



8.10.18

ג.א.ג,

הנדון: פנייה לקבלת הצעות למתן שירותי SOC מנוהל ומערכת ניטור SIEM לחברה הלאומית לאספקת פחם בע"מ

החברה הלאומית לאספקת פחם בע"מ (להלן: "החברה") פונה בזאת לקבלת הצעות למתן שירותי SOC מנוהל ומערכת ניטור SIEM בהתאם לנספח תכולת השירותים המצורף (להלן: "העבודה" או "השירות"). בכל מקרה של סתירה בין תיאור השירות במסמך זה ובין הגדרתו בנספח תכולת השירותים המצורף, יגבר האמור בנספח.

שירות ה SOC המנוהל הנדרש הנו מוקד אבטחת מידע זמין המושתת על אנאליסטים מומחים בזמינות 24-7-365 לזיהוי, התראות ותחקור אירועי אבטחת מידע וסייבר.

1. רקע כללי ומהות ההתקשרות המבוקשת

להלן רקע כללי על החברה (מידע נוסף יימסר לפי דרישה):

- החברה עוסקת ברכש פחם ושינועו מרחבי העולם אל תחנות הכוח הפחמיות של חברת החשמל – תחנת "רוטנברג" באשקלון ותחנת "אורות רבין" בחדרה.
- החברה הינה חברה ממשלתית, בבעלות מלאה של חברת החשמל.
- החברה הלאומית לאספקת פחם פזורה בארבעה אתרים גיאוגרפיים: תל אביב - ראשי, פתח תקווה – DR, סניפים: אשקלון, חדרה.
- החברה מעסיקה כ- 30 עובדים ופעילותה העיקרית הינה בתחומי שוק הפחם והספנות. שני השווקים הינם שווקים בינלאומיים גלובליים בעלי מאפיינים ייחודיים.
- בחברה ישנם כ- 115 מערכות מחשוב מתוכם: 40 תחנות עבודה, 40 שרתים והשאר ציודי רשת ואבטחת מידע. פירוט נוסף ימצא בפרק הטכני המצורף למסמך זה. בכל סניף ישנם 3 תחנות עבודה.
- ניהול וניטור המערכות מבוצע דרך האתר המרכזי בתל אביב.

2. תנאי סף

השירותים נשוא הליך זה דורשים ידע והתמחות מקצועית ייחודית בנושאים להלן:

איסוף אירועי אבטחת מידע ממערכות הלקוח ("אגרגציה"), איחוד ויצירת חוקים המתאימים לסיכונים שהוגדרו בחברה ("קורלציה"), ניתוח התראות ("אנליזה"), חקר מעמיק של אירועים ("פורנזיקה"). בהתאם לכך נקבעו תנאי סף לניסיון המציע, לפיהם רשאים להשתתף בהליך אך ורק מציעים העומדים במצטבר בכל תנאי הסף המפורטים להלן:

2.1 המציע בעל כל האישורים הדרושים לפי חוק עסקאות גופים ציבוריים, התשל"ו - 1976 ("חוק עסקאות גופים ציבוריים").

2.2 ניסיון מקצועי:

2.2.1 למציע יהא ניסיון אצל לפחות 5 לקוחות בישראל אשר לפחות לקוח אחד מתוכם הינו: בנקים, חברות ביטוח, משרדי ממשלה, חברות ממשלתיות, או ארגונים ביטחוניים.

"לקוח" לצורך סעיף זה משמע: חברה או ישות נפרדת, אתר נפרד בחברה או גוף דומה.

"ניסיון" לצורך סעיף זה משמע:

2.2.1.1 מתן שירותי מיקור חוץ למוקד ניטור אבטחת מידע (SOC) של המציע.

2.2.1.2 יישום תשתית SIEM בחצר הלקוח, הגדרת מערכת ה-SIEM לאיסוף ההתראות ממערכות המחשוב, הרשת ואבטחת המידע של הלקוח.

2.2.1.3 בניית חוקים במערכת ה-SIEM לניתוח (אנליזה) ואיחוד (קורלציה) של התראות ממערכות הלקוח וכן ליצירת התראות ממוקדות בשיתוף עם הלקוח.

2.2.1.4 כתיבת נהלי תגובה לאירועים, אפיונם ותיעדופם.

2.2.1.5 הגדרה ואפיון כוח האדם הנדרש, ניטור וטיפול באירועי סייבר.

2.2.1.6 חקירת אירוע (פורנזיקה) בחירום.

2.2.2 לצוות נותני השירות בפרויקט וצוות המוקד נדרש ניסיון מצטבר שלא יפחת משלוש שנים בהטמעת מערכת SIEM בארגון, והקמת מרכז טיפול באירועי אבטחת מידע SOC, לרבות כוח האדם הנדרש על פי תפקידים, כתיבת נהלי תגובה לאירועים כמתואר לעיל. ("מצטבר": לכל חבר צוות 3 שנים בתחום ה-SIEM הכולל ניטור וניתוח אירועי סייבר).

2.2.3 על המציע לספק את שירותי המוקד (הקמה והפעלה) באמצעות עובדים אורגניים שלו ולא על ידי קבלן משנה.

