מרכז החישובים
הבינאוניברסיטאי

מרכז החישובים הבינאוניברסיטאי

מכרז פומבי מס' 1/2019
לאספקת ותחזוקת מערכת SIEM ושירות CSOC

מכרז פומבי מס' 1/2019

לאספקת ותחזוקת מערכת SIEM

ושירות CSOC

תוכן העניינים

תקציר מנהלים

מחב"א – מרכז החישובים הבינאוניברסיטאי [להלן: "**מחב"א**"] או "**המזמין**"] , יוצא במכרז להקמת מערך שירותי SIEM-CSOC לשירות מחב"א והמוסדות החברים בה [להלן: "**המוסדות**"] שיחליטו להצטרף לשירות. לצורך כך, מחב"א מפרסם בזה מכרז הכולל מוצרים ושירותים לפתרון כולל למערכת SIEM (Security Information & Event Management) ולפונקציה תפעולית CSOC (Cyber & Security Operational Center).

הספק הזוכה יחתום על הסכם מול מחב"א באמצעותו יעניק שירות למחב"א ולמוסדות אשר יצטרפו לשירות.

א. **הצורך העסקי של המיזם**

1. סיכול אירועי סייבר/אבטחת מידע המאיימים על מערך המחשוב במוסדות
2. קבלת תמונת מצב רציפה ומעודכנת על סטאטוס שמירת הנחיות מדיניות אבטחת מידע ארגוני במערכות מידע של המוסדות
3. שיפור יכולת אכיפת מדיניות אבטחת מידע במערכות מידע של המוסדות
4. העלאת רמת זמינות שירותי מחשוב עבור המשתמשים
5. יכולת תגובה קרוב לזמן אמת מול אירועי אבטחת מידע על מנת למזער נזקים בגינם
6. מענה לצרכים חוקיים (תקנות הגנת הפרטיות, GDPR ועוד)

ב. **יעדים ומטרות המיזם**

1. הקמת מערכת מרכזית לאיסוף וניהול אירועי אבטחת מידע ממערכות ומקורות מידע במוסדות ובמחב"א, אשר תנתח לוגים ותזהה אירועי אבטחת מידע ברמת מוסד וברמת כלל המוסדות, בכדי לתת להם מענה מהיר ויעיל.
2. שיתוף מידע אודות אירועי אבט"מ בין המוסדות ומחב"א באיתור ומניעה של אירועי אבטחת מידע ובדרך התמודדות ותגובה לאירועים חוצי מוסד.
3. עמידה בדרישות רגולטוריות ובדרישות החוק, דוגמת GDPR.
4. מעבר לפעילות מונעת בתחום הגנת הסייבר ואבטחת מידע.
5. ייעול השירות באמצעות קונסולידציה ושיתוף להוזלת TCO לכל מוסד.

ג. **תכולת השירות המבוקש**

1. שירות SIEM, הכולל אחת מהחלופות הבאות:

- מערכת מרכזית מנוהלת ע"י הספק ובבעלות מחב"א, מותקנת על תשתית IaaS בענן או ברשת מחב"א
- מערכת בתצורת SaaS בניהול ובאחריות ספק השירות

מערכת SIEM רבת-ישויות (Multi-Tenancy) מרכזית, אחידה וסטנדרטית שניתן להתאימה לכל מוסד ברמת ניטור, חוקים ותהליכים.

לכל מוסד תוגדר מחיצה ממודרת שתנוהל לפי מדיניות והחלטת ממונה אבטחת מידע של המוסד.

בכל מוסד יותקנו ויוגדרו אמצעי איסוף לוגים ואירועים עבור מערכת SIEM לפי תצורה ודרישות המוסד.

משך ההתקשרות יהיה לחמש שנים עם אופציות להארכה עד לתקופה כוללת של 10 שנים.

2. שירות CSOC

פונקצית CSOC תעקוב אחר אירועים במערכת SIEM, תדווח עליהם ותמליץ על דרכי פעולה למזעור נזק ומניעה עתידית של אירועים דומים. בהתאם לחומרת אירוע ינוהל תחקיר שיוגש למוסד.

שירות שוטף יינתן ממתקן הספק באמצעות תמהיל של בקרים ואנליסטים.

ספק CSOC נדרש לעבוד בתאימות למדיניות אבטחת מידע של המוסד ועל פי נוהל תגובה לאירוע אבטחת מידע של המוסד.

משך ההתקשרות יהיה לחמש שנים עם אופציות להארכה עד לתקופה כוללת של 10 שנים.

ד. **רמת שירות**

1. חלונות שירות
   - SIEM – 7*24 למעט יום כיפור.
   - ל- CSOC הוגדרו 4 חלונות לבחירת כל מוסד: שעות עבודה, מחוץ לשעות עבודה, 7*24, 6*24 (ללא שבתות וחגים).
2. מדדים – הוגדרו 8 מדדים לרמת שירות ביניהם: משך טיפול בתקלות, ביצוע תחקירים, זמינות שירות ועוד.
3. מערכת מדידה – הספק יקים מערכת מדידה עם שקיפות מלאה ללקוח, תוך שמירה על מידור והרשאות.
4. אכיפה – למקרה של אי עמידה ברמת שירות הוגדר אירוע פיצוי מוסכם ברמת מדד וברמת מוסד ובאופן פרוגרסיבי.

ה. **פרויקט הקמת** מערכת SIEM ינוהל ברמה מרכזית/רוחבית מול מחב"א וברמה מוסדית ספציפית מול נציגי המוסדות.

ו. **מנגנוני ניהול שירות** - יוקמו ועדת היגוי מרכזית בראשות מנכ"ל מחב"א וועדת היגוי תפעולית לכלל השירותים, יוקם פורטל למעקב אחר השירות ויוכנו דוחות ותוצרים.

ז. **מחיר מוצרים ושירותים**

1. מחיר הקמת מערכת SIEM - מחיר לפרויקט בחלוקה לפי אבני דרך.
2. מחיר חודשי למערכת SIEM על בסיס שימושיות ומדידה של EPS (Events Per Second).
3. רכש מוצרים לאורך תקופת ההתקשרות על בסיס שיעור הנחה מינימלי ממחירון יצרן מעודכן.
4. מחירון שירותי שו"שים למערכת SIEM.
5. מחיר חודשי לשירותי CSOC בהתאם לחלון שירות וכמות EPS.
6. מחירון לשירותים נוספים של פונקצית CSOC, דוגמת סקר אבטחת מידע.

0. מנהלה

0.1 כללי

מחב"א מזמין בזאת הצעות לאספקת והקמת מערכת SIEM (Security Information & Event Management) ומתן שירותי CSOC as a Service (Cyber & Security Operatioanl Center), כמפורט במסמכי מכרז זה (להלן: "**השירות**" ו- "**המכרז**", בהתאמה).

מחב"א מאוגד כעמותה וחברות בה שמונה האוניברסיטאות שלהלן: טכניון, אוניברסיטת חיפה, אוניברסיטה הפתוחה, אוניברסיטה העברית, אוניברסיטת בר-אילן, מכון ויצמן למדע, אוניברסיטת תל-אביב ואוניברסיטת בן גוריון (להלן: "**לקוחות**"/ "**מוסדות**").

התקשרות מחב"א עפ"י מסמך זה תעשה עבורה ועבור המוסדות שהנן חברות בעמותה.

בכל מקום במסמך זה או בהסכם הנלווה בו מופיע המילה "מחב"א", האמור יהיה נכון גם למוסדות שיצטרפו לשירות. כל התחייבויות המציע יראו אותן כהתחייבויות עבור מחב"א והמוסדות יחד ולחוד וכל זכות שנתונה למחב"א על פי ההסכם תהיה נתונה גם למוסדות שיצטרפו לשירות.

מובהר בזאת כי הסכם ההתקשרות עם הספק הזוכה יחתם עם מחב"א בלבד, בעוד השירות יסופק למוסדות שיצטרפו להסכם, בהתאם לנספח ז' להסכם - רשימת שירותים ומוסדות.

מחב"א ו/או המוסדות אינם מתחייבים להיקף הזמנות כלשהן ואין בזכייה במכרז ו/או בחתימה על ההסכם כדי להבטיח מתן שירותים ע"י הספק בהיקף כלשהו או בכלל.

המכרז ינוהל על ידי ועדת המכרזים של מחב"א [להלן: "**ועדת המכרזים**"] על פי נוהל המכרזים של מחב"א [להלן"**הנוהל**" או "**נוהל המכרזים**"] שאותו ניתן למצוא באתר מכרזים של מחב"א.

מכרז זה הנו מכרז דו שלבי. לפיכך רק לאחר שועדת המכרזים תסיים את קביעת ציוני האיכות של הצעות המציעים תפתח ועדת המכרזים את ההצעות הכספיות.

