



12 יוני 2018
כט' סיוון תשע"ח

אל: המציעים

הנדון: מענה לשאלות מציעים במכרז למערכת הלבנת קבצים
מס' ת (7) 2017

1. רצ"ב תשובות המוסד לביטוח לאומי (להלן – "המוסד") לשאלות שהתקבלו עד לתאריך 6/6/18, לפי סדר הסעיפים במכרז.
2. הבהרות המוסד להלן מהוות חלק בלתי נפרד מתנאי והוראות המכרז ומההסכם שייחתם בין הצדדים. ההבהרות מחייבות את כל המציעים וגוברות על הנוסח המובא במכרז במקרה של סתירה ו/או אי התאמה.
3. **מודגש ומובהר בזאת כי לא יהיה סבב שאלות הבהרה נוסף.**
4. יש לצרף להצעה תדפיס של המסמך הרצ"ב, חתום על ידי מורשי החתימה של המציע, כאמור בסעיף 0.3.5.9 במכרז.

בברכה,

דני גריינר
מנהל אגף תשתיות תוכנה



מס'	רכיב במכרז	סעיף במכרז	שאלת הבהרה	תשובה
.1		0.0 - מנהלה	נבקש לקבל מועד נוסף להציג שאלות הבהרה	הבקשה אינה מאושרת.
.2		0.1.5.2	האם יש לכם מוצר לגלישה מאובטחת שיכול לשלוט בנתיב הורדת הקבצים ?	המוסד משתמש ב-Ericom Shiled בסביבת עבודה אחת (כ- 3,500 משתמשים) לגלישה מאובטחת תוך שליטה על הנתיב להורדת קבצים. ביתר הסביבות בארגון לא נעשה שימוש בשלב זה, במוצר ייעודי לגלישה מאובטחת, למעט השימוש בפירוולים של Checkpoint.
.3		0.1.5.2	איזה פיתרון Endpoint Protection ל DEVICE CONTROL קיים בארגון.	המוסד משתמש ב- AD GPO לניהול בקרת השימוש בהתקני קצה בתחנות.
.4		0.1.5.4	האם יש להם Mail Relay אחרי ה- Mail Exchange בערוץ דוא"ל ?	המוסד משתמש כיום ב-Mail Relay של Office 365 למטרה זו. המוסד שוקל להוסיף Mail Relay נוסף של צד ג'. המציע רשאי להציע פתרון עבור Mail Relay, כאופציה משלימה לפתרון ההלבנה המוצע.
.5		0.1.5.6	האם ניתן להסתפק בפיתרון מולטיסורס שמעתיק קבצים מספריות ביניים לספריות אחרות?	לא. על הפתרון המוצע לכלול תמיכה בסריקה, הלבנה והשחרת קבצים, תכנים ומסרים שונים, שמתקבלים ונשלחים באמצעות כספת וירטואלית (Cyber-Ark), כמפורט בסעיף 2.1.7 וסעיפים נוספים במכרז.
.6		0.2.4	מה הכוונה בפיתוחים, הפיתוח יתבצע ע"פ הROADMAP של היצרן ולא דווקא על פי דרישה?	המוסד שומר לעצמו את הזכות לדרוש מהזוכה (האינטגרטור) לבצע פיתוחים שונים והתאמות שונות בפתרון, בהתאם לצרכי המוסד ובתנאי שהפתרון המוצע מאפשר זאת, באמצעות ממשקי API הכלולים בו. ראה גם תשובה לשאלה 25 ביחס לסעיף 2.3.7.1.



