מערך הסייבר הלאומי

<u>פניה מוקדמת לקבלת מידע (RFI)</u>

<u>מס' 06/2020</u>

<u>בנושא: מערכת ניהול מודיעין איומי סייבר</u>

נוסח מעודכן בהתאם לקובץ הבהרות מס' 1

יוני 2020

מסמך זה הינו רכוש מדינת ישראל. כל הזכויות שמורות למדינת ישראל (C). המידע הכלול בו לא יפורסם, לא ישוכפל ולא יעשה בו שימוש מלא או חלקי לכל מטרה שהיא מלבד מענה על פנייה זו.

פנייה מוקדמת לקבלת מידע (RFI) בנושא:

1. רקע ומטרת הפנייה

1.1 מערך הסייבר הלאומי במשרד ראש הממשלה (להלן: "המערך" או "המשרד"), מבקש בזאת לקבל מידע בנוגע לשירותי איסוף, ניהול וניתוח מודיעין איומי סייבר (להלן "השירות" ו/או "השירותים").

השירות שבנדון הינו שירות טכנולוגי המאפשר קבלה, ניהול וניתוח של מודיעין איומי סייבר עדכני, מאומת ורחב ככל האפשר, על בסיס מידע מרשת האינטרנט על כל סוגיה, הן באופן שוטף והן על פי דרישת המערך, עם אפשרויות גישה מגוונות (באמצעות פורטל אינטרנטי ובנוסף באמצעות API).

2 כללי

2.1 פנייה זו הינה פנייה מוקדמת **לקבלת מידע** בהתאם לתקנה 14א לתקנות חובת המכרזים, תשנ"ג – 1993. אין בה כדי ליצור מחויבות כלשהי כלפי מי מהמשיבים ו/או לראות בה התקשרות משום סוג. הפנייה נועדה לקבלת מידע בלבד ובעקבותיה ישקול המערך את המשך פעולותיו בהתאם לשיקולים מקצועיים ועניינים.

2.2 אם וככל שיתקיים מכרז בעתיד, יהא רשאי המערך לשנות או להוסיף תנאים ודרישות, הכל לפי שיקול דעתו המקצועי ובהתאם לצרכיו.

2.3 המערך יהא רשאי לעשות שימוש במידע שיימסר לו במענה לפנייה זו, ולספק לא יהיו טענות בגין זכויות יוצרים.

2.4 מענה לפנייה זו לא יהווה תנאי להשתתפות במכרז, אם וככל שייערך בעקבותיה, ולא יקנה יתרון במכרז למי שנענה לפנייה רק בשל כך שנענה לה, ולא יחייב שיתופו במכרז או התקשרות עמו בכל דרך אחרת.

2.5 ניתן לעיין ולהוריד את המסמכים המלאים של הבקשה לקבלת מידע באתר האינטרנט של מנהל הרכש הממשלתי בכתובת: https://www.mr.gov.il/Pages/HomePage.aspx או באתר האינטרנט של מערך הסייבר הלאומי בכתובת: https://www.gov.il/he/departments/israel_national_cyber_directorate

2.6 להלן טבלת ריכוז התאריכים לפנייה זו:

הפעילות	תאריך	שעה
מועד פרסום הפנייה	21.06.2020	11:00
המועד האחרון להמצאת שאלות הבהרה מן הספקים	.08.07.2020	11:00
מועד המענה של המשרד לשאלות ההבהרה	15.07.2020	11:00
המועד האחרון להגשת מענים	29.07.2020	11:00

2.7 הדין החל על פנייה זו הינו דין מדינת ישראל וסמכות השיפוט תהיה של בית משפט במדינת ישראל בלבד, בעיר תל אביב (מקום מושבה של ועדת המכרזים).

3 מושגי יסוד:

3.1 **ישויות / סוגי ישויות** – מזהים (IOC's) נכסים טכנולוגיים – לפי סוגים ומאפיינים, חולשות והשלכותיהן, מערכי תקיפה, סוגי תוקפים, וכיוב'.

