

**מרכז החישובים הבינאוניברסטאי**

**נספח 0.11 - תבנית להגשת הצעה**

**מכרז פומבי מס' 1/2019**

**לאספקת ותחזוקת מערכת SIEM ושירות CSOC**

**מכרז פומבי מס' 1/2019**

**נספח 0.11 - תבנית להגשת הצעה**

**לאספקת ותחזוקת מערכת SIEM ושירות CSOC**

תוכן העניינים

[1. יעדים ומטרות 4](#_Toc535840432)

[1.1 תמצית השירותים: מערכת SIEM, שירות CSOC 4](#_Toc535840433)

[1.1.1 מערכת SIEM בתצורת Multi-Tenancy 4](#_Toc535840434)

[2. SOW – תיחום 4](#_Toc535840435)

[2.2 דרישות מערכת SIEM 4](#_Toc535840436)

[2.2.1 דרישות מהמוצר המוצע 5](#_Toc535840437)

[2.2.2 דרישות תצורה 7](#_Toc535840438)

[2.2.4 תהליכים 8](#_Toc535840439)

[2.3 מקורות מידע ורכיבי תשתית מנוטרים 8](#_Toc535840440)

[2.3.1 רכיבי תקשורת 9](#_Toc535840441)

[2.3.2 רכיבי אבטחה 9](#_Toc535840442)

[2.3.3 מערכות הפעלה ושירותים מבוססי Microsoft Windows 9](#_Toc535840443)

[2.3.4 תחנות עבודה 9](#_Toc535840444)

[2.3.5 מערכות מבוססות SharePoint 9](#_Toc535840445)

[2.3.6 שרותי דוא"ל על בסיס Microsoft Office 365 & Google G-Suite 10](#_Toc535840446)

[2.3.7 תשתית וירטואלית 10](#_Toc535840447)

[2.3.8 רשימת מקורות מידע 10](#_Toc535840448)

[2.4 מסכי מערכת SIEM 10](#_Toc535840449)

[2.4.1 מסכים נדרשים 10](#_Toc535840450)

[2.4.8 מסך ניהול הידע (Knowledge base) 10](#_Toc535840451)

[2.5 שירותים שוטפים למערכת SIEM 11](#_Toc535840452)

[2.5.2 תפעול ותחזוקה שוטפים 11](#_Toc535840453)

[2.7 שירותים שוטפים CSOC 11](#_Toc535840454)

[2.9 היקפים עומסים וביצועים 11](#_Toc535840455)

[2.9.2 היקפים ועומסים 11](#_Toc535840456)

[2.11 גיבויים ושרידות 11](#_Toc535840457)

[3. רמת שירות 12](#_Toc535840458)

[4. מימוש והקמה 12](#_Toc535840459)

[4.1 תפקידי מפתח 12](#_Toc535840460)

[4.1.1 מנהל פרויקט הקמה 12](#_Toc535840461)

[4.1.2 מנהל שירות CSOC 13](#_Toc535840462)

[4.1.3 אנליסט 13](#_Toc535840463)

[4.1.4 בקרי CSOC 14](#_Toc535840464)

[4.1.5 ארכיטקט 15](#_Toc535840465)

[4.1.6 מיישם SIEM 15](#_Toc535840466)

[4.2 הקמת מערכת SIEM 16](#_Toc535840467)

[4.2.2 ניהול הפרויקט 16](#_Toc535840468)

# יעדים ומטרות

## תמצית השירותים: מערכת SIEM, שירות CSOC

### מערכת SIEM בתצורת Multi-Tenancy

מערכת ניהול אירועים תתבסס על מוצר מדף ידוע ומוביל בשוק, אשר נבחן ויושם בישראל בתצורת Multi-Tenancy עם לפחות 5 לקוחות פעילים ביישום.

תינתן עדיפות למערכת SIEM שנכללת בשנים 2017/2018 ברביע ימני עליון של גרטנר ו/או ב- LEADERS של פורסטר.

**מענה המציע:**

1. טבלת לקוחות פעילים בתצורת Multi-Tenancy במוצר המוצע.

מערכת ה- SIEM המוצעת:

שם המוצר :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

שם היצרן : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| # | שם הלקוח | שם איש קשר | פרטי התקשרות: טלפון וכתובת e-mail |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. דוח גרטנר או פורסטר. יש לצרף לינק לאתר מתאים במרשתת או צרופה כמענה לסעיף.

