

משרד הבריאות	משרד:
אגף טכנולוגיות דיגיטליות ודאטה	יחידה מזמינה:
15/09/2024	תאריך:

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

הבקשה מסתמכת על תקנה 3(29) / 3(31) (סמן את התקנה המתאימה) לתקנות חובת מכרזים ועל הוראות תכ"ם, "פטור מחובת המכרז", מס' 7.8.1 והוראת תכ"ם, "בחנית קיומם של ספקים ומיזמים", מס' 7.8.2.

תיאור מהות ההתקשרות (רקע ופירוט התכונות של הטובין/השירות/העבודה)
<p>המוצר נדרש לענות על התנאים הבאים:</p> <ul style="list-style-type: none"> • זיהוי והגנת סייבר באמצעות חסימה של כתובות IP על בסיס התנהגות ולא על חתימה מוכרת. • יכולות אוטומציה מלאה ללא התערבות אנושית. • זיהוי ותגובה של איומים בזמן אמת. • זיהוי וחסימה של תוקפים בווליום נמוך (Below The Radar). • זיהוי תקיפות שלא דווחו במנגנוני Threat חיצוניים על בסיס התנהגות. (Behaviour). • ניתוח מוקדם עם תובנות עסקיות שמבוססות על נתוני הסייבר. • חקירת אירועים ותקריות סייבר על ידי כלים מתקדמים להצגת פורנזיקה. • שיפור היכולת לנבא ולהתמודד עם איומים חדשים על ידי אלגוריתמים מתקדמים מבוססי בינה מלאכותית. • הזנה של מידע בעולם הפרוקסי על האקרים שתקפו בימים האחרונים כולל מידע לגבי סוגי הפרוקסי השונים והאפשרות לחסום. • הצגה והכנה של שלושה סוגי דוחות: <ol style="list-style-type: none"> 1. דוחות הנהלה ברזולוציה גבוהה הכוללים גרפים וסטטיסטיקות. 2. דוחות טכנולוגיים המפרטים במדויק את כל תהליך התקיפה. 3. דוחות פורנזיים כולל היסטוריה. <ul style="list-style-type: none"> ○ הדוחות מופקים בפורמט של PDF, HTML, XLS • קבלת שדרוגים ועדכונים בצורה אוטומטית לחלוטין. • תמיכה מלאה בשלושת היצרנים הגדולים – צ'ק פוינט, פורטיגיט, פאלו אלטו.

האם קיים בנושא זה מכרז מרכזי של החשב הכללי או גורם ממשלתי מוסמך אחר?

סוג ההתקשרות: (סמן X במקום המתאים)

ביצוע עבודה

שירותים

טובין

New Age Tech LTD	שם הספק:
513604116	מספר הספק (ח.פ.ח.צ.ע.מ/מספר עמותה)
<input type="checkbox"/> ספק חוץ	<input checked="" type="checkbox"/> ספק יחיד
7,160,000 ₪ כולל מע"מ	אומדן / שווי ההתקשרות:
3 שנים	תקופת ההתקשרות:

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).
בוצע חיפוש טכנולוגי באינטרנט, פנייה לספקים שונים.
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) לא קיים פתרון זהה לפתרון זה מבחינה טכנולוגית.
3. נימוקים והערות נוספות

תיאור קצר:

פתרון סייבר אוטומטי מלא וייחודי המשלב בינה מלאכותית ואלגוריתמיות מתקדמות לזיהוי, התרעה וחסיומה של איומים בזמן אמת, המבטיח הגנה מלאה לנכסים הדיגיטליים שלך ללא התערבות ידנית.

יתרונות ייחודיים:

