רשות האכיפה והגבייה

מכרז מספר 22/13

מכרז פומבי להקמה, הטמעה ותחזוקת מערכת לניטור, בקרה ותגובה לאירועי אבטחת מידע

פרק 1 : <u>מינהלה</u>

1.1. <u>רקע:</u>

רשות האכיפה והגבייה, באמצעות יחידת הרכש(להלן גם: "המזמינה" או "המשרד" או "המדינה" או "הרשות"), פונה בזאת לקבלת הצעות להקמה, הטמעה ותחזוקה של מערכת ניטור, בקרה ותגובה לאירועי אבטחת מידע (SIEM).

תיאור השירות הנדרש מופיע בפרק "מסמך האפיון" המהווה חלק בלתי נפרד ממסמכי המכרז.

****הערה מקדימה:** מסמכי המכרז מנוסחים בלשון זכר מטעמי נוחות בלבד. ביטויים המופיעים בלשון זכר משמעם גם בלשון נקבה ולהיפך. ביטויים המופיעים בלשון יחיד משמעם גם בלשון רבים ולהיפך.

1.2. <u>הגדרות:</u>

במכרז זה, על נספחיו, יהיו למושגים הבאים המשמעות שבצידם:

- ✓ **"רשות האכיפה והגבייה"** או **"הרשות"** או **"המזמינה"** או **"המשרד" או "המדינה"** - רשות האכיפה והגבייה וגופים שבשליטתה.
- ✓ **"המציע"** או **"הספק"**- גוף המציע הצעה במסגרת מכרז זה כיחידה אינטגרטיבית אחת.
- ✓ **"מכרז"** - הזמנה זו להגשת הצעות על כל חלקיה ונספחיה.
- ✓ **"יצרן"** – בית תוכנה המפתח מוצר SIEM.
- ✓ **"טכנאי"** - גורם מטעם הספק הזוכה אשר הוסמך על-ידי היצרן לטפל בחומרת המוצר, תוכנת המוצר, ההגדרות המוכלות במוצר והגדרות בסיסיות. בעל תעודות וידע רלוונטי כמפורט במסמכי המכרז.
- ✓ **מומחה" -** גורם מטעם הספק הזוכה אשר הוסמך על-ידי היצרן לטפל בחומרת המוצר, תוכנת המוצר, ההגדרות המוכלות במוצר, קביעה וכתיבת חוקים במוצר ופתרון תקלות. בעל תעודות וידע רלוונטי כמפורט במסמכי המכרז.
- ✓ **"הספק הזוכה"**- מציע אשר הצעתו תזכה במכרז זה, באם יהיה כזה.

1.3. <u>מסמכי המכרז</u>

את מסמכי המכרז ניתן לקבל, ללא תשלום, באמצעות דוא"ל: michrazim@eca.gov.il. **או באתר האינטרנט של מינהל הרכש הממשלתי בקישור שלהלן:**

http://mr.gov.il/OfficesTenders/Pages/default.aspx

1.4. <u>אופן הגשת ההצעה</u>

1.4.1. ההצעה תוגש **כדלקמן:**

1.4.1.1 מענה לתנאי סף ומרכיב איכות - יוגש בשלושה עותקים בצירוף כל המסמכים הנדרשים, אשר יוכנסו למעטפה אחת עליה יצוין: שם המציע, כתובתו ומס' הטלפון ותסומן כ"מעטפת מענה לתנאי סף + איכות".

1.4.1.2 יש לצרף עותק דיגיטלי על גבי DVD/CD-ROM של תכולת ההצעה, בפורמט MS-WORD ובנוסף בפורמט PDF - יוכנסו למעטפת האיכות ותנאי הסף.

1.4.1.3 הצעת המחיר תוגש בנפרד, בשני עותקים, אשר יוכנסו למעטפה אחת עליה יצוין: שם המציע, כתובתו ומס' הטלפון ותסומן כ"מעטפת הצעת מחיר".

1.4.1.4 מעטפת מענה לתנאי סף ואיכות ומעטפת הצעת המחיר, יוכנסו למעטפה אחת כוללת. על גב המעטפה החיצונית יירשמו: שם המכרז, מספר המכרז וכתובתה של רשות האכיפה והגבייה בלבד.

1.4.2. עצם משלוח ההצעה בדואר ישראל או ע"י שירות שליחים עד המועד הנ"ל אינו מהווה מסירה כשלעצמו, אלא אם ההצעה נתקבלה ב"תיבת המכרזים" וניתן למוסר אותה אישור קבלה.

1.4.3. **אין להגיש הצעה בכל דרך אחרת. הצעה שתגיע בפקס או בדואר אלקטרוני (E-mail) או בדרך אחרת - תיפסל על הסף.**

1.4.4. כל מקום בו סומן מקום חתימה- יחתום המציע חתימה מקורית מלאה ביחד עם חותמת. אם המציע הוא חברה או שותפות רשומה- יחתום רק מי שהוסמך לכך כדין, בתוספת חותמת התאגיד.
המציע יחתום על כל עמודי הצעתו, על כל עמודי חוברת המכרז ועל עמודי המענה לשאלות ההבהרה.

1.5. <u>מועד הגשת ההצעות</u>

את ההצעות יש להגיש לא **יאוחר מהמועד האחרון להגשת הצעות- כפי שמפורט בטבלת ריכוז המועדים** להלן. ההצעות תוכנסנה לתיבת המכרזים ברשות האכיפה והגבייה ברח' ירמיהו 37, ירושלים, קומה 15. ההצעות תישלחנה בדואר רשום או במסירה אישית ועליהן להימצא בתיבת ההצעות במועד הנקוב בסעיף זה. על המציע האחריות לכך ולא תישמע ממנו כל טענה בעניין.

לתשומת הלב: בהתאם לתקנה 20 לתקנות חובת המכרזים, התשנ"ג, 1993 - ועדת המכרזים לא תדון בהצעה שלא נמצאה בתיבת המכרזים במועד האחרון להגשת הצעות ולא תשמע כל טענה בעניין זה.

1.6. <u>איש הקשר מטעם המציע</u>

למעטפה הפנימית יש לצרף מכתב ובו לציין את הפרטים כדלקמן: שם איש הקשר האחראי על ההצעה מטעם המציע. אל איש הקשר תפנה המזמינה בקשר למענה, כתובתו, מספר טלפון ישיר, מספר פקס, מספר נייד וכתובת דואר אלקטרוני.

1.7. <u>כתובת קשר של המזמינה</u>

אמצעי הקשר עם המזמינה- באמצעות מספר פקס: 02-5804021, או באמצעות דואר אלקטרוני: **michrazim@eca.gov.il**, כתובת: רח' ירמיהו 37, ירושלים. כל הפניות יבוצעו **<u>בכתב בלבד</u>** לכתובות אלו בלבד.

1.8. <u>תיאום הצעות</u>

המציע ו/או בעל עניין במציע ו/או כל גוף שהמציע הינו בעל עניין בו או נושא משרה בו- לא יפעל לתיאום הצעתו עם הצעת מציע אחר כלשהו הן לפני קיום המכרז והן בזמן תקופת המכרז. מבלי לגרוע מכלליות האמור, המדובר באיסור לתיאום הצעות לרבות: כריתה מפורשת של הסכם או הבנה מכל סוג עם אדם או גוף כלשהו ו/או קבלת או החלפת מידע, פרסום מידע או גילויו לאדם או לגוף כלשהו- כאשר אותו אדם או גוף הינו בעל עניין או נושא משרה או שלוח או עובד של מציע אחר.

1.9. <u>טבלת ריכוז מועדים</u>

תיאור הפעילות	תאריך	שעה
פרסום ההליך ע"י המזמינה	**21/10/13**	
מועד אחרון להצגת שאלות הבהרה	**10/11/13**	12:00
מועד אחרון להגשת מענה לשאלות	שבוע לפני המועד האחרון להגשת הצעות.	
המועד האחרון להגשת הצעות	**21/11/13**	12:00
תוקף ערבות מכרז	**20/2/14**	

המזמינה רשאית, על פי שיקול דעתה הבלעדי, לדחות ו/או לשנות כל אחד מהמועדים אשר נקבעו בהליך המכרז.

1.10. <u>שאלות ובירורים</u>

1.10.1. שאלות בקשר למכרז ניתן להפנות אל המזמינה, עד **לא יאוחר מהמועד האחרון להצגת שאלות הבהרה- כפי שמפורט בטבלת ריכוז המועדים לעיל**, באמצעות דוא"ל michrazim@eca.gov.il. אין לשלוח שאלות לאחר המועד האחרון לשליחת שאלות. לאחר העברת הדוא"ל ליעדו, באחריות המציע לוודא כי הדוא"ל הגיע ונתקבל ביעדו, באמצעות כתובת הדוא"ל דלעיל בלבד.

1.10.2. הפניות תכלולנה את שם המציע השואל, מענו ואמצעי תקשורת אליו. בחלקה המהותי הפנייה תכלול את זיהוי החלק והסעיף הרלוונטי במסמך זה שעורר את השאלה, ככל שניתן, או בקשת הבהרה ואת השאלה בצורה בהירה ומלאה.

1.10.3. המזמינה תהא רשאית שלא להתייחס לשאלות שתגענה לאחר המועד האחרון לשליחת שאלות, בהתאם לשיקול דעתה הבלעדי, המוחלט והסופי.

1.10.4. המזמינה רשאית שלא להתייחס לשאלות מחמת היותן בלתי ברורות, כלליות, בלתי ענייניות, מחמת החשש לחשוף מידע שראוי להישאר חבוי ו/או מכל טעם ענייני אחר, בהתאם לשיקול דעתה הבלעדי, המוחלט והסופי של המזמינה.

1.10.5. בהתחשב בשאלות שהתקבלו- המזמינה תהא רשאית לשנות את נוסח ו/או תנאי המכרז, לרבות איזה מנספחיו. במקרה זה- הנוסח החדש של המכרז, בהתאם למענה לשאלות- הוא המחייב וזאת גם אם בפועל לא תופק הדפסה מתוקנת של מסמכי המכרז. אין באמור לעיל כדי לחייב את המזמינה להסכים להסתייגויות כלשהן אשר נכללו בשאלות המציעים ו/או בכדי לבצע שינוי זה או אחר.

1.10.6. השאלות והתשובות יישלחו באמצעות דוא"ל בלבד. רק תשובות בכתב יחייבו את המזמינה. מודגש בזה, כי תשובות בכתב לשאלות בעניין הסכם ההתקשרות בין המזמינה למציע- תהיינה חלק בלתי נפרד מתנאי ההסכם וזאת גם אם בפועל לא תופק הדפסה מתוקנת של נוסח הסכם ההתקשרות החדש.

1.10.7. אין המשרד מתחייב לענות או להתייחס לכל השאלות והבקשות שיועברו אליו.

1.11. <u>תקופת ההתקשרות</u>

1.11.1. תקופת ההתקשרות עם הספק הזוכה תימשך שנה ותתחיל להימנות מיום החתימה על הסכם ההתקשרות והוצאת הזמנה חתומה כנדרש. תוקף ההתקשרות יהיה כפוף בכל עת לחוקי התקציב שבתוקף מעת לעת ולהוראות החשב הכללי.

1.11.2. לרשות האכיפה והגבייה שמורה הזכות להאריך את משך תוקפה של התקשרות זו בתקופות נוספות בנות שנה כל אחת. בעניין זה, המזמינה תודיע לזוכה, בכתב, 30 ימים מראש, אם ברצונה להאריך את תקופת החוזה. אין באיחור במסירת ההודעה משום ביטול זכותה של המזמינה להודיע על הארכת החוזה לארבע שנים נוספות ובלבד שסה"כ תקופת ההתקשרות (לרבות ההארכות) לא תעלה על 5 שנים.

1.11.3. במידה ורשות האכיפה והגבייה תחליט <u>לבטל</u>, מכל סיבה שהיא את ההתקשרות, היא תודיע על כך בכתב לצד השני 30 יום מראש. הודעה על <u>המשך</u> התקשרות, ככל שתחליט על כך המזמינה, תינתן בכתב ע"י רשות האכיפה והגבייה 30 יום מראש.

1.12. <u>היקף ההתקשרות</u>

המזמינה רשאית להגדיל את היקף ההתקשרות במכרז בכל שנה ב- 100% ולהקטין את היקף ההתקשרות במכרז בכל שנה והכול עפ"י שיקול דעתה הבלעדי ובכפוף לתקנות חובת המכרזים. יודגש, כי זכות זו של המזמינה, להרחיב ו/או להקטין את היקף ההתקשרות.

1.13. <u>ביטול המכרז</u>

המזמינה תהא רשאית לבטל את המכרז ו/או לצאת במכרז חדש- על פי שיקול דעתה הבלעדי, המוחלט והסופי של המזמינה וללא מתן שום נימוקים והסברים למציעים או לכל גורם אחר וללא הודעה מוקדמת. כמו כן, המזמינה לא תשלם בשום מקרה פיצוי מכל סוג שהוא בעקבות הביטול כאמור. המזמינה תעדכן את המציעים בדבר הביטול אולם עדכון זה לא יהווה תנאי לתקפות הביטול.

1.14. <u>שינוי המכרז</u>

כל שינוי שייעשה ע"י המציע במסמכי המכרז או בנספחים המצורפים אל מסמכי המכרז, או כל הסתייגות ביחס אליהם, בין אם על ידי תוספת בגוף המסמכים ובין במכתב לוואי או בכל דרך אחרת לא יובא בחשבון בעת הדיון בהצעה והמזמינה תראה אותו כאילו לא נכתב ואף עלול לגרום לפסילת ההצעה.

1.15. <u>תוקף ההצעה</u>

1.15.1. הצעתו של מציע תהיה בתוקף למשך 90 יום מהמועד האחרון והסופי למסירת ההצעות. תוקפה יוארך לתקופה של 60 יום נוספים אם תימסר למציעים הודעה על כך מהמשרד. אם לא תתקבל הודעה כאמור והליכי אישור המכרז לא יסתיימו לאחר 90 יום מהמועד

האחרון להגשת ההצעות, רשאי המציע לבטל את הצעתו- בכתב בלבד ותוך ציון מועד תחולה.

1.15.2. **המציע אינו רשאי לחזור בו מהצעתו, או לשנותה, בתקופה הנ"ל**.

1.15.3. נקבע זוכה תוך התקופה האמורה, תהיה הצעתו בתוקף עד תום 90 יום מיום סיום תקופת ההתקשרות.

1.16. <u>מתן שירותים בשעת חירום</u>

על מגישי ההצעות לקחת בחשבון, כי ע"פ הוראת שעה תכ"ם 7.12.6 של החשב הכללי: כל מכרז או הסכם התקשרות לרכישת טובין או שירותים שאספקתם חיונית, הספק הזוכה במכרז יחויב לספק את השירות או הטובין בכל עת, לרבות בשעות חירום, בתנאי אספקה כפי שנקבעו בהסכם ההתקשרות. הפרה של סעיף זה תהווה הפרה יסודית של הסכם ההתקשרות המקנה זכות למזמינה לנקוט בצעדים כמוגדר בהסכם.

1.17. <u>זכויות קניין רוחני</u>

1.17.1. כל השירותים שיינתנו על ידי הספק הזוכה ותוצאותיהם ו/או תוצריהם, ללא יוצא מן הכלל, ייחשבו ויהיו לקניינו המוחלט והבלעדי של המשרד. הספק הזוכה לא ישתמש במסמך או במידע או בכל תוצר של השירותים או תוצאותיהם, ללא אישור בכתב ומראש של המשרד.

1.17.2. המשרד יהיה רשאי הן במהלך מתן השירותים והן לאחריהם לדרוש מהספק הזוכה ולקבל לידיו כל תוכנית, מסמך, מידע או דבר הקשור למתן השירותים.

