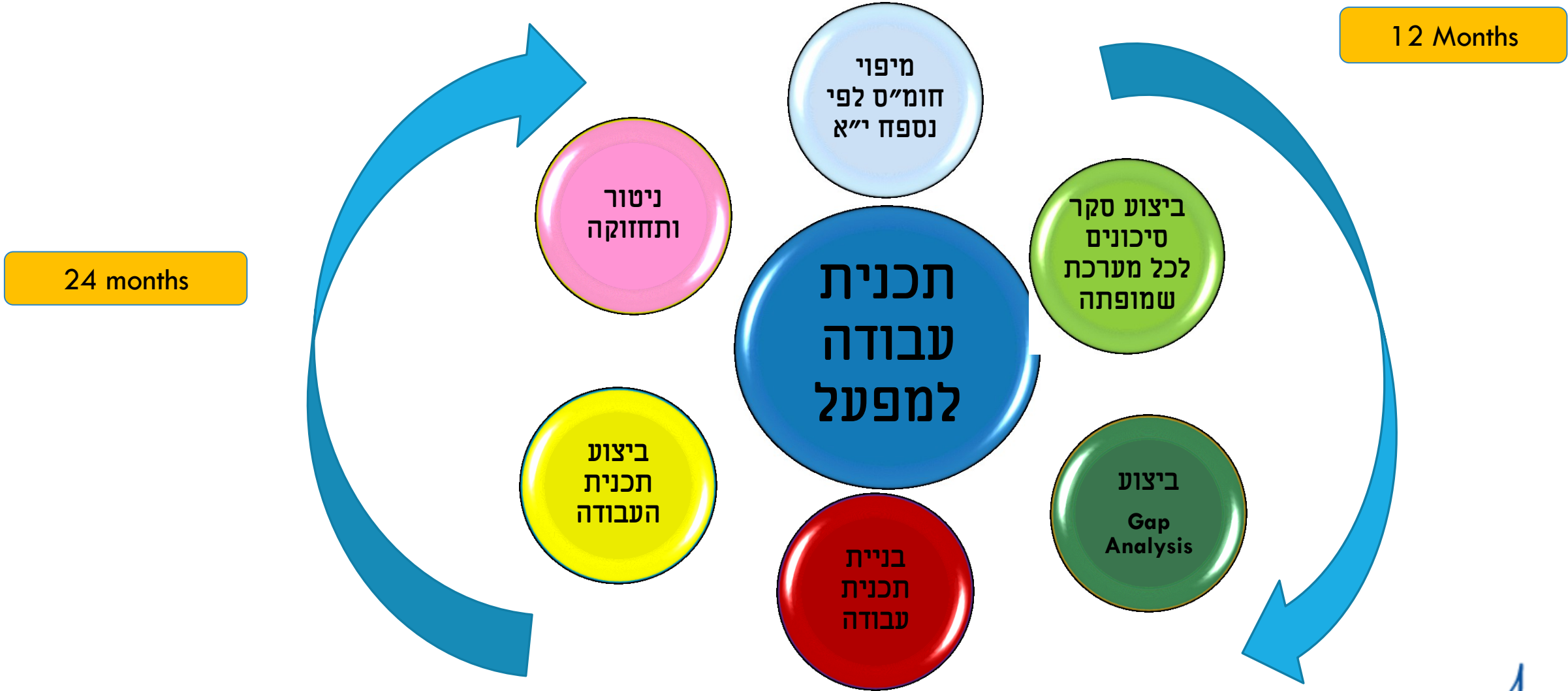
Severity	Disaster	High	Medium	Minimal
Probability				
Regularly	Critical	Critical	High	Medium
Probable	Critical	High	Medium	Medium
Occasional	Critical	High	Medium	Low
Rarely	High	Medium	Medium	Low
Unlikely	Medium	Medium	Low	Low

סקר סיכוני סייבר



הטמעת בקרות סייבר להעלאת החוסן

# תכנית עבודה למפעל



# איך לעזאזל לבצע סקר סיכונים???



המשך יבוא.....



# אירועי סייבר בתעשייה על ציר הזמן



אוסטרליה- הזרמת  
 מליון קו"ב שפכים ע"י  
 עובד ממורמר ויטק בודן



התקפת סייבר על בקר **Siemens S7**  
 בכור האיראני באמצעות וירוס  
**Stuxnet** המכיל כ-15,000  
 שורות קוד!!