# SOW – תיחום

## דרישות מערכת SIEM

להלן דרישות ממערכת SIEM מבוקשת. לשם הסרת ספק, הלקוח יהיה רשאי לעשות שימוש במלוא הפונקציונליות של מערכת SIEM המוצעת, לרבות בפונקציונאליות שלא נכללה בדרישות מקוריות של המזמין.

הנחיות למענה עבור כל דרישה:

**עמודת הקמה**

* Y –הדרישה כלולה במסגרת פרויקט הקמת המערכת.
* N –הדרישה אינה כלולה במסגרת פרויקט ההקמה, והמימוש שלה יידחה למועד מאוחר יותר לפי החלטת המזמין וישולם בנפרד.

**למילוי על ידי המציע**

* OoB – לציין Y אם דרישה זו נכללת ברמת Out Of The Box של מערכת SIEM מוצעת, ללא צורך בפיתוח חיצוני או בהפעלת API (קסטומיזציה באמצעות תפריטי מערכת תיחשב כ OoB), אחרת לציין N.
* פיתוח – לציין Y אם לשם תמיכה בדרישה זו יש צורך לבצע פיתוח חיצוני ואינטגרציה באמצעות API של המערכת, אחרת N.
* מענה המציע – מענה מפורט לאופן התמיכה והמימוש של הדרישה.