1.17.3. על אף האמור בכל דין, לא תעמוד לספק הזוכה זכות עיכבון בעבודות או בתוצרי שירותים כאמור.

1.17.4. למען הסר ספק, מודגש בזאת כי האמור בפסקה זו לעיל יחול גם על כל מידע, מסמך וכיוצא באלה שימסרו לספק הזוכה על ידי המשרד בקשר עם מתן השירותים, אלא אם כן מדובר במידע, מסמך וכיוצא באלה שהפכו לנחלת הכלל. נטל ההוכחה כי מידע, מסמך וכיוצא באלו כאמור הן בגדר נחלת הכלל - מוטל על הספק הזוכה.

1.18. <u>כללי</u>

1.18.1. **מגישי ההצעות מתבקשים לבחון היטב את תנאי המכרז ובכלל זה את מלוא ההתחייבויות שיוטלו עליהם במסגרת ההתקשרות עם רשות האכיפה והגבייה במידה ויזכו במכרז.**

1.18.2. לרשות האכיפה והגבייה נשמרת הזכות לפנות במהלך הבדיקה וההערכה אל הגוף המציע, בכדי לקבל הבהרות או בכדי להסיר אי בהירויות שעלולות להתעורר בבדיקת ההצעות. הבהרות להצעה תינתנה בכתב בלבד. כל פניה תיעשה בכפוף להוראות חוק חובת המכרזים, תקנות חובת מכרזים והוראות התכ"ם.

1.18.3. המשרד שומר לעצמו את הזכות לפסול על הסף מציע, אשר יתגלה כי כלל בהצעתו מידע שיקרי או מטעה או לא כלל מידע שאמור היה לגלותו.

1.18.4. כל הנחיה, הדרכה והוראה שניתנו או יינתנו על ידי נציגי המשרד דינן כדין הנחיית המזמין בלבד ולא יהיה בהן כדי ליצור כל יחסי עובד/מעביד עם הספק או עם עובדיו. כמו כן, לא תשחרר כל הדרכה, הנחיה או הוראה כנ"ל את הספק הזוכה ממילוי כל התחייבויותיו לפי מכרז זה ולפי ההסכם שייחתם.

1.18.5. אין רשות האכיפה והגבייה מתחייבת לקבל את ההצעה הזולה ביותר, חלק מהצעה או כל הצעה שהיא, בשלמותה או בחלקים ממנה. רשות האכיפה והגבייה רשאית לפצל את ההצעה, לקבל חלקים ממנה, או לממשה בשלבים.

1.18.6. במידה שלא תתאפשר העסקת הספק הזוכה, למזמינה שמורה האופציה לפנות למציע שדורג במקום השני לקבלת השירות, וזאת בתנאים שהציע בהצעתו ותוך הסכמתו לכך.

פרק 2 : מסמך האפיון - תיאור הפרויקט והיקפו

2.1 רקע כללי

2.1.1 בהחלטת ממשלה 3487 ממאי 2008 הוחלט על הפרדת מערכות ההוצאה לפועל והמרכז לגביית קנסות ממערכת בתי המשפט. כיום מצויים הארגונים (הוצאה לפועל והמרכז לגביית קנסות) תחת רשות האכיפה והגבייה (להלן- יכונו גם "הארגונים"), המהווה יחידת סמך עצמאית הכפופה ישירות לשר המשפטים. ההפרדה בוצעה, הלכה למעשה, ביום 1.1.09.

2.1.2 רשות האכיפה והגבייה מבקשת בזאת הצעות להקמה ויישום מערכת איסוף וניהול אירועי אבטחת מידע ממערכות ומקורות מידע שונים הקיימים אצלה. המציע שהצעתו תתקבל יספק חבילת תוכנה, ימפה את דרישות הלקוח, יאפיין פתרון, יבצע Design להטמעה ברשת המזמינה, יקים את Core המערכת, ידאג לקבל את הלוגים מהמערכות ומהאפליקציות השונות, יקשר מקורות מידע ואפליקציות כפי שמוגדר במפרט, ידריך, יתעד את ההטמעה וייתן שירותי תמיכה ותחזוקה.

2.2 מטרה

2.2.1 המטרה היא הקמת מערכת איסוף וניהול אירועי אבטחת מידע ממערכות ומקורות מידע שונים הקיימים אצל המזמינה.

2.3 הגדרות

2.3.1 טיפול באירועי אבטחת מידע משמעותו:

2.3.1.1 התראה – זיהוי האירוע ומתן התראה

2.3.1.2 תעדוף – ביצוע תעדוף בין ההתראות והאירועים, תעדוף אירוע מול תגובה.

2.3.1.3 תגובה – מתן תגובה לאירוע וסגירתו

2.3.1.4 תחקור – תחקור מלא של אירוע והסקת מסקנות לצורך אי הישנותו.

2.4 שיטה

2.4.1 מערכת ניהול האירועים תתבסס על מוצרי מדף ידועים ומובילים בשוק, אשר נבחנו וייושמו כבר בגופים דומים למזמינה.

2.5 ההצעה תכלול:

2.5.1 מערכת איסוף וניהול אירועי אבטחת מידע - תוכנה.

2.5.2 יישום והטמעת המערכת בהתאמה לדרישות המזמינה.

2.5.3 יישום איסוף האירועים מהמקורות השונים שיוגדרו.

2.5.4 יישום תגובה ותחקור אירוע.

2.5.5 קישור האפליקציות ומקורות מידע המפורטים בהמשך.

2.5.6 המערכת תכלול מנגנון לבדיקת חוקים קיימים, וחוקים חדשים על DATA היסטורי.

2.5.7 המערכת תכלול יכולת לקישור לוגי בין פרמטרים שנוצרים במערכות שונות, אך מייצגות את אותו ערך לוגי. המערכת נדרשת ליצור קשר לוגי בחיפושים ובחוקי מערכת לצורך זיהוי אותו משתמש.

2.5.8 אינטגרציה בין מערכות, מערכות הפעלה, בסיסי נתונים, אפליקציות ומוצרי הגנה הקיימים אצל המזמינה.

2.5.9 הגדרת מדיניות האבטחה במערכת האיסוף וניהול האירועים (הקשחה) בהתאמה למדיניות הקיימת אצל המזמינה.

2.5.10 ביצוע בדיקות קבלה תפעוליות.

2.5.11 תמיכה ותחזוקה שוטפת למערך שיוקם.

2.5.12 תיעוד המערך ובניית נהלים תפעוליים.

2.5.13 הדרכות על המערכת למשתמשי המערכת ולגורמי פיתוח ותפעול של המזמינה.

2.5.14 יכולת קישור למערכת שליטה ובקרה.

2.6 <u>הפרויקט יבוצע בשישה שלבים מרכזיים (אחד אחרי השני):</u>

שלב	פירוט	הערות
א	אפיון ארכיטקטורת המוצר, וממשק המשתמש	
ב	הקמת התשתית, התקנת המוצר בקונפיגורציה בסיסית, והתאמתו לדרישות המזמינה	אספקת רישוי לשנה, כולל בדיקות קבלה, מסירה והדרכה.
ג	קישור מקורות מידע תשתיתיים ותקשורתיים	כולל ובניית חוקים ודוחות מתאימים
ד	קישור מערכת לגביית קנסות	כולל ובניית חוקים ודוחות מתאימים
ה	קישור מערכת כלים שלובים	כולל ובניית חוקים ודוחות מתאימים
ו	קישור יתר מערכות המזמינה	כולל ובניית חוקים ודוחות מתאימים

2.6.1. כל שלב מבין השלבים ג-ו, יכיל את 5 התוצרים הבאים : אפיון, הטמעה, בדיקות קבלה, מסירה והדרכה.

2.7 <u>מטרת המערכת:</u>

2.7.1 יכולת ידיעה על אירועי אבטחה המתרחשים בארגון – כיום בארגון לא קיימת מערכת המבצעת איסוף אירועים והתרעה על אירועים. נוסף, לא ניתן לבצע שיתוף מידע בין המערכות השונות ולדווח על אירוע רוחבי ארגוני.

2.7.2 תגובה ותחקור אירוע – על המערכת לאפשר תיעוד אירועים, התגובה ויכולת תחקור האירועים. כמו כן השלמת הנתונים הנדרשים לתחקור אירועים והוצאת דו"חות אוטומטית מהמערכת.

2.7.3 היכולת לאיסוף ראיות – איסוף הראיות הינו הכרחי למצב בו תתבקש המזמינה לתבוע או לערב גורמים ממשלתיים כדוגמת המשטרה באירוע שארע. בשל העובדה כי המערכת הינה מערכת איסוף אירועים, המערכת עצמה תהווה את בסיס הנתונים המרכזי לאיסוף ראיות ותיעוד אירועי האבטחה.

2.7.4 דיווחי הנהלה – המערכת תאפשר הוצאת דיווחים מיידים על אירועי אבטחה, התגובה לאירוע וההשלכות על המזמינה.

2.8 <u>זמן הביצוע</u>

2.8.1 8 חודשים מקבלת הזמנה ואישור עבודה מהמזמינה.

2.8.2 כל דחייה מעבר לזמן זה דורשת אישור בכתב של מנהל אבטחת המידע של המזמינה.

2.8.3 מחזור החיים - המערכת נדרשת לשרת את המזמינה לפחות 10 שנים מיום העברתה לידי המזמינה – מעבר בדיקות קבלה.

2.9 <u>מבנה המערכת</u>

2.9.1 יישום הארכיטקטורה המבוקשת כולל איסוף של כלל מקורות המידע מהאתרים הבאים: אתר המחשוב המרכזי (Data Center), המרכז לגביית קנסות ולשכות ההוצאה לפועל.

2.9.2 המערכת שתוקם תהא מערכת שרידה, כאשר תוקם מערכת באתר הראשי ומערכת גיבוי באתר חלופי. בשלב הראשון של הפרויקט תוקם מערכת יחידה באתר ראשי ובשלב השני תוקם מערכת הגיבוי, עם זאת, תכנון הארכיטקטורה נדרש להיות כמערכת שרידה.

2.9.3 המערכת שתוקם תמוקם בסגמנט מאובטח המופרד מהתשתית הפנימית ומוגן ע״י אמצעי אבטחה. ההפרדה הבסיסית תבוצע באמצעות רשת וירטואלית ייעודית לשרתי המערכת וכן באמצעות הגנה ע״י אמצעי אבטחה כדוגמת Firewall.

2.9.4 הגישה למערכת לצורך ניהול, עדכון, טיפול בתקלות ותחזוקה יבוצע מתוך רשת המזמינה בלבד, לא תותר התחברות מרחוק לצורך ביצוע הפעילויות הרשומות לעיל.

2.9.5 המערכת תקושר לכלל הסגמנטים בארגון – פנימיים, חיצוניים, אזורי חייץ וכו׳.

2.9.6 המערכת תקושר למערכת השליטה והבקרה הקיימת לבקרה על חיות המערכות.

2.10 <u>על המציע לפרט בהצעתו:</u>

2.10.1 תצורת המערכת – ארכיטקטורה נדרשת – נדרש לצרף תרשים, רכיבים הקיימים במערכת, מיקום הרכיבים בתשתית המזמינה, תפקיד כל אחד מהרכיבים בתשתית, תרשימי זרימת המידע (חד כיווני, דו כיווני לרבות פרוטוקולים ופורטים). במידה וישנן מספר פתרונות יש לפרטן ולתת המלצה על הפתרון המועדף.

2.10.2 קישור אל המערכות המשיקות – תצורת הקישור ותרשימי זרימת המידע (חד כיווני, דו כיווני לרבות פרוטוקולים ופורטים). יש לצרף תרשים.

2.10.3 תהליך ניהול המערכת - תרשימי זרימת המידע (חד כיווני, דו כיווני לרבות פרוטוקולים ופורטים). יש לצרף תרשים.

2.10.4 תצורת איסוף נתונים ממקורות המידע השונים המפורטים בהמשך המסמך – דיאגרמה מלאה של איסוף הנתונים, פרוטוקולים, להיכן ירוכזו הנתונים, שרתי הביניים וכו׳.

2.10.5 פירוט הנדרש בסעיף זה יצורף **כנספח יז׳1 במענה להצעה**

2.11 משתמשי המערכת

משתמש	תיאור
מנהל אבטחת מידע	מנהל אבטחת מידע הינו הגורם האחראי על כלל השינויים שיבוצעו ברמת המערכת קרי, מתן הרשאות, שינויי קונפיגורציה, הוספת מסכים, שינוי חוקים וקורלציות וכדומה.
מנהל התשתיות	מנהל התשתיות הינו הגורם האחראי על כלל התשתיות של המזמינה ותפקידו לוודא שהן מתפקדות היטב והמשתמשים מקבלים את השירותים הנדרשים.
ממונה אבטחת מידע טכנולוגי	אחראי על ארכיטקטורת אבטחת המידע בארגון
צוות תפעול התשתיות	אחראים על התפעול השוטף של המערכת אצל המזמינה.
מוקדן / צופה / Help desk (עתידי)	תפקיד הצופה מורכב ממספר תפקידים שרובם ככולם מרוכזים באבחנת האירוע ומתן תגובה ראשונית. הצופה הינו חלק מ-Help Desk הקיים אצל המזמינה. פירוט התפקיד: הצופה יצפה במסכי המערכת ויבחין אם מתרחשים אירועי אבטחה, יעריך את חומרת האירוע והתגובה הנדרשים, יגיב לאירוע ויתעד את הפעילויות.

2.12 ממשקים

2.12.1 על המערכת להתממשק למערכות התשתית של המזמינה. על המציע לפרט כיצד מערכת ה SIEM מתממשקת אל כל אחת מהמערכות המבוקשות:

תיאור הממשק	דרישות הפירוט
Active Directory הזיהוי ל-Active Directory ברשת המזמינה מתבצע באמצעות כרטיסים חכמים על בסיס תעודות דיגיטליות.	על המערכת להתממשק באופן מלא לזיהוי על בסיס AD או לחלופין על בסיס זיהוי ישיר באמצעות תעודות דיגיטליות. על המציע לפרט כיצד תבוצע ההתממשקות למטרות זיהוי והרשאות על בסיס הזיהוי החכם.
מערכת השליטה והבקרה 1) מערכת SCOM מבית Microsoft אשר מבצעת ניטור שרתים ומערכות הפעלה 2) IBM Director לניטור חומרת שרתים. 3) IMC של HP לניטור ציוד	על המציע לפרט כיצד תבוצע ההתממשקות למערכות השו"ב . על הפירוט לכלול: אפשרויות ניטור, זרימת המידע (חד כיווני, דו כיווני לרבות פרוטוקולים ופורטים), צורך בהתקנת סוכן / תוכנה וכו'.

תיאור הממשק	דרישות הפירוט
תקשורת וקווי תקשורת. 4) WSUS להפצת עדכוני אבטחת מידע.	
Help Desk (עתידי) יהיה אחראי על ניהול האירועים מפתיחת התקלה ועד סגירתה. ייתכן ויהיה אחראי על תחקור האירוע בנוסף.	על המציע לפרט את יכולת המערכת להתממשק למערכת ה-Help Desk למטרות: א. פתיחת קריאה ב. העברת המידע הרלוונטי ממערכת ה-SIM ג. יכולת קבלת המידע לביצוע תחקור האירוע
תוכנות לבדיקת פגיעויות	על המציע לפרט מול איזה כלי Volunerabillity Assesment/Scanner המערכת יודעת לעבוד.
מערך SMS שליחת התראה על קבלת האירוע ב-SMS לצוות הטיפול באירוע	על המציע לפרט כיצד יתממשק למערך ה- SMS וכיצד ניתן יהיה להגדיר במערכת על אילו התראות ישלח SMS ועל אילו התראות לא ישלח SMS.
אנטי וירוס	Trend micro
DLP	Trend Micro – טרם הסתיימה ההטמעה
MDM	Trend Micro – עתידי
Firewall	Check point r75
Web Application Firewal	F5/Imperva
Load Balancer	F5
Data Bases	MS-SQL
Messaging	Orchestration ,MSMQ, Biztalk
שרתי אפליקציה	IIS 6-7.5
שירותי Proxy	Microsoft Forefront Threat Management Gateway2010
סביבות וירטואליות	VMware, Citrix, Microsoft Virtualization Hyper-V, Terminal Server
ERP	SAP
ניהול מסמכים	Sharepoint, Documentum
כספות	Cyber-Ark
מתגים	COM3 HP
שירותי דואר	Microsoft Exchange 2007
נתבים	Cisco

תיאור הממשק	דרישות הפירוט
מערכות הפעלה שרתים	Windows Server 2003, 2008 R2
מערכות הפעלה עמדות קצה	Windows XP, Windows 7

2.12.1. איסוף ההתראות - יבוצע ברמה העקרונית ללא סוכן (Agenless) במטרה להקל על פעילות התחזוקה והתפעול של המערכת, זאת למעט מספר מערכות מועט אשר המזמינה תשתכנע כי אין דרך אחרת לחברן אלא באמצעות סוכן.