0.1.1 שלבי המכרז

א. פרסום המכרז

ב. הליך הבהרות – כמפורט להלן בסעיף 0.3.3.

ג. הגשת הצעות - מציעים אשר עומדים בתנאי הסף של מכרז זה, יגישו את הצעותיהם בהתאם לדרישות המפורטות במסמכי המכרז.

ד. מיון לפי תנאי סף - מציעים שוועדת המכרזים תמצא כי לא עמדו באחד או יותר מתנאי הסף – יפסלו, והצעותיהן לא תשתתפנה בהמשך הליך בחירת הספק הזוכה.

ה. בחינה מפורטת ושקלול - מציעים שוועדת המכרזים תמצא כי עמדו בכל תנאי הסף יעברו הליך בחינה מפורט ושקלול איכותי וכלכלי משולב, שבסופו ייבחר הספק הזוכה במכרז.

0.1.2 טבלת ריכוז מועדי המכרז

פעילות	תאריך
מועד פרסום המכרז	24/02/2019
מועד כנס מציעים	17/03/2019 בשעה 10:00
מועד אחרון להעברת שאלות ובירורים בהקשר למסמכי המפרט	31/03/2019 בשעה 15:00
מועד אחרון להעברת תשובות מחב"א לשאלות ובירורים של מציעים	14/04/2019 בשעה 19:00
מועד אחרון להגשת הצעות לתיבת המכרזים	14/05/2019 בשעה 16:00
מועד תוקף ההצעה	31/12/2019

במקרה של אי התאמה בין הרשום בטבלה לעיל לבין הרשום בגוף המכרז, יקבעו הנתונים הרשומים בטבלה לעיל. ועדת המכרזים תהיה רשאית, על סמך שיקול דעתה המוחלט, לשנות כל אחד מהמועדים המפורטים בטבלה לעיל, ובכלל זה לדחות את המועד האחרון להגשת ההצעות למכרז. הודעה בדבר שינויים כאמור תפורסם בנפרד.

0.2 הגדרות

הגדרות אלה יחולו על המכרז ונספחיו (למען הסר ספק מובהר בזאת כי, בכל הנוגע לתכולת העבודה המפורטת, יחולו בנוסף ההוראות הכלולות במפרט ובנספחיו).

מונח	פירוט
אירוע	פעולה שהתרחשה באחת המערכות ועקב כך נרשמה ביומן של אותה מערכת.
אירוע אבטחת מידע	אירוע אשר עשוי להצביע על התרחשות בגינה תגרם פגיעה בשירות מיחשוב כל שהוא או שבגינו דלף מידע חסוי או פגיעה בשלמות המידע.

	לצורך תעדוף טיפול מוגדרים ארבע רמות של אירועי אבטחת מידע: נמוך\אינפורמטיבי, בינוני, גבוה וקריטי/חמור.
איש קשר	הגורם מטעם המציע אשר מונה לנהל את המכרז מול מחב"א.
הצעה	תשובת המציע להזמנה להציע הצעות על כל נספחיה.
התראה	זיהוי אירוע ומתן חיווי בתצורת אזעקה טקסטואלית במסך אירועים מרכזי של מערכת SIEM.
יצרן	בית תוכנה המפתח מוצר SIEM.
מוסדות ו/או לקוחות	אחד או יותר מהמוסדות האקדמיים החברים במחבא: הטכניון, אוניברסיטת חיפה, אוניברסיטה הפתוחה, אוניברסיטה העברית, אוניברסיטת בר-אילן, מכון ויצמן למדע, אוניברסיטת תל-אביב ואוניברסיטת בן גוריון.
מחב"א ו/או הלקוח ו/או המזמין	מרכז החישובים הבין אוניברסיטאי.
[ה]מכרז ו/או (ה)מפרט או הבל"מ	מסמך זה על נספחיו דרישותיו תנאיו, חלקיו ונספחיו.
מפ"ל	מפרט פנימי לבדיקה. מסמך המגדיר את אופן בדיקת האיכות של הצעות המציעים במכרז אשר עמדו בתנאי הסף המנהלתיים.
מציע	מגיש הצעה במכרז.
ספק ו/או החברה	המציע שזכה במכרז, לרבות קבלני משנה שהוא משתף מטעמו.
עורך המכרז	האחראי למכרז זה מטעם "מחב"א"
קבלן משנה (ספק משנה)	מי שהתקשר עם המציע לשם אספקת מוצר ו/או ביצוע שירות מוגדר כלשהוא, הנדרשים במפרט. לצורך הגדרה זו יחשב גם קבלן משנה מדור שני ומעלה (קבלן משנה של קבלן משנה של המציע).
קורולציה	הצלבת אירועים בין 2 Rules או יותר לצורך הסקת מסקנה לגבי אירוע אבטחת מידע.
שירותי CSOC ו/או שירותי תמיכה CSOC	שירותי CSOC על פי תכולת השירותים במפרט הטכני בתמורה קבועה ועל פי מחירון מוסכם של תכולת השירותים.
שירותי תפעול ותחזוקה (SIEM)	כלל הפעילויות הנדרשות לטיפול בתקלות בכל דרגי הטיפול, למתן שירות בהתאם לרמת השירות הנדרשת, ולשמירה על עדכניות השירות ואיסוף המידע, לרבות התקנת Service Packs וטלאים, שדרוגי תוכנות, דריכת פרמטרים, ניטור, פילטור, התאמת Connectors ואבטחת מידע.
תגובה	אוסף פעילויות שיש לבצע על מנת למזער נזק של אירוע אבטחת מידע.
תחקור	פעילות שמבוצעת מיד לאחר סגירת אירוע אבטחת מידע, לצורך הבנת האירוע והסקת מסקנות בכדי למנוע את הישנותו.
תיעדוף	סיווג עדיפות בטיפול בין התראות ואירועים על מנת להגיב לאירועי אבטחת מידע בהתאם למדיניות וקריטריונים שנקבעים מראש, על בסיס מידת נזק שעלול להיגרם מאירוע ומידת סבירות להתרחשותו.
תסריט	סקריפט הכולל רצף לוגי של חוקים ושילוב קורולציות במגמה לזהות אירועי אבטחת מידע מורכבים ולהפעל מדיניות פרו-אקטיבית.
תקופת התקשרות לשירותי SIEM ותשתית או תקופת מתן שירות SIEM	פרק הזמן מיום חתימת ההסכם עם הספק ועד היום האחרון למתן שירותי SIEM.
תקופת התקשרות לשירותי CSOC או תקופת מתן שירות CSOC	פרק הזמן מיום חתימת ההסכם עם הספק ועד היום האחרון למתן שירותי CSOC.
תקלה (Bug) או	אי קבלת שירות עפ"י רמת השירות המוסכמת או אירוע בו פונקציה

Incident	הכלולה בסל השירותים ואשר פעלה באופן רציף אינה עובדת או אינה מייצרת את התוצר הנדרש.
תקלה משביתה	תקלה אשר גורמת להשבתה של תהליך או שירות או תת שירות.
תקלה רגילה	תקלה אשר אינה משביתה.
SOC	Security Operational Center – מרכז לניהול ותפעול אירועי אבטחת מידע.
CSOC	Cyber & Security Operational Center – מרכז לניהול ותפעול אירועי סייבר ואבטחת מידע.
EPS	Event Per Second - מספר אירועים בשנייה. משמש כקנה מידה לעומס על מערכת SIEM וכמות עבודה נדרשת מצוות CSOC.
Incident Response (IR)	פעילות המבוצעת כתגובה לאירוע אבטחת מידע שנגרם כתוצאה מתקלה במערך אבטחת המידע.
Infrastructure as a Service (IaaS)	שירותים בהם המשתמש מקבל משאבי מחשוב לשימושו. לדוגמא שרת וירטואלי או הקצאה במערך איחסון בענן.
Security Information & Event Management (SIEM)	מערכת ניהול אירועי אבטחת מידע.
Service Level Agreement (SLA)	רמת שירות מוסכמת.
Security Operational Center (SOC)	מרכז לניהול ותפעול אירועי אבטחת מידע.
Software as a Service (SaaS) or On Demand	תוכנה המספקת למשתמש שירותים הניתנים באמצעות אירוח באתר הספק, במקום רכישת מוצר תוכנה והתקנתו בשרתי הארגון הרוכש. הפעלת שירותי התוכנה מאתר הספק היא דרך רשת תקשורת, בדרך כלל האינטרנט. המשתמש משתמש גם בתשתית חומרה, גם בפלטפורמה וגם בשירותים אפליקטיביים שפותחו על ידי הספק.
Tenant	לקוח (דייר/מחיצה) במערכת SIEM אשר מופרד וממודר מלקוחות אחרים של המערכת. לכל Tenant מידע משלו, הרשאות, משאבים, חוקים כך ש Tenant מהווה בפועל מערכת SIEM פרטית וירטואלית.
Rule	תנאי לוגי המתייחס לרצף אירועים (שונים או זהים) בפרק זמן מוגדר.

