

# שיעור 4

תורת ההגנה בסיביר 2.0 של מערך הסיביר הישראלי.  
עינויים במסגרת אבטחת הסיביר של ENISA.

## מטרת השיעור

### הכרות עם תוכניות מקבילות NIST



- להכיר את התכניות, כיצד נוצרו ולמה נועדו.
- להבין כיצד לישם את התכנית (אחת מהן) בארגונים השונים.
- לפתח גישה ביקורתית ויישומית למדייניות סייבר בארגונים!
- להבין כיצד התכניות שונות (ודומות) לתכנית ה-NIST.

## סיבות הקמה

### סיבות להקמה/פרסום

- איוםים גוברים: מתקפות סייבר הפכו לאיום ממשי המשפיע על תשתיות לאומיות, עסקים קטנים וגדולים, ומערכות ממשלתיות.
- חוסר אחידות בהגנה: ארגונים רבים התקשו להתמודד עם אתגרי הסייבר בצורה אחידה ויעילה, מה שדרש ייצירת מסגרת אחידה.
- פגיעה אפשרית במוניטין ובכלכלה: מתקפות סייבר עלולות לגרום לנזקים כלכליים כבדים ולפגיעה באמון הציבור.

## תמצית התכנית



## ההיסטוריה: למה מערך הסייבר הוקם ולמה המסמך פורסם



**צפוף מיידי למצגת – אנה עיינו בעמוד 114-115 במסמך:**

<https://www.idi.org.il/media/19666/what-is-cyber-security-part-two.pdf>