### דרישות מהמוצר המוצע

| # | דרישה | הקמה | OoB  Y/N | פיתוח  Y/N |
| --- | --- | --- | --- | --- |
| SIM01 | מערכת SIEM תכלול מנגנון לבדיקת Rules קיימים ו- Rules חדשים על DATA היסטורי הנמצא במערכת ברמת גישה Online | Y |  |  |
| מענה המציע |  | | | |
| SIM02 | מערכת SIEM תכלול יכולת חיפוש התרחשות אירוע במוסד ע"ס תבנית אירוע אבטחת מידע שזוהה במוסד אחר המקושר למערכת | Y |  |  |
| מענה המציע |  | | | |
| SIM03 | מערכת SIEM תכלול ממשקים למקורות מידע מודיעינים חיצוניים, כדוגמת מערך הסייבר, ותתמוך בפרוטוקולי תקשורת סטנדרטיים כדוגמת STIX/TAXII | Y |  |  |
| מענה המציע |  | | | |
| SIM04 | המערכת תכלול יכולת קישור לוגי בין פרמטרים שנוצרים במערכות שונות אך מייצגים אותו ערך לוגי. המערכת נדרשת ליצור קשר לוגי בחיפוש ובחוקי מערכת לזיהוי אותו משתמש | Y |  |  |
| מענה המציע |  | | | |
| SIM05 | תגובה ותחקור אירוע – המערכת תאפשר תיעוד אירועים, תגובה ויכולת תחקור אירועים. כמו כן, השלמת נתונים נדרשים לתחקור אירועים והוצאת דו"חות אוטומטית מהמערכת | Y |  |  |
| מענה המציע |  | | | |
| SIM06 | יכולת איסוף ראיות – איסוף ראיות הכרחי למצב בו אחד המוסדות יבקש לתבוע או לערב גורמים חיצוניים, כדוגמת רשויות אכיפת חוק, באירוע שאירע. בשל העובדה שהמערכת הינה לאיסוף אירועים, הרי שבסיס הנתונים המרכזי של המערכת יכלול איסוף ראיות ותיעוד אירועי אבטחה | Y |  |  |
| מענה המציע |  | | | |
| SIM07 | דיווחי הנהלה מוסדיים – המערכת תאפשר הוצאת דיווחים מיידים על אירועי אבטחה, תגובה לאירוע והשלכות על המוסד | Y |  |  |
| מענה המציע |  | | | |
| SIM08 | תצורת איסוף נתונים ממקורות מידע שונים מפורטת בהמשך המסמך – דיאגרמה מלאה של איסוף נתונים, פרוטוקולים, להיכן ירוכזו נתונים, שרתי ביניים וכו | Y |  |  |
| מענה המציע |  | | | |
| SIM09 | איסוף התראות – ברירת מחדל ללא סוכן (Agentless) - משמע קישור המערכת למשיכת נתונים ישירות ממקורות מידע/ אפליקציות, במטרה להקל על פעילות תחזוקה ותפעול של המערכת. זאת למעט מספר מועט של מערכות שמזמין/ מוסד ישתכנעו כי אין דרך אחרת או כי עדיף לחברן באמצעות סוכן | Y |  |  |
| מענה המציע |  | | | |
| SIM10 | להלן דרכי התממשקות אפשריים למערכת איסוף אירועים המקובלות על המזמין. על המציע לתמוך בכל האפשרויות המצוינות להלן. אם אחת מהאפשרויות אינה נתמכת ו/או קיימות אפשרויות נוספות, על המציע לפרטן.   * עבודה עם סוכן - קישור מערכות באמצעות התקנת סוכן מערכת לאיסוף ושליחת מידע מתוך המערכת. * שליחת לוג ב- Syslog - אחת האפשרויות להעברת לוג מהמערכת הינה באמצעות שליחת לוג לשרת Syslog ייעודי בתשתית המזמין. * העתקת לוג (דיסקים משותפים) - אפשרות נוספת להעברת לוג הינה העתקת לוג באמצעות דיסק משותף ארגוני אשר בו יכתבו כלל הקבצים ומשם יועלו למערכת האיסוף. * שליחת קובץ באמצעות מערכת א-סינכרונית - העברת לוג באמצעות שליחת קובץ באמצעות מערכת א-סינכרונית כדוגמת שרתי דואר / FTP וכד. | Y |  |  |
| מענה המציע |  | | | |
| SIM11 | בקרה על תהליך קבלת לוג/אירועים - כל תצורת התממשקות המשלבת קובץ לוג כמפורט לעיל תכיל בקרה Quality Assurance: קובץ הועתק במלואו/ הגיע במלואו לייעדו, קובץ לא הועתק, קובץ גדול מדי ועוד. בקרה מלאה על כל הפעילויות מקצה לקצה, כולל אישור תקינות קובץ והגעתו לשרת שיוגדר. על המציע לפרט מהם המנגנונים הקיימים במערכת המוצעת לאישור תקינות הקובץ. | Y |  |  |
| מענה המציע |  | | | |
| SIM12 | תיעדוף אירועים  על המערכת המוצעת להכיל מנגנון תיעדוף המשקלל מספר פרמטרים, כדוגמת רמת חומרת אירוע (אומדן נזק), רמת פגיעות מקור מידע (הסתברות להתרחשות נזק) ועוד. אם המערכת אינה מכילה מנגנון מובנה לתיעדוף, יש לפרט כיצד ניתן לשלב מנגנון כזה?  יש לתאר את מנגנון תיעדוף קיים במערכת המוצעת, מהם הפרמטרים הבסיסיים במערכת, כיצד מבוצע חישוב ואופן ביצוע התאמות. | Y |  |  |
| SIM13 | ממשק המשתמש יהיה פשוט, נוח וידידותי למשתמש מבוסס Web או GUI חלונאי. הממשק יתמוך בשילוב שדות בעברית ואנגלית, לרבות הצגת אירוע, תגובה ותחקור אירוע. | Y |  |  |
| מענה המציע |  | | | |
| SIM14 | נדרש לציין האם במערכת קיימת יכולת להוספת מודלים נוספים כגון: יכולת AI, ניתוח אירועים אוטומטי או מערכות לומדות, לצורך קבלת מפת איומים משוכללת יותר – יש לצרף עמוד רלוונטי בלבד של נספח טכני של היצרן בו יודגש המענה לרכיב המפורט. | N |  |  |
| מענה המציע |  | | | |
| SIM15 | תוכנות לבדיקת פגיעויות - על המציע לפרט מול איזה כלי Vulnerability Assessment/Scanner המערכת יודעת לעבוד. | N |  |  |
| מענה המציע |  | | | |
| SIM16 | גיבויים מעצם הגדרתם מאפשרים גישה למידע רגיש ללא הגנות מ"ה. לכן נדרש לתעד כל גישה לגיבוי וכל אחזור ולשמור תיעוד לתחקיר למקרה של אירוע דלף מידע. | Y |  |  |
| מענה המציע |  | | | |
| SIM17 | שליטה בתשתית ווירטואליזציה מאפשרת גישה מלאה למערכות המתארחות תוך מעקף הגנות מ"ה. לכן נדרש לתעד כל גישה, יצירת שרת, העתקת שרת וכו' ולשמור את התיעוד לתחקיר למקרה של אירוע אבטחת מידע. | Y |  |  |
| מענה המציע |  | | | |

### דרישות תצורה

1. תצורת המערכת וכתב כמויות של ארכיטקטורה נדרשת – נדרש לצרף תרשים, רכיבים קיימים במערכת, מיקום הרכיבים בתשתית המזמינה, תפקיד כל אחד מהרכיבים בתשתית, תרשימי זרימת מידע (חד כיווני, דו כיווני לרבות פרוטוקולים ופורטים). אם ישנם מספר פתרונות אפשריים, יש לפרט אותם ולהמליץ על הפתרון המועדף.

