

תאריך: 26.7.2026

הנדון: מכרז פומבי מספר 6/2026 לאספקה, התקנה, הטמעה, תמיכה ותחזוקה של מערכות IPS עבור מערך

הדיגיטל – קובץ הבהרות מס' 2

1. בהתאם לסמכותה על פי מסמכי המכרז, לרבות סעיף 7.2 בפרק א' למסמכי המכרז, מתכבדת בזאת ועדת המכרזים ליתן הודעה למציעים, להלן **בנספח א'**, בדבר שאלות שהועברו אל הוועדה בכתב ותשובות ועדת המכרזים או מי מטעמה, וכן הבהרות יזומות.
2. כל התשובות, ההבהרות והשינויים בהודעה זו יחשבו לחלק בלתי נפרד ממסמכי המכרז.
3. אלא אם נאמר אחרת, לכל המונחים האמורים בהודעה זו תהיה המשמעות שנקבעה להם במסמכי המכרז.
4. אין להסתמך על כל הסבר או פירוש שניתן בעל פה או בכתב או בכל דרך אחרת על ידי מי מטעם ועדת המכרזים או על ידי כל גורם אחר, ככל שניתן, בכל פורום או צורה שהיא. השינויים היחידים מהאמור במסמכי המכרז וכן כל הפירושים וההבהרות להם, הינם כמפורט בכתב זה בלבד, ובמכתבי הבהרות נוספים שיצאו מטעם ועדת המכרזים, ככל שיצאו.
5. אין בהודעה זו כדי לשנות מהוראות מסמכי המכרז, אלא ככל ששינוי כזה נעשה במפורש.

בכבוד רב,

מיטל לוגסי

מ"מ מנהלת אגף הרכש

מנהלת קטגוריית רכש טכנולוגי



נספח א' – קובץ הבהרות מספר 2

מס' שאלה	שם פרק/נספח	מספר סעיף	השאלה	מענה ועדת המכרזים
1.	פרק א/ פרק ג	סעיף 4.3.1.6 (פרק א') סעיף 4 (פרק ג')	נדרשת שרידות Active/Active או Active/Standby עם Failover של פחות משנייה. נבקש לאשר כי בעת מעבר Failover בין חיישנים ב-HA Pair, טבלת ה-State Table מסתנכרנת באופן מלא (Stateful-Synchronization), כך ש-L7 sessions קיימות העוברות ל-IPS החלופי אינן נקטעות ואינן עוקפות את מנוע הסינון והחסימה Inline.	לא נדרש סנכרון בזמן אמת
2.	פרק ב	הצעת המחיר	לאור השינויים והתנודות המסיביות בעלויות בשוק החומרה, נבקש להציע אחוז הנחה קבוע (מתוך מחירון היצרן/ספק) שיחול על כל רכש עתידי של מכונות	אין שינוי ממסמכי המכרז
3.	פרק ב	הצעת המחיר	מאחר שעלויות כוח האדם הן בשקלים, נבקש לוודא כי כלל שירותי ההקמה, ההתקנה, ההגדרה והסבת המערכת יתומחרו בשקלים חדשים (ש"ח) בלבד	אין שינוי ממסמכי המכרז
4.	פרק ג	1	נדרשת "יכולת בניית חוקים באופן עצמאי ולא רק הכנסת מזהים." נבקש להבהיר: האם המערכת נדרשת לתמוך בכתיבת חוקים מותאמים אישית (Custom Signatures) המבוססים על תחביר פתוח סטנדרטי כגון Snort/Suricata rules, כולל ביטויים רגולריים-PCRE על גבי ה-Payload, והאם חוקים אלו מורצים בהאצת חומרה בקו התעבורה ללא פגיעה ב-Throughput?	כן
5.	פרק גונספח 6	סעיף 1 ונספח 6	מצוינת היכולת ל-Auto-Signature Generation. נבקש להבהיר: האם המערכת נדרשת להפיק בעצמה חתימות ומזהים חדשים בזמן אמת באופן אוטומטי מתוך ניתוח קבצים ואיומי Zero-Day, ולהפיץ את החתימות שנלמדו ישירות לכלל חיישני ה-IPS בארגון לשם חסימה Inline ללא צורך בהתערבות ידנית?	הדרישה היא שהמערכת תייצר חתימות על בסיס תעבורה זדונית שעוברת בחיישני ה-IPS

