<u>הנדון: הודעה על כוונה להתקשר עם ספק יחיד/חוץ לרכישת טובין, עבודות ושירותים</u>

תאריך פרסום ההודעה: 15/12/2021

בהתאם לתקנה 3(18) לתקנות חוק חובת המכרזים (התקשרויות של מוסד להשכלה גבוהה), התש"ע-2010,

בכוונת האוניברסיטה להתקשר עם ספק יחיד: חברת crowdstrike דרך המפיצה חברת CMS

מהות ההתקשרות: לרכישת פתרון הגנה מתקדם לתחנות קצה כולל שירות ספק

תקופת ההתקשרות: חמש שנים (שלוש שנים + אופציה אחת להארכה לשנתיים נוספות)

אדם הסבור כי קיים ספק ישראלי נוסף המסוגל לבצע את ההתקשרות רשאי לפנות ולהודיע על כך

בתוך 10 ימים ממועד פרסום ההודעה ועד ליום 28.12.2021 בשעה 17:00

פניות כאמור יש להעביר בכתב בלבד, באמצעות כתובת הדוא"ל: michraz-haspaka@tau.ac.il

או באמצעות הפקס: 03-6407255

<u>לכל פניה יש לצרף</u>:

1. שם, מען ופרטי התקשרות של הפונה.
2. שם, מען ופרטי התקשרות של הספק המוצע.
3. סטטוס ההתאגדות של הספק המוצע.
4. פירוט בדבר ניסיונו של הספק המוצע ונשוא ההתקשרות.

פנייה אשר תתקבל במען האוניברסיטה לאחר המועד האחרון ו/או פנייה אשר תהיה חסרה איזה מהפרטים הנקובים לעיל, לא תיבחן על ידי ועדת המכרזים.

מצ"ב חוות דעת הגורם המקצועי.

הנדון: **חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד**

אנו מבקשים לאשר התקשרות עם ספק יחיד בהתבסס על תקנה 3 (18) לתקנות חוק חובת המכרזים (התקשרויות של מוסד להשכלה גבוהה), התש"ע - 2010.

מהות ההתקשרות: רכישת פתרון הגנה מתקדם לתחנות קצה כולל שירות ספק.

שם היצרן: crowdstrike
שם המפיץ: CMS
תקופת ההתקשרות: חמש שנים (שלוש שנים + אופציה להארכה לעוד שנתיים)

הנימוקים לספק יחיד:

הפתרון של CrowdStrike הינו פתרון מודרני לחלוטין שאינו נשען על מנגנונים ישנים כגון חתימות אלא משתמש במנגנונים חדשניים כגון Machine learning ו Artificial Intelligent שמאפשרים:
סובן קל משקל עם קרוב לאפס חתימת ביצועים על התחנה, ללא צורך באתחול בשום שלב לאורח חיי המוצר, זיהוי מהיר של התקפות מתקדמות ולא פחות חשוב, False Positive נמוך ביותר שמונע רעש מיותר בצוות אבטחת המידע מצומצם בגודלו.

להלן פירוט כלל היכולות הטכנולוגיים והתפעוליים הנדרשים לאוניברסיטה מהמוצר לצורך רכישת פתרון הגנה מתקדם ואשר מתקיימים במצטבר רק בcrowdstrike:

1. מערכת שאיננה דורשת אתחול של מערכות בעת ההטמעה ולאחריה (כולל שדרוגי גירסה\עדכונים ועוד).
2. פתרון שמבוסס על תשתית ענן מודרנית, גמישה ומהירה (בניגוד למוצרי On-Prem שמותקנים על גבי תשתית ענן).
3. כמות נמוכה ומוכחת של false positive.
4. מערכת מנוהלת באופן מלא על ידי ממשק ניהול יחיד, כולל כל הפיצ'רים והיכולות נוספות.
5. חתימה אפסית על תחנות הקצה – מתבקש פחות מ 50Mb שטח דיסק ופחות מחצי אחוז מהזיכרון וכח העיבוד.
6. שירות מנוהל מלא **על ידי היצרן** – הכולל הטמעת מדיניות, הגדרות, טיוב המערכת, בניית תסריטי תגובה, ניהול אירועים והתראות, Threat Hunting אנושי, באופן שוטף 7-24, ניהול תגובה מלאה בזמן אירוע, שירות "כפפות לבנות" ללא כל התערבות של הלקוח.
7. יכולת להתחבר מרחוק לכל תחנה ולהריץ עליה סקריפטים, בדיקות וניהול מרוחק בשפה אחידה, ללא תלות במערכת ההפעלה.
8. יכולת תחקור מלאה של אירועים על תחנות קצה, **לרבות Threat Hunting מלא**, גם אם התחנות מושבתות או לא נגישות לאינטרנט.
9. כלל התחקור יתבצע בענן ללא שימוש במשאבי התחנה כלל (ללא כל הפרעה או שיבוש המשך עבודה של המשתמשים).
10. יכולת חיפוש מידע (Hashes / Files / Domains / etc...) בבלוקים גדולים (חיפוש של 1000 רשומות בבת אחת למשל).
11. פתרון EDR שמגובה במודיעין סייבר של היצרן עצמו, לטובת אינטגרציה מלאה ושילוב מידע מודיעיני רלוונטי לתוך המערכת.
12. שירות Threat Hunting **אנושי** על ידי היצרן עצמו.
13. מוצר שהוא פלטפורמה אחת, ניהול אחד, ליכולות נוספות שייתכן ויוספו בעתיד, לרבות: FIM (File Integrity Manager, Cloud Workload Protection, Identity Protection (Zero Trust) ועוד.

הנימוקים לספק יחיד/חוץ:

- עבודה מול חברת CMS מפיץ רשמי ויחיד של חברת Crowdstrike-.

גל יצחק
מנהלת יחידת אבטחת מידע וסייבר, CISO, אוניברסיטת תל אביב
משרד: 03-6408944 | פקס: 03-6405158
דוא"ל: galyit@tauex.tau.ac.il | אתר: http://www.tau.ac.il