2.12.2. דרכי ההתממשקות אפשריים למערכת איסוף הנתונים – להלן מפורטים דרכי ההתממשקות האפשריים למערכת איסוף האירועים המקובלות על המזמינה, על המציע לתמוך בכל אחת מהאפשרויות המצוינות מטה. במידה ואחת מהדרכים אינה נתמכת ו/או קיימות אפשרויות נוספות על המציע לפרטן, המזמינה תדון בכל אחת מהדרכים בנפרד.

2.12.3. עבודה ללא סוכן – קישור המערכת למשיכת נתונים ישירות ממקורות המידע / האפליקציות.

2.12.4. עבודה עם סוכן - קישור מערכות באמצעות התקנת סוכן המערכת לאיסוף ושליחת המידע מתוך המערכת.

2.12.5. שליחת הלוג ב- syslog - אחת האפשרויות להעברת הלוג מהמערכת הינה באמצעות שליחת הלוג לשרת Syslog ייעודי בתשתית המזמינה.

2.12.6. העתקת הלוג - דיסקים משותפים - אפשרות נוספת להעברת הלוג הינה העתקת הלוג באמצעות יצירת דיסק משותף ארגוני אשר אליו יועתקן כלל הקבצים ומשם יועלו הקבצים למערכת האיסוף.

2.12.7. שליחת הקובץ באמצעות מערכת א-סינכרונית - אפשרות נוספת להעברת הלוג הינה באמצעות שליחת הקובץ באמצעות מערכת א-סינכרונית כדוגמת שרתי הדואר / FTP וכו'.

2.12.8. פירוט הנדרש בסעיף זה יסומן **כנספח יז'2 במענה להצעה**

2.13 <u>בקרה על תהליך קבלת הלוג / האירועים</u>

2.13.1 כל תצורת התממשקות המשלבת קובץ לוג כמפורט לעיל תכיל פעילויות Quality Assurance על הפעולה - הקובץ הועתק במלואו / הגיע במלואו לייעדו, הקובץ לא הועתק, הקובץ גדול מדי, ועוד. בקרה מלאה על כל הפעילויות מקצה לקצה כולל אישור תקינות הקובץ והגעתו לשרת שיוגדר. על המציע לפרט מהם המנגנונים האינהרנטיים הקיימים לאישור תקינות הקובץ הקיימים במערכת המוצעת.

2.13.2 לוג במקורות מידע - קיים מספר רב של מקורות מידע ברשת המזמינה. בכלל מקורות המידע למעט אפליקציות – <u>באחריות</u> הספק להגדיר את הלוג במקור המידע ולדאוג להעבירו למערכת האיסוף, קרי, במידה ולא מוגדר לוג במערכת, על הספק להגדיר למזמינה מה הלוג הנדרש וכיצד להגדירו במערכת ובמקרים בהם תבחר המזמינה להגדירו במקור המידע עצמו. בנוסף הספק יידרש להבהיר למזמינה את כלל ההשלכות של כתיבת הלוג במקור המידע לפני היישום.

2.13.3 מקורות מידע - על המציע לפרט את תצורת הקישור של כל מקור מידע המבוקש במפרט. הפירוט הבסיסי הנדרש הינו:

2.13.3.1 האם התוכנה תומכת אינהרנטית בתצורת הקישור.

2.13.3.2 מה הלוג הקיים והיכן ממוקם (למעט אפליקציות)

2.13.3.3 כיצד יבוצע איסוף המידע (פרוטוקול, תצורת קישור חד כיוונית / דו כיוונית, הגורם היוזם).

2.13.3.4 האם קיימת תמיכת יצרן בגרסא המפורטת (במידה ולא קיימת גרסא יש לפרט תוך כמה זמן תהא תמיכה).

2.13.3.5 פירוט הנדרש בסעיף זה יסומן **כנספח יז'3 במענה להצעה**

2.14 <u>פירוט רכיבי התשתית</u>

2.14.1 **<u>רכיבי תקשורת – נתבים ומתגים</u>**

2.14.1.1 ציודי התקשורת ברשת המזמינה – הנתבים, ורכיבי ה-Wireless הינם מבית Cisco. הדגמים המרכזיים הינם Cisco 2811, 2821, 7204 בגרסאת IOS 12.0 ומעלה. המתגים הינם מבית HP , Com S7906E3.

2.14.1.2 קיימים שני נתבים מרכזיים במתקן המרכזי במרכז הארץ אשר מקשרים את כלל האתרים הנוספים של המזמינה. הקישור בין האתרים מבוסס על קוי מטרו. מבוצע ניטור על איכות קווי התקשורת.

2.14.1.3 על המציע לפרט בנוסף לעיל מה העומס שיצור איסוף הלוג על קוי התקשורת ברשת הרחבה ועל תשתית הרשת הפנימית.

2.14.2 **<u>רכיבי אבטחה</u>**

2.14.2.1 רכיב אבטחה – Firewall – מבית CheckPoint , אשר מגן על הקישור לאינטרנט וכן על התשתית הרחבה.

2.14.2.2 VPN/SSL מבית JUNIPER SA2500 .

2.14.2.3 תוכנות אנטי וירוס – ברשת המזמינה קיים אנטי וירוס מבית **Trend Micro** המותקן על כלל השרתים ותחנות הקצה.

2.14.2.4 שרת רדיוס מבוסס מיקרוסופט (MS IAS) **-** שרת הרדיוס הארגוני ממוקם באזור חייץ ומשרת בעיקר זיהוי לגישה מרחוק.

2.14.2.5 Certificate Authority מבית Microsoft – ברשת המזמינה קיימת תשתית פנים ארגונית windows 2008 המשמשת את המזמינה להנפקת תעודות לשרתים DC, שרתי אפליקציה ולרכיבי התקשורת.

2.14.3 **<u>רכיבים נוספים</u>** - קיימים רכיבים נוספים אשר משרתים את המזמינה, אך אינם בניהול המזמינה. בעתיד יתכן והניהול יעבור אל המזמינה, נדרש לציין תמיכה ברכיב בלבד, ללא ביצוע אינטגרציה. להלן רשימת רכיבים אלו:

2.14.3.1 המזמינה מבצעת שימוש בשירות חדר כספות, אשר מטרתו הינה לבצע את כלל הקישורים החיצוניים בינם לבין גופים וחברות נוספות. חדר הכספות ממוקם באזור

חייץ ומנוהל מקומית. יתכן ותידרש העברת קבצי הלוג של הכספת יועברו למערך ה SIEM.

2.14.3.2 Mail Relay- השרת ממוקם באזור החיץ מבוסס על מערכת לינוקס – freebsd 2.4/2.5 עם postx. השרת מבצע סינון של המיילים הנכנסים לארגון.

2.14.3.3 Microsoft Forefront TMG 2010 – קיים פרוקסי ברשת הארגונית אשר מהווה את ה-GW המרכזי לגלישה אל מול האינטרנט.

2.14.4 **<u>מערכות הפעלה ושירותים מבוססי Microsoft Windows</u>**

2.14.4.1 ברשת המזמינה קיימים שרתי 2008 / Win2003 הממוקמים בשני אתרים מרכזיים (אתר ראשי בירושלים ובבית הדר דפנה) בנוסף ממוקמים שרתים בכל אחד מהאתרים הנוספים של המזמינה. באתרים הגדולים ישנם Domain Controller-ים ושרתי קבצים ובאתרים הקטנים שרתי קבצים.

2.14.4.2 תחנות העבודה מבוססות WinXP / Win7 – נדרש לבצע איסוף לוגים מכ-50 תחנות עבודה.

2.14.4.3 שרתי WEB – ברשת המזמינה מספר שרתי Web מבוססים IIS 6.0-7.5 המשרתים את שלל האפליקציות הפנימית.

2.14.4.4 שרתי SharePoint – מערכות ניהול המסמכים מבוססות SharePoint.

2.14.4.5 ברשת המזמינה שני שרתי Exchange 2007 ב- Cluster הממוקמים בשני אתרים. מתבצעת גישה מתוך רשת המזמינה וכן מחוצה לה באמצעות Outlook web access.

2.14.4.6 בסיסי הנתונים המרכזיים ברשת המזמינה הינם SQL2000/2008 אשר משרתים את המערכות המרכזיות. בסיסי הנתונים מאוד רגישים ומהווים את לב המערכת הן לאפליקציות והן למקורות מידע שונים.

2.14.5 **<u>תשתית וירטואלית</u>**

2.14.5.1 ברשת המזמינה תשתית וירטואלית המבוססת על VMware, ו – Microsoft HyperV.

2.14.6 **<u>גישה מרחוק</u>**

2.14.6.1 Terminal Server – ברשת המזמינה קיימים מספר שרתי Terminal Server המאפשרים עבודה מרוחקת (הן פנימית והן מהבית) על מערכות פנימיות.

2.14.6.2 Citrix – למזמינה תשתית Citrix לשולחן עבודה מרוחק ופרסום אפליקציות.

2.15 <u>פירוט האפליקציות</u>

2.15.1 המזמינה בחרה לקשר בשלב הראשון רק את האפליקציות העיקריות, ולאחר מכן את האפליקציות הנוספות.

2.15.2 שילוב האפליקציות יבוצע בסדר הבא :

סדר השילוב	האפליקציה	הערות
1	**המרכז לגביית קנסות** – מערכת מבוססת MAGIC וכותבת לוגים ל- DB מסוג SQL.	
2	**כלים שלובים** – אפליקציית ליבה חדשה המפותחת עבור המזמינה ע"י חברת TALDOR. המערכת מפותחת כולה על תשתית WINDOWS ומעבירה את הלוגים ל ל- DB מסוג SQL.	
3	**SAP** – תת מערכת של "כלים שלובים" הרגישה עקב ניהולה את מודול הכספים.	
4	**יתר האפליקציות** – כ – 10 אפליקציות מתוכן 6 אפליקציות מבוססת Dynamic CRM.	

2.15.3 **<u>על המציע לפרט:</u>**

2.15.3.1 מה תהא תצורת משיכת הלוג במערכת (פרוטוקול, תצורת קישור חד כיוונית / דו כיוונית, הגורם היוזם).
ההשפעה על משיכת הלוג באפליקציה – האם יידרשו שינויים ברמה האפליקטיבית.

2.15.3.2 מהם האירועים אשר לא ניתן יהיה לאסוף מהשרת בשל אי הבדלה בין אירוע X לאירוע Y במערכות הפעלה Microsoft Windows. כיצד ניתן לפתור את הבעיתיות.
תינתן עדיפות לספק אשר יפתור את הבעיתיות הקיימת ללא תוכנה צד ג'.

2.15.3.3 האם ישנו הבדל בלוגים בגישה לתיבות המייל באמצעות ה- OWA מול גישה רגילה מרשת המזמינה ע"ב תוכנת Outlook מהיבט איסוף הלוגים (כתיבת הלוגים, מיקום הלוג ואיסופו)

2.15.1.4. פירוט הנדרש בסעיף זה יסומן **כנספח יז'4 במענה להצעה**

2.16 <u>חוקים / התראות</u>

2.16.1 יוגדרו חוקים והתראות לכל אחד ממקורות המידע והאפליקציות. החוקים יכולים להיות חוקים פשוטים, חוקי קוראלציה או חוקי אגרגציה, אין הבדל מבחינת המזמינה בסוג החוקים. הגדרת חוק כוללת את זיהוי הרשומה בלוג, קבלת הרשומה במערכת, הגדרת החוק במערכת, בדיקת התראת החוק. חוקים שלא יבדקו ע"י הספק – לא יעברו בדיקות קבלה.

2.16.2 במהלך הפרויקט ידרש הספק הזוכה להגדיר 80 חוקים עבור כלל מערכות התשתית והאפליקציות.

2.16.3 טיוב אירועים – לאחר הגדרת כלל האירועים יבוצע שלב של טיוב האירועים במערכת, שלב הטיוב מחולק לשני חלקים עיקריים :

2.16.4 טיוב ע״י המציע – שלב בו המציע יתחייב לבצע טיוב של האירועים במערכת בכדי להוריד אירועים חלקיים / אירועים אשר לא מתקבל עליהם מידע / אירועים תקולים לרבות קבלת מספר רב של אירועים ממקור ייעודי והטיפול בכך.

2.16.5 טיוב ע״י המזמינה – שלב בו יוחלט אם יש להוריד חלק מהחוקים / להוסיף חוקים / לחדד חוקים במערכת וכו׳. שלב זה יבוצע לאחר תחילת העבודה על כלל המערכות.

2.16.6 בסיס הנתונים במערכת – בשל בקשת המזמינה לשמור רק מידע (Data) ערכי <u>יתחייב המציע</u> כי יבצע <u>טיוב של בסיס הנתונים</u> במספר היבטים:

2.16.6.1 שמירת האירועים שיוגדרו ע״י המזמינה, קרי במידה ומבוצע איסוף של כלל הלוג מהמערכות – לאחר הגעת המידע למערכת, יריץ הספק באופן אוטומטי שגרות אשר ינקו את הלוג ולא ישמרו את המידע ה״לא רלוונטי״ מבחינת המזמינה.

2.16.6.2 הודעות שגיאה / התראות חלקיות – במידה והגיע מידע לא ״שלם״ בלוג, יריץ הספק שגרה אשר מוחקת ו/או מעבירה אירועים אלו לבסיס נתונים אחר.

2.17 <u>תעדוף אירועים</u>

2.17.1 על המערכת להכיל מנגנון תעדוף המשקלל מספר פרמטרים כדוגמת רמת חומרת האירוע, רמת פגיעות מקור המידע ועוד. במידה והמערכת אינה מכילה מגנון פנימי לתעדוף, על המציע לפרט כיצד יוכל לשלב מנגנון תעדוף. פירוט הנדרש בסעיף זה יסומן **כנספח יז׳5 במענה להצעה**

2.17.2 על המציע לפרט מהו מנגנון התעדוף הקיים בתוך המערכת המוצעת, מהם הפרמטרים הבסיסיים הקיימים במערכת, כיצד מבוצע החישוב ומה נדרש על מנת לקנפג במערכת.

2.18 <u>תיחום הבקשה</u>

2.18.1 מרכיבי המערך כוללים את רכיבי התוכנה הנדרשים להקמה ולהפעלה של המערך כמכלול, למעט תשתית התקשורת עצמה. המציע נדרש להציע את מוצרי התוכנה, להקים את המערכת, לדאוג לקבלת הלוג מתוך מקורות המידע השונים והאפליקציות, לבצע אינטגרציה, לבצע הדרכות ולתחזק את המערכת.

2.19 <u>ממשק המשתמש</u>

2.19.1 **<u>כללי הנדסת אנוש</u>**

2.19.1.1 ממשק המשתמש יהיה פשוט, נוח וידידותי למשתמש מבוסס **web** או **Gui** חלונאי (בהתאמה לביצועים). הממשק יתמוך בשילוב שדות בעברית ואנגלית לרבות הצגת האירוע, התגובה והתחקור אירוע.