0.3 ניהול המכרז

0.3.1 קבלת מסמכי המכרז

את מסמכי המכרז ניתן לקבל באופן אלקטרוני באמצעות פנייה למשרד מחב״א

טלפון: 03-6460555 או ל- e-Mail: IUCC-Secretariat@mail.iucc.ac.il

או להוריד מאתר האינטרנט של מחב״א בכתובת: http://il.iucc.ac.il/he/michrazim

0.3.2 עורך המכרז

נציג מחב״א למכרז זה הוא: מר אלי בקר

טלפון: 03-6460569

דוא״ל: eli.beker@iucc.ac.il

0.3.3 נוהל העברת שאלות ובירורים

א. שאלות הבהרה ניתן להעביר בדוא"ל בלבד עד ולא יאוחר מהתאריך הנקוב בטבלה 0.1.2.

ב. שאלות מציעים תוגשנה בכתב ע"ג נספח שאלות הבהרה המצורף כקובץ אקסל למסמכי המכרז, ותועברנה באמצעות דואר אלקטרוני לעורך המכרז, בכתובת tender@iucc.ac.il. המציע יציין את הסעיף המדויק אליו מתייחסת כל שאלה באופן הבא:

מס' שאלה	סוג המסמך	הסעיף במסמך	ס"ק	השאלה
.1	מפרט	2.3.6.1	ג'	<<< דוגמא
.2	הסכם	14	ב'	<<< דוגמא
.3	נספח...	1.2	ד' 1.	<<< דוגמא

ג. תשובות בכתב של ועדת המכרזים לשאלות הבהרה (ככל שמחב"א תמצא לנכון להשיב להן), יפורסמו באתר אינטרנט מחב"א בכתובת: http://il.iucc.ac.il/he/michrazim, מבלי לחשוף את זהות הפונה.

ד. תשובות ועדת המכרזים יחשבו חלק ממסמכי המכרז. באחריות המציע לוודא כי שאלתו הגיעה ליעדה ולקבל אישור על כך. באחריות מציעים להתעדכן בתשובות לשאלות הבהרה שיפורסמו באתר.

ה. ועדת המכרזים לא תשיב לפניות שיומצאו לה לאחר המועד האחרון להעברת שאלות ובירורים.

ו. ועדת המכרזים תשיב לפניות מהר ככל הניתן ועד למועד המצוין בטבלת ריכוז מועדי המכרז שבסעיף 0.1.2, בשורה "מועד אחרון להעברת תשובות הלקוח".

ז. רק תשובות של ועדת המכרזים שתופצנה ע"י עורך המכרז מחייבות את מחב"א והן תהווינה חלק בלתי נפרד ממסמכי המכרז.

ח. ועדת המכרזים תהיה רשאית, על פי שיקול דעתה המוחלט והבלעדי, להודיע, לאחר פרסום המכרז, על תיקונים, הבהרות, שינויים ותוספות בתנאי המכרז, ומעת שתעשה כן יהוו אלו חלק בלתי נפרד ממסמכי המכרז. המציע יצרף למסמכי הצעתו את הודעת ועדת המכרזים וכל מסמך שהוסף כאמור, כשהם חתומים בחתימתו, לאישור קבלתם, הבנתם, והבאת האמור בהם בחשבון במסגרת הצעתו. שינויים, הבהרות ועדכונים כאמור לעיל, יפורסמו באתר האינטרנט ועל המבקשים להשתתף במכרז, לעקוב אחר העדכונים באתר כאמור לעיל. ניתן יהיה להירשם לקבלת נתונים על המכרז לדואר האלקטרוני של המציע. בכל מקרה, גם אם יתאפשר משלוח הודעות לדואר האלקטרוני, חובת המציע, לוודא באתר האינטרנט, בטרם הגשת ההצעה, האם נערכו שינויים כל שהם למכרז, לפני ולקראת המועד האחרון להגשת ההצעות ולא תהיה למציע כל טענה או תביעה כלפי מחב"א בגין אי משלוח הודעות לדואר אלקטרוני, בקשר למכרז.

0.3.4 כנס מציעים

כנס מציעים יתקיים במועד הנקוב בטבלה 0.1.2 במשרדי מחב"א בקמפוס אוניברסיטת תל-אביב. השתתפות נציג מטעם המציע במפגש הנה חובה וועדת המכרזים תהיה רשאית לסרב לדון בהצעה של מציע שלא השתתף בכנס. אם תמצא מחב"א לנכון לערוך פרוטוקול למפגש, הוא יפורסם באתר האינטרנט ויהווה חלק בלתי נפרד ממסמכי המכרז.

0.3.5 מסירת ההצעות

א. על המציע להכניס, בעצמו או באמצעות שליח, את הצעתו – שתערך ותארז באופן האמור בסעיף 0.11.2 שלהלן - לתיבה המיועדת לכך, במשרדי מחב"א, בניין הנדסת תוכנה, אוניברסיטת תל אביב (קומה 4), עד ולא יאוחר מהיום והשעה הנקובים בטבלה 0.1.2. אין למסור הצעות בכל דרך אחרת. הצעה שלא תוכנס לתיבת המכרזים תפסל על הסף. על המציע להביא בחשבון עיכוב אפשרי בשל הבידוק הביטחוני בקמפוס.

ב. מציע המבקש להגיש הצעתו, נדרש להגישה על גבי מסמכי המכרז שנמסרו לו על ידי מחב"א, לחתום בתחתית כל עמוד בכל אחד ממסמכי המכרז, להכניסם יחד עם יתר המסמכים הדרושים כאמור במכרז זה למעטפה סגורה וחתומה, ללא זיהוי חיצוני, ולסגור את מעטפת ההצעה. אין לכתוב או לסמן דבר על גבי מעטפת ההצעה מלבד מספר המכרז ונושא המכרז.

ג. הצעת המציע תהיה בתוקף עד למועד המופיע בטבלה 0.1.2 בשורה "מועד תוקף ההצעה". מובהר כי גם לאחר שמחב"א תתקשר בהסכם עם מציע כלשהו (אם תתקשר), ותודיע למי מהמציעים כי הצעתו נדחתה, לא יפקעו הצעות שהוגשו על פי מכרז זה ולא זכו, במשך התקופה האמורה. ועדת המכרזים תהא רשאית (אך לא חייבת) לבחור זוכה שני וזוכה שלישי וכן הלאה, למקרה שהסכם ההתקשרות עם הזוכה הראשון או השני וכן הלאה לא ייצא לפועל, מכל סיבה שהיא, או יבוטל ע"י מחב"א בתוך 6 חודשים מיום תחילתו. בחלוף המועד האמור, תהיה ועדת המכרזים רשאית לבחור בהצעה הבאה בטיבה כאמור לעיל ובלבד שהמציע נתן לכך את הסכמתו.

ד. הגשת הצעה חתומה תהווה ראיה חלוטה לכך שהמציע קרא והבין את כלל מסמכי המכרז ובחר לתת להם את הסכמתו, באופן מלא ושלם וללא הסתייגויות כלשהן.

ה. מסמכי המכרז הנם רכוש מחב"א והם מושאלים למציע לצורך הגשת הצעתו בלבד. המציע אינו רשאי לעשות כל שימוש במסמכי המכרז מלבד הגשת הצעתו. על המציע להשיב את מסמכי המכרז למחב"א עד למועד האחרון להגשת ההצעות, בין אם בחר להגיש הצעתו ובין אם לאו.

ו. כללו מסמכי המכרז הצעת מחיר במדיה מגנטית – יחולו בנוסף ההוראות הבאות:

1. המציע ימלא את המחירים באופן ממוחשב באמצעות אקסל מענה כספי.
2. לאחר השלמת הכנת הצעת המחיר על המציע להדפיס אותה ולחתום עליה בהתאם לחתימה הנדרשת על כלל מסמכי ההזמנה.
3. בכל מקרה של אי התאמה בין המחירים באקסל לבין המחירים המודפסים - יקבע המחיר על גבי המסמך המודפס.

0.3.6 ערבות השתתפות (N)

0.3.7 עיון במסמכי המכרז ובהצעה הזוכה

א. זכות העיון בהצעה הזוכה נתונה למציע המשתתף במכרז, וזאת בתנאים ובמגבלות המפורטים בנוהל המכרזים של מחב"א. לבקשה לעיון כאמור תצורף המחאה לפקודת מחב"א בסך 500 ש"ח לכיסוי העלות הכרוכה בכך.

