פורום IR

מערך הסייבר הלאומי

עדכון: 07/06/2026

מסמך זה נכתב על בסיס קול קורא שהופץ ב-10/2023 ותוקף ב-06/2026. ככל שנפלה טעות במסמך נבקש לשלוח מייל עדכון לכתובת: mirror_app@cyber.gov.il. מערך הסייבר שומר לעצמו את הזכות לעדכן את המסמך מעת לעת ובהתאם לרישומים חדשים של חברות רלוונטיות לפורום.

מערך הסייבר הלאומי

פורום חברות IR של מערך הסייבר הלאומי

1. כללי

1.1. מערך הסייבר הלאומי במשרד ראש הממשלה (להלן – "**המערך**" או "**מערך הסייבר**") פועל לפי החוק להסדרת הביטחון בגופים ציבוריים, התשמ"ח-1998 והחלטות הממשלה בתחום הגנת הסייבר לקידום ההגנה על תפקודו התקין של מרחב הסייבר הישראלי בשגרה ובחירום[1], ומהווה נקודת ממשק מרכזית בין גופי הביטחון לבין המשק הישראלי לצרכי הגנת הסייבר.

1.2. המערך פועל מול ארגונים בטיפול בתקיפות סייבר שעלולות לגרום נזק לאינטרסים ציבורים חיוניים.

1.3. על רקע המתקפה האכזרית והמשולבת שחוותה מדינת ישראל מצד ארגון הטרור חמאס ביום 7.10.2023; במטרה להעלות את החוסן הלאומי; לשם היערכות למצב של מתקפות סייבר מצד גורמים עוינים; לשם הגדלת היכולות הלאומית להתמודד עם היקף נרחב של תקיפות סייבר; ובשים לב לנכונות המשק לסייע בחזית הסייבר הוחלט על קידום מיזם זה.

1.4. בסמוך לאחר פרוץ מלחמת "חרבות ברזל", קידם מערך הסייבר הלאומי (להלן – "**המערך**" או "**מערך הסייבר**") מיזם להקמת פורום חברות העוסקות במתן שירותי תגובה לאירועי סייבר (IR) במשק הישראלי, ועומדות בקריטריונים סדורים וסטנדרט מקצועי גבוה (להלן: "**הפורום**" או "**המיזם**").

1.5. מטרת המיזם הינה להעלות את החוסן הלאומי, להיערך למצב של מתקפות סייבר מצד גורמים עוינים ולהגדיל את היכולות הלאומית להתמודד עם היקף נרחב של תקיפות סייבר .

1.6. המיזם פועל על דרך של הפניית גוף במשק שחווה תקיפה (להלן –"**הגוף**") לקבל שירות מאת חברה הכלולה ברשימה המגובשת במסגרת קול קורא זה, לטובת סיוע בחיבור מהיר בין גוף במשק שחווה תקיפה לבין החברה, נותנת השירות המופיעה ברשימת הפורום. בהתקיים צורך מבצעי מיוחד או צורך מלחמתי, לרבות אירוע סייבר רב מגזרי, באפשרות המערך להפנות גוף לנותן שירות מסוים מתוך הרשימה, בהתאם ליכולותיו של נותן השירות אשר פורטו על ידו במסגרת הליך הרישום. בכל אחד מהמצבים ההתקשרות בין הגוף לבין נותן השירות תהיה התקשרות ישירה ובאחריות הצדדים בלבד.

[1] החלטת ממשלה מס' 2444 מיום 15.12.15, החלטת ממשלה 2443 מיום 15.12.15 והחלטת ממשלה מס' 2370 מיום 17.12.17.

1.7. חברות המבקשות להצטרף למיזם, אשר עומדות בכלל תנאי הסף ודרישות הפורום המפורטות בהמשך, מתבקשות למלא את פרטיהן בקול הקורא בכתובת: https://go.gov.il/Kol_kore_ir.

1.8. ככלל, המיזם יעבוד על דרך של הפניית גופים אשר קיים חשש שחוו תקיפת סייבר לאותה רשימת חברות, לטובת סיוע בחיבור מהיר בין גוף לבין נותן שירות המופיע ברשימת הפורום. לצד האמור, בהתקיים צורך מבצעי מיוחד או צורך מלחמתי, לרבות אירוע סייבר רב מגזרי, יפנה המערך הסייבר גוף לנותן שירות מסוים מתוך הרשימה, בשים לב ליכולות המציע אשר פורטו על ידו במסגרת המענה לקול הקורא שפרסם המערך. **דגש חשוב הוא שבכל אחד מהמצבים ההתקשרות בין הגוף לבין נותן השירות תהיה התקשרות ישירה ובאחריותם בלבד, כמפורט בהרחבה בסעיף 3 שלהלן. הכולל דגשים חשובים נוספים בנוגע להתקשרות.**