2.2.4 על המציע לספק את שירותי המוקד מישראל.

2.2.5 עובדי המוקד (אנליסט) יהיו בעלי 3 שנות ניסיון בתחום ניטור והגנה מפני אירועי סייבר. עובדי המוקד יהיו עובדים אורגניים.

2.2.5.1 "עובד אורגני" לצורך סעיף זה משמע: כל מי שמתקיימים בינו לבין המציע יחסי עובד-מעביד ומקבל משכורת בתלוש שכר מאת המציע.

2.2.6 המציע יעסיק לפחות עובד אורגני אחד מומחה לתפקיד אנליסט אבטחת מידע בכיר בתפקיד מומחה.

2.2.6.1 "מומחה" לצורך סעיף זה משמע: אדם העוסק במתן שירותי ניטור וחקירת אירועי סייבר בעל ניסיון מקצועי של לפחות 5 שנים בתחום הגנת הסייבר.

2.2.6.2 מבלי לגרוע מהאמור לעיל, מצורף נספח דרישות טכנולוגיות המהווה דרישות סף אותן נדרש הספק למלא במסגרת הצעתו.

- 2.3 מהימנות עובדים :
- 2.3.1 המציע ועובדיו לא הורשעו בעבירה שיש עמה קלון ו/או עבירה שנושאה כספי (כגון אי העברת נכויים ואי דיווח לרשויות המס), זולת אם חלפה תקופת ההתיישנות לפי חוק המרשם הפלילי ותקנות השבים, התשמ"א-1981 ו/או במועד הגשת ההצעות בהליך זה, לא מתנהלים נגדו הליך משפטי ו/או חקירה בעבירות כאמור לעיל; אם המציע הוא תאגיד-נדרש כי העדר הרשעה וחקירה כאמור יתקיים גם לגבי בעל השליטה בו ונושאי המשרה שלו.
- 2.3.2 כתנאי מוקדם להשתתפות, על כל אחד מחברי "הצוות" המוצעים מטעמו של המציע לצרף הסכמה לבדיקה ביטחונית, כולל בדיקת רישום פלילי" חתום, עבור כל איש צוות המוצע לקחת חלק בפרויקט.
- 2.4 סודיות :
- 2.4.1 הזוכה מתחייב לשמור בסוד ולא להעביר, להודיע, למסור או להביא לידיעת אחר כל תוצר עבודה עפ"י הליך זה וכל מסמך ו/או ידיעה ו/או קובץ מחשב אשר הגיעו אליו בקשר או בעת ביצוע התחייבויותיו.
- 2.4.2 הזוכה מתחייב להביא לידיעת עובדיו חובה זו של שמירת הסודיות, והעונש על אי מילוייה. כל התחייבויות הזוכה בשמירת סודיות יחולו גם על כל קבלני המשנה מטעמו.
- 2.4.3 החברה רשאית להחתים את עובדי הזוכה ו/או קבלני המשנה שלו, כולם או מקצתם, על הצהרת סודיות לגבי כל מידע שייודע להם במסגרת עבודתם על פי ההסכם.
- 2.4.4 הזוכה ידאג לאבטחת כול מידע שיגיע אליו במסגרת ביצוע התחייבויותיו על פי הליך זה, ויציג לחברה על פי דרישתה את אמצעי אבטחת המידע בו הוא נוקט.
- 2.5 נהלים :
- 2.5.1 המציע מתחייב למלא אחר נהלי אבטחת המידע שיוכתבו לו על ידי החברה.
- 2.5.2 המציע מצהיר שכול התוכנות אשר ישמשו אותו במתן השירותים הינן חוקיות והינן בבעלותו.
- 2.5.3 המציע יהיה אחראי כלפי החברה על כול מידע שמועבר אליו, דרכו, לרבות דוחות, טפסים, קבצים מגנטיים, מידע לגבי נתונים אישיים ומערכות המידע של המזמין.
- 2.6 סיום התקשרות :
- 2.6.1 עם סיום הפרויקט, או סיום עבודת המציע בפרויקט מסיבה כלשהי, יחזיר המציע לחברה כל מסמך או חומר אחר הקשור בפרויקט, כולל כל העותקים והגיבויים שלהם, וימחק את הנ"ל מכל מדיה מגנטית שברשותו או ברשות כל מי מטעמו.
- 2.7 ממליצים :
- 2.7.1 הספק יעביר 3 ממליצים בהם הוטמע שירות דומה למתבקש במסמך זה.
- 2.7.2 ההמלצות יכללו: פרטי קשר של גורם ממליץ אשר עבורו סופק שירות מיקור חוץ לשירותי SOC ו-SIEM.
- 2.7.3 ההמלצות יכללו שם הלקוח, תפקיד, טלפון, דוא"ל, ותקציר על השירות אשר ניתן לקוח.
- 2.8 כוח אדם :
- 2.8.1 על המציע להעמיד צוות עובדים אשר יעמוד בתנאי הסף המפורטים בסעיפים 2.2.2 עד 2.3 לעיל וכל יתר התנאים הרלוונטיים במסמך זה.

2.8.2 על המציע להציע לצורך הוכחת העמידה בתנאי הסף או בדרישות האיכות אך ורק עובדים מטעמו אשר מיועדים ומוצעים להשתתף בפרויקט.