מס'	רכיב במכרז	סעיף במכרז	שאלת הבהרה	תשובה
7.		2.1.2.3	הפתרון המוצע יאפשר הזדהות לפי כרטיס חכם ו/או כרטיס מגנטי – צריך יצרן ודגם. כמו כן נצטרך לקבל לדינו כזה כרטיס לאחר הזכיה לצורך ולידציה (לפני שמעבירים את המערכת ללקוח). ידרוש פיתוח.	המוסד עובד עם כרטיסים חכמים מסוג Athena, המאושר לשימוש במשרדי הממשלה. לכרטיס האמור יש API מתועד. מובהר כי הזוכה יהיה אחראי לספק על חשבוננו כל פיתוח ואינטגרציה שיידרשו בפתרון על מנת לתמוך בכרטיס החכם האמור.
8.		2.1.2.4	באמצעות איזה כלי מוצפנים את המדיה הנתיקה (BitLocker או מוצר צד שלישי אחר).	כיום המדיה הנתיקה אינה מוצפנת, אולם המוסד מתכנן לשלב בעתיד פתרון הצפנה. על המציע לפרט אם פתרון ההלבנה המוצע על ידו תומך ב-BitLocker ו/או במוצרים אחרים.
9.		2.1.2.8	מה הכוונה אופציה לאספקה של תוכנת Sandbox ?	ראה סעיפים 2.1.3.9, 2.7.2.8, 5.3.2-9, 5.3.2-10.
10.		2.1.4	הבהרה בנוגע לערוץ האינטרנט	מובהר בזאת שעל הפתרון המוצע לבצע סריקה והלבנה לקבצים המורשים מרשת האינטרנט בצורה מאובטחת on-the-fly, עוד בטרם התקבלו הקבצים בתחנות העבודה, על מנת שלא לזהם ולהכניס פוגענים לתחנות הגולשות. הסריקה וההלבנה בערוץ זה חייבות להתבצע בשילוב עם Checkpoint Firewalls הפועלים במרכז המחשבים במוסד.
11.		2.1.8.2	מובהר שבהשחרת קבצים אין הכוונה ל- Content Filtering אלא סריקה ונטרול של פוגענים בהתאם לפרופיל ההשחרה המתאים.	בהשחרת קבצים כוונתנו לסריקת וירוסים כדרישת חובה ובנוסף אפשרות (אופציה) להשחרה של שדות טקסט בקבצי מסמכים (txt, pdf, office), בהתאם לחוקים שניתן להגדיר למערכת.
12.		2.1.8.3	בסעיף 2.1.8.2 כתוב שאין הכוונה ב Content Filtering אלא סריקה וניהול של פוגענים, ובסעיף 2.1.8.3 כתוב "השחרה של שדות טקסט..." - נשמח אם תוכלו להסביר מה נדרש ממנגנון ההשחרה לבצע.	סעיף 2.1.8.3 יוחלף בשלמותו בנוסח הבא: "הפתרון צריך לאפשר כמינימום סריקת וירוסים וקוד עיון באמצעות אנטי וירוס (L). תמיכה של הפתרון גם בהשחרה של שדות טקסט, בהתאם לחוקים שיגדיר המוסד, תיחשב כיתרון בדרוג האיכות. (S)



מס' במכרז	רכיב במכרז	סעיף במכרז	שאלת הבהרה	תשובה
13.		2.1.8.3	אילו סוגי קבצים יידרשו להשחרת שדות TXT (אופיס, PDF, טקסט?)	הכוונה להשחרת שדות בקבצי מסמכים מסוג Microsoft Office , pdf , txt
14.		2.1.8.4	היכן יש לשמור את הקבצים עצמם? על הדיסק המקומי של שרתי ההלבנה? האם למוסד לביטוח לאומי קיימת מערכת DLP ארגונית המבצעת השחרה ויש ליישם אינטגרציה מולה?	יש לשמור את הקבצים האמורים בדיסק מקומי בתחנה או בכונן רשתי שהמוסד יגדיר. על המערכת לאפשר אחזור של כל קובץ שעבר השחרה. בשלב זה אין למוסד מערכת DLP ארגונית. קיימת אפשרות שהמוסד יפעיל בעתיד מערכת DLP ובמקרה זה תידרש אינטגרציה מתאימה לפתרון ההלבנה המוצע, ככל שניתן טכנית לממש זאת.
15.		2.1.9.1	נבקש לקבל הסבר מפורט יותר בדרישות כיוון שכל מוצר שמפורט ברשימה הנ"ל דורש התייחסות מיוחדת, למשל, מה הכוונה ב"אינטגרציה עם office 365 outlook", האם סריקה של תיקיית ה OneDrive באופן מקומי (בהנחה שיש סוכן של OneDrive מותקן על התחנה שמבצע את הסכרון) כתיקייה מקומית רגילה - עונה על הדרישות? מה הכוונה ב"שיתוף קבצים ושליחת קבצים באמצעות קישור בדואר אלקטרוני"?	הפתרון המוצע נדרש להלבין כל קובץ שיורד מהענן בכל אחת מהדרכים הבאות: א. כאשר הקובץ ירד לתחנת העבודה באמצעות דפדפן. ב. כאשר הקובץ ירד מהענן והגיע לתחנת העבודה למיקום שבו יעבור תהליך הלבנה לפני השימוש בקובץ על ידי המשתמש. ג. בכל מקרה ששולחים את הקובץ שהורד מענן בדוא"ל למשתמש אחר. ד. לפני שהקובץ האמור מגיע לתיבת הדוא"ל של המשתמש (ב mail GW).
16.		2.1.9.2	האם סריקה של תיקיית מוצר האחסון (למשל, Google Drive, Dropbox וכו') באופן מקומי (בהנחה שיש סוכן של הפתרון מותקן על התחנה שמבצע את הסכרון) כתיקייה מקומית רגילה - עונה על הדרישות?	כן.