2.19.2 **<u>מסכים נדרשים</u>**

2.19.2.1 מסכי המערכת הבסיסיים הנדרשים יאופיינו ויוגדרו בהתאמה לדרישות המזמינה. המסכים המרכזיים הנדרשים הינם מסך הכניסה למערכת, מסך מרכזי ראשי, מסך אירועים, מסך התגובה, מסך התחקור, מסך דו״חות, מסך בקרה / מנהלים.

2.19.2.2 מערכת המציע תספק מנגנון הרשאות מפורט, וממשק מתאים עבורו, המאפשר להגדיר הרשאות צפייה וכתיבה פרטניות למשתמש או קבוצת משתמשים, לכל מסך ולכל שדה במסך.

2.19.2.3 ממשק ההרשאות ינוהל ע"י מנהל אבטחת המידע ומי מטעמו.

2.19.3 **<u>מסכי מערכת ה-SIEM</u>**

2.19.3.1 על המציע לפרט על כל אחד מהמסכים בנפרד האם המערכת תומכת באופן אינהרנטי במסך המבוקש, האם השינויים הינם שינויים בגדר "הגדרות" או שנדרש לבצע פיתוח.

2.19.3.2 על המציע לפרט על כל אחד מהמסכים בנפרד האם קיימות (ואם כן מה הן) ההגבלות הקיימות במערכת אשר ימנעו את השלמת הבקשה.

2.19.3.3 פירוט הנדרש בסעיף זה יסומן **כנספח יז'6 במענה להצעה**

2.19.4 **<u>פירוט המסכים הנדרשים:</u>**

המסכים הנדרשים	
מערכת SIEM/SOC	מסך לוגין (כניסה למערכת)
	מסך מרכזי
	מסך אירועים
	מסך פירוט האירוע
	מסך תחקור אירוע
	מסך דו"חות וסטטיסטיקות
	מסך Knowledge base

2.19.5 **<u>מסך כניסה למערכת – מערכת ה-SIEM</u>**

2.19.5.1 מסך כניסה ראשי לכלל מערכת ה- SIEM יכיל את שדות זיהוי המשתמש. כאשר נדרש ליישם שני סוגי זיהוי: הראשון יהא זיהוי משתמשים על בסיס תעודה דיגיטלית – כרטיס חכם ישירות אל המערכת או כחלק מהזיהוי אל מול הדומיין. השני יהא זיהוי שם משתמש וסיסמא – מסך ה-SIEM המרכזי אשר יפתח על בסיס משתמש גלובלי במוקד.

2.19.5.2 נדרש כי יהא הבדל בין הזיהוי של עובד על המערכת לבין משתמש המוקד הכללי הן בהיבט יכולות ביצוע והן בהיבט מדיניות המשתמשים והסיסמאות שתוכל על המשתמש.

2.19.6 **<u>מסך מרכזי – מערכת ה-SIEM</u>**

2.19.6.1 המסך הראשי במערכת בו יוצגו האירועים המתקבלים בתשתית. המסך יחולק לשלושה חלקים:

2.19.6.1.1 חלק ראשון – אירועי אבטחת המידע – חלק בו יוצגו אירועי אבטחת המידע הארגוניים על בסיס חיתוך זמן ורמת תעדוף.

הנחיות יסוד בהצגת האירועים במסך:

- לא כל האירועים במערכת יוצגו אלא רק אירועים מהרמה שתקבע באפיון המפורט ומעלה.
- לאחר X שעות שיקבעו באפיון תועלה רמת החומרה / תעדוף של האירוע באחת – ויועלה האירוע בחיתוך האירועים.
- לאחר Y שעות שלא בוצע טיפול באירוע יועבר מייל למנהל אבטחת המידע על אי טיפול באירוע עם כלל המידע על האירוע.
- שם האירוע נדרש להופיע בעברית. שם האירוע יותאם לגורמים אשר אינם מבינים באבטחת מידע.
- המידע שיוצג על האירוע יהא: תאריך וזמן, שם האירוע – כפי שהוגדר שיוצג, מקור המידע עליו בוצע האירוע, רמת החומרה, כתובת / מקור המידע אשר ביצע את האירוע.
- לחיצה – דבל קליק / לחיצה ימנית על האירוע – תפתח מסך נוסף – שלא יפריע למסך הקיים עם פרטים נוספים על האירוע בהתאם לכל מקור המידע (האפיון יבוצע במהלך היישום). בכל מקרה לא תידרש לחיצה נוספת בכדי לקבל את המידע על האירוע.
- כחלק מקבלת המידע על האירוע – יועלה מידע על האירוע.
- במקביל לקבלת המידע ניתן יהיה להחליט על ביצוע הפעולה הראשונית – התגובה הראשונית לאירוע: פתיחת אירוע במסך אירועים או סגירת האירוע – הורדת האירוע מהמסך הראשי ללא תיעוד במסך אירועים.
- במידה והוחלט על פתיחת אירוע במסך אירועים יועבר האירוע מחלקו הראשון של המסך לחלקו השני. במידה והוחלט על הורדת האירוע מהמסך – יעלם האירוע במיידית. נדרש כי לא יהא הצורך לבצע Refresh למסך.

2.19.6.1.2 **חלק שני – סטטוס אירועים מטופלים** – אירועים אשר להם נפתח אירוע במסך אירועים. בחלק השני יוצגו כלל האירועים אשר המוקדן / הבקר פתח עליהם אירוע במסך אירועים. האירועים יוצגו בהתאם לחומרה ולזמן פתיחת האירוע.

2.19.6.1.3 **חלק שלישי – תפריט / סרגל כלים** - באמצעותו ניתן יהיה לגשת לשאר המסכים במערכת כדוגמת מסך האירועים המלא וכו'.

2.19.7 **<u>מסך האירועים</u>**

2.19.7.1 כיוון שהמסך הראשי מציג אירועים רק בעלי חומרה / תעדוף מרמה מסוימת, יש לאפשר גישה לגורמים מסויימים במערכת לכלל האירועים המופיעים במערכת. מסך האירועים במערכת יחולק בשלושה אופנים (בהתאם להחלטה הסופית באפיון המפורט):

- האופן הראשון – הצגת כלל האירועים הקיימים במערכת בחיתוך של רמת חומרה / תעדוף וזמן קבלת האירוע.
- האופן השני – הצגת האירועים בהתאם למקור המידע בחיתוך של רמת חומרה / תעדוף וזמן קבלת האירוע.

- האופן השלישי – הצגת האירועים בהתאם לסביבת העבודה שתוגדר – קרי הצגת כלל מקורות המידע הקיימים באותה הסביבה בחיתוך של רמת חומרה / תעדוף וזמן קבלת האירוע.

2.19.7.2 ממסך האירועים ניתן יהיה לבצע את הפעולות הבאות:

- לקבל פירוט מלא של המידע על האירוע
- פתיחת אירוע במסך אירועים.
- סגירת אירוע – הורדת האירוע מהמסך.

2.19.7.3 כיוון שמסך זה משרת עיקר את הגורמים המבינים באבטחת מידע, נידרש כי ניתן יהיה לקנפג את המסך בקלות.

2.19.7.4 המסך הראשי יאפשר לקבל מידע על אירועים שטרם נסגרו, המסך נדרש להכיל:

- מספר אירוע
- תאריך אירוע
- שם אירוע
- גורם מעדכן
- גורם מטפל
- חומרת האירוע

2.19.8 **<u>מסך פירוט האירוע</u>**

2.19.8.1 כיוון שבמסך הראשי מוגבל המידע הניתן להצגה על האירוע, לחיצה כפולה על האירוע או לחצן ימני יאפשרו קבלת מידע מפורט על האירוע. המידע אשר נדרש להתקבל הינו כלל המידע המתאפשר מלוג המערכת.

2.19.8.2 במסך זה יוצג רק מידע רלוונטי כפי שיוחלט ע"י המזמינה, מידע שאינו רלוונטי יידרש להיות "מוסתר" או שיורד מהמסך, כך שהמסך לא יכלול שדות ריקים ו/או לא קריאים.

2.19.8.3 בשלב האפיון המפורט יוחלט כיצד יראה המסך ומהו המידע הרלוונטי בהתאם לכל אחד ממקורות המידע. המידע הבסיסי הנדרש להופיע:

מספר האירוע	
תאריך:	dd/mm/yy
שעה:	hh:mm
תשתית	סביבת העבודה עליה בוצע האירוע
מקור מידע	מקור המידע אשר עליו אירע האירוע – שם מחשב / מערכת וכו'
שם שרת	שם השרת / מערכת עליו בוצע האירוע
כתובת IP	כתובת IP של מקור המידע
חומרת אירוע	חומרת האירוע
גורם מבצע	הגורם שביצע את האירוע כדוגמת משתמש / שרת
תיאור האירוע	הסבר על מהו האירוע, השלכות וכו'

אגרגציה	שילוב של מספר אירועים יחד
חוק במערכת	החוק במערכת אשר העלה את האירוע

2.19.8.4 מסך התגובה לאירוע הינו המסך באמצעותו יטפלו באירועי האבטחה הארגוניים - הן המגיעים מה-SIEM/SOC והן אירועי אבטחה תפעוליים.

2.19.8.5 המסך יכיל חלק אינפורמטיבי אשר יאפשר קבלה של מידע ממערכת ה-SIEM/SOC אשר תעביר את הנתונים המלאים על האירוע. בחלק זה יהיה ניתן לקבל את כלל המידע על האירוע, על המערכות הקשורות, אנשי הקשר אשר נדרש ליידע וכו'.

2.19.8.6 במהלך ההטמעה יבוצע אפיון מפורט של המסך, המסך יכיל לכל הפחות את השדות הבאים:

- הפרטים הבסיסיים של האירוע
- סטאטוס הטיפול באירוע - חיתוך של כמות המשימות הנדרשות לביצוע אל מול הביצוע בפועל.
- הסבר מילולי על האירוע
- פירוט האירוע - מידע המתקבל מה-SIEM/SOC המכיל את כל הפרטים על האירוע.
- מיקום האירוע
- מידע - פרטים על המשתמש / מבצע הפעולה / הגורם - במידה וניתן מתקבלים מהפורטל הארגוני / Active Directory.
- תגובות לאירוע (מנהליות / טכנולוגיות)
- הערות לגבי האירוע
- אנשי קשר - הגורמים הרלוונטיים לאירוע / למקור המידע / סביבת העבודה - אשר נדרש ליידעם במידה וקיים אירוע. נדרש כי תהא אפשרות לשלוח מייל ליחידים ו/או לקבוצות יחד עם כל פרטי האירוע.
- תאריך ושעת סיום האירוע (לאחר סגירת אירוע אין אפשרות לפתוח אותו)

2.19.9 **<u>מסך תחקיר האירוע</u>**

2.19.9.1 תחקיר אירוע תחקיר אשר יבוצע על ידי מנהל אבטחת מידע או מי מטעמו.

2.19.9.2 דרישות בסיסיות לתחקור:

- לכל תחקור יוקצה אינדקס - מספר רץ חד ערכי.
- לא ניתן יהיה לפתוח תחקור לאחר שהגורם המבצע סגר את התחקור. במידה ונדרשות השלמות, יפתח תחקור נוסף עם המידע בתחקור הקודם.
- כלל הפרטים של האירוע יופיעו כשדות ללא שינוי.
- מסך תחקור אירוע יתחלק לשלושה חלקים –
- סרגל תחקירים - אשר באמצעותו ניתן יהיה לחפש תחקיר קיים.
- השלמת התחקיר. השדות המלאים בתחקיר יוגדרו במהלך האפיון המפורט.

- הסקת מסקנות - הגורם המטפל/המתחקר ישלים את ההתייחסות לאירוע כדוגמת למה אירע האירוע - פעילויות נוספות אשר יש לבצע להמשך הטיפול - זאת במטרה לאפשר סגירת האירוע ולהמשיך לטפל ו/או לבצע פעילות מונעת.

2.19.10 **<u>מסך דו"חות וסטטיסטיקות</u>**

2.19.10.1 דו"ח אוטומטי - אשר ייווצר ברגע סגירת האירוע ברגע בו ישלח סטאטוס "סגור" על המערכת ליצור pdf ולבצע חתימה דיגיטלית עם תעודה על התחקיר. דו"חות התחקירים ישמרו בספריה ייעודית / כספת ולא תינתן גישה לשינוי התחקור אלא לקריאה בלבד.

2.19.10.2 דו"חות סטטיסטיים של אירועים בחיתוך - טווח רמת חומרה מול סטאטוס הטיפול באירוע. דו"חות שוטפים של המוקד - כלל הדו"חות אשר יוגדרו להוצאה על בסיס יומי / שבועי / חודשי / רבעוני ושנתי.

2.19.10.3 תחקורי אירוע - שתי רמות של תחקורי האירוע - תחקורים אוטומטיים ותחקורים רוחביים.

2.19.10.4 סטטיסטיקות - כלל הסטטיסטיקות שיידרשו הן ממערכת ה-SIEM/SOC כדוגמת כמות האירוע למקור מידע X בזמן Y בפילוג של Z.

2.19.10.5 דו"ח סטאטוס אירועים - אירועים פתוחים אל מול סטאטוס הטיפול באירוע. הדו"ח יוצג בחיתוך רמת חומרת / תעדוף האירוע אל מול סטאטוס הטיפול.

2.19.11 **<u>מסך ה- Knowledge base</u>**

2.19.11.1 מסך ה-Knowledge base הינו מסך אשר יאפשר קבלת מידע ונתונים להחלטה וטיפול באירוע / סגירת האירוע, קרי על פתיחת / אי פתיחת אירוע במסך אירועים. המסך הינו מסך חשוב, כיוון שנלקחת בחשבון העובדה כי המוקדנים / הבקרים אשר מתפעלים את המערכות אינם מעורים בתחום אבטחת המידע.

2.19.11.2 המסך הנדרש מחולק לשני תתי מסכים: תת מסך ראשון – מסך המציג את המידע על האירוע ותת מסך שני – מסך הזנה – אשר כל גורם מוסמך מאבטחת מידע יוכל להזין מידע על אירועים קיימים / חדשים.

2.19.11.3 נדרשש לצרף צילומי מסך המדגימים את כל אחד מהמסכים עם ציון סוג המסך בכל צילום, הצילומים יסומנו **כנספח יז'7 במענה להצעה**

2.20 <u>תהליכים</u>

2.20.1.1 לגבי כל תהליך ותהליך המפורטים בסעיף להלן , על הספק להתייחס באופן הבא: על הספק להציג את התהליך במערכת בשלבים מתחילת התהליך ועד סופו. על הפירוט לכלול את פעולות המערכת, לאילו רכיבים המערכת פונה, באילו פרוטוקולים, תתי תהליכים של אבטחה – זיהוי, הרשאות וכו'.

2.20.2 <u>תהליך העברת המידע ממקור המידע אל מערכת האיסוף</u>

2.20.2.1 על הספק לפרט את תהליך העברת המידע ממקור המידע אל מערכת האיסוף, בדגש על מקורות המידע השונים. יש להוסיף שרטוט.

2.20.3 <u>תהליך חיות מקור מידע</u>

2.20.3.1 על הספק לפרט מה תהליך חיות מקור המידע, קרי כיצד ידע כי מקור המידע מדווח למערכת. במידה והמערכת אינה מכילה תהליך חיות אינהרנטית - על הספק לפרט איך יטמיע תהליך חיות במערכת.

2.20.4 <u>תהליך איסוף ממקור המידע – בסיס נתונים נפל / אין קישור לבסיס הנתונים</u>

2.20.4.1 על הספק לפרט מה קורה במצב בו בסיס הנתונים נפל, האם נשמרים / נאגרים הנתונים במקור המידע, כיצד תהליך ההתאוששות.