ב. מציע הסבור כי אין לאפשר עיון בחלקים של הצעתו שכן עיון בהם עלול לחשוף סודות מסחריים או סודות עסקיים (להלן – "חלקים סודיים"), יציין במפורש בסעיף זה מהם החלקים הסודיים.

ג. מציע שלא ציין מהם החלקים הסודיים שבהצעתו יראוהו כמי שמסכים למסירת ההצעה כולה לעיון מציעים אחרים, אם יוכרז כזוכה במכרז.

ד. ציון חלקים בהצעה כסודיים מהווה הודאה בכך שמבחינת המציע חלקים אלה בהצעה סודיים גם בהצעותיהם של מציעים אחרים, ומכאן שהמציע מוותר מראש על זכות העיון בחלקים אלה של הצעות מציעים אחרים.

ה. יודגש כי ההחלטה באלו חלקים של ההצעה הזוכה אין לאפשר עיון, שכן הם עלולים לחשוף סודות מקצועיים או סודות מסחריים, מסורה לשיקול דעתה של ועדת המכרזים ושלה בלבד, וכי הועדה תפעל בנושא זה בהתאם לדיני המכרזים, לדיני העיון ולאמות מדה מקובלות.

ו. החליטה ועדת המכרזים לאפשר עיון בחלקים המפורטים בהצעת הזוכה למרות שהזוכה הגדירם כסודיים, תיתן על כך ועדת המכרזים התראה לזוכה, ותאפשר לו להשיג על כך בפניה בתוך פרק זמן ההולם את נסיבות העניין.

ז. החליטה ועדת המכרזים לדחות את ההשגה, תודיע על כך ועדת המכרזים למציע הזוכה בטרם מסירת החומר לעיונו של המבקש.

ח. מבלי לגרוע מהאמור לעיל, יודגש כי שמו וכתובתו של המציע, ניסיונו ולקוחותיו לא יהוו סוד מסחרי או סוד עסקי, וזאת בכפוף לאמור בגוף המכרז. מציע שבחר להשתתף בהליך המכרז מביע בכך את הסכמתו לאמור בסעיף זה.

0.4 תכולת המכרז

בקשה זו להגשת הצעות מכילה את המסמכים הבאים:

פרק/ נספח	תכולה
פרק 0 – מנהלה	בפרק זה מצויים פרטים מנהליים כלליים של המכרז.
פרקים 1-4	החלק המקצועי בו מפורטות דרישות השירות, דרישות ופרטים לגבי המציע וקבלני משנה מטעמו.
פרק 5 – תמורה ותנאי תשלום	טבלאות התמורה ותנאי תשלום ושאר הסעיפים הקשורים בתמורה לשירות המוצע במכרז זה.
תבניות לשימוש המציע	תבנית שאלות הבהרה למכרז בו נדרש המציע להעביר את שאלותיו לעורך המכרז (נספח 0.3.3). תבנית המכרז עם כל סעיפיו ובה נדרש המציע למלא את תוכן המענה שהוא מגיש למכרז (נספח 0.11).
גיליונות עלות (קובץ Excel)	טבלאות Excel המקבילות בתוכנן לטבלאות העלות שבפרק 5 ושאותן על המציע למלא כנדרש ולצרפן ע"ג התקן זיכרון נייד (DOK) למענה לפרק 5 (נספח 5.0).

לפני העיון בחלקים אחרים של הבקשה להצעות, יש לקרוא היטב את פרק המנהלה (פרק זה) אשר מפרט את תנאי המכרז הכלליים ומגדיר במדויק כיצד יש לענות לבקשה.

0.5 אופן המענה

א. המציע מאשר כי הוא קרא את כל תנאי המכרז ודרישותיו, כי הוא הבין אותם, וכי הוא מתחייב למלא אחר כל התנאים והדרישות של המכרז, ההצעה וההסכם, בדייקנות, ביעילות, במומחיות ובמיומנות, לשביעות רצון ועדת המכרזים, ובמועדים אשר ייקבעו על ידה, והכל בכפוף להוראות המכרז וההסכם.

ב. בכל מקרה בו נדרש בנוסח הסעיף פירוט כל שהוא יש למלא בדייקנות אחר הנדרש.

ג. אין לחזור בשום מקרה על הנוסח המופיע במפרט על גבי גלופת מענה המציע. החתימה על ההצהרה המצורפת כנספח 0.6.6 ס"ק 2 – תצהיר כללי/הסכמה לדרישות המכרז, מעידה על כך שהמציע קרא והבין את כל התנאים והדרישות המנוסחים במכרז על סיווגם וכי הוא מתחייב, אם יזכה, למלא אחר כל התנאים והדרישות ללא סייג. הצהרה זו באה במקום חזרה על נוסח זה בכל סעיף וסעיף.

0.6 תנאי סף להשתתפות במכרז ואישורים שעל המציע להמציא עם הגשת ההצעה

0.6.1 כללי

א. במכרז רשאים להשתתף רק מציעים העונים במועד הגשת ההצעה על כל התנאים המפורטים בסעיף 0.6. מציע או הצעה שאינם עומדים בכל התנאים – יפסלו.

ב. תנאי סף המתייחסים למציע צריכים להתקיים במציע עצמו. קיום תנאי סף בתאגיד קשור (לדוגמה – חברה אם, חברה בת או חברה אחות), בארגון של המציע (לדוגמה – מנכ"ל), בבעל מניות או בכל גורם אחר לא ייחשב כעמידה בתנאי הסף, אלא אם נאמר במפורש אחרת.

ג. אין להגיש הצעה המשותפת למספר גופים.

0.6.2 מעמדו המשפטי של המציע

א. כתנאי מוקדם להשתתפות במכרז, על המציע להיות במועד הגשת ההצעה: תאגיד הרשום בישראל על פי דין, שאינו בעל חוב בגין אגרה שנתית למרשם הרלוונטי לשנים הקודמות

לשנת 2019, ואם הוא חברה – הוא אינו בעל רישום כחברה מפרת חוק או בעל התראה לפני רישום כאמור.

ב. אם עסקו של המציע הוא בשליטת אישה, כמשמעות הדבר בסעיף 2ב' לחוק חובת המכרזים, תשנ"ב-1992, רשאי המציע לצרף להצעתו אישור כנדרש בחוק ותצהיר המאשר זאת.

ג. על המציע לצרף להצעה אישורים כמפורט בנספח 0.6.2 למכרז:

1. העתק מאומת על ידי עו"ד של תעודה תקפה המעידה על רישום המציע כתאגיד בישראל במרשם על פי הוראות הדין הנוגעות לעניין.

2. נסח רישום תאגיד עדכני לשנת 2018. נסח כאמור ניתן להפיקו באתר האינטרנט של רשות התאגידים: www.taagidim.justice.gov.il, תחת הקישור "הפקת נסח חברה".

3. אישור עו"ד בדבר זהות מורשי החתימה אצל המציע.

4. אישור רואה חשבון כי עסקו של המציע הוא בשליטת אישה (ככל שרלוונטי).

0.6.3 עמידה בהוראות חוק עסקאות גופים ציבוריים ושמירה על דיני עבודה

כתנאי מוקדם להשתתפות במכרז, על המציע לעמוד בהוראות חוק עסקאות גופים ציבוריים, תשל"ב – 1976. על המציע לצרף בנספח 0.6.3 את המסמכים הבאים:

א. עותק מאומת על ידי עורך דין של אישור תקף על ניהול פנקסי חשבונות ורשומות לפי חוק עסקאות גופים ציבוריים (אכיפת ניהול חשבונות ותשלום חובות מס), תשל"ו-1976, וכל אישור אחר הנדרש על-פי חוק זה.

ב. תצהיר מאומת ע"י עו"ד בדבר היעדר הרשעות בעבירות לפי חוק עובדים זרים, תשנ"א – 1991, ולפי חוק שכר מינימום, תשמ"ז – 1987, כמפורט בנספח 0.6.3

0.6.4 תצהיר בדבר ניסיון המציע ו/או קבלני משנה הכלולים בהצעתו

המציע יצרף להצעתו את נספח 0.6.4 המכיל אישור עורך דין של המציע, לצורך הוכחת עמידה בתנאי הסף הבאים. לצורך כך ניתן לראות בניסיון קבלני משנה כניסיון המציע.

א. למציע ניסיון של לפחות שנתיים בהתקנה, תמיכה ותחזוקה של מערכת SIEM, מהם לפחות שנה במערכת המוצעת על ידו.

ב. המציע הנו יצרן או מפיץ מורשה של מערכת SIEM המוצעת.

ג. למציע ניסיון באספקת שירותי SIEM שעונים על כל התנאים שלהלן:

1. ניסיון באספקת שירותי SIEM לפחות ל- 5 לקוחות פעילים, מהם לפחות 3 בישראל.