מס'	רכיב במכרז	סעיף במכרז	שאלת הבהרה	תשובה
.17		2.2.2.7.1	שיוך פרופיל הלבנה לפי "מערכת מקור" – למה הכוונה?	הכוונה להגדרת פרופיל הלבנה, בין היתר, בהתאם למקור הספציפי שממנו הגיע הקובץ המיועד להלבנה, כגון: כספת וירטואלית, דוא"ל, אינטרנט, קיוסק, מדיה נתיקה בתחנה בחיבור לרשת וכדו'.
.18		2.2.2.7.10	תוכן הקובץ: קישורים, מאקרו, סקריפטים, מחרוזות וכדו' - אבקש להבהיר את הדרישה	המציע יפרט האם הפתרון המוצע מאפשר הגדרה/עדכון של מדיניות הלבנה גם בהתאם לאלמנטים שונים שנמצאו בקבצים עצמם, כגון: קישורים, מאקרו, סקריפטים וכדו'. מובהר בזאת כי דרישה זו מסווגת S ואינה מוגדרת כתנאי סף.
.19		2.2.2.7.11	ביטויים רגולריים (REGEX) - מחרוזת תווים המשמשים להגדרת תבניות חיפוש - אבקש להבהיר את הדרישה	המציע יפרט האם הפתרון המוצע מאפשר הגדרה/עדכון של מדיניות הלבנה בהתאם למחרוזות תווים (REGEX) שנמצאו בקבצים הנסרקים, בהתבסס על תבניות חיפוש שניתן להגדיר למערכת. מובהר בזאת כי דרישה זו מסווגת S ואינה מוגדרת כתנאי סף.
.20		2.2.2.7.11	האם מדובר בתהליך הלבנה או השחרה? באילו פורמטים יש לתמוך ביכולת זו?	מדובר בתהליך הלבנה ולא בהשחרה. המציע יפרט את הפורמטים השונים שנתמכים על ידו.
.21		2.2.2.7.12	רשימות דינאמיות חיצוניות ו/או פנימיות – נבקש לדעת על אילו רשימות: HASH של קבצים? שמות? נתיבים? וכדו'	בנוסף לדרישה להגדרת רשימות שחורות/לבנות לפי סוג קובץ בסעיף 2.2.5.1, המציע יפרט האם הפתרון המוצע מאפשר הגדרת white/black lists מסוגים נוספים ועל פי מאפיינים נוספים, לדוגמא: המציע יפרט האם הפתרון תומך בבדיקה מול רשימות HASH פנימיות שהפתרון בונה בעצמו באופן דינמי ו/או בהתבסס על רשימות HASH שניתן לייבא לפתרון מבחוץ, כגון: רשימות מזהות של פוגענים שנשלחות על ידי מערך הסייבר הלאומי.