2.20.5 <u>תהליך שדרוג מערכת</u>

2.20.5.1 על הספק לפרט ברמה הכללית את תהליך שדרוג המערכת – שלבים, השלכות.

2.20.5.2 דו״חות ושאילתות – על המערכת להפיק דו״חות וסטטיסטיקות עצמאית. הדו״חות יופקו בתהליך יזום ע״י משתמש מורשה ו/או ע״י טריגר (כדוגמת scheduler) בפורמט pdf
ו-html, יוצגו בפורטל האבטחה ובנוסף ישלחו באמצעות דואר אלקטרוני לגורמים שונים אצל המזמינה – עפ״י רשימת תפוצה מוגדרת מראש. הדו״חות יופקו בפורמט שיוגדר ע״י המזמינה (לוגו, יחידת אבטחת מידע וכו׳).

2.20.5.3 פרוט הנדרש בסעיף זה יסומן **כנספח יז׳8 במענה להצעה**

2.21 <u>אבטחת מידע</u>

2.21.1 **<u>כללי – הבהקים</u>**

2.21.1.1 המידע הקיים ברשתות המזמינה הינו מידע רגיש בהיבט צנעת הפרט, בהתאמה לכך נדרש יישום אבטחת מידע במערכת.

2.21.2 **<u>ארכיטקטורה</u>**

2.21.2.1 ארכיטקטורת המערכת תהא ארכיטקטורה מרכזית.

2.21.2.2 המערכת תמוקם בסגמנט ייעודי ותאסוף מידע מכלל מקורות המידע ברשת המזמינה.

2.21.2.3 על שליחת ההתרעות ממקור המידע אל המערכת המרכזית להתבצע באופן מאובטח (מזוהה ומוצפן). על המציע לפרט כיצד מבוצע הזיהוי וההצפנה.

2.21.3 **<u>הזדהות</u>**

2.21.3.1 זיהוי אל מול המערכת יבוצע באמצעות כרטיס חכם ממשלתי. הזיהוי יתאפשר אל מול האפליקציה באמצעות התעודה הדיגיטלית או לחלופין אל מול הדומיין. על הספק לפרט את יכולת תמיכת המערכת בזיהוי באמצעות תעודה דיגיטלית, במידה ובשלב זה המערכת אינה תומכת, יש להגדיר מתי תהא התמיכה (שבועות / חודשים).

2.21.3.2 על המערכת לאפשר יישום מדיניות סיסמאות – אורך, מורכבות, נעילה, היסטוריה וכו׳ בהתאמה למדיניות הקיימת במזמינה, למשתמשים גנריים כדוגמת משתמש המוקד.

2.21.3.3 זיהוי תוכנה – על הרכיבים במערכת להיות בעלי מנגנון חיתום שלא יאפשר ריצה של תוכנה זדונית או עויינת.

2.21.4 **<u>הרשאות</u>**

2.21.4.1 ההרשאות במערכת יינתנו על בסיס ה"צורך לדעת". על המערכת לתמוך בהגדרת מספר תפקידים בעלי הרשאות שונות: לדוגמא:- מוקדן, מנהל תשתיות, מנהל אבטחת המידע, מנהל מערכת תפעולי, מנהל מערכת אבטחתי, מבקר. יישום ההרשאות יוגדר לכלל רכיבי המערכת, כאשר משתמש לא יקבל הרשאה שאינה מוגדרת בתפקידו.

2.21.4.2 על המערכת להתממשק למערכת ה- AD של המזמינה להגדרת המשתמשים והרשאותיהם.

2.21.5 **<u>הצפנה</u>**

2.21.5.1 על התווך בין מקור המידע למערכת המרכזית להיות מאובטח ומוצפן. על הספק לפרט את שיטת ההצפנה (מערכי אלגוריתמים, ארכי מפתחות, רמת חוזק על פי תקן מוכר), מידע על ניהול מפתחות וניהול מערכי ההצפנה ברשת .

2.21.6 **<u>ניהול הרכיב</u>**

2.21.6.1 ניהול הרכיב יבוצע מעמדות מוגדרות מראש תוך זיהוי והצפנה של התווך. על הספק לפרט מהם פרוטוקולי הניהול.

2.21.7 **<u>בקרה</u>**

2.21.7.1 המערכת תאפשר בקרה על כלל פעילויות הניהול שיבוצעו עליה – כדוגמת זיהוי, שינוי הגדרות, עדכונים וכו'.

2.21.7.2 המערכת תתעד את כל האירועים ותרשום לוג מפורט. על הלוג להיחתם או להיות מוגן מפני שינוי הנתונים מרגע שנרשמו. על רישום הלוג להיות "Tamper proofed", נגיש וקריא למערכות חיצוניות.

2.21.7.3 על המערכת עצמה לשלוח אירועים ולהציגם במידה וארע אירוע על המערכת המרכזית ו/או בסיס הנתונים.

2.21.8 **<u>הקשחות</u>**

2.21.8.1 על המערכת להיות מוקשחת בהתאמה למדיניות המזמינה. ההקשחה חלה הן על מערכות ההפעלה והן על בסיס הנתונים.

2.22 <u>נפחים עומסים וביצועים</u>

2.22.1.1 על הספק לפרט מהם ביצועי המערכת לכל אחד ממקורות המידע ומהן העומסים אשר תוכל המערכת לעמוד בהם.

2.22.1.2 ביצועים : דיווח הרכיבים לבסיס הנתונים לא יעלה על 3 דקות. תצוגת האירוע לא תעלה על 5 שניות מזמן קבלת האירוע בבסיס הנתונים.

2.22.1.3 עומסים – על המוצר לתמוך ברישום כמות של 3,000 אירועים בשנייה

2.22.1.4 פירוט הנדרש בסעיף זה יסומן **כנספח יז'9 במענה להצעה**

2.23 גיבויים ושרידות

2.23.1.1 המערכת תקושר למערכת האחסון המרכזית ברשת המזמינה. שרתי המערכת יגובו בהתאם לסטנדרטים הקיימים במזמינה. הספק ידרש למלא תיק שרת שיגדיר מהם הקבצים הנדרשים לגיבוי ומה תצורת הגיבויי המועדפת.

2.23.1.2 לפני העלאה לייצור יבוצע Image לשרתים למטרות שחזור.

2.23.1.3 שחזור הנתונים ייבדק, כאשר הספק ידרש להעלות את הנתונים הקיימים מגיבוי בכדי לבדוק תקינות הגיבוי ולבחון את השלכות השחזור.

2.23.1.4 נדרש יהיה להגדיר תצורה לשימור הנתונים למניעת איבודם, במידה ואחד מהרכיבים "יפול", הספק יידרש לתת פתרון לכל אחד מהרכיבים הקיימים בשרשרת.

2.23.1.5 יש להגדיר זמן התקנת המוצר ללא קונפיגורציה, במידה והשרת נפל, כמה זמן יקח עד ששרת זה יהיה פעיל שוב, ללא יישום קונפיגורציה.

2.24 תכנית עבודה

2.24.1 עקרונות מנחים להטמעת המערכת

2.24.1.1 כלל העבודה בפרויקט תבוצע כצוות, ההחלטות הסופיות יתקבלו ע"י המזמינה.

2.24.1.2 העבודה בפרויקט תבוצע באופן מתודולוגי אשר יכלול את שלב האפיון, העיצוב, העיצוב המפורט, הטמעת מערכת, בדיקות קבלה ותיעוד המערכת. העבודה תבוצע בהתאם לתוכנית עבודה משותפת שתקבע בתחילת הפרויקט. המציע יקצה מנהל פרויקט שיהיה Point of Contact היחידי למזמינה.

2.24.1.3 ארכיטקטורת הטמעת התשתית - אפיון ועיצוב מפורטים יבוצעו לאחר בחירת זוכה.

2.24.1.4 הטמעת המערכת תבוצע ע"פ 7 השלבים כפי שמפורט בפרק זה, וכמפורט בהמשך.

2.24.1.5 המזמינה מבצעת עבודה עם מערכות המחשוב במשך 24 שעות, 7 ימים בשבוע. הטמעת המערכת לא תפגע בעבודה השוטפת של המזמינה אל מול מערכות פנימיות, במידה ותידרש הפרעה (השבתה, מניעת פעילות המערכת) תהא מינימלית, תתוזמן מראש, כאשר יינתן חלון זמן מתאים לספק לביצוע הפעילות.

2.24.1.6 במהלך ההטמעה יבוצעו פגישות טכניות וסטטוס לעדכון השלבים שבוצעו והשלבים הבאים ולפתרון בעיות.

2.24.1.7 להקמת המערכת תוקצה לספק תחנת עבודה וכלי עבודה בסיסיים כדוגמת טלפון, קישור לאינטרנט וכו. באם קיימות דרישות נוספות יש לפרטן בהצעה, כדי שהמזמינה תוכל להיערך לנושא.

2.24.1.8 התקנות ברשת המזמינה דורשות תיאום מראש עם כלל הגורמים הרלוונטים, התקנה שלא תתואם לא תבוצע.

2.24.1.9 התקנות על מערכות ייצוריות יכולות להתבצע אך ורק לאחר קבלת אישור מנהל התשתיות, על הספק להיערך בהתאם. על הספק ללמוד את מגבלות המזמינה לפני בניית תוכנית העבודה המפורטת.

2.24.1.10 לפני כל התקנה תבוצע פגישה עם מנהל התשתיות או מי שימונה על ידו למשימה, במטרה להבהיר מה המשמעות של ההתקנה, כיצד עלולה ההתקנה להשפיע על תהליכי העבודה או פעילותן של מערכות המחשוב אצל המזמינה, הסבר על ההתקנות, דרכים ונהלים לטיפול בבעיות אפשריות וכו׳.

2.24.1.11 יקבעו ישיבות שבועיות להפקת לקחים במהלך הפרויקט של הספק ונציגיו עם נציגי המזמינה, הספק מחויב להיות נוכח בישיבות וכן לקחת בהן חלק פעיל.

2.24.2 **<u>תוכנית עבודה כללית לפרויקט:</u>**

2.24.2.1 תוכנית העבודה תחולק בהתאם לשלבי הפרויקט.

2.24.2.2 על הספק לפרט את שלבי העבודה הכלליים המפורטים מעלה וכן שלבי לימוד, אפיון, עיצוב, התאמות (כולל זמן פיתוח), פיילוט, הקמת המערכת, הטמעה, אינטגרציה, דו״חות ותוספות, בדיקות עומסים, בדיקות קבלה, הדרכה, תיעוד, נהלים, תחזוקה.

2.24.2.3 על הספק לצרף גאנט בפורמט MS-Project שיכיל את כלל השלבים המוצעים.

2.24.2.4 על הספק לפרט בתוכנית העבודה את הפעילויות התלויות בספק ואת הפעילויות הנוספות שידרשו מהמזמינה (כדוגמת פעולות הכנה וכו׳), זאת במטרה לקצר את זמן הפעילות.

2.24.2.5 השלבים להלן מפורטים כבסיס לתכנית, והספק נדרש להתייחס אליהם ולכלול אותם בתכנית שתוצע על ידו, כך שהלו״ז לסיום השלבים יהיה בהתאמה ע״פ הנדרש בפרק 0:

אבן דרך	הפעילות	תתי פעילות מרכזיים	אחריות
ראשונה	**אפיון ארכיטקטורת המוצר, וממשק המשתמש**	פגישות ללימוד הארכיטקטורה הקיימת ודרישות המזמינה	ספק, מזמינה
		ביצוע עיצוב ארכיטקטוני לשילוב המערכת	ספק, מזמינה
		הזמנת חומרה נדרשת	ספק, מזמינה
		הוצאת מסמכי אפיון, עיצוב והוכחת יכולת	ספק, מזמינה
		תיאומים, קביעת תאריכי ושלבי התקנה	ספק, מזמינה
		לימוד מקורות מידע והאפליקציות המפורטות במפרט	ספק
		אפיון מפורט של המסכים הנדרשים בסעיף 1.15	ספק
		עיצוב המסכים	ספק
שנייה	**הקמת התשתית, התקנת המוצר בקונפיגורציה בסיסית, והתאמתו לדרישות המזמינה**	הקמת תשתית מערכת ה- SIEM באתר הראשי	ספק
		התקנת מערכת ה SIEM באתר הראשי כולל רישוי לשנה	ספק
		בניית המסכים המבוקשים בסעיף 1.15	
		הקמת רכיבי הקישור / שרתי הביניים לתשתית	ספק
		ביצוע בדיקות קבלה, ותיקונים על פי הנדרש	ספק, מזמינה
		ביצוע הדרכה בסיסית	ספק

אבן דרך	הפעילות	תתי פעילות מרכזיים	אחריות
שלישית	**קישור מקורות מידע תשתיתיים ותקשורתיים**	תהליך לכל אחד ממקורות המידע: עיצוב תצורת קישור מקור המידע למערכת המרכזית קישור טכנולוגי של מקור המידע במידה ולא קיים פרסר, בניית פרסר למקור המידע הגדרת החוקים הרלוונטיים למקור המידע בחינת ישימות החוקים בדיקת עומסים וביצועים במערכת	ספק
		הוצאת מסמך המגדיר את החוקים והקורלציות הדרושות לכל אחד ממקורות המידע - יינתן עד שבועיים לאחר עיצוב תצורת הקישור.	המזמינה
		הטמעת קישורים לרכיבי אבטחה	ספק
		הטמעת קישורים לשרותים מבוססי Windows	ספק
		הטמעת רכיבי התקשורת	ספק
		הטמעת בסיסי הנתונים	ספק
		ביצוע בדיקות קבלה, ותיקונים על פי הנדרש	ספק, מזמינה
		ביצוע הדרכה	ספק
רביעית	**קישור אפליקציית מג"ק**	הוצאת מסמך המגדיר את החוקים והקורלציות הדרושות לאפליקצייה	מזמינה
		הגדרת תצורת קישור האפליקציות למערכת המרכזית	ספק
		הוצאת מסמך עיצוב מפורט לקישור האפליקציה למערכת ה SIEM	ספק
		קישור האפליקציה – קישור טכנולוגי / העברת לוג האפליקציה, בניית פרסר	ספק
		הגדרת חוקים	ספק
		בדיקת ישימות החוקים	ספק
		ביצוע בדיקות קבלה, ותיקונים על פי הנדרש	ספק, מזמינה
		ביצוע הדרכה	ספק
חמישית	**קישור אפליקציית כלים שלובים**	הוצאת מסמך המגדיר את החוקים והקורלציות הדרושות לאפליקצייה	מזמינה
		הגדרת תצורת קישור האפליקציות למערכת המרכזית	ספק
		הוצאת מסמך עיצוב מפורט לקישור האפליקציה למערכת ה SIEM	ספק
		קישור האפליקציה – קישור טכנולוגי / העברת לוג האפליקציה, בניית פרסר	ספק
		הגדרת חוקים	ספק
		בדיקת ישימות החוקים	ספק

אבן דרך	הפעילות	תתי פעילות מרכזיים	אחריות
		ביצוע בדיקות קבלה, ותיקונים על פי הנדרש	ספק, מזמינה
		ביצוע הדרכה	ספק
שישית	**קישור יתר אפליקציות המזמינה**	הוצאת מסמך המגדיר את החוקים והקורלציות הדרושות לאפליקצייה	מזמינה
		הגדרת תצורת קישור האפליקציות למערכת המרכזית	ספק
		הוצאת מסמך עיצוב מפורט לקישור האפליקציה למערכת ה SIEM	ספק
		קישור האפליקציה – קישור טכנולוגי / העברת לוג האפליקציה, בניית פרסר	ספק
		הגדרת חוקים	ספק
		בדיקת ישימות החוקים	ספק
		ביצוע בדיקות קבלה, ותיקונים על פי הנדרש	ספק, מזמינה
		ביצוע הדרכה	ספק

2.24.2.6 בסיום הפרויקט יועבר תיק תיעוד מערכת מפורט לצוות התשתיות של המזמינה כמפורט בהמשך בסעיף 1.20.6.