2. לפחות ל- 3 לקוחות ניתן ביום הגשת ההצעה שירות באמצעות מערכת SIEM המיושמת בשיטת Multi Tenancy או בעלת פונקציונאליות דומה.

3. היקף הניטור ל- 3 לקוחות הנו לפחות 10,000 EPS בממוצע לכל לקוח במחצית האחרונה של שנת 2018.

ד. למציע, אשר כלל בהצעתו חלופת SaaS, יש לפחות 3 לקוחות כלולים ביום הגשת ההצעה בשירות SaaS של SIEM.

ה. ספק שירותי CSOC עומד בדרישות חוקי הגנת הפרטיות בישראל.

ו. למציע ניסיון באספקת שירותי SOC לפחות ל- 10 לקוחות פעילים, ובנוסף עונה על התנאים הבאים:

1. לפחות ל- 3 לקוחות פעילים ניתן שירות באמצעות פונקצית SOC המיושמת בשיטת Multi Tenancy או בעלת פונקציונאליות דומה.

2. היקף הניטור ל- 3 לקוחות הנו לפחות 10,000 EPS בשיא לכל לקוח במשך שנה עד ליום הגשת ההצעה.

0.6.5 תצהיר בדבר היעדר ניגוד עניינים

א. תנאי מוקדם להשתתפות במכרז הינו שלמציע, לא ידוע על תפקידים ועניינים שעלולים להעמידו במצב של חשש לניגוד עניינים במסגרת אספקת השירותים והמוצר נשואי מכרז זה.

ב. המציע יצרף להצעתו תצהיר בנוסח המפורט בנספח 0.6.5 למכרז, בדבר היעדר ניגוד עניינים כאמור.

0.6.6 תצהיר כללי

כתנאי מוקדם להשתתפות במכרז על המציע לצרף להצעה תצהיר חתום בפני עורך-דין בנוסח המפורט בנספח 0.6.6 למכרז והכולל: הסכמה לדרישות המכרז, הצהרה על שימוש בתוכנות מקוריות וזכויות קניין, הצהרה בנוגע לאבטחת מידע והצהרה בדבר אי תיאום הצעות במכרז.

0.6.7 תצהיר בדבר העסקת אנשים עם מוגבלות

על המציע לצרף להצעתו תצהיר מאומת ע"י עו"ד בדבר העסקת אנשים עם מוגבלות, בהתאם לחוק שיוויון זכויות לאנשים עם מוגבלות, תשנ"ח – 1998, כמפורט בנספח 0.6.7

0.6.8 העדפת תוצרת הארץ

במכרז זה תינתן העדפה לטובין תוצרת הארץ, בהתאם לתקנות חובת המכרזים (העדפת תוצרת הארץ), תשנ"ה – 1995. לצורך קבלת העדפה, יש לצרף בנספח 0.6.8 להצעה אישור רואה חשבון בדבר שיעור המרכיב הישראלי במחיר ההצעה (ללא חשיפת המחירים עצמם). העדפה כאמור תחול על מכרז זה ככל שאינה סותרת התחיבויות המדינה באמנה או הסכם בינלאומי.

0.6.9 תצהיר בדבר זמינות מיידית

על המציע לצרף תצהיר מאומת ע"י עו"ד בדבר זמינותו המידית וזמינות המועמדים מטעמו לספק את השירותים נשוא מכרז זה, לרבות עמידה בדרישות הטכנולוגיות המפורטות במסגרת פנייה זו, כמפורט בנספח 0.6.9.

0.6.10 ריכוז אישורים ומסמכים שנדרש לצרף להצעה

סעיף	שם אישור/מסמך	סימון ✓ שצורף
0.6.2	מעמדו המשפטי של המציע	
0	עמידה בהוראות חוק עסקאות גופים ציבוריים ושמירה על דיני עבודה	
0.6.4	תצהיר בדבר ניסיון המציע ו/או קבלני משנה הכלולים בהצעתו	
0.6.5	תצהיר בדבר היעדר ניגוד עניינים	
0.6.6	תצהיר כללי	
0.6.7	תצהיר בדבר העסקת אנשים עם מוגבלות	
0.6.8	העדפת תוצרת הארץ	
0.6.9	תצהיר בדבר זמינות מיידית	

0.7 בדיקת ההצעות והערכתן

המציע לא ישנה דבר ממסמכי המכרז בכל דרך, לרבות ע"י מחיקה, השמטה, תוספת, תיקון או הסתייגות, בין במסמכים עצמם ובין במכתב נפרד, ואם יעשה זאת תהיה ועדת המכרזים רשאית, לפי שיקול דעתה המוחלט והבלעדי, לפסול את הצעתו של המציע או להתעלם מכל שינוי כאמור ולראות בהצעת המציע כהצעה בלתי מסויגת; במקרה של אי הצגת מחיר ו/או שיעור הנחה ליד סעיף כל שהוא תהיה ועדת המכרזים רשאית לפנות למציע בשאלת הבהרה או לראות כאילו המחיר כלול ביתר הסעיפים. במקרה של סטייה עקב טעות אריתמטית בין המחיר ליחידה לבין מכפלת המחיר ליחידה במספר היחידות, המחיר שייקבע הינו המחיר ליחידה.

א. אופן שקלול ההצעות

הליך בחירת הספק הזוכה יתבצע באופן הבא:

1. בדיקת עמידת ההצעות בתנאי הסף.

ועדת המכרזים – או מי שזו תמנה לצורך כך - תבחן האם המציע עומד בתנאי הסף המפורטים במסמכי המכרז. מינתה הועדה גורם לבחינת העמידה בתנאי הסף יהיו ממצאיו טעונים את אישורה. רק מציע שיעמוד בכל תנאי הסף יעבור לשלב בדיקת האיכות. מציעים אשר לא יעמדו בכל תנאי הסף, יקבלו ציון "נפסל" ותועבר להם הודעה על כך.

2. ועדת המכרזים הסמיכה ועדת משנה לבדיקת איכות מעני המציעים. להלן הרכב הוועדה:

- אלי בקר – יו"ר הוועדה ונציג מחב"א.
- נציג אוניברסיטת תל-אביב
- נציג האוניברסיטה העברית
- נציג הטכניון
- נציג אוניברסיטת בן-גוריון
- נציג אוניברסיטת חיפה
- נציג אוניברסיטת בר-אילן
- נציג האוניברסיטה הפתוחה
- כרמל פירוטין – יועץ חיצוני למחב"א.
- אהרן שבי – יועץ חיצוני למחב"א.

3. בדיקת איכות ההצעות תבוצע על ידי ועדת המשנה בהתאם למפ"ל ניקוד איכות המפורט בנספח 0.7. הכולל רשימת קריטריונים לבחינה ומשקל יחסי בגין כל קריטריון. מובהר בזאת כי לצרכי ניקוד האיכות של ההצעה רשאית ועדת המכרזים לזמן את המציעים להציג את הצעותיהם, כפי שהוגשו, וזאת בהודעה שתישלח לפחות שבוע מראש. הצעה אשר תכלול מענה מלא עבור 2 חלופות לתצורת SIEM תקבל ציון עבור כל חלופה בנפרד. **ציוני האיכות שינתנו על ידי ועדת המשנה יהיו טעונים אישור של ועדת המכרזים שתהיה רשאית להכניס בהם שינויים**.

4. רק ההצעות אשר עמדו בציון סף איכות של 75% יעברו לשלב הבא. הצעות שיקבלו ציון נמוך יותר יפסלו. במידה ותוגש הצעה אחת בלבד ציון האיכות למעבר לשלב הבא ירד ל-70%.
מעטפות המענה הכספי של המציעים שיעמדו בציון סף האיכות יפתחו רק לאחר אישור ציוני האיכות על ידי ועדת המכרזים.

5. בדיקת מענה כספי. בגין הצעה אשר תכלול מענה מלא עבור 2 חלופות לתצורת SIEM ו-2 החלופות יעמדו בציון סף האיכות, יחושב TCO נפרד לכל חלופה.

6. יחס עלות תועלת יחושב כסכום של:

- מחיר (עלות) - 50% מהציון המשוקלל של המציע.
- איכות (תועלת) - 50% מהציון המשוקלל של המציע.

ב. אופן בחינת ניסיון המציע

1. ועדת בדיקת האיכות רשאית לפנות לאנשי הקשר (לכולם או לחלקם) ולגורמים אחרים על פי שיקול דעתה כחלק מקביעת ניקוד האיכות.

2. הפנייה לאנשי קשר ואחרים אפשר שתכלול בין היתר קבלת חוות דעתם לרמת שירות, זמינות, שביעות רצון משירותי המציע ועוד. על המציע להביא בחשבון את האמור לעיל ולציין בטבלה את הלקוחות המתאימים ביותר.