חברת הנפט ARAMCO בסעודיה  
 ווירוס בשם Shamoon הדביק ופגע כאמור  
 בכ-30 אלף תחנות עבודה ובכאלפיים  
 שרתים. הווירוס מחק קבצים כמו מסמכים,  
 גיליונות אלקטרוניים, ודואר אלקטרוני,  
 ובמקומם הוצגה תמונה של דגל ארה"ב  
 עולה באש. התקפות נוספות 2016, 2018



מפעל היתוך פלדה שני בגודלו  
 בגרמניה מושבת עקב תקיפת מייל  
 של אחד העובדים (פישינג)

2000

2010

2012

2014

# אירועי סייבר בתעשייה על ציר הזמן



# אירועי סייבר בתעשייה בישראל



11.2.2018

## נוזקה לכריית מטבעות וירטואלים הותקנה במפעל תשתית קריטית

עמי רוחקס דומבה חברת ישראלית מצאה תוכנה זדונית מותקנת במתקן תשתית קריטית לאספקת מים שמטרתה כריית מטבעות וירטואלים.

החברה גילתה התקפה זו כחלק משגרת ניטור מתמשך של רשת OT של לקוח שירות מים. החברה מדווחת כי בהתקפה זו הותקפו מספר שרתים ברשת OT כדי לכרות מטבע מסוג Monero כותבים בדיווח של החברה.

התקפות תוכנה זדונית לכריית מטבעות וירטואלים צורכות משאבי CPU ורוחב פס מהרשת, וגורמות לזמני תגובה גדולים מצד כלים המשמשים לפקח על שינויים פיזיים ברשת ה OT כגון שרתי SCADA ו HMI. **עובדה זו מפחיתה את השליטה של מפעיל התשתית הקריטית על פעילותו ומאטה את זמני התגובה.**



חדשות בארץ

צה"ל מנע ניסיון איראני לפגוע במערך ההתרעה של פיקוד העורף

חטיבת ההגנה בסייבר של צה"ל סיכלה בשנה שעברה כ- 130 מתקפות סייבר, שברובן הופעלו מאיראן share

07.02.19 | ב' אדר א' התשע"ט | גבי שניידר

פעילות הסייבר התוקפנית של איראן מנוהלת על ידי משמרות המהפכה האיראניים, וזוכה למימון נכבד המוערך ביותר **ממיליארד דולר לשנה**. האיראנים מפעילים לשם כך עשרות קבוצות, והמעקב אחרי אחת מהן הוא שהוביל לחשיפת המתקפה על פיקוד העורף ולנטרולה.

2018

2019



# אירועי סייבר בתעשייה בישראל



**חשד למתקפת סייבר חריגה על שורת מתקני מים בישראל.**  
<https://www.ynet.co.il/articles/0,7340,L-5720969,00.html>

ל- ynet נודע כי בסוף השבוע הותקפו לפי החשד מתקנים מצפון עד דרום, במטרה להשתלט על מערכות תפעול ולשבש פעילות משאבות. התאגידים התבקשו לשנות סיסמאות, אך "לא אירע נזק תפעולי". רשות המים: "הנושא מטופל"

אחיה ראב"ד פורסם: 15:15 , 26.04.20



## חדשות מתפרצות

<https://www.maariv.co.il/breaking-news/Article-764070>

דיווח בפוקס ניוז: "איראן ביצעה מתקפת סייבר נגד תשתיות המים של ישראל בחודש שעבר"

מקורות מסרו לפוקס ניוז כי איראן השתמשה בשרתים אמריקאים על מנת לבצע מתקפת סייבר נגד תשתיות מים בישראל בחודש שעבר.

סוכנויות הידיעות 14:08 07/05/2020



**מערך הסייבר מזהיר: האקרים פרו-איראנים יפתחו במתקפה נגד ישראל.**

מאת יוסי הטוני 13 במאי 2020, 13:29  
 ההאקרים ינצלו את התקופה שסביב יום ירושלים - האיראני והישראלי - וצפויים לתקוף את ישראל בסייבר לדברי המערך, "ההישענות המוגברת על טכנולוגיה בעקבות משבר הקורונה יצרה משטח תקיפה רחב, שעלול להיות מנוצל על ידם"

<https://www.pc.co.il/news/315672/>

2020

הוא ציין כי "במקרה הגרוע יותר, מאות אנשים היו בסיכון לחלות". עוד אמר כי מתקפת הסייבר הייתה מתוככמת יותר ממה שחשבו תחילה בישראל. "זה היה קרוב להצליח, ולא ברור בוודאות שזה לא הצליח".

מנגד, גורם במשטר האיראני דחה בפני העיתון את ההאשמות. "איראן לא יכולה להרשות לעצמה לנסות להרעיל אזרחים ישראלים. ואם איראן עשתה זאת, איפה התגובה ההולמת הישראלית?", תהה. "החשד שלנו הוא שהישראלים רוצים עוד כסף מהאמריקנים והם המציאו את כל הסיפור. אבל האמריקנים לא טיפשים".

גם עלי רזה מיר-יוספי, דוברו של שגריר איראן באו"ם, ציין כי פעולות הסייבר של איראן הן "הגנתיות לחלוטין". לדבריו, "נקורבן של לוחמת סייבר וחבלות סייבר אחרות, אנחנו יודעים היטב כמה הפעולות יכולות להיות הרסניות. אנחנו מטרה קבועה של כוחות זדוניים ונמשיך להתגונן בפני כל מתקפה".