**מענה המציע:**

1. קישור אל מקורות מידע (לפי רשימה בנספח 2.3.8) – נדרש לפרט תצורת קישור ותרשימי זרימת מידע (חד כיווני ודו כיווני, לרבות פרוטוקולים ופורטים).

**מענה המציע : במסגרת המענה לנספח 2.3.8**

1. תהליך ניהול מערכת - תרשימי זרימת מידע (חד כיווני ודו כיווני, לרבות פרוטוקולים ופורטים). יש לצרף תרשים.

**מענה המציע:**

### תהליכים

על המציע לפרט את אופן מימוש התהליכים שלהלן במערכת, עפ"י שלבים מתחילתם ועד סופם. על הפירוט לכלול את פעולות המערכת, לאילו רכיבים המערכת פונה, באילו פרוטוקולים, תתי תהליכים של אבטחה – זיהוי, הרשאות וכו'.

1. **תהליך איסוף ממקור מידע** – יש לתת דגש על מקורות מידע שונים. עבור נפילת בסיס נתונים/ בעית תקשורת וכד’ - על המציע לפרט מה קורה במצב בו בסיס נתונים נפל? האם נשמרים/ נאגרים נתונים במקור מידע? כיצד מתבצע תהליך התאוששות?
2. **תהליך אימות מקור מידע** - על המציע לפרט כיצד יאמת שמקור מידע מדווח למערכת? אם המערכת אינה מכילה תהליך אימות אינהרנטי, על המציע לפרט איך יטמיע תהליך אימות במערכת.
3. **תהליך שדרוג מערכת** - על המציע לפרט ברמה כללית את תהליך שדרוג המערכת, שלבים, השלכות.
4. **דוחות ושאילתות** – על המערכת להפיק עצמאית דוחות וסטטיסטיקות. דוחות יופקו בתהליך יזום ע"י משתמש מורשה ו/או ע"י טריגר אוטומטי (כדוגמת scheduler), בפורמט PDF ו-HTML, יוצגו בפורטל אבטחה וכן יישלחו בדואר אלקטרוני לגורמים שונים אצל המזמין, עפ"י רשימת תפוצה מוגדרת מראש.

**מענה המציע:**

## מקורות מידע ורכיבי תשתית מנוטרים

על המערכת להתממשק למגוון מערכות בכל מוסד ובנוסף למערכות שונות במחב"א. המזמין יתעדף הצעות שכוללות פרסר מובנה לאיסוף וניטור מערכות מידע שנמצאות ברשות המוסדות. על המציע לפרט אופן קישור עבור כל מקור מידע מבוקש, בהתאם לרשימת מקורות מידע (סעיף 2.3.8).

הפירוט הבסיסי הנדרש, ברמה של כל מקור מידע, הינו:

1. האם מערכת SIEM תומכת OoB באיסוף מידע של מקור המידע?
2. יכולות סינון אירועים ברמת נקודת קצה.
3. אילו גרסאות מקור מידע נתמכות על ידי היצרן? אם אין תמיכת יצרן בגרסה עדכנית של מקור המידע, יש לפרט מועד מתוכנן לתמיכה כזו.
4. אם אין תמיכת יצרן למקור מידע, האם הספק פיתח פרסר ייעודי לאיסוף ממקור המידע, שניתן לעשות בו שימוש במערכת SIEM המוצעת?

**מענה המציע : יש למלא את נספח 2.3.8**

בנוסף, יש לפרט ברמה הכללית של מערכת SIEM:

1. כיצד יבוצע איסוף מידע (פרוטוקולים, תצורת קישור חד/דו כיוונית, גורם יוזם)?
2. האם קיימת תמיכה בהסתרת מידע פרטי (כמו ת.ז., שדה סיסמא וכו’) ואי העברתו למערכת?
3. מהם ביצועי המערכת לכל אחת משיטות איסוף מידע? לציין עומסים שבהם המערכת תעמוד.