3. ועדת המכרזים תהיה רשאית להתחשב בנסיון הנצבר במחב"א בהתקשרויות קודמות עם המציע ככל שהיו.

4. הצעה זוכה תהה זו שתקבל ציון משוקלל איכות ומחיר גבוה ביותר.

0.8 תוקף ההצעה

ההצעה למכרז תהיה בתוקף בהתאם למופיע בסעיף 0.1.2 - טבלת ריכוז מועדי המכרז, בשורה "מועד תוקף ההצעה".

המציע יאריך את תוקף ההצעה, לבקשת מחב"א, עד לקבלת החלטה סופית של זכייה במכרז זה.

0.9 הסכם התקשרות חתום בראשי תיבות

המציע יחתום על הסכם ההתקשרות המצורף להלן כנספח 0.9. ההסכם ייחתם בראשי תיבות על ידי מורשה/י החתימה של המציע ויוחתם בחותמת התאגיד בכל עמוד מעמודיו וכן בחתימה מלאה ובחותמת התאגיד במקום המיועד לכך בסוף ההסכם.

חתימה זו מעידה על הסכמת המציע לתנאי ההסכם. השלמת החתימות והפרטים כגון עדכון ההסכם בעקבות מענה לשאלות הבהרה והגשת נספחים (ערבות ביצוע, ביטוח וכדומה), תעשה בתוך 30 יום מיום הכרזת ועדת המכרזים על המועמד להיות הספק הזוכה.

0.9.1 מועד כניסת ההתקשרות לתוקף

מועד כניסת ההתקשרות לתוקף מותנה בהשלמות האמורות בסעיף 0.9 לעיל, עם השלמת החתימות והפרטים המועמד להיות הספק הזוכה יוכרז כספק הזוכה בפועל.

במקביל להשלמת החתימות והפרטים מצד הספק וכתנאי לחתימת ההסכם, ישלים מחב"א את נספח ז' להסכם אשר יתחם את פרויקט ההקמה ויכלול הזמנת שירותים וציוד בפועל, והכל בהתאם למענה הספק הזוכה.

הפרטים אשר יכללו במסגרת הנספח:

א. מספר ושמות המוסדות אשר יכללו במסגרת ההתקשרות.

ב. מועד הצטרפות כל מוסד לשירות (מידי, בשנה ראשונה, בשנה שנייה).

ג. חלון שירות עבור כל מוסד במסגרת שירותי CSOC.

ד. שירותים נדרשים על מנת לממש את ההתקשרות בהתאם לכמות המוסדות בפועל ולתצורת SIEM שבהצעה הזוכה.

מועד החתימה על ההסכם בפועל יהווה את מועד תחילת פרויקט ההקמה (ARO).

0.10 זכויות עורך המכרז

0.10.1 ביטול המכרז

ועדת המכרזים של מחב"א רשאית על פי שיקול דעתה המוחלט והבלעדי, לבטל את המכרז או לפרסם מכרז חדש. אם המכרז יבוטל לפני בחירת הזוכה, ההודעה על ביטולו תישלח לכל המציעים אשר הגישו הצעות למכרז.

במקרה של ביטול המכרז, לא יינתן פיצוי למציעים בכל צורה שהיא.

0.10.2 שאלות הבהרה

ועדת המכרזים ו/או מי שיוסמך מטעמה רשאית לבקש מכל מציע, בכל שלב של הליך המכרז, הבהרות בכתב או בעל פה להצעה כולה או מקצתה, ובלבד שלא יהיה בכך כדי לאפשר למציע לשנות את הצעתו או להעניק לו יתרון בלתי הוגן על מציעים אחרים. ההבהרות יהיו חלק בלתי נפרד מההצעה.

ועדת המכרזים ו/או מי שיוסמך מטעמה רשאית לדרוש מכל מציע השלמת מידע חסר, המלצות או אישורים המתייחסים לדרישות המפורטות במכרז, לצורך בחינת עמידתו של המציע בתנאי המכרז, וכן לבצע כל פעולה אחרת הדרושה לבחינת ההצעה, לרבות ביקור במתקני המציע.

ועדת המכרזים ו/או מי שיוסמך מטעמה רשאית להורות על תיקון פגם שנפל בהצעה או להבליג על הפגם, אם מצאה כי אין בכך כדי לפגוע בשוויון בין המציעים וכי החלטה זו משרתת באופן המרבי את טובת מחב"א ואת תכליתו של מכרז זה.

0.10.3 פסילת הצעה

ועדת המכרזים שומרת לעצמה את הזכות לפסול הצעה, בין היתר, מבין המקרים הבאים:

א. הצעה מסויגת או מותנית

- מציע לא יסייג את הצעתו או יתנה אותה באופן שאינו עולה בקנה אחד עם דרישות המכרז, ובכלל זה ימנע מכל שינוי, הסתייגות או התניה על דרישות ההסכם ונספחיו.
- מציע הסבור כי דרישות המכרז ראויות להתניה או להסתייגות, רשאי להעלות את השגותיו או את הערותיו במסגרת הליך ההבהרות בלבד. המזמין ישקול את פנייתו וישיבו, הכול בהתאם לקבוע בסעיף 0.3.3 לעיל. אין להסתייג או להשיג על תנאי ההליך במסגרת ההצעה גופה.

ב. הצעה שהיא בלתי סבירה או שחסרה בה התייחסות מפורטת לסעיף מסעיפי המכרז שלדעת ועדת המכרזים מונע הערכת ההצעה כדבעי. ככל שמוצאת הועדה לנכון לפסול כאמור, תעניק הועדה למציע את הזכות לטעון טענותיו בכתב בטרם קבלת החלטה סופית בסוגיה.

ג. הצעה תכסיסנית - הצעה הכוללת מידע מטעה או הצעה הלוקה בחוסר תום לב. ככל שמוצאת הועדה לנכון לפסול כאמור, תעניק הועדה למציע את הזכות לטעון טענותיו בכתב בטרם קבלת החלטה סופית בסוגיה.

0.10.4 היקף ההתקשרות

מחב"א יהיה רשאי להגדיל את היקף ההתקשרות במכרז בכל עת או להקטין את היקף ההתקשרות מול הספק הזוכה על פי תנאי המכרז והכול עפ"י שיקול דעתו הבלעדי.

0.11 הצעת הספק

הצעת המציע תוגש באמצעות תבנית מסמך וורד, הכוללת את כל סעיפי המכרז ואת פירוט הדרישות למענה המציע – נספח 0.11 תבנית להגשת הצעה.

0.11.1 מבנה כללי

א. מבנה ההצעה יהיה תואם באופן מלא לדרישות המכרז. חובה לענות לפי המבנה והפירוט שבכל סעיף. ועדת המכרזים תהיה רשאית לפסול הצעה אשר תוגש שלא במבנה זה או לא תהיה שלמה, וזאת על פי שיקול דעתה המוחלט והבלעדי.

ב. נספחי המכרז מהווים חלק בלתי נפרד ממסמכי המכרז. עם זאת, במקרה של סתירה בין נספחי המכרז לבין גוף המכרז יגבר האמור בגוף המכרז.

ג. תוכן ומבנה ההצעה בכל רכיב (סעיף ותת סעיף) יתאים לסעיף המקביל במכרז. המציע רשאי להוסיף הערות והצעות משלו. במקרה של הצעה ארוכה יש להפנות לנספח בסוף ההצעה שיסומן במספר הרכיב המפנה. השימוש בנספחים יהיה על מנת לפשט את גוף ההצעה ולהקל על קריאתה. חומר מקצועי ופרסומי יצורף כנספח לסעיף הרלוונטי ויסומן כמפורט לעיל.

ד. מסמכים שהמציע יצרף ושאינם מהווים חלק מדרישות המכרז יצורפו כשהם מתויקים בכריכה נפרדת (תיק, קלסר) והם מסומנים בהתאם לסעיף הרלוונטי.

ה. יובהר, כי ועדת המכרזים אינה מחויבת להתחשב בדפים, חוברות, DoK, מצגות וכד', שאינם נדרשים במפורש או שהגשתם לא הותרה במפורש.

0.11.2 מספר עותקים

ההצעה למכרז תוגש בשלושה (3) עותקים מודפסים זהים כשכל עותק כולל מדיה (Disk-On-KEY).

עותק המקור יסומן כ"עותק מקורי"; בעותקים אלו - העמוד הראשון (על כל מסמכיו, נספחיו והאישורים המצורפים) יוחתם בחותמת התאגיד של המציע ובחתימה מלאה של מורשי החתימה המוצהרים. ביתר העמודים, ניתן לחתום בראשי תיבות בחתימת מורשי החתימה כאמור.