2.8.3 יובהר כי לא יחליף המציע נותני שירותים שהוצעו בהליך אלא אם המחליפים עונים לדרישות והשינוי באישור נציג החברה מראש ובכתב.

להוכחת עמידתו של המציע בתנאי הסף דלעיל, יגיש המציע:

- אישור עו"ד/רו"ח המאשר את העסקתו של מומחה בתחומי אבטחת מידע וסייבר.
- תצהיר חתום על ידי עו"ד המאמת את האמור בסעיף 2.3 לתנאי ההליך.
- המציע יצרף את כל האישורים הנדרשים לפי חוק עסקאות גופים ציבוריים, תשל"ו-1976 והתקנות שהותקנו מכוחו, לרבות האישור המצורף בנספח ב' לתנאי ההליך, הכל כאמור בסעיף 2.5 לתנאי ההליך.

3. תיאור השירותים הנדרשים מופיע במסמך האפיון המצורף המהווה חלק בלתי נפרד ממסמכי ההליך.

4. אמות המידה לבחירת ההצעה המיטבית

4.1 אמות המידה לבחירת ההצעה הזוכה הינן כדלקמן:

מחיר – 100%

המחיר הינו המחיר המוצע בשקלים חדשים, לא כולל מע"מ, עבור מתן השירות

המחיר יהיה קבוע ולא יישא הצמדה כלשהי.

5. הערות כלליות

- 5.1 פנייה זו לקבלת הצעות נעשית בהליך תחרותי פטור ממכרז פומבי.
- 5.2 הצעת המחיר תכלול את כל העלויות הכרוכות בביצוע השירות, למעט מע"מ כדון.
- 5.3 החברה תהיה רשאית בכל עת לפנות למציע לבירורים ו/או לקבלת הבהרות (ללא התייחסות למחירים).
- 5.4 החברה שומרת לעצמה את הזכות לנהל מו"מ עם כל המציעים אשר יקבעו במסגרת קבוצת המציעים הסופית (לעניין סעיף זה – בקבוצת המציעים הסופית יכללו כל המציעים שיעמדו בתנאי ההליך). בסיום המו"מ יהיה כל מציע, כאמור, רשאי במועד בו תקבע החברה, להגיש לתיבת המכרזים הצעה סופית. מציע אשר לא יגיש הצעה נוספת, הצעתו הראשונה תיחשב כהצעה סופית. לאחר הגשת ההצעות הסופיות החברה לא תנהל עוד משא ומתן עם המציעים. החברה תבדוק את כל ההצעות שיוגשו, לרבות ההצעות הראשונות ותקבל החלטתה.
- 5.5 במקרה בו רק מציע אחד ייכלל בקבוצת המציעים הסופית, החברה תהא רשאית לנהל עמו מו"מ ותהא רשאית להחליט כי המציע לא יהא חייב להגיש הצעה סופית לתיבת המכרזים, אלא להגישה בכתב או בכל דרך אחרת שתקבע. כמו כן, החברה רשאית להחליט שלא ינוהל עמו משא ומתן.