**מענה המציע לסעיפים ה'- ז' :**

### רכיבי תקשורת

נתבים ומתגים: סוגי ציוד תקשורת במוסדות השונים הינם מגוונים (יצרנים ודגמים). על המציע לפרט כיצד יתממשק לרכיבים אלה?

מהו טווח העומס שייצור איסוף לוג על קווי תקשורת רחבה בין רשת מוסדית למחב"א ועל תשתית רשת פנימית במוסד.

**מענה המציע:**

### רכיבי אבטחה

לכל מוסד תשתית אבטחת מידע עצמאית הנשענת על מגוון רכיבים נפרדים כגון Firewall אחד או יותר, אשר מגן על הקישור לאינטרנט וכן על תשתית התקשורת הפנימית, מערכות גישה מרחוק, תוכנות אנטי-וירוס ועוד, חלקם מצוינים בנספח 2.3.8.

עבור כל רכיב המצוין בנספח יש לציין את הממשק אליו. כמו כן, האם מדובר בממשק קיים במוצר או שיש צורך לפתח ממשק ייחודי?

**מענה המציע:**

### מערכות הפעלה ושירותים מבוססי Microsoft Windows

ברשת המוסדות קיימים מגוון שרתי Windows לשימושים שונים כגון: Active Directory, Domain Controller, WEB. על המציע לפרט יכולת איסוף מידע ממוקד ממערכות אלה, כולל יכולת סינון אירועים ברמת נקודת קצה.

**מענה המציע:**

### תחנות עבודה

ייתכן שבחלק מהמוסדות יוחלט לאסוף אירועים מתחנות עבודה (משתמשים - בעיקר MS Windows אך לא מחייב), חלקן או כולן (לפי החלטת המוסד המזמין). על המציע לפרט יכולת איסוף מידע ממוקד ממערכות אלה, כולל יכולות סינון אירועים ברמת נקודת קצה.

**מענה המציע:**

### מערכות מבוססות SharePoint

מערכות SPS שבחלקן מותקנות On-Prem ובחלקן כשירות בענן (של 365), מאחסנות מידע רגיש שיש לנטר את הגישה אליו. על המציע לפרט אם קיימת יכולת כזו וכיצד ניתן לממשה.

**מענה המציע:**

### שרותי דוא"ל על בסיס Microsoft Office 365 & Google G-Suite

על המציע לפרט יכולות איסוף מידע ממערכות אלה, אופי מידע שנאסף, האם מדובר ביכולות מובנות במערכת SIEM או באמצעות מוצר צד שלישי.

**מענה המציע:**

### תשתית וירטואלית

תשתית ווירטואלית במוסדות השונים מבוססת ברובה על VMWare. על המציע לפרט את הממשק שלו למערכת, אילו אירועים יכול לאסוף למערכת SIEM, ועבור אילו אירועים יש צורך בפיתוח נוסף.

**מענה המציע:**

### רשימת מקורות מידע

1. הספק נדרש לתמוך בכל גרסאות התוכנה המותקנות במוסדות.
2. הספק אינו מחויב לתמוך בגרסאות אשר אינן נתמכות על ידי היצרן ומוגדרות כ- EOL.
3. המציע יציין יכולת תמיכה במערכות מדף ומוצרי קוד פתוח.
4. המציע יפרט בנספח [2.3.8](#_נספח_2.3.8_רשימת) את יכולותיו לאיסוף מידע ממקורות המידע השונים המפורטים בנספח.

**מענה המציע : יש למלא את נספח 2.3.8**

## מסכי מערכת SIEM

### מסכים נדרשים

1. על המציע לפרט בנפרד עבור כל אחד מהמסכים להלן, האם המערכת תומכת ברמת ונילה במסך המבוקש או נדרשת התאמה ברמת קסטומיזציה או שנדרש לבצע פיתוח חיצוני.

| מערכת SIEM/SOC - מסכים נדרשים | מענה המציע |
| --- | --- |
| מסך Login (כניסה למערכת) |  |
| מסך מרכזי |  |
| מסך אירועים |  |
| מסך פירוט אירוע |  |
| מסך תחקור אירוע |  |
| מסך דו"חות וסטטיסטיקות |  |
| מסך Knowledge base |  |