שני העותקים הנוספים יהיו צילום של העותק המקורי.

בכל מקרה של סתירה בין האמור בעותק המקור להעתקי ההצעה למכרז, יגבר העותק המקורי.

המציע ידביק על הצד החיצוני של הצעת המקור, מעטפה סגורה היטב, ללא פרטי המציע על גבה, ובתוכה יופיעו שם המציע ופרטי איש קשר מטעמו (מספר טלפון וכתובת) לשם החזרת המעטפה במקרה הצורך.

ההצעה תוגש ארוזה באריזה אחת שעליה ירשם "**מכרז פומבי מספר 1/2019 לאספקת מערכת SIEM ושירותי CSOC**". כל עותק יוגש באריזה נפרדת ובתוכה 3 מעטפות שתכולתן תהייה כדלהלן:

1. **מעטפה ראשונה: (תסומן "פרק 0 - מנהלה")**

   המעטפה תכלול את מענה המציע לפרק המנהלה כשהוא כרוך ומוחתם עפ"י המצוין לעיל, כולל כל מסמכי המקור של האישורים והנספחים הנלווים שיש להגיש כמענה לפרק המנהלה.

   כמו כן, המעטפה תכלול DoK עם כל המסמכים שבמעטפה. המענה יכלול מסמכי מקור בפורמט PDF ועותק של מסמכי המקור במסמך Word.

2. **מעטפה שנייה: (תסומן כ"פרקים 1 עד 4")**

   המעטפה תכלול את מענה המציע לפרקים 1 עד 4 כשהוא כרוך וחתום על פי המצוין לעיל, כולל כל מסמכי המקור של האישורים והנספחים שיש להגיש במסגרת פרקים אלו של המכרז.

   כמו כן, המעטפה תכלול DoK עם כל המסמכים שבמעטפה, המענה יכלול מסמכי מקור בפורמט PDF ועותק של מסמכי המקור במסמך Word.

3. **מעטפה שלישית: (תסומן כ"פרק 5")**

   המעטפה תכלול מענה המציע לפרק 5 כשהוא כרוך ומוחתם על פי המצוין לעיל, כולל כל מסמכי המקור של האישורים והנספחים שיש להגיש במסגרת פרק זה של המכרז. המעטפה תכלול גם עותק מודפס וחתום של נספח 5.0 - אקסל מענה לפרק עלות.

   כמו כן, המעטפה תכלול DoK עם כל המסמכים שבמעטפה, המענה יכלול בנוסף לקובץ אקסל, במידת הצורך, מסמכי מקור נוספים בפורמט PDF ועותק של מסמכים אילו במסמך Word.

ועדת המכרזים תהיה רשאית לפסול הצעה שלא תוגש על פי האמור.

0.11.3 מספר הצעות

מציע יכול להגיש למכרז הצעה אחת בלבד.

0.12 בעלות על המכרז ועל ההצעה

0.12.1 בעלות על מסמכי המכרז והשימוש בהם

מסמכי המכרז הינם קנינה הרוחני הבלעדי של מחב"א, ומועברים למציע לצורך הגשת ההצעה בלבד. אין לעשות בהם שימוש כלשהו שאינו לצורכי הכנת הצעת המציע.

0.12.2 בעלות על ההצעה ושימוש בה

הצעת המציע (המענה לבקשה להצעות) היא רכושו של המציע. למחב"א תהא האפשרות להשתמש בהצעה ובמידע שבה לכל צורך הקשור בתהליך זה של בקשה להצעות עד להשלמת ההתקשרות.

0.12.3 חשיפת פרטי הצעה לצדדים שלישיים

א. עורך המכרז מתחייב לא לגלות היבטים רגישים מסחרית מתוכן ההצעה שקיבל לצד שלישי, זולת היועצים המועסקים על ידו, אשר גם עליהם חלה חובת סודיות.

ב. ועדת המכרזים תאפשר למציעים שלא הוכרזו כזוכה במכרז, לעיין בפרוטוקול ועדת המכרזים ובמסמכי ההצעה הזוכה על פי המוגדר לעיל בסעיף 0.3.7.

0.13 מחירים

א. כל המחירים שיהיו נקובים בהצעה יהיו סופיים, ויכללו את כל מרכיבי העלות. ככלל, מחירי השירותים יהיו נקובים בשקלים, ללא מע"מ, ומחירי המוצרים ב- $ ארצות הברית ללא מע"מ.

ב. בעת פתיחת ההצעות הכספיות תבוצע המרה של העלות הדולרית לש"ח על בסיס שער יציג של בנק ישראל מעודכן ליום פתיחת ההצעות.

ג. כל המחירים יכללו את מלוא המסים (למעט מע"מ), ההיטלים או תוספות אחרות, לרבות כל תשלום מסוג כלשהו לצד שלישי בגין תמלוגים ו/או זכויות שימוש.

0.14 תקופת ההתקשרות

א. משך ההתקשרות לשירות הוא 5 שנים מיום חתימה על הסכם ההתקשרות עם הספק הזוכה. למחב"א שמורה הזכות להאריך את תקופת ההתקשרות בכל פעם לתקופה של 12-36 חודשים עד ל- 10 שנים בסך הכל. למחב"א שמורה הזכות לסיים את ההתקשרות לפני תום התקופה בהתאם למפורט במסמכי המכרז.

ב. מחב"א יודיע לזוכה, בכתב, 90 ימים מראש, אם ברצונו להאריך את תקופת ההתקשרות.

0.15 היררכיה בין מסמכים, פרשנות וסמכות שיפוט

א. בכל מקרה של סתירה שאינה ניתנת ליישוב בין נוסח המכרז לבין נוסח ההסכם, יגבר נוסח ההסכם.

ב. ביטויים המופיעים בלשון יחיד משמעם גם בלשון רבים ולהיפך; ביטויים המופיעים בלשון זכר משמעם גם בלשון נקבה ולהיפך.

ג. כותרות הסעיפים במכרז ובנספחיו הן למטרות נוחות ולא ישמשו לצרכי פרשנות.

ד. סמכות השיפוט הבלעדית לדון בתובענה שעילתה במכרז זה נתונה לבית המשפט המוסמך במחוז תל-אביב.

ה. אין בסעיפי המכרז כדי לגרוע מזכויותיו של מחב"א על פי כל דין.

1. יעדים ומטרות

1.1 מטרות

להקים מערכת SIEM מרכזית לשירותי איסוף לוגים, ניטור, בקרה ותגובה עבור אירועי אבטחת מידע המתרחשים במערכות המידע של האוניברסיטאות אשר תזמנה את השירות. המערכת תותקן ותוגדר בתצורת Multi Tenant, כאשר כל מוסד יוגדר כ- Tenant בפני עצמו.

לקבל שירותי SIEM באחת מהחלופות הבאות:

1. **SaaS** - קבלת שירות SIEM באמצעות SaaS בענן, בתצורה של מספר Tenants כמספר המוסדות שיצטרפו לשירות.
2. **שירות מנוהל**

- רכש מערכת SIEM, הקמת מערכת וקבלת שירותי תפעול ותחזוקה. שירות שוטף יכלול תחזוקת מערכת, טיפול בתקלות, עדכון גרסאות, הוספת חוקים וניטורים.
- תשתית המערכת באמצעות שירות IaaS או רכש תשתית להרצה במתקן מחשב בקישור ישיר לרשת מחב"א (On Premise).

לקבל שירות לפונקצית CSOC מקצה לקצה באחריות כוללת של ספק השירות. מוסדות שיזמינו את השירות יקבלו אותו מ- CSOC שמוצב בחצר הספק, מאויש על ידי מומחי הספק ומפעיל מערכת SIEM מרחוק ובאופן מאובטח.

1.2 רקע כללי

על מנת לתת מענה אבטחת מידע לסביבת איומים משתנה, מוסדות החברים במחב"א החליטו על מיזם משותף להקמת מערך SIEM-CSOC. פנייה זו נועדה לספק למחב"א ולמוסדות שירותי SIEM-CSOC מנוהלים, תחת מסגרת משותפת.

כל מוסד יהווה לקוח בפני עצמו במערכת ויוגדר כ- Tenant עצמאי.

מערכת SIEM תסופק בתצורת SaaS בענן או בבעלות מחב"א ותנוהל על ידי הספק (להלן מערכת SIEM מנוהלת). תשתית המערכת בחלופת מערכת SIEM מנוהלת תסופק על ידי שירות IaaS בענן או כתשתית ייעודית בבעלות מחב"א.

נדרשת פריסת מערכת איסוף אירועים (Collector) מקומית בכל מוסד, אשר תשלח את האירועים למערכת SIEM מרכזית Multi-Tenancy, כאשר לצוותי CSOC של הספק תהיה גישה למערכת למתן שירות בהתאם לבחירת כל מוסד.