2. קריטריונים ודרישות סף

כלל החברות בפורום הצהירו על עצמן שהן עומדות בתנאים הבאים, בהתאם לדרישות מערך הסייבר הלאומי:

2.1. למבקש נציגות רשמית במדינת ישראל;

2.2. למבקש שני אנשי צוות לפחות, על לפחות 2/3 מאנשי הצוות להיות בעלי 2 שנות ניסיון, או יותר;

2.3. המבקש מספק שירותי תגובה לאירועי סייבר (IR);

2.4. המבקש והשירות המוצעים על-ידו פועלים בהתאם להוראות הדין;

2.5. למבקש ניסיון בהתמודדות עם מתקפות סייבר בעלות רמת תחכום גבוהה מבחינת הכלים בהם השתמשו התוקפים ויכולותיהם;

2.6. למבקש יכולת סיפוק מודיעין על איומי סייבר ושימוש בו כתגובה לאירועים;

2.7. למבקש יכולת ניתוח בסיסי/מתקדמת של תוכנות זדוניות;

2.8. למבקש יכולת לאתר ולזהות נקודות קצה נגועות;

2.9. למבקש יכולת ניתוח לוגים;

2.10. למבקש יכולת לבצע פורנזיקה דיגיטלית;

2.11. המבקש מתחייב לנקוט בכל הפעולות הנדרשות, לרבות משפטיות, טכנולוגיות ותהליכיות, לשם שמירה על סודיות והגנה על תהליך איסוף המידע, אחסונו, ניתוחו והעברתו לכל גורם מוסמך ורלוונטי;

2.12. המבקש מתחייב לשתף עם מערך הסייבר כל מידע בעל ערך הגנתי המתקבל במסגרת החקירות ואירועי הסייבר שיטופלו על ידו במסגרת השתתפותו במיזם, בין אם מדובר על מידע שנאסף על ידו במישרין, ובין אם מדובר על מידע שנאסף על ידי נציגים או קבלני משנה של המבקש, או בכל תצורה אחרת הנלווית לטיפול באירוע הנובע ממיזם זה, לרבות תוצרי חקירה, מזהים ודו"ח חקירה. כמו כן, המבקש מתחייב על שמירת סודיות המידע אשר יתקבל אצלו ע"י המערך, הכל כמפורט בנספח א'.

2.13. המבקש מצהיר כי מחזיק ברשותו ביטוח, אשר כולל את מערך הסייבר כמבוטח נוסף, ביחס לשירותים ולפעולות המבוצעות על ידו נשוא קול קורא זה.

3. דגשים בכל הנוגע להתקשרות בין גוף לבין חברת IR מהרשימה

3.1. השירותים מוצעים על ידי חברות ה- IR המנויות ברשימה, מוצעים מטעם עצמן ואין לראות ברשימה משום המלצה מטעם מערך הסייבר הלאומי על התקשרות עם מי מהחברות, או בכלל.

3.2. ברשימה נכללות רק חברות IR שהצהירו על עמידתן בתנאים שהוגדרו ב"קול קורא" פומבי שהופץ על ידי המערך ביום 23.10.23 (להלן- "הקול הקורא"). לא בוצעה בדיקה של מערך הסייבר מעבר לכך למעט הצהרת החברה על עמידה בתנאי הסף. האחריות לבדיקה מעמיקה חלה על הגוף וחברת ה IR.

3.3. ההתקשרות בין הגוף לבין חברת IR המנויה ברשימה (להלן- "הצדדים") על כל רבדיה היא התקשרות ישירה ובאחריות הצדדים לה בלבד. בכלל האמור ומבלי לגרוע, מערך הסייבר אינו לוקח חלק במימון ההתקשרות, אינו צד להסכם ההתקשרות בין הצדדים ואינו אחראי למהלך או לתוצאות השירות.

3.4. יובהר כי גם במקרה בו הציע מערך הסייבר לגוף על על הסתייעות בחברת IR מסוימת מתוך הרשימה, האמור מתבסס על הנתונים שהוצהרו על ידי החברה, ואין באמור כדי לגרוע מאחריותם הבלעדית של הצדדים לבחינת האפשרויות העומדות בפניהם ותנאי ההתקשרות.

3.5. מערך הסייבר לא יישא באחריות לנזק, אובדן, עוגמת נפש וכל נזק אחר, בין אם ישיר ובין אם תוצאתי, אשר יגרם למי מהצדדים במסגרת ההתקשרות בניהם.