- 5.6 במקרה בו תוגש הצעה יחידה להליך, או שתיוותר הצעה יחידה לדיון, רשאית החברה להחליט על בחירת ההצעה או על עריכת הליך חדש.
- 5.7 החברה אינה מתחייבת לקבל את ההצעה הזולה ביותר או כל הצעה שהיא.
- 5.8 יובהר, כי חזרה מהצעה במסגרת הליך זה לאחר מועד ההודעה על הזכייה בהליך, תהווה הפרת חוזה לכל דבר ועניין. הפרת חוזה כאמור תקנה לחברה את הזכות לקבל פיצוי על פי כל דין, בגין הנזקים הישירים והעקיפים שנגרמו לה. כמו כן, במקרה של חזרה מהצעה כאמור לעיל, החברה שומרת לעצמה את הזכות לקבל את ההצעה המיטבית הבאה בתור או לצאת בהליך חדש, לפי שיקול דעתה הבלעדי.
- 5.9 מציע שלא זכה בהליך יהיה רשאי, בתוך 14 ימים ממועד מסירת ההודעה בדבר תוצאות ההחלטה הסופית של החברה, לעיין בפרוטוקול ועדת המכרזים, בהתכתבויותיה עם המציעים, בחוות דעת מקצועית שהוכנו לבקשתה, בעמדת היועץ המשפטי בוועדה ובהצעת הזוכה בהליך, ולקבל עותקים ממסמכים אלה, כאמור בסעיף 21(ה) לתקנות חובת המכרזים, התשנ"ג-1993, למעט:
- א. בחלקים של ההחלטה או ההצעה הזוכה אשר העיון בהם עלול לדעת החברה לחשוף סוד מסחרי או מקצועי, או לפגוע בביטחון המדינה, ביחסי החוץ שלה, בכלכלתה או בביטחון הציבור.
- ב. בחוות דעת משפטית שנערכה במסגרת ייעוץ משפטי לוועדה, לרבות בחינת חלופות אפשריות שונות לפעולה או להחלטתה של ועדת המכרזים, או הערכת סיכויים וסיכונים הנובעים מקבלת החלטות כאמור בהליכים משפטיים עתידיים.
- 5.10 לאור זכות העיון המוקנית למציעים בהליך על-פי דין, מציע שיש לו התנגדות למתן זכות עיון בהצעתו במלואה או בחלקה בשל סוד מסחרי או מקצועי שלו, שלדעתו כלול בהצעה, נדרש לסמן את החלקים החסויים בהצעתו ולציין את הנימוקים הרלוונטיים לחיסיון.
- 5.11 חלקים בהצעה אשר לא יסומנו על ידי המציע כחסויים ו/או לא יצוינו לגביהם הנימוקים לחיסיון יחשבו ככאלה שמבחינת המציע העיון בהם מותר. החברה אינה מחויבת לפנות למציע כדי לברר אם חלקים בהצעתו חסויים ו/או את הנימוקים לחיסיון, במקרה שאלו לא צוינו בהצעתו.
- 5.12 יובהר כי בכל מקרה ההחלטה בדבר חשיפה או חיסיון של חלקים בהצעה הינה בסמכות ועדת המכרזים של החברה, אשר רשאית לחשוף גם חלקים שהמציע ציין אותם כחסויים. בכל מקרה ולמרות האמור בכל הצעה, החברה תהיה רשאית לגלות את מחירי ההצעה הזוכה לכל מציע אשר יבקש גילוי כאמור.
- 5.13 מציע יהיה מנוע ומושתק מלטעון כי הוא זכאי לעיין בהצעת מציע אחר, בחלקים המקבילים לאלה אשר סומנו כסודיים בהצעתו.
- 5.14 מתן זכות עיון כאמור לעיל יהיה מותנה בתשלום לחברה בסך 350 ₪ כולל מע"מ.
- 5.15 אין לערוך כל מחיקות ושינויים במסמכי ההליך ואין להוסיף תנאים, תניות, בקשות או הסתייגויות מחיקות, שינויים, תוספות ע"ג המסמכים. יש לערוך כל תוספת ו/או בקשות במסמך נפרד. הסתייגויות או בקשות לשינויים יקנו לחברה זכות לפסול את ההצעה, או לחלופין, להתנות את שקילת ההצעה בהסרת המחיקות, השינויים, התוספות, ההסתייגויות ו/או הבקשות, תוך פרק זמן שייקבע ע"י החברה.
- 5.16 נוסף לכל המקרים האחרים שבהם החברה רשאית לבטל את ההליך על-פי דין, לחברה תהיה זכות לבטל את ההליך, בכל שלב שהוא, בכל אחד מהמקרים הבאים:

- א. מקרים שבהם מצאה החברה שהתקיים פגם מהותי בהליך הוצאת/ניהול ההליך או בהליך בחירת ההצעה הזוכה או ההצעה שהייתה אמורה להיות הזוכה.
- ב. במקרים שבהם גילתה החברה טעות או חסר במפרט או בתנאים המוקדמים להשתתפות, לאחר הוצאת ההליך.
- ג. חל שינוי נסיבות או השתנו צורכי החברה באופן המצדיק, לדעת החברה, ביטול ההליך.
- ד. יש בסיס סביר להניח שהמציעים או חלקם תיאמו הצעות או מחירים, או פעלו באופן המהווה הגבל עסקי או עבירה על חוק כלשהו.
- ה. מסיבות תקציביות ו/או ביצוע עצמי.
- 5.17 החברה לא תהא אחראית לתשלום כל פיצוי למציע כלשהו ו/או למי מטעמו בקשר לביטול ההליך בנסיבות המפורטות לעיל ובנסיבות אחרות שבהן היא רשאית לבטל את ההליך על-פי דין. אם יוחלט בחברה על ביטול ההליך, הודעה מתאימה תימסר למציעים.
- 5.18 החברה רשאית שלא לרכוש ו/או לממש ו/או לנצל כמות כלשהי של שירותים ו/או חלקי סעיף בהליך ו/או בהזמנה.
- 5.19 החברה תהא רשאית, בכל עת, לא לקבל הצעת משתתף בהליך, בהתאם לשיקול דעתה הבלעדי, אם על-פי הערכת החברה באשר לאיתנותו הפיננסית של המשתתף יימצא כי אינה מתאימה למתן השירות ולאספקת המוצרים הנדרשים ו/או לעמידה בכל ההתחייבויות הכלולות בתנאי ההתקשרות. תימסר הודעה מתאימה למציעים.
- 5.20 לאחר מתן הודעת הזכייה בהתקשרות, וניהול מו"מ אם יידרש, החברה תעביר למציע הזוכה הסכם/חוזה בכתב לחתימה. החוזה יוחזר לחברה חתום כדין ע"י המציע הזוכה, תוך 14 יום מתאריך משלוחו. אי החזרת החוזה לחברה, חתום כדין, תוך פרק הזמן שמצוין לעיל, יהווה הפרת חוזה מהותית מצד המציע הזוכה, אשר תקנה לחברה זכות לבטל את הודעת הזכייה ואת החוזה שנוצר בגין הודעת הזכייה, וזאת בנוסף לכל סעד אחר, שיעמוד לרשות החברה עפ"י דין. כ"כ, אי החזרת החוזה חתום כדין, לחברה, תקנה לחברה זכות להשהות כל תשלום, המגיע למציע הזוכה, עד למועד החזרת החוזה, חתום כדין, לחברה.
- 5.21 עם חתימת החוזה ע"י שני הצדדים, יחייב החוזה, על כל תנאיו ותניותיו, את הצדדים. תנאי או תניה, שלא נכללו בחוזה ובנספחיו, או במסמך אחר, הכלול בחוזה על דרך ההפניה, לא יחייב את הצדדים.

