

התקשרויות ורכישות	פרק ראשי:
התקשרות בפטור ממכרז	פרק משני:
7.6.3	הוראה מקשרת:
7.6.3.1.ט	מספר טופס:
01	מהדורה:

משרד האוצר
אגף החשב הכללי
תכ"ם - התקשרויות ורכישות



אל: ועדת המכרזים

משרד הבריאות	משרד:
אגף טכנולוגיות דיגיטליות ודאטה	יחידה מזמינה:
01/07/2024	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, "בחנינת קיומם של ספקים ומיזמים", מס' 7.8.2.

תיאור מהות ההתקשרות (רקע ופירוט התכונות של הטובין/השירות/העבודה)
<p>המוצר נדרש לענות על כל התנאים הבאים:</p> <ul style="list-style-type: none"> • איתור ופתרון אוטומטי לבעיות ברציפות התפקודית (קרי תשתיות ה-IT והתקשורת) של ארגוני הבריאות הנגרמות ממוצרי אבטחת המידע בארגון – זיהוי חסימות תקשורת ו-outage, latency הנגרמים כתוצאה מהפיירוול, EDR, WAF, SASE, MDM. על הפתרון לאפשר לפתור את הבעיה ללא צורך של המשתמש להיכנס למערכת ההגנה וממנה לבצע את השינוי בצורה ידנית. • הצפת "חורי אבטחה" אשר ניתן לסגור אותם בשימוש במוצרי אבטחת המידע הקיימים בארגוני הבריאות וסגירה של חורי אבטחה אלו בצורה אוטומטית באופן ישיר מול מערכות ההגנה (בלי צורך במערכות צד שלישי), תוך כדי מניעה מפגיעה ברציפות התפקודית. על המוצר להציף את הפערים על בסיס ניתוח של צרכי ארגוני הבריאות הספציפיים על בסיס ניתוח שוטף – לדוגמא, חולשות, אפליקציות, טכנולוגיות, איומים ומתקפות • חיבור למערכות ההגנה במקביל וניתוח הגדרות עומק – התחברות וניתוח קונפיגורציות עומק, טלמטריות מערכת ולוגים של כלל המוצרים הבאים: Check Point, Palo Alto Networks, Fortinet, Cisco, F5, CrowdStrike, Microsoft Defender, Microsoft Intune, Microsoft SCCM, BigFix, Cloudflare, Claroty, Prisma, Cynet, Radware, Harmony, Armis, Ticura, Tenable, Medigate, Qualys, Rapid7, TrendMicro Apex, TrendMicro Vision One, SentinelOne, Netskope, AWS WAF, Azure WAF. בכל אחד מהמוצרים הללו, נדרשת ניתוח עומק של בעיות בקונפיגורציית כלל הטכנולוגיות. לדוגמא, בפירוול נדרש ניתוח עומק של קונפיגורציות המוצרים הבאים: Anti-Malware, Anti-Phishing, Intrusion Prevention, Anti-Spyware, CDR, Anti-Spyware, Sandbox File Inspection • בפורטינט לדוגמא, התמיכה הנדרשת מבוססת policy based, profile based של Firewall standalone, cluster, FortiAnalyzer, FortiManager, VDOM, ADOM, both on prem and cloud deployment עבור כל אחד מטכנולוגיות ההגנה – threat protection, intrusion prevention, malware protection, application control, antivirus • מודל LLM המאפשר שאילת שאלות עומק על סטטוס קונפיגורציות העומק של מוצרי ההגנה שצוינו לעיל, בדגש על סטטוס ההגנה, וחיבור לממצאי פערי אבטחה הניתנים לסגירה באופן אוטומטי • איתור תקלות בקונפיגורציות הגנת הסייבר שהובילו לניסיונות תקיפה לעבור את מוצרי האבטחה הקיימים (ובדגש על הצגת הפער במוצרי ההגנה המוטמעים בארגון) וסגירה

פרק ראשי:	התקשרויות ורכישות
פרק משני:	התקשרות בפטור ממכרז
הוראה מקשרת:	7.6.3
מספר טופס:	ט.7.6.3.1
מהדורה:	01