ה-IPS אמור להגיב לאירועים שמתקבלים ממערכות Soar, הוא לא אמור להפעיל רכיבי צד ג ע"י שליחת אירועי SOAR	נדרשת "תגובה אוטומטית מבוססת טריגרים (SOAR-like)". נבקש להבהיר: האם המערכת מאפשרת להגדיר מנוע חוקי תגובה אוטומטי ב-Manager המאפשר הרצת סקריפטים חיצוניים (כגון /PowerShell/ Python) בעקבות התראות או חריגות סף, תוך העברת פרמטרים דינמיים מהאירוע (כדוגמת Attack, Source IP, Hash, Name), לצורך ביצוע פעולות אכיפה במערכות צד שלישי?	1	פרק ג	6.
הדרישה היא שהמערכת תייצר חתימות על בסיס תעבורה זדונית שעוברת בחיישני ה IPS	נדרשת "הפקת IOC מתוך תקיפה בזמן אמת" וזיהוי פרוטוקולים. נבקש להבהיר: האם החיישן נדרש לבצע חילוץ קבצים מלא (File Extraction), מתוך תעבורת ftp, smtp, http/s, smb, ברמת החיישן ולחשב עבורם MD5 /SHA256 באופן עצמאי, והאם ניתן לייצא נתונים אלו בזמן אמת ל-Syslog/SIEM בפורמט Cef/Json?	1	פרק ג	7.
עדכון מזהים נדרש להיות מבוצע בשוטף, להשפיע בזמן אמת (near real time), ללא פגיעה בשירות או אתחול הרכיבים כולל רכיבי הניהול	נדרש "API נרחב לתפעול (הוספה/עדכון/הסרה של מזהים וחוקים), השפעה ב-Near Real Time". נבקש להבהיר: האם קריאות ה-API להוספת או עדכון מזהים מיושמות באופן ישיר בזיכרון (In-Memory Injection) ללא צורך בביצוע Re-compile, הפצת Policy מלאה או אתחול שירותים ב-IPS?	2	פרק ג	8.
הדרישה היא שמזהים של המערך לא ישותפו עם לקוחות אחרים ולא יעשה בהם שום שימוש אחר ע"י היצרן	מופיעה הדרישה: "שמירת מזהים לוקאלית בלבד - ללא שליחה לענן או אפשרות לביטול שימוש". נבקש לאשר כי כלל בסיס הנתונים של המזהים, החוקים והלוגים נשמר ומעובד אך ורק בתוך שרתי הניהול והחיישנים המקומיים של המזמין (On-Premises), וכי המערכת מסוגלת לתפקד באופן מלא בסביבה מבודדת (Air-Gapped Network) אינטרנט ומנותקת	2	פרק ג	9.
אכן זאת הדרישה. ניתן להעביר מזהים בצורה מקובצת (BULK), נדרש שהעברת המזהים לא תפגע בביצועים	נדרשת "תמיכה בכמות גבוהה של מזהים עצמאיים (עד חצי מיליון)". נבקש להבהיר: האם התמיכה ב-500,000 מזהים מיושמת ברמת ה-Sensors ב-Inline ללא ירידה בביצועי העיבוד של הרשת, והאם ניתן לטעון מזהים אלו בצורה מקובצת ((Bulk Import/API בזמן אמת?	2	פרק ג	10.