6. פרטים נוספים

- 6.1 משך ההתקשרות – שנה.
- 6.2 לחברה שמורה הזכות להאריך את משך תוקפה של התקשרות זו ב 2 תקופות נוספות בנות שנה כל אחת בתנאים זהים. בעניין זה, החברה תודיע לזוכה, בכתב, 30 ימים מראש, אם ברצונה להאריך את תקופת ההתקשרות. אין באיחור במסירת ההודעה משום ביטול זכותה של המזמינה להודיע על הארכת ההתקשרות.
- 6.3 החברה שומרת לעצמה את הזכות לבטל את הסכם ההתקשרות בכל עת על ידי מתן הודעה מוקדמת בכתב 30 יום מראש.
- 6.4 תנאי תשלום:
- תשלום חודשי בגין החודש הקודם.
- או בהתאם למו"מ שיתקיים עם נותן השירות.

7. הבהרות והשלמות

7.1 לשאלות והבהרות טכניות ניתן לשלוח דואר אלקטרוני למר יוסי זמיר בכתובת yossiz@ncsc.co.il.

נא לא לשלוח את הצעות המחיר לכתובת דוא"ל זו או לפקס של החברה, שכן הצעות אלו יפסלו ולא ידונו.

7.2 **בנוסף, על המציע להתעדכן בפרסומים באתר האינטרנט של החברה לגבי הבהרות טכניות להליך, עדכונים ותשובות לשאלות שנשאלות על ידי מציעים ועדכונים נוספים לגבי ההליך עד למועד האחרון להגשת הצעות.**

8. אופן הגשת הצעות

8.1 הנכם מתבקשים להעביר את הצעתכם (על גבי נספח ב' המצ"ב), מלאה וחתומה כדין עד ליום **31.10.18, בשעה 12:00** (להלן: "המועד האחרון לקבלת הצעות"), למייל מאובטח להלן:

tenders@ncsc.co.il

עבור

"שירותי SOC מנוהל ומערכת ניטור SIEM"

8.2 החברה שומרת לעצמה את הזכות לדחות את המועד האחרון שנקבע להגשת הצעות בכל עת לפני המועד הנ"ל.

8.3 הגשת ההצעה פירושה כי המציע מביע הסכמתו לכל האמור לעיל.

8.4 האחריות להגעת ההצעה למייל המאובטח הנ"ל עד המועד לקבלת ההצעות, חלה במלואה על המציע. הצעה שלא תגיע לתיבה זו במועד האמור לקבלת ההצעות לא תידון.

8.5 על מנת למנוע איחורים בהגשת ההצעה אנא דאגו להעביר הצעתכם לפני המועד האחרון לקבלת ההצעות.

בכבוד רב,

החברה הלאומית לאספקת פחם בע"מ

נספח ב'

תאריך: _____

לכבוד: החברה הלאומית לאספקת פחם בע"מ ("החברה")

באמצעות אימייל לכתובת: tenders@npsc.co.il

א.ג.נ.,

הנדון: למתן שירותי SOC מנוהל ומערכת ניטור SIEM

בהתאם למפורט בבקשתכם לקבלת הצעות מחיר למתן השירותים שבנדון אנו נהיה מוכנים לבצע את השירותים במחיר כדלקמן:

ש"ח לחודש עבור ביצוע השירותים (fixed price) בתוספת מע"מ כדין. _____

ש"ח בגין עלות הקמה ראשונית. _____

(לא מחיר לשעה, אלא מחיר כולל).

ההצעה בתוקף עד ליום **15.12.18**.

הסכמה לתנאי ההליך והחזרה

הנני מצהיר בזאת כי קראתי היטב והבנתי את נוסח מכתב הפנייה לקבלת הצעות למתן שירותי ביצוע העבודה וכי אני מסכים לכל האמור בהם ללא הסתייגויות כלשהן.

מסמכים הדרושים לפי חוק עסקאות גופים ציבוריים – התשל"ו - 1976

הריני להצהיר בזאת כי במועד הגשת ההצעה היו קיימים בידי כל המסמכים והאישורים הנדרשים לפי חוק עסקאות גופים ציבוריים (אישור מעודכן של עוסק מורשה לתשלומי מע"מ, אישור ניהול ספרים כדין) וכן לא הוצאו כנגדי / כנגד החברה האמורה או כנגד כל בעל זיקה אלי / אל החברה האמורה פסקי דין חלוטים, המרשיעים ביותר משתי עבירות, שנעברו לאחר יום 31 באוקטובר 2002 לפי חוק עובדים זרים (איסור העסקה שלא כדין והבטחת תנאים הוגנים), התשנ"א – 1991 ו/או לפי חוק שכר מינימום, התשמ"ז-1987 עד למועד האחרון להגשת הצעות.