- אלגוריתמיקה המבוססת על התנהגות התוקף ולא על חתימה מוכרת, יכולת משמעותית המאפשרת לזהות תוקפים לא מוכרים שניות מרגע התקיפה.
- אוטומציה מלאה: המערכת פועלת ללא התערבות אנושית, יכולת חשובה המקטינה טעויות ומגבירה בצורה מהותית את יעילותה.
- זיהוי בזמן אמת: המערכת מזהה ומגיבה לאיומים בזמן אמת, מה שמאפשר חסימה מיידית של כתובות זדוניות.
- זיהוי תקיפות בווליום מאוד נמוך (Below the radar) – האקרים מקצועיים ומנוסים לא תוקפים בצורה אגרסיבית אלא ילמדו על פני ימים ואף שבועות את רשת הלקוח, ימצאו את המשאבים שפתוחים שיאפשרו להם לכתוב ולחפש פגיעויות – כל אלה, מתחת לראדר בצורה שלא תאפשר לכלים הנוכחיים לזהות אותם. מערכת רבייב על ידי אלגוריתמיות מתקדמות תדע לזהות ולחסום.
- זיהוי תקיפות שלא דווחו באף מנגנון Threat חיצוני, זיהוי על פי התנהגות (Behaviour)
- בכל תהליך POC המערכת מצליחה להראות תקיפות שלא מזוהות על ידי כלי סייבר אחרים.

יכולות מתקדמות:

- יכולת BI (Business Intelligent) מערכת רבייב מאפשרת ניתוחים מתקדמים ותובנות עסקיות שמבוססות על נתוני הסייבר.
- פורנזיקה: המערכת כוללת כלים מתקדמים לחקירת אירועים ותקריות סייבר.
- בינה מלאכותית: אלגוריתמים מתקדמים לשיפור היכולת לנבא ולהתמודד עם איומים חדשים.

זיהוי מתקדם של עולם הפרוקסי:

- מערכת רבייב באמצעות הענן מחוברת לשרתי Threat intelligent חיצוניים, באמצעות API, המאפשרים לה לקבל מידע חיוני לגבי האקרים שתקפו בימים האחרונים כולל מידע לגבי סוגי פרוקסי שונים והאפשרות לחסום.
- לדוגמה
 - ניתן להגדיר חוק (IN and OUT) שמאפשר לחסום Proxy type TOR, זהו למעשה פרוקסי שהאקרים מתחברים ממנו בעולם של ה-DARK NET - מערכת רבייב תזהה את הגישות, תצליב את האינפורמציה מול הענן ותחסום במיידית בצורה אוטומטית.

דוחות:

מערכת רבייב מאפשרת לקבל שלושה סוגים של דוחות:

- דוחות הנהלה ברזולוציה גבוהה הכוללים גרפים וסטטיסטיקות
- דוחות טכנולוגים המפרטים במדויק את כל תהליך התקיפה
- דוחות פורנזיים כולל היסטוריה
 - הדוחות מופקים בפורמט של PDF, HTML, XLS

שדרוגים אוטומטיים:

מערכת רבייב באמצעות הענן שלה מאפשרת ללקוחות לקבל עדכונים בצורה אוטומטית לחלוטין. כל עדכון גרסה במצב PUBLIC יאפשר למשתמש לקבל עדכון שישנה גרסה חדשה בענן והוא יוכל להחליט מתי לשרג את הגרסה. כל התהליך הזה מאופשר בצורה מוצפנת עם ערכים חד חד ערכיים של הרישוי בסביבת הלקוח כולל VALIDATION מדוקדק כדי לוודא שהקבצים שמוכלים הם הקבצים הנכונים והאותנטיים.


תמיכה במערכות פירוולים:

מערכת רבייב תומכת בצורה מלאה בשלושת היצרנים הגדולים, צקפוינט, פורטיגיט ופאלו אלטו.

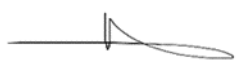
עלות הרישוי הינה 5 מילון שקל לא כולל מע"מ והינה ל-60 ארגוני בריאות שכולל 10 שעות הטמעה והדרכה לכל ארגון. עלות שעת עבודה הינה 360 שקל (נדרש לרכוש בחבילות של 10 שעות).

חוות דעתי זו ניתנת מתוקף היותי הסמכות המקצועית לנושא זה.

בכבוד רב,

	CTO משרד הבריאות	ראובן אליהו
חתימה	תפקיד בעל הסמכות המקצועית	שם בעל הסמכות המקצועית

בהתאם לסעיף 2.6.4.3. להוראת תכ"מ 7.6.3 (מהדורה 08) שכותרתה "בחינת קיומם של ספקים ומיזמים" והואיל ובעל הסמכות המקצועית אינו עובד מדינה, הנני מאשר בחתימתי את האמור בחוות הדעת.

	מוסמכת רכש	אמויאל דורין
חתימה	תפקיד בעל הסמכות המקצועית	שם בעל הסמכות המקצועית