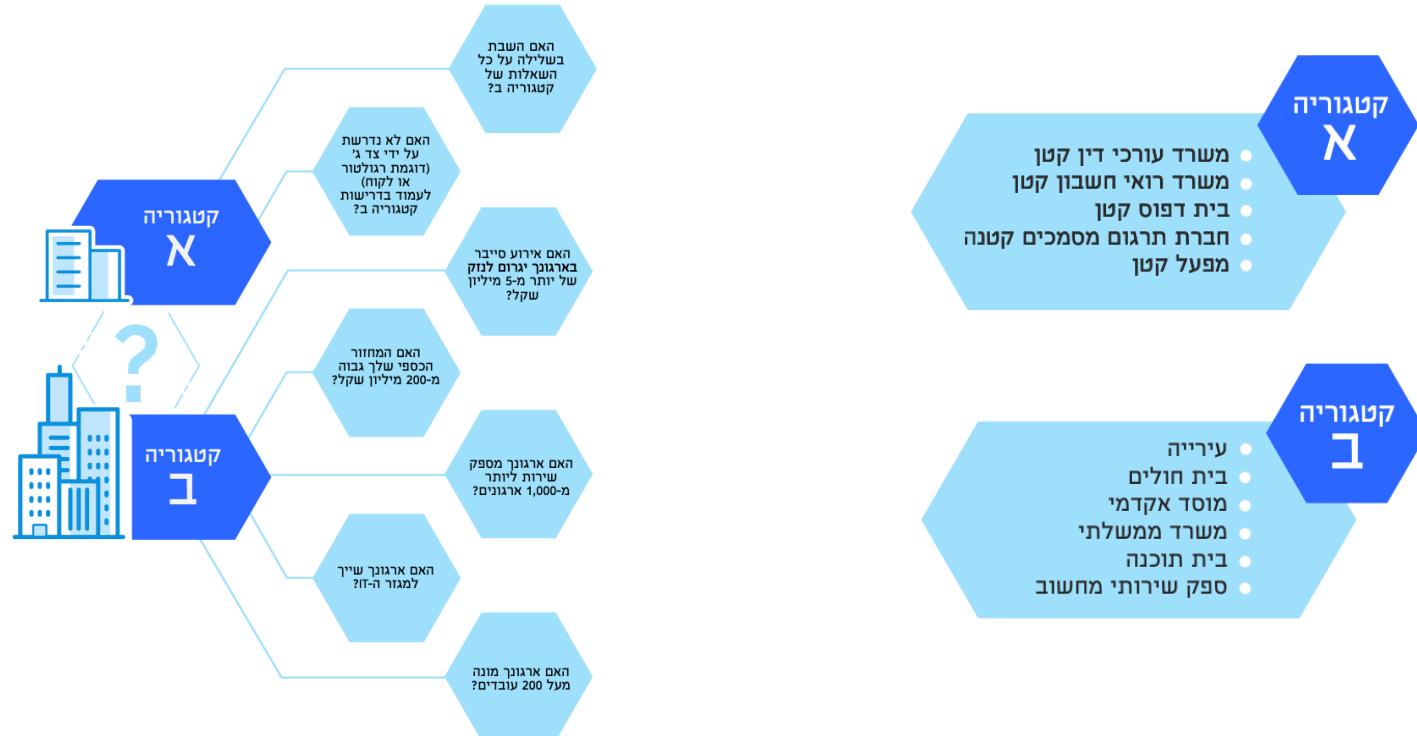
## תמצית התכנית

### קטגוריזציה:

ארגוני מחולקים לשתי קטגוריות עיקריות לפני פוטנציאל הנזק מאיrhoע סיבר:

- **קטgorיה א'**: ארגונים עם פוטנציאל נזק ביןוני-نمוך.
- **קטgorיה ב'**: ארגונים עם פוטנציאל נזק גבוה, הדורשים תהליכי ניהול סיכון מרחבים.

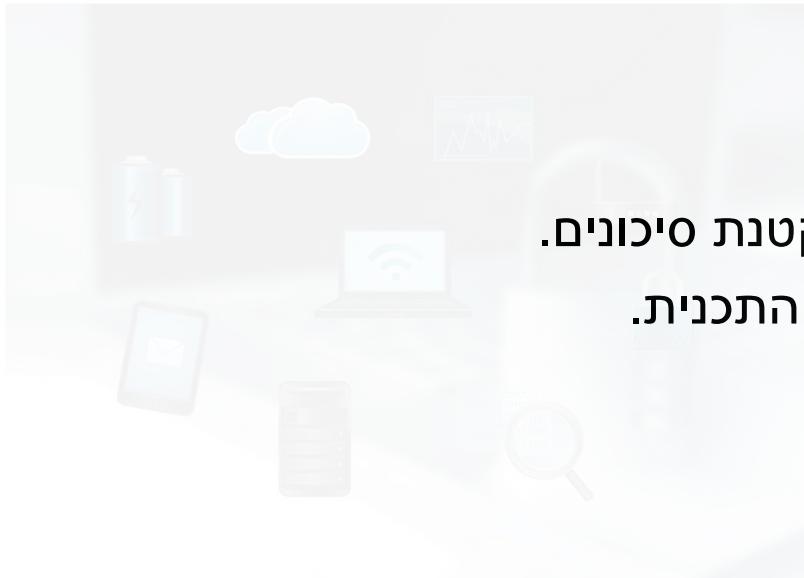
# תמצית התכנית



## תמצית התכנית

### תהליכי ניהול סיכונים

- הגדרת קטgorיה: מיפוי הארגון.
- זיהוי ואפיון סיכונים: הבנת האיומים והערכתם.
- בניית תוכנית פעולה: הכנת תוכנית מותאמת להיקטנת סיכונים.
- ביקורת ובקירה: ביצוע בדיקות שוטפות לתקפות התוכנית.



### עקרונות מרכזיים

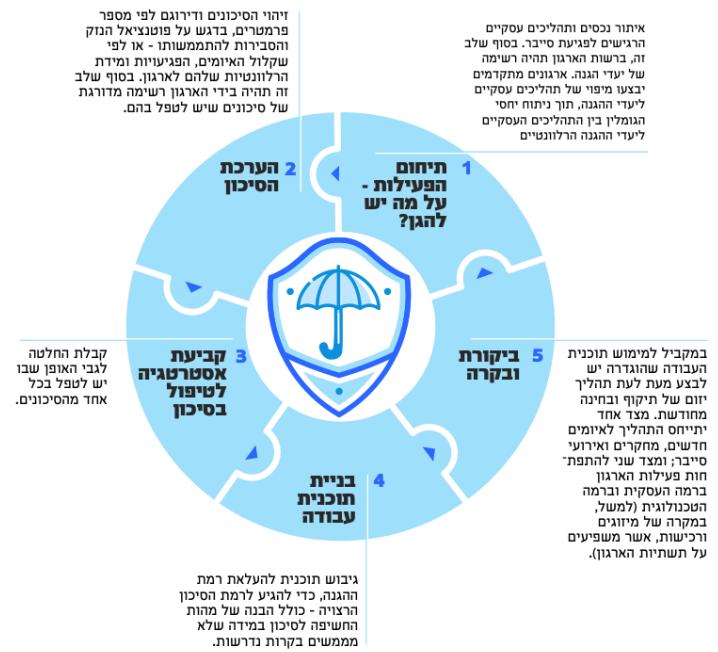
- אחריות הנהלה על ניהול הסיכונים.
- שימוש במידען עדכני.
- התאמת רמת ההגנה לפוטנציאל הנזק.