חתימה וחתימת

שם החברה

מספר חברה

תאריך

תפקיד

שם החותם

נספח א

לפניה לקבלת הצעות למתן שירותי SOC מנוהל ומערכת ניטור SIEM

לחברה הלאומית לאספקת פחם בע"מ

דרישות מקצועיות ואפיון שירותים נדרשים

תוכן עניינים

3	הקדמה	.1
3	דרישות פונקציונליות - מערכת SIEM	.2
5	דרישות פונקציונליות - מיקור חוץ מוקד ניטור (SOC)	.3

1. הקדמה

1.1.1. מטרות

- 1.1.1.1. הספק יספק שירותי אינטגרציה (הטמעה, טיוב) למערכת ה-SIEM וגם יספק את שירותי הניטור (מוקד ה-SOC).
- 1.1.1.2. ניטור מרכזי של ארבעת אתרי החברה הלאומית לאספקת פחם : תל אביב (משרד מרכזי), אשקלון, חדרה, אתר DR (פתח תקווה).
- 1.1.1.3. הקמת מוקד שירות ניטור (Security Operation Center) SOC הכולל מערכת ניטור (Security Information and event management) SIEM. אשר תסופק ביחד עם השירות.
- 1.1.1.4. הפתרון יאפשר חיווי והתראות בזמן אמת לאירועים אשר יוגדרו ביחד עם החברה ויתריע עליהם לאנשי הקשר הרלוונטיים בחברה. להלן: שירותי איסוף אירועי אבטחת מידע ממערכות החברה ("אגרגציה"), איחוד ויצירת חוקים המתאימים לסיכונים שהוגדרו בחברה ("קורלציה"), ניתוח התראות ("אנאליזה"), חקר מעמיק של אירועים ("פורנזיקה").
- 1.1.1.5. השירות יינתן על ידי ספק מיקור חוץ (להלן: "הספק"), שבעה ימים בשבוע לאורך כל השנה לרבות ימי חג ושבטון.
- 1.1.1.6. השירות יבטיח כי התראות אלה, ידווחו בזמן אמת לאנשי הקשר הרלוונטיים בחברה אשר ישקלו את חומרת האירועים ודרך המענה האפקטיבית הנדרשת בטיפולם.

1.2. שיטה

שלבים עיקריים בפרויקט :

- 1.2.1. בניית תפיסת העבודה התואמת את יכולת החברה והצעת חלופות אפשריות על בסיס הדרישות המובאות במסמך זה. כאשר הניטור יעשה ממקום מרכזי (תל אביב) לכל ארבעת האתרים (תל אביב - ראשי, פתח תקווה - DR, סניפים : אשקלון, חדרה).
- 1.2.2. הקמת פתרון טכנולוגי התואם את סביבות העבודה הקיימות בארגון וגיבוש הארכיטקטורה שלו בניית תוכנית הטמעה, טיוב חוקה, בדיקות.
- 1.2.3. אפיון מרכז הבקרה לרבות העמדת כוח האדם הנדרש.
- 1.2.4. הפעלת השירות באופן מלא.

2. דרישות פונקציונליות - מערכת SIEM

2.1. סוג השירות

- 2.1.1. מערכת ה-SIEM תסופק כשירות (Software As a Service) ותוטמע בחצר החברה על תשתית וירטואלית של החברה

- 2.1.2. מערכת ה-SIEM אשר תסופק, תמוצב כ- Leader (על פי דוח גרטנר לשנת 2017 ובהם : IBM, SPLUNK, McAfee, Log Rhythm).
- 2.1.3. הסנסור וממשק הניהול יותקנו ברשת המחשוב של החברה ויתריעו על אירועים למנהל הרשת וגם לספק שירותי ה-SOC באמצעות ממשק מאובטח שיוקם לצורך השירות.

2.2. הדרכה וליווי טכני (בהקשר עם מערכת ה-SIEM)

- 2.2.1. בעת הפעלת השירות וכן בעת כל שדרוג מהותי (דוגמת שינוי גרסה), יקיים הספק הדרכות למנהל הרשת בתפעול, תחזוקה, ניהול חוקה, ניהול דוחות. ללא כל עלות נוספת.
- 2.2.2. הספק יקצה נציג טכני אשר יהא בקיא בטכנולוגיות המערכת, סוג השירות ומערכות החברה. זמינות הנציג תהא באופנים הבאים :
- 2.2.2.1. זמן שגרה - זמינות במהלך שעות פעילות החברה.
- 2.2.2.2. זמן חירום – 24/7/365 באמצעות אנליסט בכיר במוקד ה-SOC, או כל גורם טכני בכיר אשר יוגדר על ידי הספק לצורך כך.