ראש מערך הסייבר: "המתקפה הייתה עלולה לגרום לאסון"

## מתקפת הסייבר על מתקני המים: "איראן ניסתה להעלות את רמת הכלור"

גורם מערבי אמר ל"פייננשל טיימס" כי במתקפת הסייבר שמיוחסת לאיראן ונחשפה לראשונה ב-ynet, נרשם ניסיון להעלות את רמת הכלור במים שמוזרמים לאזרחים: "מאות היו בסיכון לחלות, אלפים עלולים היו להישאר בלי מים". באיראן הכחישו מעורבות: "ישראל רוצה עוד כסף מארה"ב".



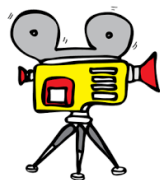
ynet פורסם: 01.06.20, 03:29



(צילום: רועי עידן)

גורם מודיעין מערבי חשף אמש (יום א') בפני העיתון הבריטי "פייננשל טיימס" פרטים חדשים על מתקפת הסייבר על מתקני המים בישראל, שיוחסה לאיראן ונחשפה לראשונה ב-ynet. על פי הגורם, מטרת התקיפה הייתה העלאת רמת הכלור שבמים המוזרמים לבתי האזרחים בישראל.

ארבעה גורמים ישראליים ואותו גורם מערבי סיפרו לעיתון כי האיראנים פרצו לתוכנות שמפעילות את משאבות המים בישראל לאחר שעברו בשרתים אמריקניים ואירופיים כדי להסתיר את מקור הקוד. לדברי הגורם המערבי, מתקפת הסייבר שמיוחסת לאיראן עלולה הייתה להוביל להשבתת המשאבות לאחר גילוי החריגה הכימית, דבר שעלול היה להותיר אלפי אזרחים ללא מים בברזים בזמן גל החום האחרון שפקד את המדינה.





# אירועי סייבר בתעשייה בישראל - כלור

## ידלין על המתקפה האיראנית: "תקיפת סייבר ברמה גבוהה שעוד לא ראינו כמותה"

ראש אגף המודיעין לשעבר התייחס באולפן ynet לדיווח על הניסיון להגביר את רמת הכלור במי הברזים בישראל: "זו יכולת לצאת מהממד הקיברנטי ולפגוע במערכות פיזיות". עם זאת הוא הרגיע: "לישראל יש מערכת הגנה טובה על התשתיות"



אלכסנדרה לוקש וניר (שוקו) כהן | פורסם: 01.06.20, 18:33

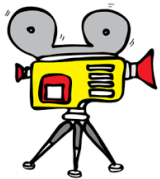
ראש המכון למחקרי ביטחון לאומי

שידור חי | אלוף (במיל') עמוס ידלין | ראש המכון למחקרי ביטחון לאומי

**"איראן ניסתה להעלות את רמת הכלור"**  
לפי הגורם המודיעיני: מתקפת הסייבר יועדה לפגוע באורחי ישראל דרך מתקני מים

10:05 | סדרות, בתי קפה וספרקים | הערכה בארה"ב: כ-4,100 נעצרו מאז תחילת ההפגנות | החמיית: עלייה קלה בסמפרטורות | הקורונה במקסימום 151 חולי

אולפן ynet: ראיון עם אלוף במיל' ידלין (צילום: אלי סגל)



## מתקפת סייבר השביתה חלק מקווי הייצור של טאואר

6 ספטמבר, 2020

מערכות המידע של החברה זיהו חדירה לשרתי הארגון. בצעד מניעתי השביתה החברה חלק מקווי הייצור. עדיין לא ברור מתי תשוב הפעילות לסדרה ומהו הנזק שנגרם לחברה. גם קבלניות הייצור X-Fab ו-TSMC הותקפו בעבר




מאז האירוע,  
הותקפו מספר מפעלים המכילים  
חומרים מסוכנים

קבלנית ייצור השבבים טאואר סמיקונדקטור (Tower) דיווחה הבוקר (א') על "אירוע סייבר", שחייב את החברה לבצע השבתת ייצור בחלק ממתקניה בעולם. טאואר מסרה כי מערכות אבטחת המידע זיהו עדות לחדירה במערכות מסוימות, וכצעד מניעתי השביתה החברה חלק מהשרתים ועצרה באופן יזום את הפעילות של חלק מקווי הייצור.