משרד האוצר
אגף החשב הכללי
תכ"ם – התקשרויות ורכישות



- אוטומטית של חורי אבטחה אלו במוצרי ההגנה עצמם. ניתוח אחר של השינויים לטובת הוכחת וידוא כי אין פגיעה ברציפות התפקודית של ארגוני הבריאות.
- יכולת להטמיע את המוצר בתשתיות ארגוני הבריאות (On-Prem) בטכנולוגיית Kubernetes on-prem תוך כדי קבלת עדכונים אוטומטיים
 - יכולת תמיכה בהתקנת המוצר בטכנולוגיות הבאות – Nutanix, VMware vSphere (ESXi), AWS EC2, AWS EKS, AZURE AKS, GCP – COMPUTE ENGINE, ORACLE VM VIRTUAL BOX, CITRIX HYPERVISOR
 - הצפת איכות השימוש במוצרי אבטחת המידע הקיימים – על הפתרון לחשוף ציון הגנתי ולאפשר למשתמש להבין כיצד ניתן לשפר את הציון (ולבצע את השיפור מתוך המערכת עצמה בצורה אוטומטית עם וידוא אחר כי השינוי לא פגע במערכות ארגוני הבריאות)
 - הנגשת תמונת על המציגה את איכות השימוש במוצרי אבטחת המידע הקיימים בראי כלל ארגוני הבריאות - בחלוקה למוצרי ההגנה השונים (Firewall, SASE, WAF, EDR,) (EPP, VA, VM, MDM, CAASM)
 - וידוא כי כל עדכון או שינוי הגדרה במוצרי אבטחת המידע לא פוגע ברציפות התפקודית של ארגוני הבריאות והוכחה על בסיס ניתוח טלמטריות מערכת כמו ניתוח זיכרון ולוגים

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:	ורטי סקיריטי בע"מ
מספר הספק (ח.פ.ח.צ.ע.מ/מספר עמותה)	516435153
ספק זה הנו:	<input checked="" type="checkbox"/> ספק יחיד <input type="checkbox"/> ספק חוץ
אומדן / שווי ההתקשרות:	4,000,000 כולל מע"מ
תקופת ההתקשרות:	שנתיים

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 שנקטו (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

התקשרויות ורכישות	פרק ראשי:
התקשרות בפטור ממכרז	פרק משני:
7.6.3	הוראה מקשרת:
7.6.3.1.ט	מספר טופס:
01	מהדורה:

משרד האוצר
אגף החשב הכללי
תכ"ם – התקשרויות ורכישות



ורטי הינה מערכת ייחודית אשר מאפשרת העלאת רמת האבטחה הארגונית על ידי הגברת השימוש במוצרי אבטחת המידע (בכלל טכנולוגיות ההגנה הרלוונטיות - מ-, FW, WAF, SASE, MDM, VA, VM, EDR) בהתאם לצרכי ארגוני הבריאות (על בסיס ניתוח עומק של מתקפות, חולשות, טכנולוגיות ופרוטוקולי תקשורת) על מנת להוריד את הסבירות להתקפת סייבר מוצלחת, תוך כדי שמירה על הרציפות התפקודית של התהליכים הארגונים והעסקיים בחברה. כיום, מוצרי האבטחה הינם מורכבים ודינאמיים, ואחד הסיבות המרכזיות למתקפות סייבר בארגונים הינה המורכבות לניהול מוצרי האבטחה בשגרה. ורטי, כמערכת, יודעת לאתר פערי אבטחה כתוצאה משימוש לא מקסימלי במוצרי האבטחה עצמם, וכן לאתר בעיות תקשורת ותשתיות הנוצרות כתוצאה משימוש לקוי במוצרי האבטחה בתשתיות ארגוני הבריאות.

לורטי מספר היבטים של ייחודיות בשוק – ניתוח העומק של הקונפיגורציות של מוצרים רבים, מנועי אינטליגנציה מלאכותית שנכתבו לראשונה בורטי לבעיות מותאמות לצרכים של ארגוני הבריאות, היכולת לבצע את שינויי הקונפיגורציה הנדרשים ברמת הכירורגיה הנדרשת תוך כדי וידוא שאין פגיעה ברציפות התפקודית. מנועי האינטליגנציה המלאכותית של ורטי יודעים לאתר בצורה מדויקת פגיעה בתשתיות ארגוניות והצפת "חורי אבטחה" הקיימים בארגון ואותם נדרש לסגור בהתבסס על מוצרי ההגנה הקיימים ובמקביל לוודא כי השימוש המקסימאלי במוצרי אבטחת המידע לא פוגע בארגון.