### מסך ניהול הידע (Knowledge base)

1. מסך ניהול ידע הינו מסך שישמש את אנשי המוסד הרשאים לגשת למערכת ואת אנשי SOC.
2. המסך יאפשר קבלת מידע ונתונים להחלטה וטיפול באירוע/סגירת אירוע, קרי על פתיחת/אי פתיחת אירוע במסך אירועים. המסך הינו חיוני, מאחר ובקרים שמתפעלים מערכות אינם מכירים באופן מעמיק את המוסדות.
3. המסך הנדרש יחולק לשני תתי מסכים: תת מסך ראשון – יציג מידע על אירוע ותת מסך שני – מסך הזנה שכל גורם מוסמך מאבטחת מידע יוכל להזין מידע על אירועים קיימים/חדשים.
4. המציע נדרש לצרף צילומי מסך המדגימים את כל אחד מהמסכים עם ציון סוג המסך בכל צילום.

**מענה המציע** : צירוף מסכי ניהול ידע כנדרש.

## שירותים שוטפים למערכת SIEM

### תפעול ותחזוקה שוטפים

**מענה המציע**: המציע נדרש לפרט משאבים קיימים ברשותו בישראל לתפעול, שירות ותחזוקת המערכת. יש לפרט הסמכות יצרן מערכת, התמחויות וכמויות מומחים הנמנים על עובדי המציע או עובדי קבלן משנה, ככל שקיים.

## שירותים שוטפים CSOC

**מענה המציע:** המציע נדרש לפרט משאבים קיימים ברשותו בישראל לשירותי CSOC. יש לפרט , הסמכות רלוונטיות בתחום אבטחת המידע, התמחויות וכמויות מומחים הנמנים על עובדי הספק או עובדי קבלן משנה, במידה וקיים כזה עבור שירותי CSOC.

## היקפים עומסים וביצועים

### היקפים ועומסים

1. עבור חלופת SIEM מנוהל על המציע לפרט את תצורת וכתב כמויות המערכת על מנת לתמוך בדרישות, וכן כיצד תצורת וכתב הכמויות ישתנו כתוצאה מגידול בכמות האירועים (EPS). בהתאם לדרישות, על המציע לתכנן ארכיטקטורה עבור פתרון IaaS ועבור תצורת תשתית נדרשת למקרה של הרצה ב- On Prem.

**מענה המציע**:

**פתרון נדרש עבור תשתית SIEM מנוהל על בסיס IaaS**

**פתרון נדרש עבור תשתית SIEM מנוהל על בסיס תשתית On Prem**

## גיבויים ושרידות

המציע נדרש לספק פתרון גיבוי ושרידות לכל אחד מרכיבי המערכת, לשימור נתונים ותצורה, למניעת אובדן ולהתאוששות מהירה. עבור כל פתרון שרידות, על המציע לפרט תהליך מלא של שחזור המערכת.

הספק יידרש לספק נוהל גיבוי ושחזור של מערכת SIEM. הנוהל יגדיר מהם קבצי המערכת ומיקום קבצי האירועים הנדרשים לגיבוי, את תצורת הגיבוי המועדפת וכן תדירות גיבוי מומלצת.

לפני העלאה לייצור בתצורת מערכת במחב"א יופק Image לשרתים למטרות שחזור.

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

**מענה המציע:**

# רמת שירות

# מימוש והקמה

## תפקידי מפתח

### מנהל פרויקט הקמה

1. **אחריות**

* ניהול פרויקט הקמת המערכת והשירות.
* Single Point of Contact למזמין.

1. **דרישות**

* ביצע תפקיד מנהל פרויקט במשך חמש שנים לפחות בעשור האחרון.
* ביצע תפקיד מנהל פרויקט בתחומי השירות המבוקשים במשך שלוש שנים לפחות ב-5 שנים קודמים להגשת ההצעה.
* בעל ידע מוכח באבטחת מידע והגנת סייבר.
* בעל ידע מוכח במתודולוגיה של ניהול פרויקטים
* **השכלה** – אקדמית.

1. **מענה המציע**

המציע יצרף קורות חיים של המועמד לתפקיד.

המציע יספק תיאור של המועמד המוצע בטבלאות שלהלן. על הטבלאות לשקף את אופן עמידת המועמד בדרישות.