11.	פרק ג	4	נדרשת תמיכה בקצבי תעבורה של 5 Gbps, 10Gbps, 20Gbps ו-40Gbps. נבקש לאשר כי דרישת ה-Throughput מתייחסת לביצועים בפועל תחת עומס רשת אמיתי (<i>Mix Real-World Traffic</i>), כאשר מנועי ה-DPI, הגנת L7 וסריקת האנומליות פועלים באופן אקטיבי, ולא לבדיקות מעבדה.	הדרישה מתייחסת לעבודה בעומס רשת אמיתי כפי שידרש בסביבות המערך
12.	פרק ג	4	נדרשת הצפנה/פענוח SSL/TLS כולל TLS 1.3. נבקש להבהיר: האם הפענוח והסריקה של תעבורת TLS 1.3 מבוצעים ישירות על גבי ה-IPS המוצע (<i>Inline Decryption</i>), והאם נפח התעבורה הנדרש (עד 40Gbps) בטבלת התמחור נדרש להיתמך גם כאשר מופעל פענוח SSL/TLS אקטיבי בחישוב?	העמידה בעומס מתייחסת לתעבורה שמגיעה לא מוצפנת, יחד עם זאת המוצר צריך לתמוך בפענוח תעבורה עצמאית
13.	פרק ג	4.1.1.4	נבקש להבהיר מה הכוונה בדרישה ל-site License, שכן מודל הרישוי המקובל אצל היצרן אינו מוצע במתכונת זו	הכוונה בסעיף אינה בהכרח לרישוי במודל Site License אלא לכך שהמזכיר יכול בהצעתו את כלל רישיונות התוכנה הנדרשים לצורך התקנה, הפעלה ושימוש מלאים בפתרון המוצע, בהתאם למודל הרישוי של היצרן. ככל שנדרשים רישיונות נוספים עבור רכיב כלשהו (לרבות, לדוגמה, סביבת Sandbox או כל רכיב אחר), עלותם תיכלל במחיר ההצעה ולא תידרש רכישה נפרדת על ידי המזכיר.
14.	פרק ג	כללי - ארכיטקטורה	נבקש להבהיר: 1. כמה מכונות נדרשות לפריסה בפועל בכל סביבה? 2. כמה סביבות קיימות בסך הכל? 3. האם נדרשת מכונת ניהול מרכזית אחת או מכונת ניהול נפרדת לכל סביבה?	ראה סעיף 1.2 בפרק א' למסמכי המכרז, יובהר כי המערך אינו מתחייב לכמות כלשהי ויפעל בהתאם לצרכים משתנים, המערך צופה כי ידרשו 3 סביבות ניהול (סביבת ניהול אחת תנהל שתי סביבות IPS)
15.	פרק ד	1	נבקש להבהיר האם סעיף זה עוסק בהמשך מתן השירותים והמחירים כחלק מהזמנת המשך עתידית?	לא. סעיף 1 בהסכם ההתקשרות אינו עוסק בהמשך מתן השירותים או במחירים במסגרת הזמנות עבודה עתידיות. הסעיף קובע כי מסמכי המכרז וההבהרות שפורסמו במסגרתו מהווים חלק בלתי נפרד מההסכם, ויחולו על ההתקשרות ועל הזמנות העבודה שיוצאו מכוחו, בהתאם לתנאי המכרז וההסכם. אין בסעיף זה כדי לשנות את מנגנון המחירים או ליצור התחייבות להזמנות עבודה עתידיות



יובהר כי כוונת הסעיף היא שבמקרים שבהם, במהלך תקופת ההתקשרות, נרכשו רכיבים או שירותים הכוללים תקופת תחזוקה ותמיכה מוגדרת, מתחייב הספק להמשיך ולספק את שירותי התחזוקה והתמיכה עד לתום תקופת התחזוקה שנקבעה עבור אותם רכיבים או שירותים, גם אם תקופת ההתקשרות הסתיימה קודם לכן. אין באמור כדי להאריך את תקופת ההתקשרות מעבר לקבוע בהסכם, אלא רק להבטיח את קיום התחייבויות התחזוקה והתמיכה שנרכשו כדין במהלך תקופת ההתקשרות.	נבקש להבהיר מהי כוונת המזמין בהתחייבות הנדרשת מהספק/אינטגרטור למתן תמיכה גם לאחר תום תקופת ההתקשרות?	2	פרק ד	16.
מקובל	לצורך נוחות ויעילות במענה ובבדיקתו, נבקש לקבל את מסמך המענה והצעת המחיר בפורמט WORD עריך (ולא רק כקובץ סגור / PDF)		כללי	17.