3.2 **רשימות נתונים** - רשימות המכילות נתונים או ישויות לחיפוש ומאפשרות חיפוש רב פעמי לגבי כמויות גדולות של נתונים.

3.3 **רשימות קבועות** – רשימות אשר תשמשנה בסיס לשאילתות קבועות והתרעות לגביהן.

3.4 **רשימות משתנות** – רשימות אשר תשמשנה לחיפושים זמניים ומיוחדים.

3.5 **שאילתה** –פנייה לקבלת מידע.

3.6 **ניתוח ראשוני של אנליסט** - ניתוח המידע הקיים בתוספת תובנה אנושית, אימות, ועדכון.

3.7 **גורמים סביבתיים** - אירועים מדינתיים ו/או עולמיים.

4 מפרט דרישות

4.1 במסגרת RFI זה מבקש המערך לקבל מידע מפורט אודות השירות המסופק תוך התייחסות אל היכולות המפורטות להלן:

4.1.1 נתונים אודות הספק - לרבות היקף פעילות, וותק פעילות בתחום מודיעין איומי סייבר, נציגות ישראלית (אם יש), סוגי לקוחות כולל מאפייני לקוח, פרטי לקוח ופירוט השירות הניתן לו (תוכן והיקף, סוג הטמעה, לו"ז) ושימושים לשירות המסופק.

4.1.2 נתונים אודות מקורות המידע – לרבות היקף, תחומי המידע המנותח, שפות מנותחות, רמת עדכניות המקורות, מקורות היסטוריים, היקף ועומק הכיסוי בכל סוגי רשת האינטרנט, יכולות להרחבת והעמקת הכיסוי, יכולת אינטגרציה של מידע ממקורות פנימיים וחיצוניים.

4.1.3 עדכניות המידע - עדכון על בסיס יומיומי הכולל התייחסות לאירועי סייבר בעולם.

4.1.4 יכולות אימות המידע, רמת האימות ומנגנון חיווי לגבי רמת אימות (לדוגמא, - אימות באמצעות הצלבת מקורות וציון מספר המקורות, אימות באמצעות אנליסט, אימות משולב וכו').

4.1.5 פירוט לגבי יכולות טיוב המידע ומנגנון חיווי לגבי רמת טיוב (לדוגמא, מספר מקורות רלוונטיים, זהות מקורות, מועד האימות וכו')

4.1.6 פירוט לגבי יכולת הוספת מקורות ואינטגרציה למוצרים ומקורות חיצוניים לשירות על פי דרישה (פירוט ניסיון קודם, הערכת לוחות זמנים ומשאבים נדרשים להוספה/אינטגרציה כאמור, מנגנון תימחור).

4.1.7 יכולות ניהול סיכונים - אפשרות לקבלת תמונת איומי סייבר וציון סיכון בחתכים / איחודים שונים (ארגונית, מגזרית וכו').

4.1.8 אפשרויות ההתקנה של המערכת – התקנה מקומית, מרוחקת וכו'.

4.1.9 אמצעי הגישה למערכת, סוגי הפרוטוקולים והיכולות הזמינות בכל ממשק גישה – תוכנה ייעודית, דפדפן, ממשק תוכנתי (API) וכו'.

4.1.10 מפרט תשתיות - חומרה, תוכנה, אלגוריתמיקה, יכולות שמירת נתונים ואפשרויות גיבוי.

4.1.11 מערך תמיכה – מודלי תמיכה אפשריים, פירוט יכולות, שפות נותני שירות בתמיכה, שעות זמינות, SLA.

4.1.12 מערך ההדרכה – פירוט יכולות, שפות נתמכות, מיקום ההדרכות (מקוון/אתר הספק/אתר הלקוח).

4.1.13 יכולת ייצור שאילתות מורכבות המבוססות על ישויות, רשימות מוגדרות, קורלציות בין נתונים שונים ועוד.

4.1.14 יכולת לקבל מידע באופן שוטף ובדחיפה (בזמן אמת ו/או ע"פ הגדרת תכיפות) בהתקיים מענה על תנאי שאילתות.