## תמצית התכנית

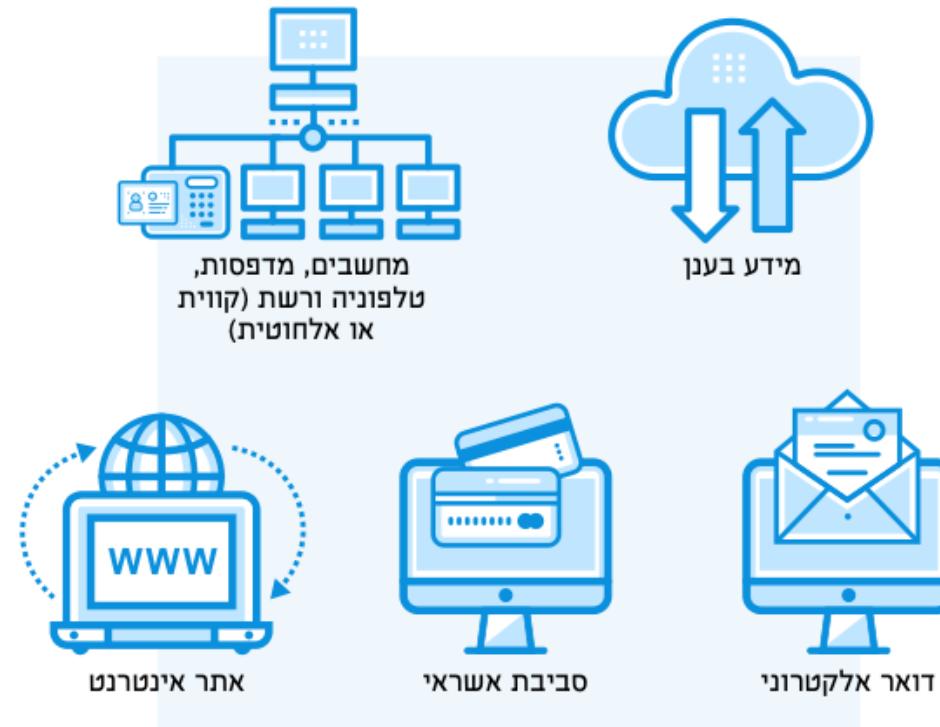
עבור ארגון מקטגוריה ב:



עבור ארגון מקטגוריה א:



## תמצית התכנית



דוגמה למייפוי ייעדי הגנה בארגון מקטגוריה A'