במקביל, יידעה החברה את רשויות החוק ופועלת בשיתוף מומחי סייבר לפתרון הבעיה כדי שניתן יהיה להפעיל מחדש את המערכות המושבתות. בטאואר עדיין לא יודעים להעריך מתי יחזרו קווי הייצור לפעילות ומה היקף הנזק שנגרם לחברה בעקבות התקרית. לטאואר יש 6 מפעלי ייצור בישראל, ארצות הברית ויפן. שני המפעלים בישראל מתמחים בייצור רכיבים דיסקרטיים ואנלוגיים כמו



אוקטובר 2021	מאי 2021	פברואר 2021
<p><b>פריצת הסייבר לבית החולים: הלל יפה עדיין מושבת</b></p> <p>מספר ימים לאחר מתקפת הסייבר יוצאת הדופן בבית החולים, מודיעים במשרד הבריאות כי התקלה עדיין לא תוקנה, אך לא נגרם נזק: "נמשכת העבודה במטרה להחזיר את מערכות המידע"</p> <p>מתי ברנהרט, חדשות סחונים 08:26 17.10.21</p>  <p>צילום RickP, ויקימדיה</p>	<p><b>דיווחים: קולוניאל פייפליין נאלצה לשלם כופר של 5 מיליון דולר להאקרים</b></p> <p>הכופר שולם לכנופיית דארקסייד, שהשביחה את מחשביה של החברה המפעילה צינור דלק מרכזי בארצות הברית; למרות החרזת הפעילות, תחנות דלק במזרח המדינה ממשיכות לדווח על מחסור</p> <p>חדשות חוץ 10:40, 15.05.21</p> <p>תגיות: דארקסייד סייבר כופר קולוניאל פייפליין</p> <p>קולוניאל פייפליין (Colonial Pipeline), המפעילה את אחד מצינורות הדלק המרכזיים בארצות הברית, שילמה לפי הדיווחים כופר של קרוב ל-5 מיליון דולר לכנופיית האקרים דארקסייד (DarkSide), <a href="#">לאחר שהמחשבים שלה הותקפו ופעולתה הושבתה</a>.</p>	<p><b>האקרים ניסו להרעיל מתקן מים בעיר בפלורידה ארה"ב</b></p> <p>אחד העובדים במתקן שבמחוז טמפה, זיהה את ניסיון ההרעלה בסודה קאוסטית והציל כ-15 אלף איש; לפני כשנה נעשה ניסיון תקיפת סייבר על חברת מקורות ע"י ניסיון להחדיר למים כמויות גדולות של כלור</p> <p>רפאל קאהאן 09.02.21 18:00</p> <p>תגיות: טמפה פלורידה האקרים הרעלה עריית אולדסמר</p> <p>האקרים הצליחו אמש (ב') לחדור למתקן מים עירוני במחוז טמפה בפלורידה, ארה"ב וכמעט הצליחו להרעיל את מאגר המים העירוני של העיר אולדסמר (Oldsmar).</p> <p>אחד העובדים העיד כי האקרים השתמשו בתוכנת גישה מרחוק בשם TeamViewer, וזוהו בגלל שהמחשב שהתחברו אליו באותו רגע היה מאויש, כך שהעובד הבחין בזמן אמת בניסיון ההרעלה. מתקן המים משמש לאספקת מים של כ-15 אלף תושבים וגם עסקים.</p> <p>לדברי השרף, האקרים ניסו להגדיל עד פי 100 את הכמות של נתון הידרוקסידי (סודה קאוסטית, שמשמשת לפתיחת סתימות בייוב בבתים). חומר זה משמש לנטרול חומציות ומזרז בכמויות מזעריות למי השתייה של העיר. אם האקרים היו מממשים את זממם, אלפי תושבים היו נפגעים. נתון הידרוקסידי מסוכן מאוד למגע עקב פעילותו הכימית ועלול לגרום כוויות. עבודה עם החומר מחייבת לבישת כפפות והרכבת משקפי מגן.</p>
<p>במשרד הבריאות מודיעים כי בית החולים הלל יפה עדיין מושבת, לאחר שביום רביעי האחרון הותקף המקום באירוע סייבר מסוג כופרה, שפגע במערכות המחשוב של בית החולים.</p> <p>"במהלך סוף השבוע זוהו על ידי מרכז הסייבר של משרד הבריאות עלייה בניסיונות למתקפות כנגד מספר בתי חולים וארגונים רפואיים", נמסר בהודעה משותפת של משרד הבריאות ומערך הסייבר הלאומי. "הערכות מוקדמת ותגובה מהירה של המרכז הצוותים בשטח בלמה את הניסיונות ולא נגרם נזק".</p>	<p>ההתקפה אירעה בסוף השבוע שעבר והובילה לעצירת השירותים של החברה למשך חמישה ימים, מה שגרם לשיבושי אספקה ברחבי ארצות הברית. בכלי התקשורת במדינה, ובהם CNN, "ניו יורק טיימס" ובלומברג, דיווחו כי החברה שילמה כופר. עם זאת, מהחברה סירבו להגיב בעניין.</p>	