4.1.15 ניהול שאילתות וישויות- סוגי שאילתות, סוגי מידע, טיוב שאילתות, שמירת שאילתות ועוד.

4.1.16 פרמטרים להגדרת איכות וכמות לשאילתות - כמות רשימות נתונים מינימלית ומקסימלית, כמות שאילתות מינימלית ומקסימלית, פירוט SLA/ וכדומה.

4.1.17 שירותי אנליסט בהתאם לדרישת לקוח (שירות נפרד) – ניסיון הספק והאנליסטים מטעמו, פירוט SLA.

4.1.18 תמיכה בשפות במערכת ובכלל ממשקיה (כולל API).

4.1.19 פירוט הגמישות ויכולות הפיתוח והפרסונליזציה בתחום ממשק המשתמש במערכת (למשל, קונפיגורציה עצמאית ודינמית המאפשרת סינון וחיתוך מידע נושאי לפי דרישות המשתמש, תצוגה ועוד).

4.1.20 הצגת ממשק משתמש בהתייחס למפרט הדרישות.

4.1.21 יכולת ייצור והפקת דו"חות – פירוט פרמטרים קבועים ומשתנים בדו"ח, יכולת פרסונליזציה ליצירת והפקת דו"חות והצגת דוגמאות.

4.1.22 ממשקי ההתרעה על הודעות והתרעות בזמן אמת- דיווח לממשק המערכת, הודעה למייל, משלוח מסרון וכו'.

4.1.23 מודל הרישיון למערכת - סוגי רישיון, תמיכה בהיררכיות משתמשים והיררכית עבודה, מדרג שימוש וכו'.

4.1.24 אפשרות ליבוא ויצוא נתונים לתוך המערכת וממנה (פירוט האמצעים למימוש הדרישה ומגבלות, אם קיימות, לייצוא/שיתוף המידע) ושיתוף מידע במערכות חיצוניות.

4.1.25 מנגנון לשתף מידע בין משתמשים בתוך המערכת.

4.1.26 מעקב אחר נתוני השימוש הכמותיים במערכת בחתכים שונים (כמויות, שעות שימוש וכו'), סוגי שימוש על פי רישיונות.

4.1.27 אמצעי התיעוד של כלל פעילות המערכת.

4.1.28 מנגנון ניהול המשתמשים במערכת (מקומי, חיבור למערכות ניהול משתמשים מרכזיות וכו').

4.1.29 פירוט תהליך ואמצעי אבטחת המידע הקיימים במערכת – איך המערכת מוגנת, איך המשתמשים מוגנים, איך פעילות המשתמשים מוגנת וכו'.

4.1.30 עמידה בתקינה בינלאומית – תקני אבטחת מידע, תקני פרטיות וכו'.

4.2 המענה מטעם הספק יכלול נתונים בדבר כמויות, מדדים, יחידות, זמני ביצוע, נתוני בקרה וכיוב.

4.3 המענה מטעם הספק יפרט תפיסות יישום, אפשרויות מימוש וכל מידע אחר הרלוונטי לשירות.

4.4 מודל עסקי להתקשרות לרבות מודל תימחור, מסלולי רישוי (רכישה, חכירה) ואופציות להרחבת שירות.

5 המענה המבוקש

5.1 על המענה להתייחס לכל אחת מהדרישות המפורטות בסעיף 4 לעיל, ובכלל זה לכלול התייחסות לנושאים הבאים:

5.1.1 הצגת יכולות **בהתייחס לכלל הדרישות המפורטות בסעיפים 4.1.1 – 4.1.30** (במקרה בו היכולת לא קיימת אצל בשירות המסופק יש לציין זאת במפורש במענה הספק)

5.1.2 היצע פתרונות עם יכולת התאמה לארגונים שונים – גודל, סיווג (בלמ"ס, מסווג, תפעולי), מבנה רשתות – פתוח/סגור.

5.1.3 דרישות התקנה, תפעול ועדכון.