## תמצית התכנית

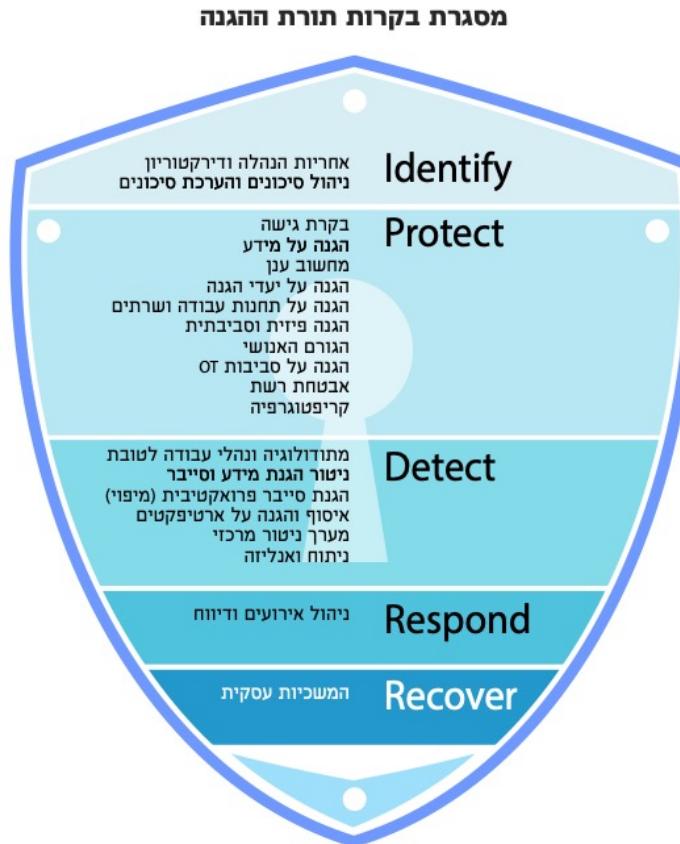


להלן טבלת עוזר למילוי נתוניים:

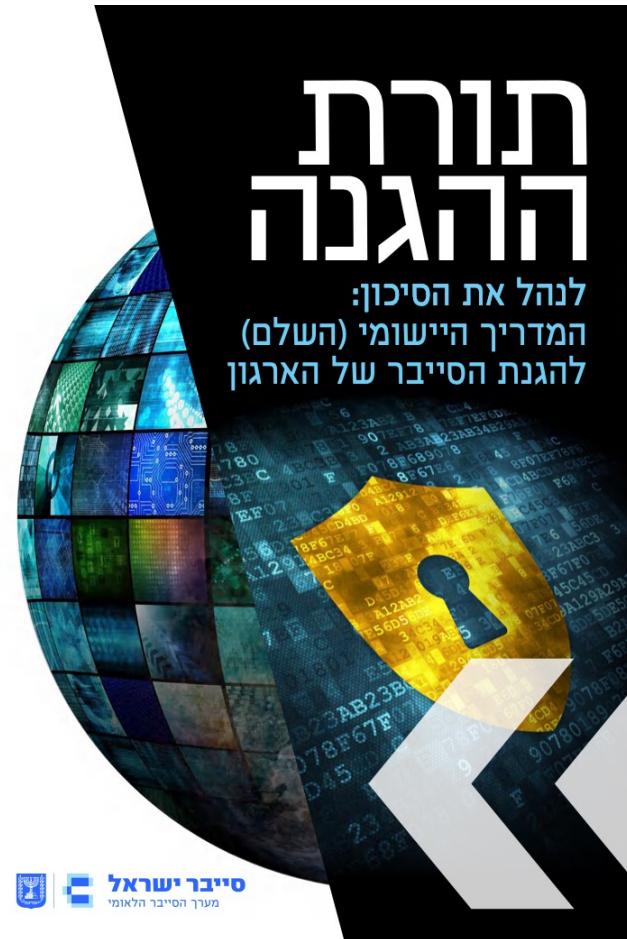
יעדי הגנה שמופיעו בארגון		כוגן: אתר אינטרנט, מאגר ל��וחות, מעדות קצה, שרת מילימ', שירות גיבום וכו'				
הנתונים/תעדות	שקלול	שימוש	עלות	אפקטיביות	הבקשה	קיים/לא
					משפחת הבקשה	
					אחריות הנהלה	
					מניעת קוד זדוני	
					הצפנה	
					מחשבוב ענן ורכיש תוכנות	
					הגנה על המידע	
					הגנה על מחשבים	
					משאבי אנוש	
					תיעוד וניטור	
					abweחת רשות	
					המשכיות עסקית	

תוכנית העבודה המוצעת תואושר על ידי מנהל/ת הארגון.

