שם הטופס: חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ספק חוץ

פרק ראשי: התקשרויות ורכישות	מספר הוראה: 7.8.2
פרק משני: פטור ממכרז	מספר טופס: ט. 7.8.2.1

אל: ועדת המכרזים

משרד:	משרד המשפטים
יחידה מזמינה:	אגף מערכות מידע
תאריך:	7/08/2022

הנדון: <u>חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ ספק חוץ</u>

הבקשה מסתמכת על תקנה ☒ 3(29) / ☐3(31) (סמן את התקנה המתאימה) לתקנות חובת מכרזים ועל הוראות תכ"ם מס' 7.8.1 ו-7.8.2.

תיאור מהות ההתקשרות (רקע ופירוט התכונות של הטובין/השירות/העבודה)
<u>חידוש רישוי שירות שנתי</u> עבור - **TrapX – Deception Grid** המותקן במשרד המשפטים בפריסה מלאה. הפתרון הינו מערך התקנים וירטואליים המשמש לגילוי, זיהוי, איתור וחקירה של מתקפות סייבר ונסיונות גישה לא מורשים למשאבי מערכות מידע.
במתקפת סייבר, אחד השלבים המתקדמים והקשים לאיתור הינה גישה למערכות על מנת לאתר ולאסוף מידע המעניין את התוקף על מנת לעשות בו שימוש למטרותיו הכלכליות\אידאולוגיות, או על מנת לגרום נזקים משמעותיים לתשתיות הממשלה. איתור אירוע של גישה בלתי מורשית לשרת אמיתי (או התקן אחר) הינו קשה מאוד עד בלתי אפשרי, וזאת בשל כמות הגישות המותרות למשאבים המרובים של הרשת ושל המערכות השונות והיכולת הדלה להבחין בין גישה לגיטימית לגישה אסורה שעשויה להיות חלק מתקיפה. על מנת לאתר תוקף פוטנציאלי, אחת השיטות הטובות והמוצלחות ביותר הינה 'מלכודת דבש'. חברת **Trapx** הינה חברה ישראלית שפיתחה את השיטה והביאה אותה לדרגות הגבוהות ביותר והכוללות יכולות יחודיות. המוצר שהחברה המציאה ורשמה עליו שני פטנטים המבדילים אותה מהמתחרים, מאפשר הטמעת רשת וירטואלית שלמה של 'מלכודות דבש' אשר מושכות את התוקף הפוטנציאלי. גישה למלכודת הינה בהכרח לא תקינה, זאת כיוון שמשתמשים רגילים ויישומים במערכות לא אמורים לפנות אליה כלל. על אף זאת, המערכת מאפשרת לזהות אם הגישה היתה כי הגורם "סתם עבר בסביבה" או שהפעילות אותה הוא מבצע הינה זדונית ולהתריע על הפעילות הזדונית ואף לנקוט פעולות אקטיביות לחסימת התוקף. מערכת **Deception Grid** של **TrapX**, הינה היחידה היודעת לייצר העתקים של מיגוון ממשקים למערכות הקיימות במשרד ובכך להסוות באופן מיטבי את המלכודת, לתפוס את התוקף בזמן אמת, ולהבין מהיכן התחבר, מה ניסה לבצע ומה חיפש.

המערכת נותנת מענה גם ל'איום הפנימי' הנובע מעובד ממורמר, סקרן או מדליף ומאפשר לתחקר ולהגיע לממצאים איכותיים.

ממשק הניהול הינו פשוט ונח לתפעול, שמבטיח שימושיות גבוהה וקלות תפעולית.

נציין גם שהמוצר מוטמע באחת מיחידות המשרד בהצלחה.

עוד חשוב לציין כי החברה הינה חברת ישראלית אשר הפיתוח שלה מבוצע כולו בארץ קיימת מאז 2012 וכי החברה הינה בעלת ניסיון רב בשוק, עם מאות לקוחות בארץ ובעולם.

יכולות המוצר נפרשות על רבדים רבים ובכך המערכת מאפשרת הטמעת אסטרטגיית הונאה מלאה בארגון:

רובד ראשון – אינטראקציית הונאה נמוכה (פתיונות), המאפשרים לספק תשובות, לשאלות שתוקף ישאל ברגע שיאחז באחת מתחנות הארגון, באמצעות מידע אשר יפוזר בתחנות הקצה, ללא התקנת סוכן, וישתול נתונים לפתות התוקף לתקשר עם המלכודות ברבדים הגבוהים יותר.

רובד שני – אינטראקציית הונאה בינונית (מלכודות אמולציה) כוללת אמולציות אשר יהוו מלכודות וידמו שלל נכסים אמיתיים בארגון (החל מווינדוס, יוניקס, ציוד תקשורת, **Scada, Swift, ATM, Voip** ועוד) ללא צורך במשאבי מחשוב, רישיונות או תחזוקה

רובד שלישי – אינטראקציית הונאה גבוהה (מערכת הפעלה מלאה) מאפשרת לארגון להמיר מערכות הפעלה אמיתיות לכדי מלכודת ללא תלות באפליקציה המותקנת על גבי מערכת ההפעלה.