**FOX 13**

5:00 77°

**LINDA HURTADO**

**CYNTHIA SMOOT**





11,100ppm



מה עשו? 100ppm

איך עשו? השתלטות על ה-HMI דרך TeamViewer



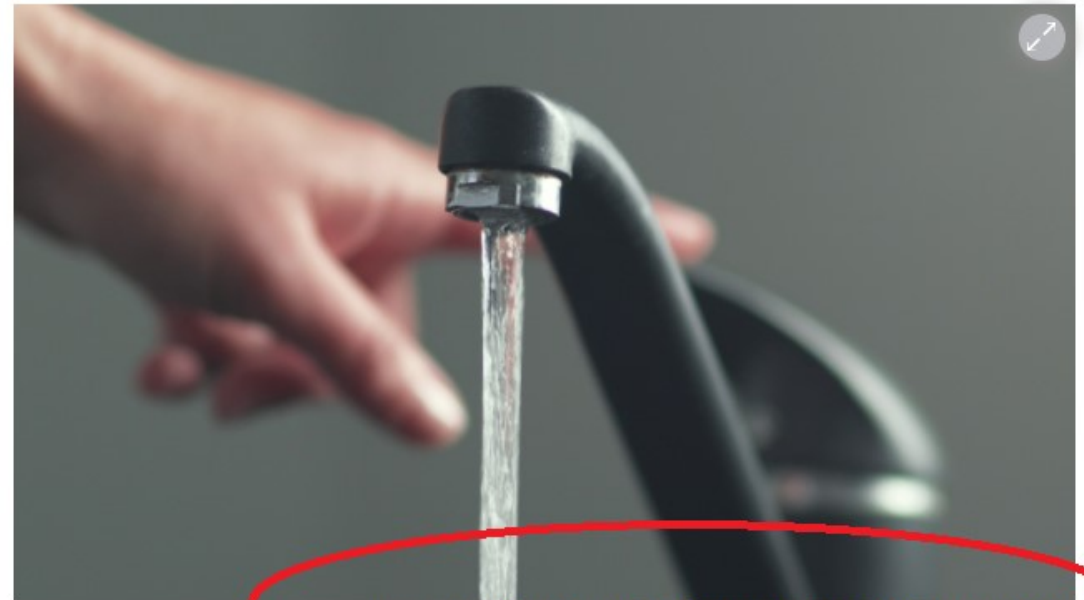
## האקרים ניסו להרעיל את המים בעיר בפלורידה

פחות משנה אחרי הפריצה למתקני המים בישראל, מתקפה דומה בארה"ב: האקרים השתלטו מרחוק על המחשב במתקן בעיר בת 15,000 תושבים, והעלו לגובה מסוכן את רמת הנתרן ההידרוקסידי במי השתייה. פקח הבחין בעכבר זז מעצמו וסיכל את הפריצה: "קריאת השכמה"



סוכנויות הידיעות פורסם: 09.02.21, 12:03

האקרים הצליחו להשתלט על מערכת הניהול מרחוק של מתקן המספק מים לעיר בת 15,000 תושבים בפלורידה - וכמעט הצליחו להרעיל אותם. כך חשפו אמש (ב') הרשויות במחוז פינלס הסמוך לטמפה, תוך שהן מדגישות כי הניסיון הזה התגלה במהירות על ידי אחד הפקחים במתקן שנפרץ - וסוכל.



מ-100 חלקיקים למיליון ל-11,100. האקרים ניסו להרעיל, וכמעט הצליחו (צילום: shutterstock)




<https://www.ynet.co.il/news/article/HJYZtAyZ00>



## NIOSH Pocket Guide

[Sodium hydroxide](#)