תמצית הຕביה



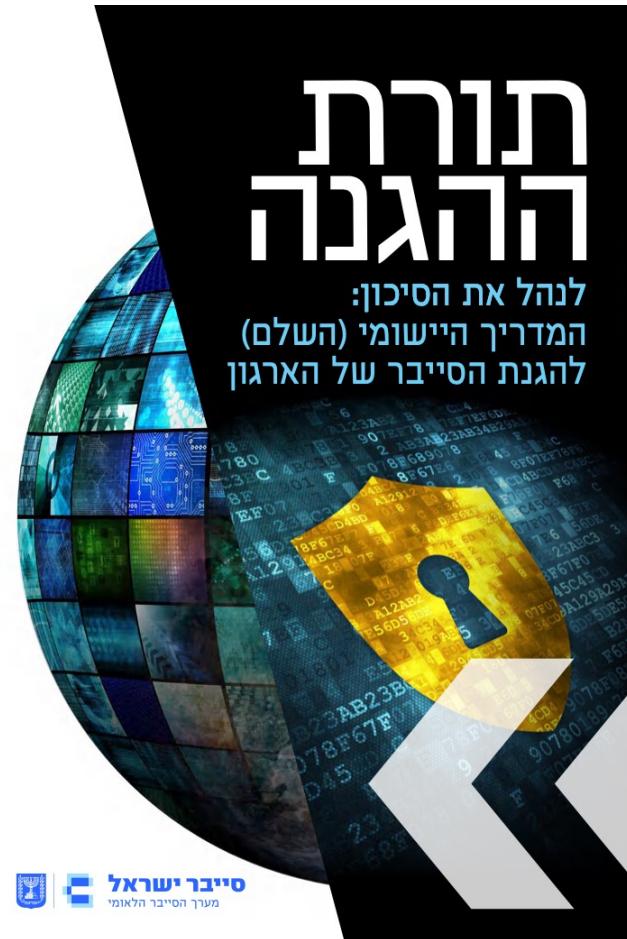
## קריאה מtower התכנית עצמה



**מקור:**

[https://www.gov.il/he/pages/cyber\\_security\\_methodology\\_2](https://www.gov.il/he/pages/cyber_security_methodology_2)

## קריאה מtower התכנית עצמה



**מקור:**

[https://www.gov.il/he/pages/cyber\\_security\\_methodology\\_2](https://www.gov.il/he/pages/cyber_security_methodology_2)

# ארגון ה- The European Union Agency for Cybersecurity

שאלה: מדוע יש צורך בארגון ומוסמכי מדיניות/נהלים כל-אירופהים?



# ארגון ה- The European Union Agency for Cybersecurity

## הקמה

- ENISA הוקמה ב-2004 בעקבות רגולציה (אמ' EC 460/2004) של הפרלמנט האירופי והמועצה.
- הסיבות להקמה כללו את הצורך בתיאום ושיתוף פעולה בין מדינות האיחוד בתחום אבטחת סייבר, במיוחד לאור העלייה באומי סייבר והצריך בהגנה על תשתיות קריטיות.

## מטרות ותפקידים

- ENISA שואפת להשיג רמה גבוהה ומשותפת של אבטחת סייבר ברחבי האיחוד האירופי.
- הסוכנות תורמת למדייניות הסייבר של האיחוד, מחזקת את אמון הציבור במקרים, שירותי ותהליכי דיגיטליים באמצעות תכניות הסמכה, ומשתפת פעולה עם מדינות החברות וגורם נוספים.

