**The National Coal Supply Corp. Ltd.**
20 Lincoln St. Tel-Aviv 6713412 Israel
Tel. +972-3-6257000; Fax. +972-3-6257001
E-mail: ncsc@ncsc.co.il

**החברה הלאומית לאספקת פחם בע"מ**
רחוב לינקולן 20 תל-אביב 6713412
טל. 03-6257000; פקס. 03-6257001
E-mail: ncsc@ncsc.co.il

23.10.18

## שאלות, תשובות והבהרות (2) בפנייה לקבלת הצעות למתן שירותי SOC מנוהל ומערכת ניטור SIEM לחברה הלאומית לאספקת פחם בע"מ

**להלן תשובות לשאלות אשר נשאלו על ידי משתתפים בהליך:**

**יודגש כי התשובות המפורטות במסמך זה מהוות חלק בלתי נפרד ממסמכי הפנייה.**

| סעיף | שאלה | תשובה |
|---|---|---|
| 2.2.1.1 | מבקשים להבהיר כי כוונת החברה הינה למוקד SOC אשר מנטר מספר לקוחות בו זמנית (כלומר לא SOC ייעודי). | ראה בנספח א סעיף 3.1.2 |
| 2.2.1.2 | האם הכוונה כי המערכת כולה מקצה לקצה תותקן בחצר הלקוח (All-In-One) או שמדובר בתצורת ענן כאשר רכיב איסוף מותקן בחצר הלקוח ומעביר אל כל המידע לענן . | הרכיב יותקן בחצר החברה. |
| 2.2.1.3 | מספר החוקים שניתן לכתוב הינה אינסופית ולכן נבקש להגדיר מספר אבסולוטי של חוקים על מנת שיהיה ניתן לתמחר ב.FIX | ניתן לקבוע כי יוגדרו כ 50 -חוקים בשיתוף המציע .אולם החברה תוכל להוסיף חוקים בעצמה ככל שיידרש ללא הגבלה וללא עלות נוספת (סעיף 2.3.4 בנספח א). |
| 2.2.14 | כנ"ל - מספר נהלי התגובה לאירועים - נדרש להגדיר מספר אבסולוטי של נהלי תגובה על מנת שיהיה ניתן לתמחר בFIX | ראה תשובה לשאלה קודמת. |
| 2.2.1.6 | על מנת לבצע פורנזיקה ברמה גבוהה נדרש שיהיו כלים מתאימים ברשת הלקוח .האם מותקנת ברשת מערכת המאפשרת ביצוע פורנזיקה לתחנות קצה) דוגמת CARBON (BLACK, SECDO | לא .אולם, הדרישה היא למקצועיות כ"א בשירות הניתן .כלומר, ניתן לספק שירותי פורנזיקה גם ללא מערכות אלה . נדרש ניסיון בנושא. |
| 2.2.1.6 | על מנת לבצע פורנזיקה ברמה גבוהה נדרש שיהיו כלים מתאימים ברשת הלקוח .האם מותקנת ברשת מערכת המאפשרת ביצוע פורנזיקה לתעבורת רשת) דוגמת NetWitness RSA)? | לא .אולם, הדרישה היא למקצועיות כ"א בשירות הניתן .כלומר, ניתן לספק שירותי פורנזיקה גם ללא מערכות אלה . נדרש ניסיון בנושא. |
| 2.2.2 | לא ניתן להתחייב שכל האנליסטים יהיו בעלי 3 פלוס שנות ניסיון שכן מדובר בצוות גדול) כ 25 עובדים (אשר חלקו מורכב מעובדים עם יותר ניסיון וחלקו עם פחות. | מדובר בדרישת סף - עבור אותם עובדים שנותנים את השירות לחברה, לא עבור כלל העובדים בחברה. |
| 2.2.3 | נבקש לאשר כי חיבור ה SIEM יתבצע יחד עם שותף עסקי בעל הניסיון גדול ביותר עם מערכת הQradar IBM | מקובל .האחריות הכוללת היא של המציע. |

| | | |
|---|---|---|
| 2.5.1 | נדרש לקבל מראש את נהלי אבטחת המידע על מנת שניתן יהיה להתחייב | ניתן לעיין בחומר הנדרש בתיאום מראש במשרדי החברה בת"א בימים ראשון עד חמישי בין השעות 30 :16-30 :8 ובכפוף לחתימה על הסכם סודיות .לתיאום : יוסי זמיר - yossiz@ncsc.co.il |
| 1.1.3 | האם הכוונה ל מערכת במודל של שירות מנוהל בתצורת ענן או בחצר הלקוח? | בחצר הלקוח. |
| 1.1.3 | במידה ומדובר בשירות בתצורת ענן ,האם המידע שנאסף מחוייב להישמר בגבולות מדינת ישראל ? | לא מדובר בשירות ענן. |
| 2.1.1 | האם הכוונה לקולקטור שיותקן ויאסוף את המידע ויעביר לספק או את כל המערכת עצמה מותקנת בחצר הלקוח | כן. |
| 2.3.1 | במידה ומעוניינים לגעת בחוקים ולשנות חוקים - מדובר בדרישה להרשאות אדמין אותה לא יהיה ניתן לאפשר כאשר השירות בתצורת שירות מנוהל בענן אלה רק בהתקנה מקומית של המערכת. | מדובר בדרישת סף .כאמור המערכת תותקן בחצר הלקוח. |
| 2.4 | נבקש רשימה מפורטת כולל כמויות מדויקות של הרכיבים אותם החברה רוצה לנתר על מנת שיהיה ניתן לתמחר ב.FIX | ניתן לעיין בחומר הנדרש בתיאום מראש במשרדי החברה בת"א בימים ראשון עד חמישי בין השעות 30 :16-30 :8 ובכפוף לחתימה על הסכם סודיות .לתיאום : יוסי זמיר - yossiz@ncsc.co.il |
| 2.5 | מערכות ה SIEM אינן בנויות במקור לביצוע ניטור של כשלים ועומסים במערכות תשתית ,לרוב נהוג להתקין מערכת NOC המיועדת לנושא. | יש לייצר התראות גם בנושא כשלים ועומסים. |
| 3.1.2 | מבקשים הבהרה/פירוט לגבי הדרישה לסביבה נפרדת | תשתית נפרדת בחצר הספק המבטיחה כי מידע של החברה לא ימצא בסביבת מידע של לקוחות נוספים של הספק (תחנות עבודה ,מסד ,ממשק ניהול נפרד וכדומה). |
| 3.2.4 | נבקש לעדכן בדרישה כי תכנית ה BCP וה DR תועבר רק לאחר קבלת אישור הזכייה וחתימה עלNDA | מקובל. |
| 3.5.6 | האם בדיקת תחקיר בטחוני מספקת בסעיף זה ? | לא. תחקיר בטחוני קובע סיווג בטחוני, שאינו נדרש, ולא נושאי מהימנות. |
| 3.10.1 | הסעיף ניתן ליישום במידה והמערכת מותקנת בחצר הלקוח בתצורה של - (All-In-One) כלומר לא בתצורת ענן | יותקן בחצר הלקוח. |
| | נבקש לקבל את כמות ה EPS הנדרשת אותה החברה מעוניינת לרכוש | ניתן לעיין בחומר הנדרש בתיאום מראש במשרדי החברה בת"א בימים ראשון עד חמישי בין השעות 30 :16-30 :8 ובכפוף לחתימה על הסכם סודיות .לתיאום : יוסי זמיר - yossiz@ncsc.co.il |