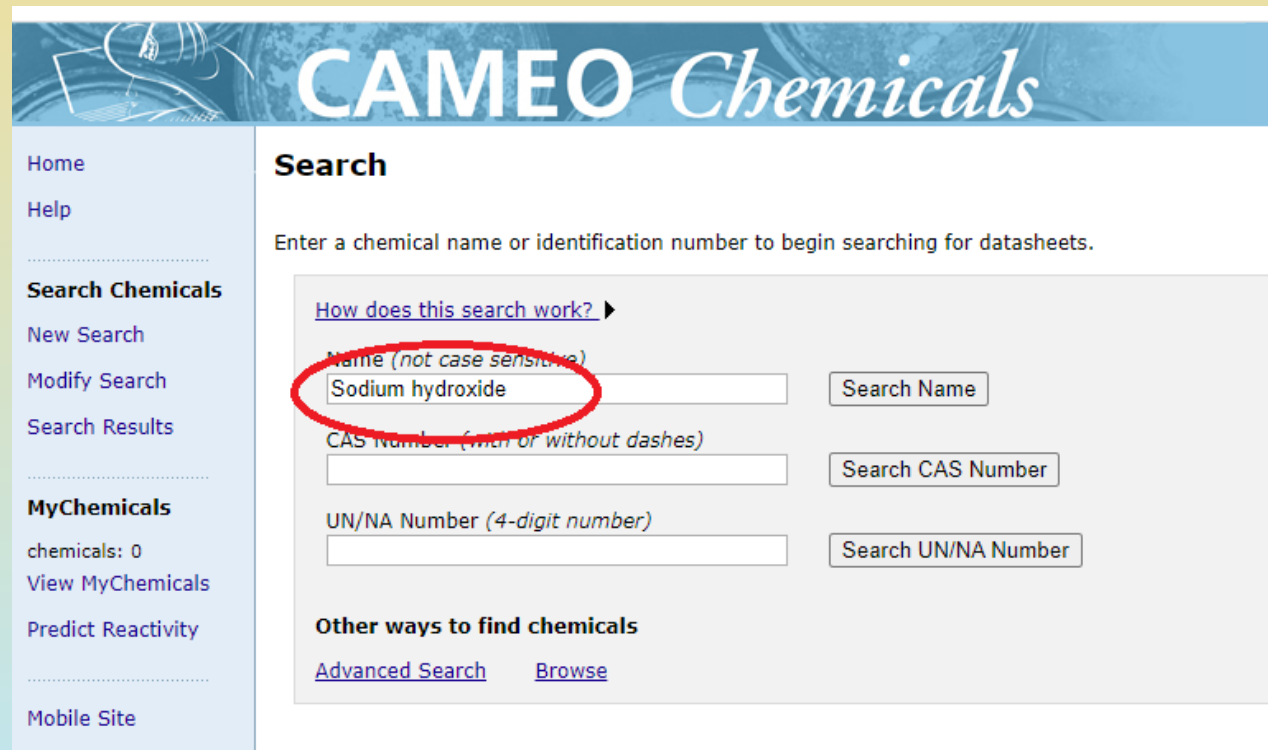
### NFPA 704

Diamond	Hazard	Value	Description
	Health	3	Can cause serious or permanent injury.
	Flammability	0	Will not burn under typical fire conditions.
	Instability	1	Normally stable but can become unstable at elevated temperatures and pressures.
	Special		

(NFPA, 2010)

### PACs (Protective Action Criteria)

Chemical	PAC-1	PAC-2	PAC-3
Sodium hydroxide (1310-73-2)	0.5 mg/m <sup>3</sup>	5 mg/m <sup>3</sup>	50 mg/m <sup>3</sup>



**CAMEO Chemicals**

Home  
Help

**Search**

Enter a chemical name or identification number to begin searching for datasheets.

[How does this search work?](#)

Name (not case sensitive)

CAS Number (with or without dashes)

UN/NA Number (4-digit number)