מס'	רכיב במכרז	סעיף במכרז	שאלת הבהרה	תשובה
.22		2.2.5.3	סעיף 2.2.5.3 – חסימת קבצים שהסיומת שלהם שונתה מספר פעמים – נדרשת הבהרה כיצד ניתן לזהות דבר כזה מבחינה טכנולוגית או לפרט את הדרישה.	על המציע לפרט האם הפתרון המוצע יכול לזהות קבצים שהסיומת שלהם שונתה מספר פעמים, בתנאי שניתן לזהות מקרה זה. מובהר כי דרישה זו מסווגת S ואינה מוגדרת כתנאי סף.
.23		2.2.6.3	סעיף 2.2.6.3 – לא מובנת הדרישה. מה הכוונה בהשטחה אקראית?	סעיף 2.2.6.3.3 ישונה כדלקמן: המילים "אקראית" תמחק. אין שינוי ביתר חלקי הסעיף. הכוונה בסעיף 2.2.6.3.3 היא העתקת והשטחת תוכן המסמך לקובץ אחר, כדי להסיר ולסלק אובייקטים שמוסותרים בו.
.24		2.3.1.1	האם במסגרת התשתית שהמוסד לביטוח לאומי מספק, יסופק גם Load Balancer חיצוני שתשתית ההלבנה תוכל לעשות בו שימוש?	כן, המוסד משתמש במכונות F5.
.25		2.3.7.1	חבילת SDK - האם אפשר לקבל דוגמא ?	על המציע לפרט האם הפתרון המוצע כולל חבילת פיתוח תוכנה (API) שבאמצעותה המוסד ו/או הזוכה (האינטגרטור) יוכלו לבצע שינויים והתאמות בפתרון על פי צרכי המוסד מזמן לזמן, <u>שלא באמצעות היצרן</u> . מובהר שהדרישה הזו מסווגת S ואיננה דרישת סף.
.26		2.4.1.5	מהו סוג הכרטיס? של איזה יצרן? האם יש לקורא הכרטיסים API מולו ניתן לעבוד? האם יש תיעוד המסביר כיצד ניתן לעבוד מול הקורא שברשותכם?	המוסד עובד עם כרטיסים חכמים מסוג Athena, המאושר לשימוש במשרדי הממשלה. לכרטיס האמור יש API מתועד. מובהר כי הזוכה יהיה אחראי לספק על חשבוננו כל פיתוח ואינטגרציה שיידרשו בפתרון על מנת לספק תמיכה מלאה בכרטיס החכם האמור.



מס' במכרז	רכיב במכרז	סעיף במכרז	שאלת הבהרה	תשובה
27.		2.5.6	האם אינטגרציה עם BufferZone שכבר קיים במוסד לביטוח לאומי, באה בחשבון? (יש לנו פתרון מובנה אך רצינו לדעת אם יכולת זו גם כן אפשרית כדי לא לשנות את חווית המשתמש שהעובדים במוסד כבר מכירים)	בשלב הנוכחי המוסד עדיין לא החליט האם להמשיך ולהתבסס על Bufferzone אם לאו. Bufferzone בגרסה הפועלת במוסד אינו מספק מסך פתיחה כל שהוא ויש בעיות באינטגרציה בינו לבין AV במוסד. המוסד מעוניין בפתרון Sandbox, שיגן על התחנות והרשת מפני פוגענים, ישתלב במערכת ההלבנה המוצעת, ידע לעבוד עם כל AV וינוהל מאותה מערכת (הלבנה), באופן כזה שתהליך ההלבנה יתבצע בסביבה נפרדת ומבודדת, מבלי לסכן את תחנת העבודה ו/או את הרשת הארגונית בהדבקת פוגענים. על המציע לכלול בהצעתו פתרון מתאים לבעיה הנ"ל, אם באמצעות פתרון המובנה בפתרון ואם באמצעות פתרון של צד שלישי.
28.		2.5.6	באיזה אופן לצרף דוגמא/מצגת? צילומי מסך מודפסים? צילומי מסך דיגיטליים כנספח?	יש לצרף צילומי מסך דיגיטליים לנספח 2 בהצעה.
29.		2.7.2.5	סעיף 2.7.2.5 – חסימת גישה להתקנים חיצוניים – האם קיימת מערכת לניהול התקנים מולה יהיה צורך להתממשקות או באמצעות GPO?	המוסד משתמש ב-Active Directory GPO.
30.		כללי	כמו כן, האם נוכל לתאם שיחת ועידה לעבור על תכנון הקיבולת (Sizing) שלכם?	לא ניתן להעביר שאלות לעורך המכרז שלא באמצעות דואר אלקטרוני, כאמור בסעיף 0.3.5.1 במכרז (נוהל שאלות הבהרה).