2.3. ממשק ניהול וחוקה

- 2.3.1. ממשק הניהול יהא חשוף למנהל הרשת בחברה.
- 2.3.2. הגדרת החוקים במערכת ה-SIEM של החברה וטיובם יעשו בשיתוף מנהל הרשת בחברה ביחד עם הספק, אלא אם יוסכם אחרת.
- 2.3.3. מנהל הרשת יאשר את החוקה המוגדרת ב-SIEM.
- 2.3.4. מנהל הרשת יהא רשאי לשנות, להוסיף, להסיר ולערוך את החוקה. ואין בשינויים אלה משום עילה לבקשה לתוספת עלות לחברה.

2.4. ניטור מערכות צד ג'

- המערכת תקבל התראות או תיזום איסוף התראות מהמערכות הבאות :
- 2.4.1. אבטחת מידע : אנטי וירוס, מלכודות דבש HIPS, Firewall וכדומה.
- 2.4.2. מערכות תקשורת : מתגים, נתבים, Firewall, SSL VPN.
- 2.4.3. מערכות הפעלה : מיקרוסופט, Linux, DC, ESX, SQL.
- 2.4.4. שירותי אינטרנט : Web Services (Proxy) Mail Relay + Exchange.
- 2.4.5. מערך אחסון.
- 2.4.6. מדפסות רשת.
- 2.4.7. מערכת UPS.
- 2.4.8. תתכנה הוספת מערכות נוספות, הספק יסייע בחיבור מערכות חדשות לצורך ניטור.

2.5. דיווחים והתראות

- 2.5.1. המערכת תתריע ותדווח בזמן אמת על האירועים הבאים :

- אירועי אבטחת מידע ממערכות הניטור וההגנה.
- כשלים ועומסים במערכות תשתית.
- יצירה/הוספת/שינוי באובייקטים (משתמשים וקבוצות) חדשים, משתמשים חסומים, ניסיונות שימוש בחשבונות חסומים/נעולים, שינויים בהרשאות, כשלים/הצלחה בהזדהות למערכות המחשוב, התנתקות (Log Off), תקשורת ואבטחת מידע, שינויים במדיניות, יצירת שיתופים מקומיים, שינוי סיסמא.
- יצירת משתמשים לוקליים בתחנות עבודה, שרתים, מערכות תקשורת ואבטחת מידע.
- התקנת/הסרת תוכנות מתחנות עבודה ושרתים.
- ניטור גישה לתיקיות וקבצים רגישים.
- מחיקת קבצים או הודעות דוא"ל מאסיבית.
- התראות בגין אי זמינות של מערכת ה-SIEM (לדוגמא Sensor Down, או מערכות אשר יוגדרו כקריטיות על ידי החברה.

2.5.2. החברה תהא רשאית באופן עצמאי להוסיף/להסיר, לערוך חוקים ודוחות בהתאם לצרכיה. ואין בשינויים אלה משום עילה לבקשה לתוספת עלות לחברה.

2.6. דוחות סיכום ודוחות מתוזמנים

- 2.6.1. המערכת תייצר דוחות סיכום ודוחות מתוזמנים (יומי, שבועי, חודשי, רבעוני) בהתאם לחוקים שיוגדרו במערכת על כלל ההתראות אשר פורטו לעיל בסעיף 2.5 דיווחים והתראות.
- 2.6.2. הגדרת הדוחות תשתנה בהתאם לצרכי החברה.

3. דרישות פונקציונאליות - מיקור חוץ מוקד ניטור (SOC)

3.1. דרישות קדם

- 3.1.1. השירות יינתן משרדי הספק ממערכות מחשוב שאושרו על ידי החברה.
- 3.1.2. השירות יינתן מסביבה נפרדת שתוקם עבור החברה.
- 3.1.3. הספק יקיים בקרות אבטחה פיזית להגנה מפני גישה לא מורשית למתחם המוקד.

3.2. זמינות השירות

- 3.2.1. השירות יינתן 24/7/365.
- 3.2.2. יוגדרו זמני תגובה (להתראה או תגובה על בסיס בנק שעות) מקסימליים (SLA) בהם יתחייב הספק לעמוד.
- 3.2.3. הספק יעדכן בכל מקרה בו השירות אינו זמין מכל סיבה שהיא.

3.2.4. הספק יקיים תכנית המשכיות עסקית (BCP) והתאוששות מאסון (DR) הכולל אתר חלופי. תכנית זו תבטיח זמינות 24/7/365 של השירות הניתן. הספק יעביר עותק מהתכנית לחברה.

3.3. סוג השירות

- 3.3.1. הספק ילמד ויכיר את מבנה רשת המחשוב של החברה, מערכות המחשוב והטכנולוגיות הקיימות בחברה וכן את מתאר האיומים.
- 3.3.2. הספק נדרש לספק שירותי מיקור חוץ למוקד ניטור SOC וכן לפתרון למערכת SIEM. שני הפתרונות יינתנו על ידי אותו ספק כשירות (As A Service).
- 3.3.3. שירותי ה-SOC יינתנו ממשרדי הספק החיצוני, תוך שימוש במערכות הניטור המוצעת על ידי הספק כפתרון ה-SIEM.
- 3.3.4. השירות יספק התראות טלפוניות למנהל הרשת על בסיס מקרים ותגובות שיוגדרו ביחד עם החברה.
- 3.3.5. בשוטף לא תתאפשר גישה ישירה של הספק לניהול ותחזוקת מערכות המחשוב בחברה. לספק לא תהיה גישה ישירה למערכות המחשוב והוא יקבל את ההתראות דרך ממשק מאובטח בין מערכת ה-SIEM לבין מערכות הספק.
- 3.3.6. אופציונלי: הספק יציע בנוסף בנק שעות אשר ישולם על בסיס ביצוע בפועל וישמש בעת הצורך צוות תגובה מטעם הספק (Incident Response). החברה אינה מתחייבת לבצע שימוש בשירות זה.