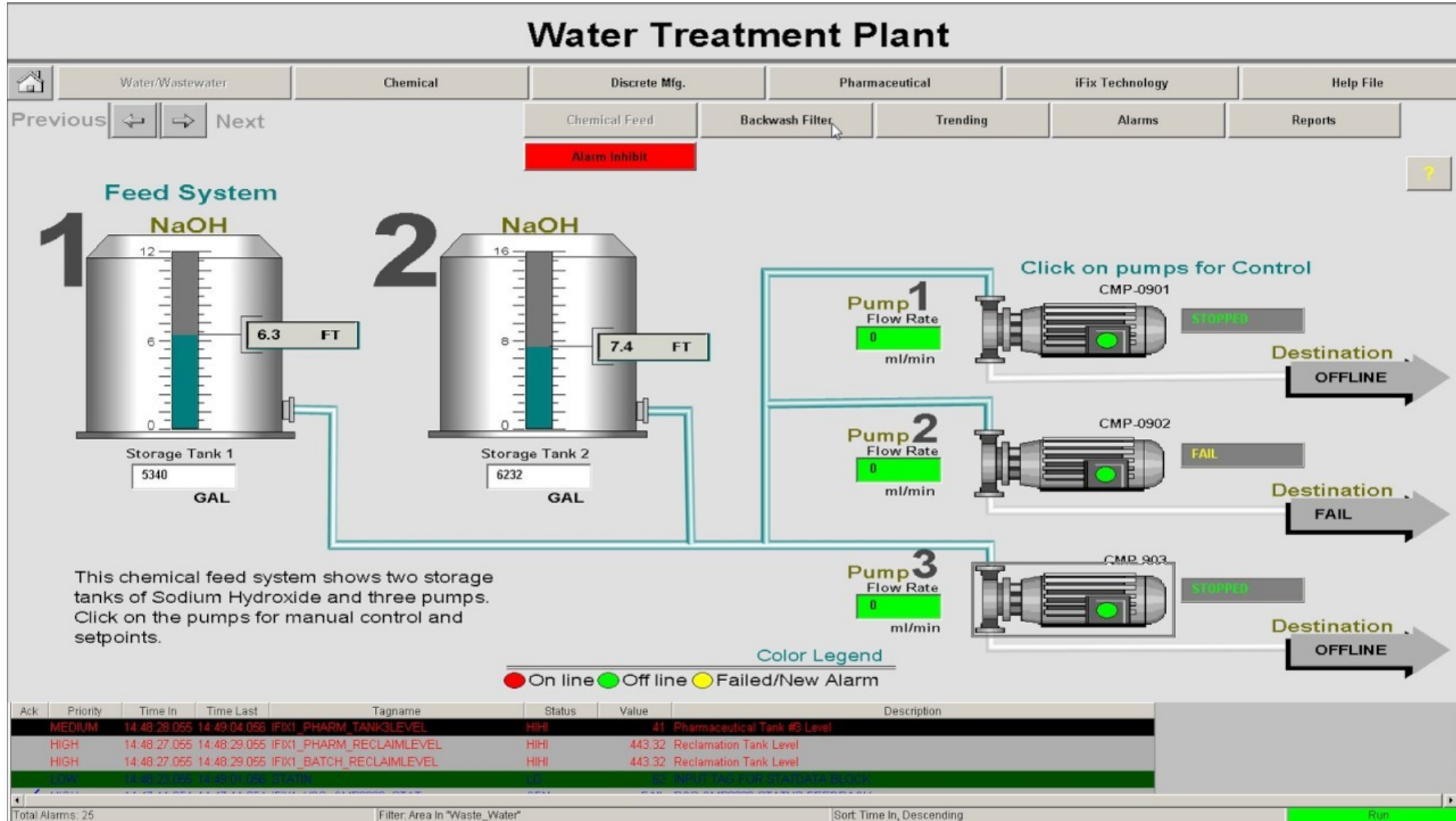
**Other ways to find chemicals**

[Advanced Search](#) [Browse](#)

Search Chemicals  
 New Search  
 Modify Search  
 Search Results

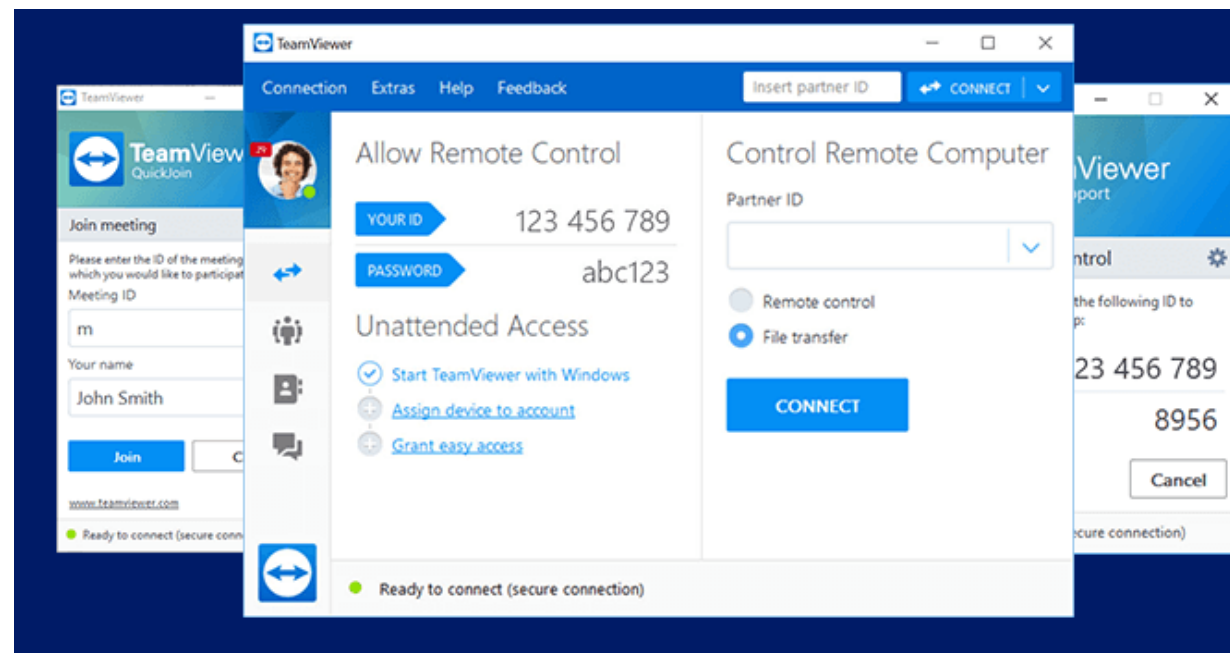
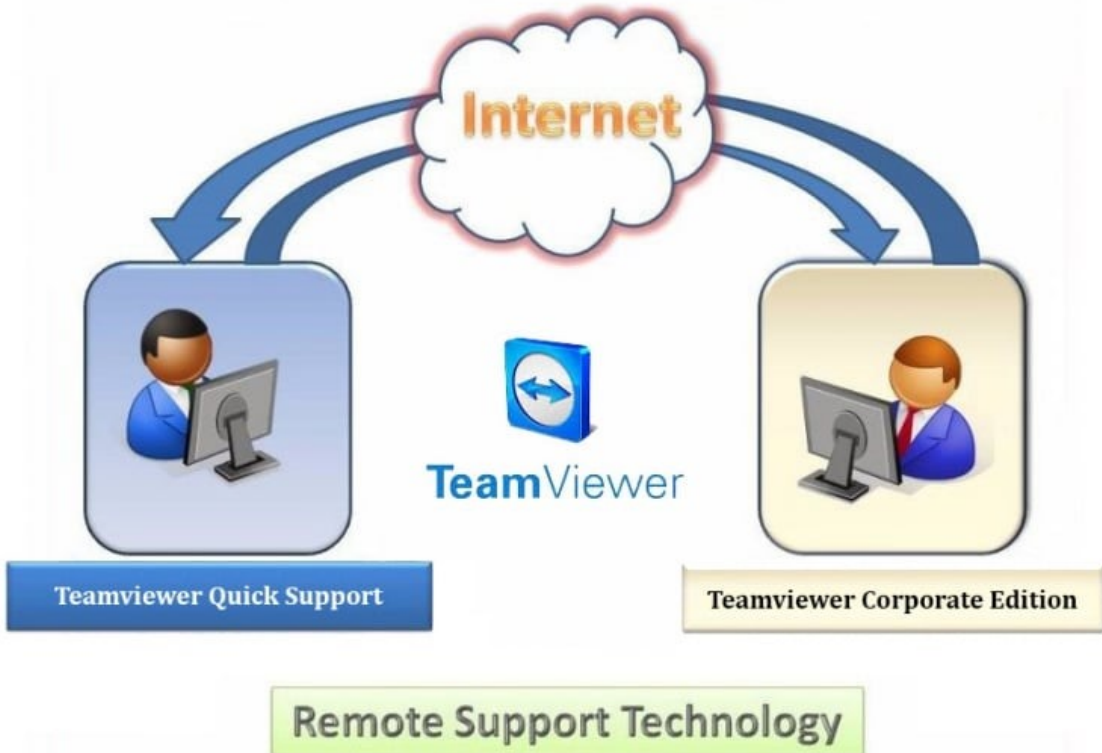
**MyChemicals**  
 chemicals: 0  
 View MyChemicals  
 Predict Reactivity