3.6. על גורם המבקש להתקשר עם חברת IR מהרשימה, מוטלת האחריות לקרוא את תנאי הקול הקורא. בכלל זה, יובהר כי חברות ה- IR התחייבו:

א. לנקוט בכלל הפעולות הנדרשות, לרבות משפטיות, טכנולוגיות ותהליכיות, לשם שמירה על סודיות והגנה על תהליך איסוף המידע, אחסונו, ניתוחו והעברתו לכל גורם מוסמך ורלוונטי.

ב. לשתף עם מערך הסייבר כל מידע בעל ערך הגנתי המתקבל במסגרת החקירות ואירועי הסייבר שיטופלו על ידה, כמפורט בקול הקורא.

4. פרטי החברות

4.1. להלן פרטי החברות, אשר הצהירו שעומדות בקריטריונים המפורטים בסעיף 2 לעיל שנקבעו על ידי מערך הסייבר הלאומי כתנאי סף להשתתפות במיזם זה.

4.2. כל החברות הרשומות מטה העבירו אלינו דוחות ומסמכים לבחינת ההתאמה לפורום.

4.3. סדר הרשימה נקבע לפי תאריכי ההרשמה ואינו מעיד על מהות או טיב השירות.

פרטי החברות בעמודים הבאים

4.4. פרטי החברות ליצירת קשר:

שם החברה	איש הקשר	כתובת דוא"ל של המבקש	טלפון
BDO	אופיר זילביגר	Leeg@bdo.co.il	052-3809477
CodeBlue	רפאל פרנקו	office@codebluecyber.com	02-3761215
10root	עדי מכלוף	IR@tenroot.io	052-889-8673
2bsecure	רחל ברזילאי	rachel.barzilay@2bsecure.co.il	054-9429480
Madsec Security LTD	תומר דרורי	tomer@madsec.co.il	052-2372465
חברת פיי.סי.לאבס סייבר סקריוט	גיא אדרי	guy@pclabsec.com	054-2121313
חברת סייפוקס טכנולוגיות בעמ	הילה מרקוביץ	hila@cyfox.com	052-2522219
CWG cyberwallglobal	ניב ביאזי	niv@cyberwallglobal.com noamp@cyberwallglobal.com	052-4255941
סיגניה קונסלטינג	אריאל רוטמן	Ariel.r@sygnia.co	050-9310875
כובע לבן	שרון נימירובסקי עמית הרטמן	sharon@white-hat.co.il amit_hartman@epam.com	058-4443232 054-6749462
ד.ד. סייפר אבטחה בע"מ	omri shdaimah	nir@sayfer.os	052-4203779
אקספריס סייבר בע"מ	Menashe kamara	menashek@experis-cyber.com	052-3817328
אינטנסיטי גלובל	רוני רויטמן	Ronir@intensity.co.il	052-8364394
איונסק סייבר סקיוריטי	מורן כלפון	moran@ionsec.io	050-3003775
Rsecurity	רועי מושיאלוב	Operations@rsecurity.tech	052-5594598

שם החברה	איש הקשר	כתובת דוא"ל של המבקש	טלפון
סיטאדל קונסולטינג בעמ	מוטי קארו	ginat@citadel.co.il moti@citadel.co.il	08-6191664 054-2566640
Hackerseye (Anytech)	דין בר	dean@hackerseye.net	052-4257718
Cyght	שי נחום	shay@cyght.co	058-7876544
אייאר-סאק בע"מ	יוסי מגור	ymagor@eyer-sec.com	053-7141545
סקדהוסו בע"מ	יגאל גויטע	scadasudo@gmail.com	053-4239847
קבוצת שביט בע"מ	ניר שביט	nir@shavit-security.com	054-2002999
OP Innovate	עומר פינסקר	omer@op-c.net	054-6536698
SOPHTIX Security LTD	גד אבוחצירא	gad.a@sophtix.com	054-7625990
Solveo	כפיר אזולאי	kfir@solveo.co.il	054-3111844
Force Majeure Ltd.	דן לוינסון	dan@f-m.co.il	03-6259898 050-7419943
CyberTeam360	אורן אלימלך	Orene@cyberteam360.com	050-5375385
irone	אלי זילברמן כספי	eli@irone.io	052-6006829
אופק אייץ' אנד או בע"מ	עופר ישראלי	ofer@ofekdist.com	054-7881885
Trusnet	אביב מזרחי	Avivm@trustnet.co.il	054-2532100
Persist Security	פז שורץ	pazs@persistsec.com	050-4000553