3.4. חוקים והתראות

- 3.4.1. הספק והחברה יפעלו יחדיו מעת לעת ובהתאם לצרכי החברה, להגדרת וטיוב החוקים בשוטף לצורך שיפור ההתראות וצמצום התראות False Positive.
- 3.4.2. החברה תהיה רשאית להוסיף התראות וכן הוספת תוכנות אבטחת מידע / סייבר נוספות ואין בהוספת מערכות וחוקים משום עילה לבקשה לתוספת עלות לחברה.

3.5. כוח אדם

- 3.5.1. השירות יינתן על ידי מומחי סייבר בעלי ניסיון מוכח של 3 שנים לפחות בניהול ותחקור אירועי SOC.
- 3.5.2. הספק יפרט את כמות האנליסטים המבצעים עבודה במוקד אשר יוקצו לצורך ניטור האירועים ממערכות החברה.
- 3.5.3. השירות לחברה ינתן על ידי עובדים שאושרו על ידי החברה. עובדי הספק שלא אושרו על ידי החברה, לא יחשפו למידע של החברה ולא יספקו שירותים לחברה.

- 3.5.4. הספק יקצה אנליסט בכיר בעל ידע טכני שימש כגורם מומחה בהסלמת אירועים. האנליסטים הבכירים ידרשו גם בראיון אישי, אשר יבוצע להם במשרדי החברה, לבדיקת התאמתם לשירות. אנליסט בכיר אשר לא יאושר על ידי החברה, לא יוכל לספק שירותים במסגרת שירות זה והספק ידרש למצוא גורם בכיר אחר.
- 3.5.5. כלל העובדים אשר יספקו שירותים במסגרת הפרויקט ידרשו בחתימה על הסכם סודיות אישי.
- 3.5.6. החברה תהא רשאית לדרוש מהעובדים לעבור בדיקות מהימנות אצל בודק מוסמך בלתי תלוי, על חשבון הספק.

3.6. ממשקי עבודה

- 3.6.1. החברה והספק יבנו תהליך מאובטח להעברת ההתראות בין החברה ומערכת ה-SIEM, לספק ולמוקד הניטור.
- 3.6.2. הספק יבצע אנליזה לאירועים המתקבלים ממערכות הניטור ואבטחת המידע בממשק הניהול של המערכת המוצג עבורו.
- 3.6.3. הספק יסייע לחברה להגדיר סט תרחישים ותגובות, אשר יחייבו את הספק בדיווח התראה למנהל הרשת ו/או מי מטעמו. בנוסף החברה תגדיר לספק סט תרחישים ייעודיים על פי גורמי סיכון שיאופיינו על ידה.
- 3.6.4. תתאפשר הגדרת אסקלציה של דיווח במקרה של אי-זמינות הגורם האחראי בחברה בהתאם לרשימה שתוגדר מראש.

3.7. דיווח אירועים (Events)

- 3.7.1. החברה תגדיר לספק אירועים אשר בגינם יהא צורך לפנות לאנשי הקשר בחברה.
- 3.7.2. הדיווח לאנשי הקשר יעשה טלפונית ויועבר תיעוד במייל.
- 3.7.3. בעת הצורך יעביר הספק הנחיות טכניות להתמודדות עם אירוע בעת גילויו לרבות ליווי טכני עד לסגירת האירוע.

3.8. דוחות (Reports)

- 3.8.1. הספק יעביר דיווח יומי כל בוקר עם סגירת המשמרת וכן לאחר סופי שבוע/חגים.
- 3.8.2. הספק יעביר דוחות ודיווחים שבועיים וחודשיים על התראות.
- 3.8.3. הספק יעביר דוח מגמות על בסיס חודשי ושנתי.

3.9. סקרים וביקורות

- 3.9.1. הספק יסכים לשיתוף פעולה עם גופי הביקורת של/מטעם החברה במידה ויעלה צורך לבחינת מוכנות לבדיקת חוסן חברה, סקר בחצרות הספק, בחינת אפקטיביות השירות וכדומה.
- 3.9.2. החברה תהא רשאית לבצע ביקורת פתע בחצר הספק על מנת לוודא פעילות כמסוכם.

3.9.3. החברה תהיה רשאית לבצע סקר בחצרות הספק לרבות בחינה טכנולוגית למקורות בהם מוחזק מידע על החברה (במערכות הספק).

3.10. סיום ההתקשרות

3.10.1. בעת סיום ההתקשרות מכל סיבה שהיא, תהיה לחברה אפשרות להמשיך ולבצע שימוש במערכת ה-SIEM וברישוי על בסיס החוקה שהוגדרה בה בתנאים שייקבעו על ידי הצדדים.