Mobile Site



# איך עובד TEAM-VIEWER?

השתלטות ממחשב  
השתלטות מטל סלולרי





14 | 18 | 46

מאגר בית יואב

גובה מים מעבר

מתח פיקוד 24 וולט תקין

תקין vac N.V.R מתח 230

5.900 meter

מכת בית ניר

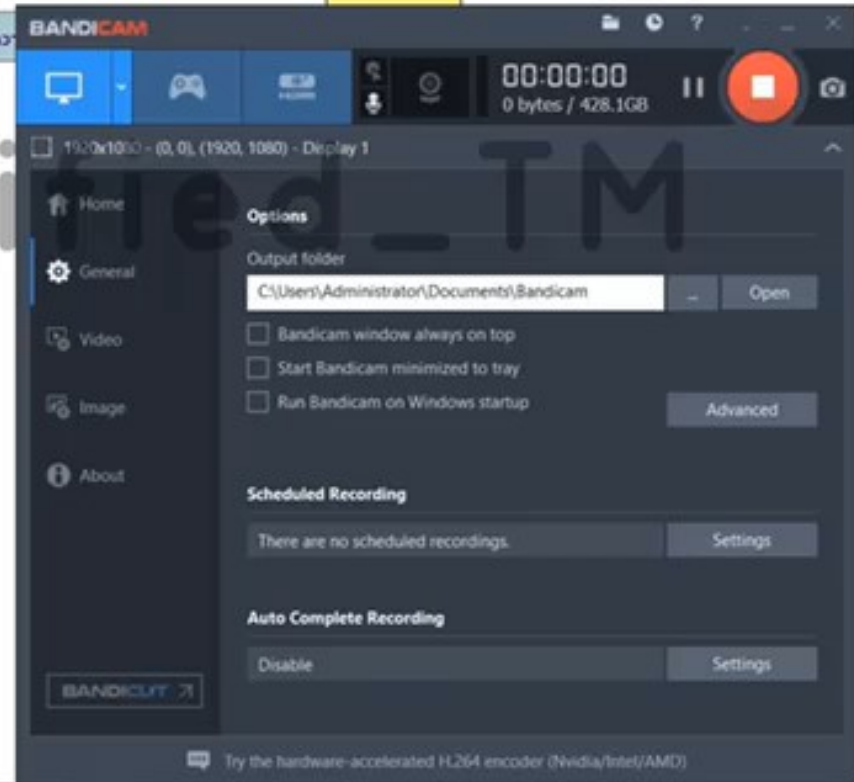
מערכת שדה יואב

מסך תקלות

גרפיק בית ניר

גרפיק שדה יואב

@Unidentified\_TM



# שאלות ותשובות