2.25 <u>מקום ביצוע העבודה</u>

2.25.1 ככלל העבודה מבוצעת באתר המזמינה בירושלים ואתר נוסף בארץ. הספק יידרש לגשת לכל אחד מהאתרים הרלוונטיים. פיתוח המסכים יכול להתבצע בבית המציע, עם זאת לא ניתן יהיה להוציא מידע רגיש מרשת המזמינה. האחריות ללוגיסטיקה, אמצעי תקשורת, אמצעי תחבורה ותובלה וארגון העבודה יהיו באחריות מלאה של המציע.

2.26 <u>איכות ובקרה</u>

2.26.1 המזמינה רשאית לבקר באופן שוטף את העבודה המתבצעת ולדרוש כל מידע רלוונטי. הספק יתחייב לתקן את התקלות שדווחו על ידי המבקר. מידי שבוע יעביר הספק דו"ח התקדמות מפורט ותיערך פגישת עבודה בינו לבין מנהלת הפרויקט בה ילובנו הבעיות, ידונו המהלכים שבוצעו ויתואמו המהלכים הבאים. לדוחות ההתקדמות יצורפו תרשימי גאנט מפורטים המשקפים את סטאטוס הפרויקט ביחס לתכנון.

2.27 <u>תפעול שוטף</u>

2.27.1 התפעול השוטף של המערך לאחר מסירתו ועמידה בכל בדיקות הקבלה, יבוצע ע"י אנשי התפעול של המזמינה.

2.27.2 על הספק לקשר את מתחזקי המערכת במזמינה לרשימת Mailing List שתיידע את המתחזקים על נושאי תפעול שוטפים – עדכוני גרסאות, חדשות הספק, וכו'.

2.27.3 התפעול השוטף במהלך ההטמעה יהא באחריות הספק עד לסיום ההטמעה ולהעברת המערכת לייצור ולשליטת המזמינה באורח מלא.

2.27.4 הספק יתעד כל תקלה במערכת תקלות במטרה ללמוד ולהפיק לקחים לעתיד.

2.27.5 הספק ידאג לביצוע גיבויים למידע הערכי במערכות ולשחזור הנתונים אם ידרש.

2.27.6 תקלה שאינה משביתה את הרכיב במערכת תטופל עד כשבוע לאחר זיהוי התקלה.

2.27.7 הספק יבצע בדיקות תפעוליות למערכת במהלך הקמתה. ההתייחסות למערכת הינה כי המערכת הינה מערכת ייצורית לאחר סיום בדיקות הקבלה והעלאתה לאויר.

2.28 <u>תיעוד מערכת</u>

2.28.1 תכולת תיק תפעול:

- הסברי מערכות ורכיבים
- אפיון ועיצוב הטמעת הפתרון
- ספרות מלאה על כל רכיבי ההצעה
- תיעוד מלא של אופן התקנת הרכיבים וקבצי ההתקנה על מנת לאפשר שחזור ההתקנה ללא צורך ברכיבים נוספים.
- תיעוד הגדרות במערכת
- נוהלי התקנה, תחזוקה, תפעול וטיפול מונע.
- פרטי הספק הנותן שירות.
- ספרות מלאה לכל רכיבי הציוד והתוכנה.
- כל חומר עזר נוסף לצורך תחזוקה וטיפול במערכת.

2.28.2 במהלך הפרויקט יכתוב הספק נהלים פנימיים מתאימים לתפעול שוטף בשפה העברית ובמבנה הנוהל המקובל במזמינה. כל הנהלים ייכללו במסגרת תיק תפעול, שיכיל את כל ההנחיות הדרושות לתפעול השוטף של המערכת - עדכונים ושדרוגים, מעקב אחר השרתים, טיפול בתקלות, גורמים אליהם יש לפנות במקרה תקלות וכד', פירוט הנהלים הנדרשים:

- נוהל תפעול יומי של המוקד – חיות מערכת, בדיקות בסיסיות וכו'.
- נוהל טיפול בתקלה – דרג א' – הגדרת השלבים הבסיסים לביצוע בעת תקלה.
- נוהל שדרוג מערכת – פירוט השלבים של שדרוג מערכת.
- נוהל טיפול במצב בו הסוכן לא מתפקד / אין איסוף מידע מצד ה- Client.
- נוהל טיפול במצב בו שרת האיסוף אינו מתפקד.
- נוהל מעבר לאתר גיבוי - טכנולוגי.
- נוהל תחזוקת מערכת ה- HelpDesk.
- נוהל הוספת מקור מידע למערכת.
- נוהל הגדרת חוקים במערכת.
- נוהל הגדרת דו"ח.

2.29 <u>שירות ותחזוקה</u>

2.29.1 בתקופת האחריות יהיה הספק אחראי לתקינות המערכות שסופקו על ידו, ולמתן התמיכה למערכות. באחריות הספק לתקן או להחליף כל רכיב במערכת אשר יצא משימוש בתקופת האחריות.

2.29.2 תקופת האחריות של שלוש שנים תכלול, ללא תוספת תשלום, שירות תחזוקה ותיקונים, הגעה לאתר המזמין על פי קריאה לביצוע תיקונים, ביצוע תיקונים לרכיבים שסופקו.

2.29.3 ביצוע תיקונים לתקלות שאינן מכוסות באחריות יבוצע במחיר של עלות שעת עבודה (שעת עבודה לא תעלה על עלות מחירון הספק) ועלות חלקי חילוף על פי מחירון הספק, או מחירון שיוצע למזמינה, (הכולל הנחת ספק) מתן תשובות לשאלות ולבעיות באמצעות הטלפון לכלל הגורמים המקצועיים המעורבים בהפעלת המערך.

2.29.4 תקופת השירות של יצרן התוכנה תהא 10 שנים לפחות שתכלול עדכוני תוכנה, התאמת גרסאות, תיקון באגים במערכת, והתאמה לשפה הרלונטית.

2.29.5 תקופת השירות של הספק תהא 5 שנים, ללא יכולת ביטול מצדו ובכפוף לחוזה תחזוקה שיחתם בין הצדדים. השירות יכלול את כלל מרכיבי המערכת כולל חלקים שפותחו ע"י הספק.

2.29.6 על הספק להתחייב לספק שירות ותחזוקה באתרי הלקוח.

2.30 <u>מרכז תמיכה (HelpDesk (Call Center</u>

2.30.1 המענה הראשוני יינתן ע"י המזמינה. על הספק להציע הדרכות, ונהלים מפורטים לפתרון תקלות בדרג הבסיסי. במקרה של תקלות שלא נפתרו יופעל המוקד של הספק.

2.30.2 חלון קריאה

- תקלה רגילה ימים א-ה, 8.00 - 17.00. יום ו' , 8.00 - 13.00.
- תקלה קריטית ימים א-ה, 8.00 - 20.00. יום ו' , 8.00 - 13.00.

2.30.3 זמני תגובה לקריאת שירות.

- 4 שעות עבודה - לתקלה המשביתה את המערכת/תת מערכת או קבוצה המונה יותר מ 4 מקורות מידע / משתמשים וכן מקור מידע / אפליקציה / משתמש המוגדר ע"י המזמינה כקריטי.
- 24 שעות עבודה - לתקלה ברמת מקור מידע בודד / משתמש בודד.
- הספק יפעל ברציפות לפתרון התקלה לשביעות רצון המזמין. במקרה של תקלה שתיקונה לא יסתיים בתוך פרק הזמן המוגדר לתגובה (4 שעות לתקלה קריטית, 24 לתקלה לא קריטית). יסופק ציוד חליפי ללא עלות נוספת.

2.30.4 הגדרת מהי תקלה קריטית / משביתה - תבוצע לאחר ביצוע אפיון קישורי המערכות. ההחלטה על סוג התקלה תהא בידי המזמינה.

2.30.5 הספק יפרט במענה למכרז את המשאבים הקיימים ברשותו בישראל לתפעול, שירות ותיקון המערכת.

2.31 <u>הסכם שירות לאחר תקופת האחריות</u>

2.31.1 לאחר תקופת האחריות , תהיה המזמינה רשאית לחתום עם הספק על חוזה שירות ותחזוקה שנתי בתשלום נפרד, עם אופציה לחדשו. הסכם השירות יבטיח קיום התנאים המפורטים במכרז, בתקופת הסכם השירות, לרבות עלות תיקון או החלפת חלקים אשר התקלקלו.

2.32 <u>טיפול מונע</u>

2.32.1 לכל מוצר יבוצע טיפול מונע לפי הוראות יצרן המערכת במסגרת שנות האחריות וגם במסגרת חוזה תמיכה / תחזוקה.

2.32.2 אחת לשנה תבוצע ביקורת באתר לאיתור יזום של תקלות בסיום סבב הביקורת יגיש הספק למזמין דו״ח ביקורת עם סיכום הממצאים, הפעולות שבוצעו והמלצות להמשך.

2.33 <u>דיאגנוסטיקה מרחוק</u>

2.33.1 בשלב זה לזוכה לא תתאפשר הפעלת דיאגנוסטיקה מרחוק מסיבות אבטחתיות.

2.34 <u>הדרכות</u>

קהל היעד	ימי / שעות הדרכה	תוכן ההדרכה	הדרכת ספק / יצרן
עובדי המזמינה (עד 20 איש)	יומיים	הצגה בסיסית של המוצר. הגדרות מערכת - כיצד לבצע שינויים במערכת, הגדרות בסיסיות, הגדרות אבטחת מידע. תפעול ותחזוקה שוטפים למערכת – גיבויים, שרידות, טיפול בתקלות, ביצוע בדיקות בסיסיות למערכת – חיות וכו׳. תפעול המערכת ברמת משתמש, הפקה ונתוח דו״חות אירועים, טפול באירועי אבטחה.	ספק

2.35 <u>בדיקות קבלה</u>

2.35.1 באחריות הספק לבצע בדיקות קבלה על המערכת לפני ביצוע בדיקות הקבלה של המזמינה. בדיקות הקבלה אשר נדרשות להתבצע ע״י הספק יכללו: בדיקות תפעוליות לכלל עבודת המערכת, בדיקות ביצועים ועומסים.

קבלת מערכת לידי המזמינה תבוצע לאחר ביצוע בדיקות קבלה, כאשר בדיקות הקבלה יכללו: בדיקות תפעוליות, בדיקות הגדרה במערכת, בדיקות ביצועים ועומסים, הקשחת מערכת.

2.36 <u>זמינות ושרידות</u>

2.36.1 הפתרון המוצע יתמוך בתהליכי גיבוי ושיחזור של כל המרכיבים, ובפרט: גיבוי קונפיגורציה של המערכת, בסיס הנתונים, נתוני בקרה .

על הספק לפרט את תצורות ההתאוששות האפשריות למערכת.

פירוט הנדרש בסעיף זה יסומן **כנספח יז׳10 במענה להצעה**

2.37 <u>דרישות טכניות נוספות</u>

2.37.1 נדרש לציין האם למערכת קיימת יכולת להוספת מודלי IDS וניטור DB , לצורך קבלת נתונים נוספים לגבי תעבורת הרשת ומצב ה-DB – יצורף **העמוד הרלוונטי בלבד** של הנספח הטכני של היצרן בו יודגש המענה לרכיב המפורט, **יצוין כנספח יז'11 במענה להצעה.**

2.38 <u>על המוצר המוצע לעמוד בדרישות הבאות :</u>

2.38.1 מערכת ה-SIEM המוצעת נדרשת לאפשר להחיל מדיניות אבטחת מידע בממשק הניהול המרכזי של מוצרי ה Anti Virus שמוצעים בחשכ"ל נכון למועד מכרז זה, מתוך ממשק הניהול של מערכת ה- SIEM , באופן ידני\אוטומטי על מנת לספק יכולת תגובה מהירים לאיומים שונים בהתאם. יש לצרף אישור יצרן כנספח **יז' 12 במענה להצעה.**

2.38.2 מערכת ה-SIEM המוצעת נדרשת לביצועים סבירים לחיפוש בעולם ה BIG DATA. נדרש ששאילתה המבוצעת על כ 10 מיליון אירועים תחזיר נתונים בפרק זמן סביר של עד 5 דקות. המזמינה רשאית לדרוש תצוגת יכולת המוכיחה ביצועים לנדרש בסעיף זה.

2.38.3 פירוט הנדרש בסעיף זה יסומן **כנספח יז' 13 במענה להצעה.**

2.39 <u>אמנת שירות SLA:</u>

2.39.1 אי עמידה באמנת השירות תגרור קנסות בהתאם לטבלה המצורפת:

מהות	זמן תגובה	קנס
איחור באספקת המערכת	חודש	5,000 לכל חודש איחור
טיפול בתקלה משביתה מרגע הודעה לספק - תקלה קריטית	4 שעות	200 ₪ על כל שעת איחור
טיפול בתקלה ברמת מקור בודד/משתמש יחיד	24 שעות	150 ₪ לכל יום איחור
העברת דוח ביקורת לאחר ביצוע סיור יזום לאיתור תקלות	אחת לשנה	5,000 ₪ לכל שנה שבה לא בוצע סיור והועבר דיווח.
אי עמידה בדרישות המכרז		ועדת המכרזים תקבע את גובה הקנס בהתאם לחומרת המקרה

- **יודגש: במניין השעות של זמן התגובה- לא תיספרנה השעות החלות בשבת, דהיינו: החל משעתיים לפני כניסת שבת ועד שעתיים לאחר מוצאי שבת.**
- **בנוסף, במניין הימים של זמן התגובה- לא תובא בחשבון היממה החלה בשבת.**
- **הטלת הקנסות יכול שתיעשה במסגרת חילוט ערבות הביצוע – וזאת לאחר שניתנה לספק אפשרות לתיקון הליקוי או באמצעות קיזוז מהתשלומים המגיעים לספק.**

פרק 3 : **תנאי סף**

3.1 **תנאי ראשון- התאגדות כדין.**

3.1.1 על המציע להיות יחידה אורגנית, המהווה אישיות משפטית אחת כשותפות או כחברה, או שהוא עוסק מורשה. להוכחת האמור על המציע לצרף תעודת התאגדות כחברה או כשותפות מהמרשם הרשמי הרלוונטי או תעודת עוסק מורשה.

3.1.2 ככל שהמציע מאוגד כחברה או שותפות- יצרף המציע נסח של התאגיד אשר במסגרתו יצוין כי לתאגיד אין חובות לרשם הרלוונטי (רשם החברות/ רשם השותפויות).במידה ומפורט חוב לרשם התאגידים בנסח המצורף, יש לצרף אישור על תשלום החוב לרשם התאגידים.

את המסמך המפרט את המידע הנ"ל יפיק המציע, ללא תשלום, באתר הרשמי של רשם התאגידים בקישור שלהלן:

http://147.237.72.24/WebOJSite/CompaniesList.aspx .

תעודת ההתאגדות מהמרשם הרשמי הרלוונטי-או תעודת עוסק מורשה (לפי העניין), תצורף ותסומן ***כנספח א'.***

נסח התאגיד המעודכן ליום הגשת ההצעות, מהאתר הרשמי של רשם התאגידים- כמפורט לעיל- (מדובר בשני עמודים להדפסה) יצורף ויסומן ***כנספח ב'.*** (לנוחות המציעים, מצורפת דוגמא אשר מסומנת ***כנספח ב'*** למסמכי המכרז).

3.1.3 על המציע העונה על דרישות הוראות ס' 2א לחוק חובת המכרזים, התשנ"ב-1992 (להלן: "החוק") לעניין עידוד נשים בעסקים, להגיש ביחד עם הצעתו אישור ותצהיר לפיו העסק הוא בשליטת אישה.