המציע יתאר תפקידי ניהול פרויקט רלוונטיים שביצע המועמד. המציע ימלא פרטים בטבלה שלהלן עבור כל תפקיד. יש למלא עד 4 פרויקטים לכל היותר. ניתן לשכפל בהתאם את הטבלה.

|  |  |  |
| --- | --- | --- |
| **מועמד לתפקיד מנהל פרויקט** | | |
| **שם המועמד** | |  |
| **הארגון בו נהל פרויקט** | |  |
| **השנים בהן בוצע התפקיד** | |  |
| **תיאור הפרויקט אותו ניהל** | | |
|  | | |
| **פירוט נושאים שהיו כלולים בניהולו** | | |
|  | | |
| **הגורם שהיה הממונה בארגון** | **שם** |  |
| **תפקיד** |  |
| **טלפון** |  |

### מנהל שירות CSOC

1. **אחריות -** ניהול מרכז שירות **CSOC**.
2. **דרישות**

* ביצע תפקיד מנהל SOC במשך שלוש שנים לפחות בעשור האחרון.
* בעל ידע מוכח באבטחת מידע והגנת סייבר.
* בעל הסמכה בתחום אבטחת מידע והגנת סייבר.
* **השכלה** – אקדמית באחד מהתחומים הבאים - מדעי המחשב, מערכות מידע, מדעים מדויקים, הנדסה מחשבים/חשמל/מערכות מידע.

1. **מענה המציע**

המציע יצרף קורות חיים של המועמד לתפקיד.

המציע יספק תיאור של המועמד המוצע בטבלאות שלהלן. על הטבלאות לשקף את אופן עמידת המועמד בדרישות.

המציע יתאר תפקידים רלוונטיים שביצע המועמד. המציע ימלא פרטים בטבלה שלהלן עבור כל תפקיד. יש למלא עד 4 תפקידים לכל היותר. ניתן לשכפל בהתאם את הטבלה.

|  |  |  |
| --- | --- | --- |
| **מועמד לתפקיד מנהל שירות CSOC** | | |
| **שם המועמד** | |  |
| **הארגון בו נתן תמיכה ב- SOC** | |  |
| **השנים בהן בוצע התפקיד** | |  |
| **תיאור התפקיד אותו מילא** | | |
|  | | |
| **פירוט נושאים שהיו כלולים בניהולו** | | |
|  | | |
| **הגורם שהיה הממונה בארגון** | **שם** |  |
| **תפקיד** |  |
| **טלפון** |  |

### אנליסט

1. **אחריות –אנליסט עבור מחב"א והמוסדות.**
2. **דרישות**

* ביצע תפקיד אנליסט במשך לפחות שנתיים באמצעות מערכות SIEM-SOC.
* בעל ידע מעמיק ומוכח בנושא אבטחת מידע והגנת סייבר.
* בעל הסמכה בתחום אבטחת מידע והגנת הסייבר.

1. **מענה המציע**

המציע יצרף קורות חיים של המועמד לתפקיד.

המציע יספק תיאור של המועמד המוצע בטבלאות שלהלן. על הטבלאות לשקף את אופן עמידת המועמד בדרישות.

המציע יתאר תפקידים רלוונטיים שביצע המועמד. המציע ימלא פרטים בטבלה שלהלן עבור כל תפקיד. יש למלא עד 4 תפקידים לכל היותר. ניתן לשכפל בהתאם את הטבלה.

|  |  |  |
| --- | --- | --- |
| **מועמד לתפקיד אנליסט** | | |
| **שם המועמד** | |  |
| **הארגון בו בוצע הפרויקט** | |  |
| **השנים בהן בוצע התפקיד** | |  |
| **תיאור התפקיד אותו מילא** | | |
|  | | |
| **פירוט נושאים שהיו כלולים** **בתחום אחריותו** | | |
|  | | |
| **הגורם שהיה הממונה בארגון** | **שם** |  |
| **תפקיד** |  |
| **טלפון** |  |

### בקרי CSOC

1. **אחריות – בקרי קו ראשון עבור מחב"א והמוסדות.**

בסעיף זה יש להציע ולפרט 2 בקרי קו ראשון בפונקצית CSOC, שיעניקו שירות שוטף.

המציע נדרש לספק פרטים של לקוחות ממליצים עבור בקרי ה- CSOC.

1. **דרישות**

* ביצעו תפקיד בקר לפחות במשך שנה במערכות SIEM-SOC.
* בעלי היכרות ושליטה בתפעול מערכת SIEM מוצעת.
* בעלי ידע מוכח בתחום אבטחת מידע והגנת סייבר.