מטבען, תשתיות התקשורת וה-IT בארגוני הבריאות מורכבות. ישנו אתגר משמעותי ביכולת לאבטח את ארגוני הבריאות תוך כדי מניעת בעיות תקשורת ברכיבים הרפואיים השונים. ורטי יודעת לגשר על פער זה על ידי למידת התנהגות התקשורת בארגוני הבריאות וידוא שהעלאת רמת האבטחה הארגונית לא מייצרת פגישה בתשתיות הקריטיות.

ורטי ייחודית בשוק בהיבטים הבאים:

1. חיבור וניתוח עומק של קונפיגורציות, לוגים וטלמטריות של מערכות ההגנה השונות בארגוני הבריאות – ובפרט, כלל המוצרים הבאים: Check Point, Palo Alto, Palo Alto Networks, Fortinet, Cisco, F5, CrowdStrike, Microsoft Defender, Microsoft Intune, Ticura, Microsoft SCCM, BigFix, Cloudflare, Claroty, Prisma, Cynet, Medigate, Armis, Radware, Harmony, Tenable, Qualys, Rapid7, TrendMicro Apex, TrendMicro Vision One, SentinelOne, Netskope, AWS WAF, Azure WAF.

בכל אחד מהמוצרים הללו, נדרשת ניתוח עומק של בעיות בקונפיגורציית כלל הטכנולוגיות. לדוגמא, בפירוול נדרש ניתוח עומק של קונפיגורציות המוצרים הבאים: Anti-Malware, Anti-Phishing, Intrusion Prevention, Anti-Spyware, CDR, Anti-Spyware, Sandbox File Inspection

בפורטינט לדוגמא, התמיכה הנדרשת מבוססת policy based, profile based Firewall standalone, cluster, FortiAnalyzer, FortiManager, VDOM, ADOM, both on prem and cloud deployment עבור כל אחד מטכנולוגיות ההגנה – threat protection, intrusion prevention, malware protection, application control, antivirus

התקשרויות ורכישות	פרק ראשי:
התקשרות בפטור ממכרז	פרק משני:
7.6.3	הוראה מקשרת:
7.6.3.1.ט	מספר טופס:
01	מהדורה:


משרד האוצר
אגף החשב הכללי
תכ"ם – התקשרויות ורכישות



2. אינטליגנציה מלאכותית שמטרתה לוודא כי כל שינוי הגנתי בארגון לא ייצור בעיה ברציפות התפקודית של הארגון (קרי בעיות IT ותקשורת שנגרמות כתוצאה משימוש במוצרי האבטחה). לא קיים יצרן אשר מרכז הערך שלו הוא וידוא כי המוצרים הקיימים בארגון לא מייצרים בעיה ברציפות התפקודית עם הדגש על הגנת הסייבר ומודלי ההגנה הרבים השונים.
3. אינטליגנציה מלאכותית שיודעת לזהות בעיות IT ותקשורת שנגרמות כתוצאה משימוש במוצרי האבטחה ותיקונים באופן אוטומטי, זאת על בסיס שילוב בין ניתוח הטופולוגיה הרשתית הספציפית ברמת ה-ASSET לשכבת ה-THREAT PREVENTION.
4. התאמת קונפיגורציות המוצרים לצרכים המשתנים של ארגוני הבריאות, על בסיס ניתוח צרכים ומאפיינים (ניתוח טכנולוגיות, אפליקציות, חולשות, איומים ומתקפות)
5. היכולת לבצע את השינוי מתוך וריטי וללא צורך להיכנס למוצרי האבטחה עצמם ולאחר היכן לבצע את השינוי הנדרש, ללא מערכות צד שלישי, תוך כדי וידוא ששינויים אלה לא יגרמו לבעיות במוצרי ההגנה.
6. הטמעת המוצר ב-On Prem (קרי תשתיות ארגוני הבריאות) תוך כדי שימוש בטכנולוגיית Kubernetes on prem והיכולת לשמור את כלל המידע הרגיש שנאסף בתוך רשת הלקוח וללא צורך לשלוח אותו אל מחוץ לרשת לאנליזה מתקדמת (יצרנים דורשים חיבור ל-Cloud על מנת לאסוף ולנתח מידע, וריטי מבצעת את הניתוח בתוך המערכת ללא צורך בשיתוף מידע רגיש החוצה). בנוסף, יכולת תמיכה בהתקנת המוצר בכלל הטכנולוגיות הנ"ל ייחודית גם – AKS, GCP – COMPUTE ENGINE, ORACLE VM VIRTUAL BOX, CITRIX HYPERVISOR, Nutanix, VMware vSphere (ESXi), AWS EC2, AWS EKS, AZURE
7. מודל LLM מתקדם המאפשר לארגוני הבריאות לשאול שאלות עומק על סטטוס הקונפיגורציה בכלל מערך האבטחה, ולחבר זאת לפערים קיימים בשטח הניתנים לפתרון דרך המערכת באופן אוטומטי.