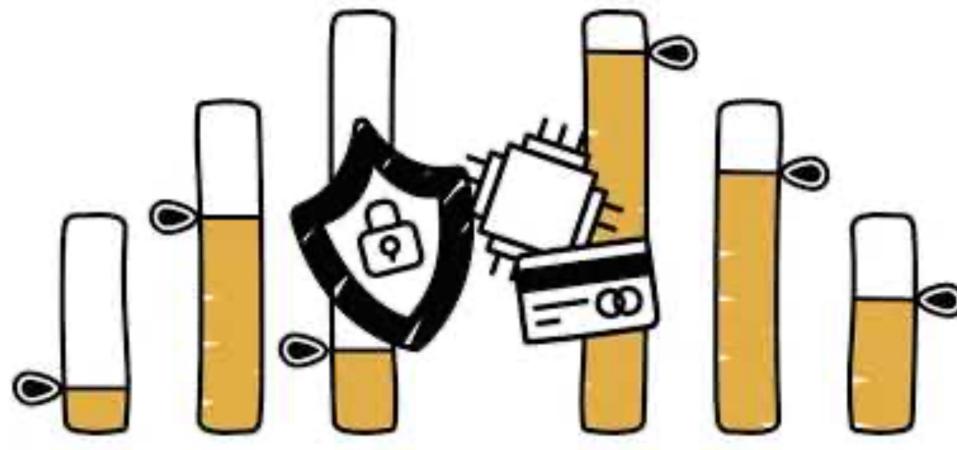


# ארגון ה- The European Union Agency for Cybersecurity



# ארגון ה-Cybersecurity

---



# uninim במחומי ה- The European Union Agency for Cybersecurity

 Awareness Raising	 Certification	 Cloud
Awareness Campaigns, SME Cybersecurity, All-in-a-box	Cybersecurity Certification Framework, From Candidates to Certification Scheme	Cloud Security
 COVID-19	 Critical infrastructure	 Cryptography
Telecom sector, Energy sector, Health sector, Finance sector, Maritime sector, Rail sector, Aviation sector, Internet infrastructure		
 Cyber Crisis Management	 Cyber Threats	 Cybersecurity Policy
Threat Landscape	Policy Observatory, NIS Directive 2, eIDAS, European Electronic Communications Code, Data Protection	
 Education	 Emerging Technologies	 Foresight
European Cybersecurity Challenge (ECC), International Cybersecurity Challenge (ICC), European Cybersecurity Risk Framework (ECRF)	Internet of Things (IoT), Artificial Intelligence (AI)	
 Incident Reporting	 Incident response	 Market
For Trust Providers, For Digital Service Providers (DSPs) Directive, Cybersecurity Incident Report and Analysis System – Visual Analytics	EU CYBERSECURITY CSIRT Network, CSIRT Maturity, Cooperation with CSIRT-EU, Situational awareness, with CSIRT Inventory, Glossary	Annual cybersecurity market analysis, Cybersecurity Market Analysis framework
 National Cybersecurity Strategies	 Research and Innovation	 Risk Management
National Cybersecurity Strategies Guidelines & tools, National Cybersecurity Strategies (NCSs) Map, Public-Private Partnerships (PPPs), Information Sharing and Analysis Centers (ISACs)	R&D Roadmap, R&D Observatory, EU funding in cybersecurity	
 Standards	 Training and Exercises	 Vulnerability Disclosure
Cyber Exercises, Trainings for cybersecurity specialists		

uninim  
בנושאים  
ומושגים:

<https://www.enisa.europa.eu/topics>



2025-2026

ד"ר לב טופור

80

## מגזרים שונים ומשונים

Country	Framework	Focus	Strengths	Weaknesses	Target Audience
USA	<u>NIST Cybersecurity Framework (CSF)</u>	Risk-based, voluntary	Flexible, customizable, integrates with other frameworks	Lacks prescriptive guidance, may be complex for small organizations	Businesses of all sizes, government agencies
Independent/ Switzerland	<u>ISO 27001:2013</u> <u>ISO 27002:2022</u>	Information security management, prescriptive	Well-established, globally recognized, comprehensive	Can be rigid, bureaucratic, expensive to implement	Organizations of all sizes seeking certification
Cross-European	<u>ENISA Cybersecurity Framework</u>	Risk management, threat intelligence	EU-focused, considers emerging threats, <b>filtered!</b>	Less mature than other frameworks, limited adoption outside EU	EU organizations, public administrations
China	<u>TC260</u>	National security, critical infrastructure	Government-backed, compliance-driven	Lacks transparency, limited international recognition	Chinese organizations, critical infrastructure providers, personal use, by industry
UK	<u>NCSC Cyber Essentials; Small Business Guide</u>	Basic cyber hygiene, essential controls	Simple, affordable, good starting point	Not as comprehensive as other frameworks, may not be sufficient for high-risk organizations	Small and medium businesses, organizations with limited resources
Israel	תכנית מכון ארגוני למשבב סיבת תורת ההגנה	Basic cyber hygiene, essential controls, <b>local</b>	Simple, affordable, good starting point	Not as comprehensive as other frameworks, may not be sufficient for high-risk organizations	Management level, public

## סיכום ושאלות



# שיעור 5

הסמכות ומוסגרים בינלאומיים:  
יעוד ISO2700X, SOC2, CSA, GDPR