על פי החוק לאחר שקלול התוצאות, אם קיבלו שתי ההצעות או יותר תוצאה משוקללת זהה שהיא התוצאה הגבוהה ביותר, ואחת מההצעות היא עסק בשליטת אישה, תיבחר ההצעה האמורה כזוכה במכרז ובלבד שצורף לה, בעת הגשתה, אישור ותצהיר כאמור.

3.2 **תנאי שני- ניהול ספרים ופנקסים**

3.2.1 על המציע לנהל את החשבונות והרשומות שעליו לנהל על-פי פקודת מס הכנסה [נוסח חדש] וחוק מס ערך מוסף, התשל"ו-1976, וכן לדווח לפקיד השומה על עסקאות המוטלות עליהן מס ערך מוסף, כנדרש בחוק עסקאות גופים ציבוריים (אכיפת ניהול חשבונות ותשלום חובות מס) תשל"ו 1976, בחתימתו של פקיד מורשה כהגדרתו שם, ובתקנות עסקאות גופים ציבוריים (אכיפת ניהול חשבונות) (אישורים), התשמ"ח-1987 וכללי עסקאות גופים ציבוריים (אכיפת ניהול חשבונות), התשנ"א-1991. המציע יצרף את המסמכים כדלקמן:

3.2.2 אישור תקף מפקיד מורשה, רואה חשבון או יועץ מס על ניהול ספרים ופנקסי חשבונות על-פי הוראות הדין האמורות. **האישור יסומן *כנספח ג'***

3.2.3 תצהיר על פי חוק עסקאות גופים ציבוריים בנוסח ***נספח ד'*** למסמכי המכרז.

3.3 <u>תנאי שלישי- אי תיאום מכרז</u>

3.3.1 על המציע לצרף תצהיר בדבר אי תיאום מכרז, **בנוסח *נספח ה'* המצ"ב למסמכי המכרז.**

3.4 <u>תנאי רביעי – הסכמה בדבר עיון במרשם הפלילי</u>

3.4.1 על המציע או מורשה החתימה מטעמו לצרף הסכמתו לעיון המזמינה במרשם הפלילי, לכלל הגורמים המעורבים ישירות בביצוע הפרויקט **בנוסח *נספח ו'* המצ"ב למסמכי המכרז**.

3.5 <u>תנאי חמישי – הצהרה בדבר זמינות מיידית</u>

3.5.1 על המציע לצרף הצהרה חתומה על ידו בדבר זמינותו המידית וזמינות המועמדים מטעמו ליתן את השירותים נשוא מכרז זה, לרבות עמידה בדרישות הטכנולוגיות המפורטות בפרק 2 – מסמך האיפיון, בנוסח ***נספח ז'*** **המצ"ב למסמכי המכרז.**

3.6 <u>תנאי שישי- צירוף תצהיר מאומת כדין ע"י כדין</u>

3.6.1 על המציע לצרף תצהיר מאומת כדין ***<u>בנוסח נספח ח' המצ"ב</u>***, בין היתר על עמידתו בכל הדרישות המפורטות בפרק האיפיון.

3.7 <u>תנאי שביעי- ניסיון</u>

3.7.1 המציע התקין במהלך השנים 2011-2013 לפחות 5 פרויקטים של SIEM במגזר הביטחוני ו/או הממשלתי בכמות שלא תפחת מ-300 רכיבים מנוטרים לכל פרויקט, יש לפרט את שם הלקוח, מועדי ההתקשרות, כמות וסוגי רכיבים מנוטרים ואנשי קשר מטעם הלקוח. **<u>הנתונים יפורטו בנספח ט' למסמכי המכרז</u>**.

3.1.1 על המציע להציע מומחה אחד או יותר, בעל ניסיון של שנתיים בהתקנה ואחזקה של מערכת SIEM, בתחומים המפורטים להלן:

3.1.1.1 ניסיון בהגדרה של חוקים בסיסים ומתקדמים במערכת SIEM המוצעת.

3.1.1.2 ניסיון בניטור, הגדרת חוקים וחבור מערכת SIEM לבסיסי נתונים MSSQL ו/או ORACLE .

3.1.1.3 ניסיון בניטור, הגדרת חוקים וחיבור מערכת SIEM לשרותי IIS.

אם מדובר במומחה אחד- עליו למלא את כל התנאים המפורטים להלן באופן מצטבר, אם מדובר במספר מומחים (לא יותר מחמישה) עליהם למלא יחדיו אחר כל התנאים המפורטים להלן באופן מצטבר ואין צורך שכל אחד מהם ימלא אחר כל התנאים המפורטים להלן באופן מצטבר.

3.1.2 על המציע להציע טכנאי/ם בעלי ניסיון של שנתיים בהתקנה ואחזקה של מערכת SIEM, בתחומים המפורטים להלן:

3.1.2.1 ניסיון באפיון הגדרה של קונפיגורצית המערכת בסביבת IT פעילה.

3.1.2.2 ניסיון בניטור שרתים וחומרה של יצרנים מובילים HP ו/או ,DELL ו/או IBM ו/או Microsoft על ידי מערכת ה SIEM המוצעת.

אם מדובר בטכנאי אחד- עליו למלא את כל התנאים המפורטים להלן באופן מצטבר, אם מדובר במספר טכנאים (לא יותר מחמישה) עליהם למלא יחדיו אחר כל התנאים המפורטים להלן באופן מצטבר ואין צורך שכל אחד מהם ימלא אחר כל התנאים המפורטים להלן באופן מצטבר.

פירוט שמות הטכנאים/מומחים והניסיון בנספח ט'1 למסמכי ההצעה.

3.2 <u>תנאי שמיני- תנאים טכנולוגיים:</u>

3.2.1 על המציע לצרף אישור יצרן כי מערכת ה-SIEM המוצעת מאפשרת החלת מדיניות אבטחת מידע בממשק הניהול המרכזי של מוצרי ה Anti Virus שמוצעים בחשכ"ל נכון למועד מכרז זה, מתוך ממשק הניהול של מערכת ה- SIEM , באופן ידני/אוטומטי על מנת לספק יכולת תגובה מהירים לאיומים שונים בהתאם. האישור יצורף **כנספח יז' 12 למסמכי ההצעה**.

3.3 <u>תנאי תשיעי - הסמכות</u>

3.3.1 **המציע מעסיק עובדים אשר זמינים במידת הצורך לתמוך בכל שלב בצוות הפרויקט (אפיון, התקנה, תחזוקה, פתרון תקלות) בעלי ההסמכות הבאות:**

3.3.1.1 הסמכת CCIE/CISSP לאבטחת מידע

3.3.1.2 הסמכת MCSE/MCITP או הסמכה דומה בתחום מערכות הפעלה ותשתיות מייקרוסופט

3.3.1.3 הסמכת CCSP/CCSA למוצרי Checkpoint

3.3.1.4 הסמכת CCIE/CCNP לתקשורת

התעודות יצורפו כנספח ט'2 למסמכי ההצעה.

3.4 <u>תנאי עשירי- אישורים</u>

3.4.1 המציע בעל אישור מטעם יצרן המערכת להתקנה ותפעול שוטף של מערכת SIEM המוצעת. יש לצרף את המסמך כאשר הוא חתום כנדרש. **<u>האישורים יצורפו כנספח ט'3 למסמכי ההצעה.</u>**

3.4.2 ליצרן המערכת המוצעת ע"י המציע ישנה נציגות פעילה בארץ אשר מפעילה מערך תמיכה עצמאי. יש להמציא אישור יצרן – **<u>יצורף כנספח ט'4 למסמכי ההצעה.</u>**

3.5 <u>תנאי אחד עשר- ערבות מכרז</u>

3.5.1 על המציע לצרף ערבות בנקאית או ערבות חברת ביטוח **<u>בנוסח שבנספח י'</u>** לקיום תנאי המכרז, מטעם המציע לפקודת המזמינה **בסך 9,000** ₪ כולל מע"מ. הערבות תהיה בתוקף עד למועד הקבוע בטבלת המועדים לעיל. **אין להצמיד את ערבות המכרז.**

שם המציע שיירשם בערבות יהיה זהה לשמו של המציע כפי שהוא מופיע במסמכי ההתאגדות.

<u>יודגש: על כתב הערבות להיות מנוסח בדיוק כמו הנוסח המצ"ב למכרז זה בנספח י'. ערבות החורגת מהנוסח המצ"ב למכרז זה, אף אם תהיה מיטיבה – תיפסל (!).</u>

לאחר תום הליכי המכרז וההכרזה על הספק הזוכה- תוחזרנה הערבויות למציעים שלא יזכו במכרז.

ערבות הזוכה תוחזר לו עם החתימה על החוזה כנגד קבלת ערבות ביצוע להמשך תקופת ההתקשרות.

בהגשת הצעתו מתחייב המציע לעמוד בכל תנאי הצעתו למכרז. אם לא יעשה כן, תהא המזמינה רשאית לממש את הערבות שצירף להצעתו ובנוסף לכך לתבוע מהמציע כל נזק שנגרם ו/או שיגרם למשרד כתוצאה מאי עמידתו של המציע בתנאי הצעתו למכרז, והעולה על גובה הערבות שצרף המציע למכרז.

המצאת האישורים והמסמכים המפורטים לעיל הנה תנאי סף להשתתפות במכרז. על אף האמור לעיל, המשרד שומר לעצמו את הזכות לאפשר למציע אשר לא צירף אישור מהאישורים המפורטים לעיל, להשלים את הגשת המסמכים במועד המאוחר למועד פתיחת המעטפות (להלן: "צירוף מאוחר"). צירוף מאוחר כאמור לעיל, יתאפשר רק מקום שהוברר, כי המסמכים לא צורפו בשל טעות בתום לב של המתמודד ובלבד שבמועד הגשת ההצעות, היו האישורים הדרושים מצויים בידי המתמודד.

פרק 4 : <u>הקריטריונים לבחירת המציע</u>

4.1 <u>להלן השלבים בבדיקת ההצעות:</u>

בדיקת המכרז תיעשה בשלושה שלבים:

4.1.1 שלב ראשון: בדיקת עמידה בתנאי סף

תחילה תיבדק הצעתו של המציע מבחינת עמידתה בתנאי הסף כפי שפורטו בפרק 3 למכרז זה. הצעות שעמדו בתנאי הסף, תעבורנה לשלב הבא שהינו שלב בדיקת האיכות.

4.1.2 שלב שני: הערכת האיכות- משקל סעיף האיכות בציון המשוקלל הוא 50%.

הערכת האיכות תעשה בהתאם לאמור להלן, <u>ציון הסף הכולל המהווה תנאי למעבר</u> לשלב הבא הוא 80 נקודות.

מציע שינוקד בסעיף האיכות בציון נמוך מ-80 נקודות, לא יעבור לשלב הבא. במידה ולא יהיו שלושה מציעים שיעברו את ציון האיכות הקובע, שומרת הרשות את הזכות לבחון מציעים נוספים.

4.1.3 שלב שלישי: מרכיב המחיר- משקל ציון המחיר בהצעה הוא 50%

4.2 <u>מרכיב האיכות:</u>

משקל סעיף האיכות המשוקלל הוא 50%.

בדיקת פרמטר האיכות תתבצע בהתאם למשקלות הנקובים להלן ובנוסח המפורט **<u>בנספחים המצורפים למסמכי ההצעה</u>** והמתייחסים למידע שיתקבל ממסמכים שיצרף המציע בהתאם למבוקש:

תיאור	ניקוד לתת סעיף	הניקוד
מענה מקצועי לתצורת המערכת בהתאם לדרישות המכרז כפי שמפורטות בפרק האיפיון – **יוגש כנספחים יז-1-יז׳ 13 (למעט נספח יז׳2) למסמכי ההצעה** בהתאם למשקולות שלהלן:		30%
נספח יז׳ 1	1.5	
נספח יז׳ 2	1.5	
נספח יז׳ 3	1.5	
נספח יז׳ 4	1.5	
נספח יז׳ 5	1.5	
נספח יז׳ 6	1.5	
נספח יז׳ 7	1.5	

נספח יז׳ 8	1.5	
נספח יז׳ 9	5	
נספח יז׳ 10	1.5	
נספח יז׳ 11	5	
נספח יז׳ 13	6.5	
המערכת המוצעת ממוקמת ברביע ה Leaders של הGartner SIEM Magic Quadrant בשנים 2012 ו2013. הנתונים יילקחו מנתוני המערכת, כפי שיצורפו בנספח **יז׳1 למסמכי ההצעה.**		15%
כמות המומחים/טכנאיים אצל המציע אשר הינם בעלי ניסיון מוכח בהתקנה / תחזוקה של מערכות SIEM - מעל וכולל 5 עובדים יינתן ניקוד מקסימאלי, על כל עובד מתחת ל- 5 עובדים יינתן ניקוד של 2%. **הנתונים יילקחו מנספח ט׳1 למסמכי ההצעה.**		10%
מהירות תגובה של המערכת המוצעת. ההשוואה תבוצע על בסיס הרצת שאילתה על 10 מיליון אירועים. המציע יגיש דוח ביצועים לגרסה האחרונה של במערכת, **יוגש כנספח יז׳13 למסמכי ההצעה**. ניקוד מקסימאלי יינתן עבור המערכת אשר תציג את הנתונים בזמן הטוב ביותר, והיתר ינוקדו באופן יחסי לזמן הטוב ביותר. מהירות תגובה להרצת השאילתה שתעלה מעל ל-5 דקות לא תזכה את המציע בניקוד במרכיב זה. **הערה – הרשות שומרת לעצמה את הזכות לבדוק בסביבת מעבדה אצל המציע את הנתונים שהוגשו כנספח.**		10%
למערכת יכולת להוספת מודלי IDS וניטור DB לצורך קבלת נתונים נוספים לגבי תעבורת הרשת ומצב ה-DB – יצורף **העמוד הרלוונטי בלבד** של הנספח הטכני של היצרן בו יודגש המענה לרכיב המפורט, **יצוין כנספח יז׳11 למסמכי המכרז.**		5%
חוות דעת ממליצים. יש לצרף מכתבי המלצה מלקוחות על התקנת / תחזוקת מערכות SIEM, כל מכתב יקנה 2% מהציון עד למקסימום של 5 מכתבי המלצה, כאשר מתוכם לפחות 3 המלצות של גופים ממשלתיים/בטחוניים. מכתבי ההמלצה יסומנו **כנספח טז׳ למסמכי ההצעה**. יש לציין ע״ג כל מכתב המלצה שם של איש הקשר מטעם הלקוח ופרטי התקשרות. הרשות שומרת את הזכות לפנות לממליצים ולאמת את הנכתב במכתבים.		10%
התרשמות מהצגה מפורטת של פרויקט אחד מרכזי מבין 5 הפרויקטים שבוצעו בשנת 2011-2013 תוך התייחסות למרכיבים הבאים : תיאור כללי של הפרויקט, גודל הארגון, היקף שעות העבודה, כמות הרכיבים המנוטרים, היקפי המשתמשים אותם המערכת משרתת, כמות חוקים, רכיבי ה-SIEM/SOC שהוקמו, סביבות עבודה / מקורות מידע / אפליקציות ששולבו, שלבים מרכזיים בביצוע הפרויקט, צוות הפרויקט, התאמות שבוצעו, בעיות מהותיות במהלך ההטמעה, האם המציע ממשיך לתמוך בפרויקט מסמך פירוט הפרויקט יסומן **כנספח יח׳ למסמכי ההצעה**		15%
התרשמות המזמינה מאיכות הגשת הצעתו המנהלית והטכנית של המציע		5%
סה״כ		**100%**

4.3 השלב השלישי - הצעות המחיר-50%

4.3.1.1 מציעים שקיבלו ציון של 80% ומעלה ברכיב האיכות יעברו לשלב זה- בו תיבחן הצעת המחיר כפי שתצורף **<u>כנספח יא' למסמכי ההצעה</u>** ויינתן ציון כדלקמן:

מרכיב המחיר	משקל הציון
עלות אספקה והתקנת המערכת בהתאם לשישה השלבים המפורטים באבני הדרך, הכוללת: • רישוי לשנה, • אינטגרציה – אפיון, התקנה, חיבור מערכות, קביעת ויישום חוקים, הדרכה • תחזוקה ל-3 שנים	70%
עלות רישוי לשנה נוספת (החל מהשנה השנייה)	10%
עלות תחזוקה לשנה נוספת (מעבר ל-3 שנים)	5%
עלות שעת עבודת מומחה לעבודות שלא כלולות בהיקף המכרז	10%
עלות שעת עבודת טכנאי שלא כלולות בהיקף המכרז	5%

4.4 <u>הבהרות בנוגע להצעת המחיר</u>:

4.4.1 הצעת המחיר תוגש בש"ח לא כולל מע"מ.