הערות

1. התקשרות הינה עבור רישוי ל-60 ארגוני בריאות בישראל.
2. מחיר שעת עבודה הינה בעלות \$135 לפי מע"מ
3. חבילות שירות

התקשרויות ורכישות	פרק ראשי:	משרד האוצר אגף החשב הכללי תכ"ם – התקשרויות ורכישות	
התקשרות בפטור ממכרז	פרק משני:		
7.6.3	הוראה מקשרת:		
7.6.3.1.ט	מספר טופס:		
01	מהדורה:		

חבילת T1 כוללת:

- אינטגרציה וקונפיגורציה באופן שוטף
- תחזוקה ומענה לסוגיות שימושיות במערכת
- הדרכות שוטפות למשתמשי המערכת

חבילת T2 כוללת:

- מפגשים קבועים עם מומחה וריטי למעבר על המערכת - ניתוח משותף של פערי אבטחה שנמ
- ייצור דו"ח על בסיס חצי שנתי של סטטוס ההגנה בארגון, לרבות פערי אבטחה וממצאי המערכ
- רמידיאציה בשיתוף עם מומחה וריטי
- כל שירותי חבילת T1

חבילת T3 כוללת:

- הכנה והנגשת דו"חות על בסיס חודשי של סטטוס שיפור מערך האבטחה בראי המערכת על ב
- – כמות מתקפות שנמנעו, חולשות שהסיכון בהן ירד
- מתן וניתוח התרעות על בסיס שוטף ממצאים דחופים הדורשים רמידיאציה
- אנליזת מומחה וריטי למקרי פגיעה ברציפות התפקודית של מוצרי ההגנה
- ייעוץ מקצועי בנושאי מערך האבטחה וטיוב מערכות ההגנה בהתאם לממצאים השוטפים
- כל שירותי חבילת T2

חבילת פרמיום – שירות מנוהל:

- שירות מנוהל – מומחה וריטי אשר מנהל באופן שוטף את השימוש במערכת במקום הלקוח
- ניתוח מודל MITRE אל מול קונפיגורציות מוצרי ההגנה
- הקשחת אינדיקטורים של התקפה בצורה אוטומטית
- מודל LLM המאפשר שאילת שאלות רחבות על קונפיגורציות

4. עלות חבילות השירות

- חבילת T1 – 4000\$ לארגון (כולל 32 שעות עבודה)
- חבילת T2 – 6000\$ לארגון (כולל 50 שעות עבודה)
- חבילת T3 – 11000\$ לארגון (כולל 100 שעות עבודה)
- חבילת פרמיום – 10000\$ לארגון לשנה

חוות דעתי זו ניתנת מתוקף היותי הסמכות המקצועית לנושא זה.


בכבוד רב,



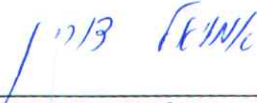
	CTO משרד הבריאות	ראובן אליהו
חתימה	תפקיד בעל הסמכות המקצועית	שם בעל הסמכות המקצועית

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.

טופס:

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

התקשרויות ורכישות	פרק ראשי:	משרד האוצר אגף החשב הכללי תכ"ם - התקשרויות ורכישות	 החשב הכללי
התקשרות בפטור ממכרז	פרק משני:		
7.6.3	הוראה מקשרת:		
7.6.3.1.ט	מספר טופס:		
01	מהדורה:		

		
חתימה	תפקיד בעל הסמכות המקצועית	שם בעל הסמכות המקצועית

עמוד 6 מתוך 6

מנהל מינהל הרכש הממשלתי

לפניות ושאלות: takam@mof.gov.il

לקבלת עדכונים במערכת: לחץ כאן

בתוקף מיום: 01.01.2010

שם המאשר: ליאור אגאי

אתר הוראות תכ"ם: קישור לאתר