רובד רביעי – דינמיות כך שמלכודות יחליפו כתובת ברוטציה כל אינטרוול על פי הגדרה וכמות כתובות שסופקו למלכודת

רובד חמישי – תקשורת מינימלית בין מלכודות על מנת לאפשר לתוקף לצוטט לרשת ולזהות המלכודות כמערכות חיות ופעילות

רובד שישי - אינטגרציה רשמית עם מערכות צד שלישי כך שהפתרון יתממשק למגוון מוצרי אבטחת מידע ארגוניים, החל מפתרון איסוף לוגים **SIEM,** ועד לפתרונות אקטיביים כגון **NAC, AV** על מנת להכיל אירוע ולחסום אותו אוטומטית בכלל הארגון

רובד שביעי – ניטור תקשורת יוצאת על מנת להצליב אירועים ולזהות פעילות חריגה ברשת ותקשורת אל מול שרתי **C&C**

לאור כל האמור לעיל, נבקש לאשר את חידוש הרישוי למערכת ה **DeceptionGrid** של חברת **TRAPX** כספק יחיד.

בנוסף, מעבר ליכולות אלו של המערכת, למערכת ישנן יכולות נוספות מהותיות הנותנות גם יכולת להתמודד עם **Ransomware** המתפשט בארגון ויכולות תחקור מתקדמות ללא צורך בסוכן בתחנות הקצה.

המערכת מוטמעת בהצלחה במשרד המשפטים בפריסה נרחבת, וייצרה ערך אמיתי באיתור חשד לנסיונות תקיפה ואירועי סייבר.

בנוסף המערכת מוטמעת בהצלחה הגנה וייצרה ערך אמיתי במשרדי ממשלה רבים ובהם משרד החוץ, כנסת, הנהלת בתי משפט, משרד לביטחון פנים וגופים ביטחוניים כגון יחידות צבא, רפא"ל ועוד.

שם הטופס: חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ספק חוץ

פרק ראשי: התקשרויות ורכישות	מספר הוראה: 7.8.2
פרק משני: פטור ממכרז	מספר טופס: ט. 7.8.2.1

שם הטופס: חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ספק חוץ

פרק ראשי: התקשרויות ורכישות	מספר הוראה: 7.8.2
פרק משני: פטור ממכרז	מספר טופס: ט. 7.8.2.1

האם קיים בנושא זה מכרז מרכזי של החשב הכללי או גורם ממשלתי מוסמך אחר? ☐ כן ☑ לא

סוג ההתקשרות: (סמן **X** במקום המתאים)

☒ טובין ☐ שירותים ☐ ביצוע עבודה

שם הספק:	**Wise**	
מספר הספק (ח.פ/ח.צ/ע.מ/מספר עמותה)	**513676452**	
ספק זה הנו:	☒ ספק יחיד	☐ ספק חוץ
אומדן / שווי ההתקשרות:	156,175$	
תקופת ההתקשרות:	שנה	

נימוקים כי הספק הוא ספק יחיד או כי הטובין הם טובי חוץ
(במקרה הצורך ניתן לצרף עמודים נוספים וכל מסמך רלוונטי נוסף)

נא להתייחס לסעיפים הבאים:

1. **האמצעים שבהם נערכו בדיקות לאיתור ספקים נוספים והכנת חוות דעת** כולל פירוט מקורות מידע ופעולות שננקטו (לדוגמה חיפוש באינטרנט, התכתבות עם ספקים, פגישה או שיחה עם ספקים וכדומה).

בבדיקה מול היצרן התקבל מסמך רשמי הממנה את חברת **WISE** כספק ומטמיע בלעדי של מוצריו בסקטור הממשלה.

2. **ממצאי הבדיקה** (אם ישנם ספקים נוספים בתחום ההתקשרות, יש לפרט את הסיבות לאי התאמתם לביצוע ההתקשרות עימם ואת הסיבות להיות הספק שלגביו נכתבה חוות הדעת ספק יחיד/ספק חוץ)

בבדיקה מול היצרן התקבל מסמך רשמי הממנה את חברת **WISE** כספק ומטמיע בלעדי של מוצריו בסקטור הממשלה.

3. נימוקים והערות נוספות

מדובר בחידוש רישוי למערכת קיימת המותקנת בפריסה משמעותית במשרד המשפטים, המערכת הינה היחידה העונה על כלל צרכי המשרד כמפורט לעיל.

לאור הנימוקים שמניתי לעיל אנו מבקשים לערוך ההתקשרות בהליך פטור ממכרז.

חוות דעתי זו ניתנת מתוקף היותי הסמכות המקצועית לנושא זה.

בכבוד רב,

שם בעל הסמכות המקצועית	תפקיד בעל הסמכות המקצועית	חתימה
מתן שני	מנהל אבטחת מידע	ששון סופרי ראש אגף בכיר טכנולוגיות מידע משרד המשפטים X מתן שני מנהל אבטחת מידע