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

תאריך פרסום ההודעה: 09/10/2024

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

בכוונת האוניברסיטה להתקשר עם ספק יחיד: crowdstrike באמצעות המפיץ סי.אמ.אס. קומפיוסנטר בע"מ

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

תקופת ההתקשרות: שש שנים (שלוש שנים + אופציה להארכה לשלוש שנים 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 30.10.2024 בשעה 10:00

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.

9.10.2024

לכבוד

וועדת המכרזים – אוניברסיטת תל אביב

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: סי.אמ.אס. קומפיוסנטר בע"מ

תקופת ההתקשרות: שש שנים (שלוש שנים + אופציה להארכה לשלוש שנים נוספות)

הארכה משוערת של שווי ההתקשרות: כשמונה מיליון שקלים

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:

סוכן 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. ניטור מלא של כל הזהויות, הקונפיגורציות, החולשות, ההגדרות השגויות - עם הסבר פשוט מה הסיכון, איך לתקן ואיזה זהויות חשופות אליו.

5. מיפוי של כל הזהויות בארגון ומתן "Insights" רבים ומגוונים על הזהויות, לרבות משתמשים פריווילגים, סיסמאות חשופות, משתמשים שלא מחוברים מתחנה בדומיין, משתמשים רגילים עם הרשאות גבוהות מסוכנות, משתמשים לא פעילים, מיפוי של Service Account ועוד המון המון מידע חשוב לתפעול וניטור של סביבות ה AD.
6. מערכת מנוהלת באופן מלא על ידי ממשק ניהול יחיד, כולל כל הפיצ׳רים והיכולות הנוספות.
7. חתימה אפסית על תחנות הקצה – מתבקש פחות מ 50Mb שטח דיסק ופחות מחצי אחוז מהזיכרון וכח העיבוד.
8. שירות מנוהל מלא **<u>על ידי היצרן</u>** – 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.
9. יכולת להתחבר מרחוק לכל תחנה ולהריץ עליה סקריפטים, בדיקות וניהול מרוחק בשפה אחידה, ללא תלות במערכת ההפעלה.
10. יכולת תחקור מלאה של אירועים על תחנות קצה, **לרבות Threat Hunting מלא**, גם אם התחנות מושבתות או לא נגישות לאינטרנט.
11. כלל התחקור יתבצע בענן ללא שימוש במשאבי התחנה כלל (ללא כל הפרעה או שיבוש המשך עבודה של המשתמשים).
12. יכולת חיפוש מידע (Hashes / Files / Domains / etc...) בבלוקים גדולים (חיפוש של 1000 רשומות בבת אחת למשל).
13. פתרון EDR שמגובה במודיעין סייבר של היצרן עצמו, לטובת אינטגרציה מלאה ושילוב מידע מודיעיני רלוונטי לתוך המערכת.
14. שירות Threat Hunting **<u>אנושי</u>** על ידי היצרן עצמו. השירות רשם מספר פטנטים ייחודים בעולמות ה Threat Hunting.
15. מוצר שהוא פלטפורמה אחת, ניהול אחד, ליכולות נוספות שייתכן ויוספו בעתיד, לרבות: FIM (File Integrity Manager, Device Control, Vulnerabilities Manage (OS and 3rd Parties Apps), Cloud Workload Protection, Identity Protection (Zero Trust) ועוד.

בברכה,

גל יצחק

מנהלת תחום אבטחת מידע וסייבר, CISO , אגף למחשוב וטכנולוגיות מידע.

אוניברסיטת תל אביב
בעקבות הדא נודע