5.2 בנוסף למענה המבוקש כמפורט לעיל, המשיבים רשאים להציג גם תפיסה ורעיונות קיימים ועתידיים בתחומים שונים, לרבות הטמעת טכנולוגיות חדשות/עתידיות בשירות.

6 אופן הגשת שאלות הבהרה ומענה לפנייה זו

6.1 איש קשר

איש/אשת הקשר מטעם המערך בנוגע לפנייה זו הוא/היא שרון בוסידן, טל' 052-8224475_ דוא"ל sharonbu@cyber.gov.il.

6.2 שאלות הבהרה

6.2.1 שאלות הבהרה בנוגע לפנייה זו יש להגיש בכתב בלבד, לא יאוחר מהמועד האחרון להמצאת שאלות הבהרה כמפורט בטבלה שבסעיף 2.6, לאיש/אשת הקשר בדוא"ל sharonbu@cyber.gov.il על הספק לוודא ששאלותיו הגיעו בשלמות לאשת הקשר, בטל' 052-8224475.

6.2.2 המערך שומר לעצמו את הזכות לנהל סבב אחד או יותר של שאלות הבהרה בהתאם לשיקול דעתו הבלעדי.

6.2.3 שאלות ההבהרה יוגשו בשפה העברית או האנגלית, במבנה הבא:

מספר הסעיף בפנייה	פירוט השאלה

6.2.4 מענה לשאלות ההבהרה יועבר על ידי המערך אל הפונים, וכן יפורסם באתר האינטרנט של מינהל הרכש הממשלתי ושל מערך הסייבר הלאומי בכתובות המפורטות בסעיף 2.5 לעיל. מובהר כי תשובות ההבהרה ינוסחו באופן שאינו חושף את זהות השואלים.

6.3 <u>הגשת מענה לפנייה</u>

6.3.1 המענה לפנייה יהיה **<u>בשפה העברית או האנגלית בלבד</u>**, בהיקף כולל של עד 50 עמודים המציגים את המענה. בנוסף על כך ניתן לצרף נספחים ומפרטים טכניים ללא הגבלת היקף

6.3.2 את המענה לבקשה לקבלת מידע יש להגיש בעותק דיגיטלי עד למועד האחרון להגשת מענים המפורט בטבלה שבסעיף 2.6 לעיל באמצעות דוא"ל rfi-michrazim@cyber.gov.il. ולוודא אישור קבלה בטל' ___052-8224475_____. בנושא הדוא"ל יירשם: "פניה מוקדמת לקבלת מידע (RFI) בנושא מערכת ניהול מודיעין איומי סייבר".

6.3.3 המערך רשאי לדחות את המועד האחרון להגשת מענה לפי שיקול דעתו הבלעדי. הודעה על כך תישלח לכל מי שהשיב לפנייה, וכן תפורסם באתר האינטרנט של מינהל הרכש הממשלתי ושל המערך בכתובות המפורטות בסעיף 2.5 לעיל. בהודעה יצוין המועד החדש להגשת המענים.

6.3.4 במסגרת המענה יפורטו פרטי המשיב:

מס"ד	המידע המבוקש	מענה
1	שם המשיב	
2	כתובת המשיב	
3	מס' טלפון	
5	שם איש קשר מטעם המשיב	
6	מס' טלפון של איש הקשר	
7	כתובת דואר אלקטרוני של איש הקשר	

7 בדיקת המענה

7.1 **המערך שומר לעצמו את הזכות לפנות, ככל שיידרש, למשיבים לפנייה זו בבקשה להשלמת מידע והבהרות, להצגת מצגות והדגמות, לביקור באתרי הלקוחות ובאתרים של מי שהשיב לפנייה זו, בהתאם לשיקול דעתו של המערך.**

7.2 במסגרת בחינת המענים, המערך שומר לעצמו את הזכות להזמין את כל מי שנענה לפניה, להציג את הפתרון המוצע על-ידו בפני צוות מקצועי מטעמו במיקום ובמועד שיקבע המערך.