4.4.2 כל פריטי התוכנה יסופקו בגרסתם העדכנית ביותר נכון למועד תחילת העבודה, אלא אם הוחלט אחרת ע"י המזמינה.

4.4.3 כל הציוד בפרויקט שיסופק ע"י המציע, יהא ציוד חדש שאינו משומש.

4.4.4 המחירים שיוגשו ע"י המציע, יהיו תקפים גם במקרה בו החליטה הרשות לממש את האופציה להארכת תוקף המכרז.

4.5 **<u>סיכום ציונים ובחירת ספק</u>** – המזמינה תקבע כזוכה את ההצעה בעלת הציון הגבוה ביותר, לאחר שקלול כל ההצעות עפ"י אמות המידה של איכות ומחיר, לכדי ציון אחד משוקלל.

4.6 <u>דגשים והבהרות בעניין זה</u>:

4.6.1 לרשות האכיפה והגבייה שמורה הזכות לבקש הבהרות, תוספות ושינויים בכל שלב שלפני קבלת ההחלטה בנוגע לבחירה הסופית של הזוכה.

4.6.2 במידה ושני מציעים או יותר, יקבלו ציון זהה, רשאית המזמינה לערוך סבב " Best & Finals " בין המציעים שקיבלו ציון זהה, ו/או לבחור באחד מהמציעים בהתאם לשיקול דעתה הבלעדי והמוחלט, ללא צורך במתן הסברים ו/או נימוקים להחלטת המזמינה. לא תישמע כל טענה בעניין זה.

פרק 5 : <u>מסמכים ואישורים שיידרשו מהספק הזוכה עם קבלת ההודעה על הזכייה במכרז</u>

5.1 עם היוודע לו דבר זכייתו במכרז ולא יאוחר מחלוף 14 ימים ממועד זכייתו במכרז, ימציא הספק שיזכה במכרז זה את המסמכים והאישורים הבאים. מציע שלא ימציא המסמכים האמורים לא יוכל לממש את זכייתו ורשות האכיפה והגבייה תהא רשאית לפנות למציע שדורג במקום השני.

5.1.1 חתימה על דוגמת החוזה המצורפת למכרז זה ***<u>ומסומנת כנספח יב' הרצ"ב</u>***.

5.1.2 ערבות ביצוע בסך של 5% מסכום ההתקשרות בחוזה, בהתאם **לנספח י"1 למסמכי המכרז,** לפקודת הרשות, צמודה למדד המחירים לצרכן, להבטחת ביצוע הצעתו וכל התחייבויותיו בהסכם ההתקשרות ובגין מכרז זה. הערבות תהא ערבות בנקאית או ערבות של חברת ביטוח ישראלית שברשותה רישיון לעסוק בביטוח על פי חוק הפיקוח על עסקי הביטוח, התשמ"א – 1981, הערבות תהיה אוטונומית, בלתי מותנית ובלתי ניתנת לביטול. הערבות תהיה בתוקף למשך כל תוקפו של ההסכם ולמשך 60 ימים נוספים לאחר מכן.

5.1.3 על המציע ו/או מי מטעמו - כפי שיורה לו נציג המזמינה, לצרף הצהרתו החתומה בדבר היעדר ניגוד עניינים, **בנוסח *<u>נספח יג'</u>* המצ"ב למסמכי המכרז**.

5.1.4 על המציע ו/או מי מטעמו – כפי שיורה לו נציג המזמינה, לצרף התחייבותו החתומה לשמירה על סודיות, **בנוסח *<u>נספח יד'</u>* המצ"ב למסמכי המכרז**.

5.2 מציע שלא ימציא המסמכים האמורים לא יוכל לממש את זכייתו ורשות האכיפה והגבייה תהא רשאית לפנות למציע שדורג במקום השני.

פרק 6 : <u>התמורה בגין השירות</u>

6.1 ביצוע העבודה ייעשה אך ורק על פי האמור במכרז זה ובהסכם ההתקשרות. חריגה שאינה מלווה באישור מורשי החתימה במשרד לא תאושר.

6.2 **<u>אבני הדרך לתשלום</u>**

6.2.1 התשלום עבור כלל הפעילות בפרויקט והרישוי יבוצע בהתאמה לאבני דרך הבאות:

שלב	% התשלום מעלות הפרויקט	התנאי לתשלום	הערות
א	20%	אפיון ארכיטקטורת המוצר, וממשק המשתמש	
ב	30%	הקמת התשתית, התקנת המוצר בקונפיגורציה בסיסית, והתאמתו לדרישות המזמינה	אספקת רישוי לשנה, כולל בדיקות קבלה, מסירה והדרכה.
ג	10%	קישור מקורות מידע תשתיתיים ותקשורתיים	כולל ובניית חוקים ודוחות מתאימים
ד	10%	קישור מערכת לגביית קנסות	כולל ובניית חוקים ודוחות מתאימים
ה	15%	קישור מערכת כלים שלובים	כולל ובניית חוקים ודוחות מתאימים
ו	15%	קישור יתר מערכות המזמינה	כולל ובניית חוקים ודוחות מתאימים

6.2.2 כל אבן דרך תכלול 5 שלבים: אפיון, הטמעה, בדיקות קבלה, מסירה והדרכה.

6.2.3 המזמינה שומרת לעצמה את האופציה לשנות את סדר השלבים בהטמעה בהתאם להמלצות המציע.

6.2.4 התמורה שתשלם המזמינה עבור מתן השירותים לפי הסכם זה תהיה בהתאם למחיר שהוצע ע"י המציע במענה למכרז.

6.3 עבור ביצוע העבודה, ובסיום אבן הדרך, יגיש הספק הזוכה חשבונית לתשלום שתועבר לאישורו של הגורם המקצועי או מי מטעמו.

6.4 לאחר שיאושרו החשבוניות ע"י הגורמים הרלוונטיים, כאמור, יועברו החשבוניות לתשלום ליחידת הרכש המרכזית של המזמינה.

6.5 תשלום החשבוניות ייעשה עפ"י הוראת החשב הכללי שמספרה 1.4.3 המסומנת **כנספח טו'.**

6.6 הגדרות בנושא הצמדה

6.6.1 **תאריך הבסיס** – המועד האחרון להגשת הצעות במכרז כמפורט בטבלת המועדים במכרז..

6.6.2 **תאריך התחלת הצמדה** – המועד **שממנו** והלאה מחושבת ההצמדה – 20/5/15

6.6.3 **מדד התחלתי** – המדד הידוע בתאריך **התחלת** ההצמדה, מדד חודש: 5/15

6.6.4 **המדד הקובע** – המדד האחרון הידוע ביום מועד ביצוע ההצמדה.

6.6.5 הצמדה שלילית – הצמדה **המבוצעת** כאשר המדד או הרכב המדדים הקובע ירד אל מתחת לשיעור המדד ההתחלתי.

6.6.6 **מדד המחירים לצרכן** – **כפי** שמפורסם על ידי הלשכה המרכזית לסטטיסטיקה או מי שהוסמך על ידי ממשלת ישראל להחליפה.

6.7 עקרונות ביצוע הצמדה

6.7.1 המחירים יוצמדו לשינויים במדד המחירים לצרכן (להלן: "המדד").

6.7.2 סכום ההצמדה שיחושב יתווסף (או יופחת, אם חלה ירידה במדד הרלוונטי) לתעריפים שנקבעו בהתקשרות.

6.7.3 ביצוע הצמדה יהיה גם במקרים שבהם מדובר בהצמדה שלילית.

6.8 מנגנון ביצוע הצמדה

6.8.1 ביצוע ההצמדה יחל לאחר תום 18 חודשים מתאריך הבסיס, למעט במקרה המפורט בסעיף 6.8.3. המדד הידוע ביום זה ייקבע כמדד ההתחלתי.

6.8.2 ההצמדה תתבצע מדי חודש.

6.8.3 על אף האמור בסעיף 6.8.1, אם במועד מסוים (להלן: "יום השינוי") במהלך 18 החודשים הראשונים מתאריך הבסיס, יחול שינוי במדד – כך שיהיה גבוה בשיעור של 4% ויותר מהמדד הידוע בתאריך הבסיס, יחל חישוב ההצמדה מנקודה זו ואילך, באופן הבא:

6.8.3.1 המדד הידוע ביום השינוי ייקבע כמדד ההתחלתי.

פרק 7 : שמירת סודיות

7.1 הספק מתחייב לשמור בסוד ידיעות ומידע שיגיעו אליו עקב ביצוע מכרז זה.

7.2 הספק ידאג לאבטח את כל המידע המגיע אליו במסגרת מכרז זה, ולוודא שלא ייעשה בו כל שימוש אחר. כן יוודא השמדת כל הקבצים והרישומים של כל הפעילים בתוכניות השונות בתום ההתקשרות, אלא אם יידרש אחרת ע"י המשרד.

7.3 הספק יבחר ויעסיק רק עובדים העונים על ההנחיות הביטחוניות של קב"ט המשרד ולאחר שעברו בדיקה ביטחונית מקיפה המתאימה לאירועים מהסוג הנ"ל.

7.4 הספק לא ימסור ידיעה או מידע לאדם שלא יהיה מוסמך לקבלה ללא הרשאה בכתב מהמשרד.

7.5 הספק ידאג שכל עובדיו וקבלני המשנה שלו ישמרו על המידע כאמור בחוק הגנת הפרטיות, התשמ"א - 1981 ותקנות הגנת הפרטיות (תנאי אחזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו - 1986.

7.6 הספק יחזיר למשרד כל חומר שיימסר לו בהקשר לפעילות זו בכל עת שיידרש לכך.

פרק 8 : יחסי הצדדים

8.1 השירותים יינתנו במסגרת ארגוניות של המציע בלבד. לעניין זה "מסגרת ארגונית" – לרבות איתור עובדים ו/או קבלני משנה, העסקתם, ניהול כל משא ומתן עמם, השגחה מתמדת על פעילותם, תשלום שכרם וכל תשלום סוציאלי נלווה אגב העסקתם, פיטוריהם והאחריות לכך, והטלת משמעת כמקובל במסגרת המציע.

8.2 המציע מצהיר, כי ידוע לו ולכל העובדים המועסקים על ידיו לצרכי ביצוע מכרז זה, כי הינם עובדים ומעוסקים במסגרת הארגונית של המציע, ולא של המשרד. המציע בלבד יהיה אחראי כלפי כל המועסקים על ידיו לפי דיני העבודה והנזיקין. כן יהיה המציע לבדו אחראי לכל נזק שיגרם על ידיו, או בגין רכושו ונכסיו ועל ידי המועסקים על ידו למטרות חוזה זה. אם על אף האמור יחויבו המשרד כדין, לשאת חבות, או לעשות מעשה כלשהו, יפצה אותו על כך המציע באופן מלא.

8.3 בכל הקשור למערכת היחסים בין המשרד לבין המציע, יחשב המציע, כמציע עצמאי לכל דבר ועניין. המציע מודע לכך שלא מתקיימים יחסי עובד-מעביד בינו ו/או עובדיו ו/או קבלני המשנה מטעמו לבין המשרד.

8.4 המציע אחראי לעובדים, לאיכות העבודה, לגיבוי למילוי מקום, להכשרת עובדים בהתאם לצרכים ובכלל זה השתלמויות וקורסים על חשבונו על פי צרכי השירותים במכרז.

8.5 המציע אינו רשאי להמחות (להעביר) לזולת את זכויותיו או את חובותיו לפי תנאי מכרז זה כולן או חלקן ללא הסכמה בכתב מראש של המשרד.

8.6 אין המציע רשאי להעביר את ביצוע החוזה כולו או חלקו במישרין או בעקיפין לאחר, ללא הסכמה בכתב ומראש של המשרד. הסכמה כאמור, אם ניתנה, לא תיצור יחסי חוזה כלשהם בין המשרד לבין מציע אחר, והמציע הזוכה יהיה בכל מקרה אחראי כלפי המשרד לביצוע השירותים.

8.7 בידי המציע יהיו כל האמצעים המנהליים, הארגוניים והמשרדיים הנדרשים לצורך מתן השירותים המשפטיים באופן מלא, ועליו לשלוט באופן מלא בהפעלתם, כנדרש במסמכי המכרז.

8.8 במקרה של סתירה או אי- בהירות בין האמור במכרז לבין האמור בהסכם ההתקשרות, תכריע עמדת היועצת המשפטית של רשות האכיפה והגבייה.

<u>לנוחות המציעים, להלן ריכוז הנספחים שעל המציע לצרף להצעתו:</u>

נושא	מס׳ פרק	לציין כנספח
חוברת המכרז+ נספחים+ קובץ שאלות ותשובות – ייחתמו בתחתית העמוד ע״י המציע	1	
תעודת ההתאגדות מהמרשם הרשמי הרלוונטי-או תעודת עוסק מורשה	3	א׳
נסח התאגיד	3	ב׳
אישור <u>תקף</u> מפקיד מורשה, רואה חשבון או יועץ מס על ניהול ספרים ופנקסי חשבונות	3	ג׳
תצהיר על פי חוק עסקאות גופים ציבוריים	3	ד׳
תצהיר בדבר אי תיאום מכרז	3	ה׳
הסכמה לעיון המזמינה במרשם הפלילי	3	ו׳
הצהרה על זמינות המידית	3	ז׳
תצהיר על עמידה בדרישות המפורטות בפרק האיפיון (פרק 2)	3	ח׳
פירוט על 5 פרויקטי SIEM שבוצעו במהלך 2011-2013	3	ט׳
שמות המתקינים הרלוונטיים לפרוייקטים שהוצגו בנספח ט׳	3	ט׳1
תעודות והסמכות בעלי תפקידים	3	ט׳2
אישור מטעם יצרן המערכת להתקנה ותפעול מערכת ה SIEM המוצעת	3	ט׳3
אישור על קיום נציגות פעילה בארץ	3	ט׳4
ערבות המכרז	3	י׳
הצעת מחיר למכרז	4	יא׳
מכתבי המלצה מלקוחות	4	טז׳
פירוט תצורת המערכת	2	יז׳1
פירוט תצורת הממשקים לרכיבים המנוטרים	2	יז׳2
בקרה על תהליך קבלת הלוג / אירועים	2	יז׳3
תיאור קבלת הלוגים מהאפליקציות והתייחסויות מיוחדות	2	יז׳4
התייחסות ליכולת תעדוף אירועים	2	יז׳5
תמיכה אינהרנטית במסכים המבוקשים	2	יז׳6
צילומי מסכים נדרשים	2	יז׳7
תהליכים	2	יז׳8
נפחים עומסים וביצועים	2	יז׳9
זמינות ושרידות	2	יז׳10
יכולת להוספת מודלי IDS וניטור DB	2+4	יז׳11
אישור יצרן התחברות ממשק הניהול לרכיב end point security של מוצרי אבטחה המוצעים בחשכ״ל.	2+3	יז׳12
דו״ח ביצועים בחיפוש	2+4	יז׳13
תיאור מפורט של פרויקט אחד מרכזי	4	יח׳