1. **מענה המציע**

המציע יספק תיאור מפורט של ניסיון מקצועי של המועמדים המוצעים בטבלאות שלהלן. על הטבלאות לשקף את אופן עמידת המועמדים בדרישות לניסיון קודם ומומחיות.

|  |  |
| --- | --- |
| **מועמד ראשון לתפקיד בקר CSOC** | |
| **שם המועמד** |  |
| **תיאור ניסיון קודם** | |
|  | |
| **פרטי הכשרה ומומחיות** | |
|  | |
| **מועמד שני לתפקיד בקר CSOC** | |
| **שם המועמד** |  |
| **תיאור ניסיון קודם** | |
|  | |
| **פרטי הכשרה ומומחיות** | |
|  | |

פרטי ממליצים, עד 5, עבור מועמדים לבקרי CSOC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | שם מועמד | שם ארגון | שם איש קשר | פרטי התקשרות: טלפון וכתובת e-mail |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### ארכיטקט

1. **אחריות –** **ארכיטקט מערכת SIEM.**
2. **דרישות**

* ביצע תפקיד ארכיטקט מערכות אבטחת מידע במשך 5 שנים לפחות.
* בעל ידע מעמיק ומוכח באבטחת מידע והגנת סייבר.
* בעל הסמכה בתחום אבטחת מידע והגנת סייבר.

1. **מענה המציע**

המציע יצרף קורות חיים של המועמד לתפקיד.

המציע יספק תיאור של המועמד המוצע בטבלאות שלהלן. על הטבלאות לשקף את אופן עמידת המועמד בדרישות.

המציע יתאר תפקידים רלוונטיים שביצע המועמד. המציע ימלא פרטים בטבלה שלהלן עבור כל תפקיד. יש למלא עד 4 תפקידים לכל היותר. ניתן לשכפל בהתאם את הטבלה.

|  |  |  |  |
| --- | --- | --- | --- |
| **מועמד לתפקיד ארכיטקט** | | | |
| **שם המועמד** | |  | |
| **הארגון בו בוצע הפרויקט** | |  | |
| **השנים בהן בוצע התפקיד** | |  | |
| **תיאור התפקיד אותו מילא** | | | |
|  | | | |
| **פירוט נושאים שהיו כלולים** **בתחום אחריותו** | | | |
|  | | | |
| **הגורם שהיה הממונה בארגון** | **שם** | |  | |
| **תפקיד** | |  | |
| **טלפון** | |  | |

### מיישם SIEM

1. **אחריות –** מיישם מערכת SIEM.
2. **דרישות**

* ביצע תפקיד מיישם מערכת SIEM מוצעת במשך שנתיים לפחות.
* בעל ידע מעמיק ומוכח באבטחת מידע והגנת סייבר.
* בעל הסמכה בתחום אבטחת מידע והגנת סייבר.

1. **מענה המציע**

המציע יצרף קורות חיים של המועמד לתפקיד.

המציע יספק תיאור של המועמד המוצע בטבלאות שלהלן. על הטבלאות לשקף את אופן עמידת המועמד בדרישות.

המציע יתאר תפקידים רלוונטיים שביצע המועמד. המציע ימלא פרטים בטבלה שלהלן עבור כל תפקיד. יש למלא עד 4 תפקידים לכל היותר. ניתן לשכפל בהתאם את הטבלה.

המציע יתאר פרויקטים רלוונטיים שביצע המועמד. המציע ימלא את הפרטים בטבלה שלהלן עבור כל פרויקט ופרויקט. יש למלא עד 4 פרויקטים לכל היותר.

|  |  |  |  |
| --- | --- | --- | --- |
| **מועמד לתפקיד מיישם SIEM** | | | |
| **שם המועמד** | |  | |
| **הארגון בו בוצע הפרויקט** | |  | |
| **השנים בהן בוצע התפקיד** | |  | |
| **תיאור התפקיד אותו מילא** | | | |
|  | | | |
| **פירוט נושאים שהיו כלולים** **בתחום אחריותו** | | | |
|  | | | |
| **הגורם שהיה הממונה בארגון** | **שם** | |  |
| **תפקיד** | |  |
| **טלפון** | |  |

## הקמת מערכת SIEM

### ניהול הפרויקט

1. להקמת המערכת תוקצה לספק תחנת עבודה וכלי עבודה בסיסיים כדוגמת טלפון, קישור לאינטרנט. אם למציע דרישות נוספות הרי שעליו לפרטן בהצעה, כדי שמוסד/מחב"א יוכלו להיערך להן בהתאם.

**מענה המציע :**