כל מוסד ייחשף רק לאירועים מתוך המערכות שלו, בעוד גישת ספק CSOC תהיה ממודרת בהתאם להנחיות המוסד.

1.3 תמצית השירותים: מערכת SIEM, שירות CSOC

1.3.1 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:

א. 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			
.2			
.3			
.4			
.5			

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

1.3.2 שירות CSOC

CSOC יתבסס על תשתית SIEM מוצעת ויעניק שירות למוסדות להם מספר רב של משתמשים, מערכות ואירועים.

1.3.3 מרכיבי ההצעה

א. חלופת SIEM מנוהל

1. אספקת מערכת תוכנה SIEM לאיסוף וניהול אירועי אבטחת מידע.
2. אפיון דרישות תשתית (פיזית או בענן) להקמת מערכת SIEM מרכזית ולמערכות איסוף אירועים במוסדות.
3. אספקת IaaS בענן עבור מערכת SIEM או רכישת תשתית להרצת מערכת מותקנת באתר רשת מחב״א. המציע יציע שתי חלופות לבחירת הלקוח.
4. התקנת מערכת SIEM עפ״י אופציה שתבחר ע״י הלקוח מבין IaaS בענן לתשתית באתר רשת מחב״א.
5. יישום והטמעת מערכת SIEM בהתאמה לדרישות המזמין.
6. יישום איסוף אירועים באמצעות 20 מערכות מידע שונות לפחות למוסד (ראה פירוט בסעיף 2.3.8), שיוגדרו וייוצגו באופן קריא (נרמול) במערכת SIEM.
7. מימוש מדיניות אבטחה ופרטיות ארגונית במערכת איסוף וניהול אירועים (הקשחה), בהתאמה למדיניות קיימת בכל אחד מהמוסדות.
8. כתיבת Rules פרטניים נוספים, מעבר לקיימים במערכת, בהתאם לדרישות המוסד (במסגרת פרויקט ההקמה יוגדרו 50 Rules ו- 25 תרחישים\קורלציות לכל מוסד). כל Rule ותרחיש פרטני שיוגדר עבור מוסד כלשהו יועמד לשימוש יתר המוסדות ללא תשלום ומחוץ למסגרת הכמות לעיל.

9. קישור דו כיווני בין מערכת SIEM למערכת שליטה ובקרה של המוסד בפרוטוקולים מקובלים, לצורך דיווח בין המערכות על אירועים כגון נפילת משאב, חוסר מקום במערך אחסון ועוד (על הספק לפרט פתרון מוצע).

10. בנק של 100 שעות מומחי מערכת SIEM לכל מוסד בשנה ראשונה לשירות, שישמש לפעילות מעבר למוגדר במפרט, וייכלל במסגרת תחזוקת המערכת. החל משנה שנייה להתקשרות, בנק השעות יעמוד על 50 שעות לכל מוסד.

ב. **חלופת SIEM בתצורת SaaS - אספקת שירות SIEM בענן,** שיכסה את ס"ק 5 – 10 בחלופת SIEM מנוהל המתואר בסעיף א' לעיל.

ג. **שירותי CSOC**

1. הספק יישם נוהל תגובה ותחקור אירוע במערך CSOC על בסיס נוהל קיים בכל מוסד וכן יכין הוראת עבודה לצוות CSOC המבוססת ותואמת לנוהל המוסד. אם למוסד אין נוהל תגובה ותחקור אירוע, הספק יציע נוהל כזה ובאחריות המוסד להתאים אותו למדיניות ולתהליכים הקיימים במוסד, ולאחר ההתאמה יכין הספק את הוראת העבודה לצוות CSOC.

2. אספקה שוטפת של שירות CSOC בהתאם להגדרות של כל מוסד וסיוע בניהול אירועי אבטחת המידע, בהתאם לנדרש בסעיפים 2.8 ו- 2.9.

1.4 משתמשי המערכת

המערכת תנהל גישה למשאבים/לוגים ותגדיר הרשאות לכל סוג משתמש. יצירת סוגי משתמש והתאמתם ליכולות הנדרשות יוגדרו בשלבי התכנון.

הגדרת משתמשים ועדכון הרשאות יבוצעו כחלק מהעבודה השוטפת.

משתמש	תיאור
מוקד CSOC צוות CYBER	מספקים מבט לרוחב ולעומק על אירועים שמתרחשים במוסדות השונים, תוך יכולת בחינה והשלכה של אירועי אבטחת מידע ממוסד למוסד.
מכאן ומטה הסתכלות מוסדית - כל מוסד ינהל את הנגזרת שלו בתוך המערכת, משתמשים, אירועים וכדומה	
מנהל אבטחת מידע מוסדי	אחראי על כלל השינויים שיבוצעו ברמה המוסדית של המערכת: מתן הרשאות, שינויי קונפיגורציה, הוספת מסכים, שינוי Rules וקורלציות וכו.
מנהל תשתיות מוסדי	אחראי על כלל תשתיות המוסד (בהתאמה) ותפקידו לוודא שהן מתפקדות היטב והמשתמשים מקבלים את השירותים הנדרשים.
ממונה אבטחת מידע טכנולוגי מוסדי	אחראי על ארכיטקטורת אבטחת מידע במוסד.
נאמני אבטחת מידע מוסדיים	אחראי ברמת אירוע אבטחת מידע במוסד אשר אתו מתקשר צוות CSOC בעת אירוע אבטחת מידע. הנאמן פועל בכפיפות למנהל אבטחת המידע מוסדי.

1.5 מחזור חיים

א. מחזור החיים של מערכת SIEM - המערכת נדרשת לשרת את המזמין לפחות 10 שנים מתחילת עבודה בייצור.

ב. משך החיים של חומרת מערכת SIEM, ככל שתרכש, הוא 5 שנים, במהלך תקופה זו ניתן יהיה לבצע שדרוגים ותוספות בשטח.

2. SOW – תיחום

2.0 דרישות כלליות

המציע נדרש להציע עד 2 שתי חלופות לשירותי SIEM, שיתבססו על מערכת מרכזית למספר מוסדות ושתכלול גם איסוף לוגים:

א. SIEM מנוהל - מערכת בבעלות מחב"א על גבי תשתית פיזית IaaS בענן או תשתית פרטית, מנוהלת, מופעלת ומתוחזקת על ידי הספק.

ב. שירות SIEM בתצורת SaaS.

בכל אחת מהחלופות לעיל, בכל מוסד יותקן Collector שיזרים אירועים באופן מאובטח למערכת SIEM מרכזית. גישת המוסדות למערכת SIEM תהיה ממודרת, כאשר כל מוסד יחשף רק לאירועים הרלוונטיים לו. הספק יהיה אחראי לחבר את מערך CSOC המוצע למערכת SIEM ולהפיק אתראות לכל מוסד בהתאם.

על מערכת SIEM לאפשר איסוף מידע ואירועים ממקורות מידע נוספים אשר אינם כלולים בתכולת הוונילה של המוצר, מתשתית מבוזרת והטרוגנית של המוסדות וכן אירועים נוספים המגיעים ממערכות הממוקמות במחב"א.

בחלופת SaaS, מרכיבי ההצעה יכללו את כל רכיבי התוכנה והחומרה הנדרשים להקמה ולהפעלה של המערך כמכלול. המציע נדרש לספק מוצרי תוכנה, לרבות רכיבי תוכנה נוספים הנדרשים על מנת לעמוד בדרישות המפורטות במסמך זה, להקים את המערכת, לתאם את קבלת הלוג מתוך מקורות מידע שונים ואפליקציות, לבצע אינטגרציה, לבצע הדרכות ולתחזק את המערכת לאורך כל תקופת ההתקשרות.

בחלופת SIEM מנוהל, מחב"א ירכוש מהספק תשתית פרטית נדרשת או ישלם דמי שירות ל IaaS, ובנוסף ישלם דמי שכירות או ירכוש את תוכנת SIEM.

מוסד יהיה רשאי לרכוש רישוי עבור מערכת SIEM בהתקנה מקומית (On Premise) שתשרת את המוסד בלבד, עפ"י מחירים שייכללו בהצעה. במקרה הנ"ל מחירי הקמה ו/או שירות CSOC ייקבעו במו"מ בין המוסד לספק.

2.1 ארכיטקטורה

במחב"א חברים מספר מוסדות אקדמאיים בעלי מאפיינים וצרכים דומים בתחום מערכות מידע ואבטחת מידע ויחד עם זאת עם תפיסת עולם שונה בכל הקשור ליישום ופריסת מערכות אבטחת מידע בארגון. לפיכך, על מנת לספק את צרכי המוסדות השונים באופן משותף תחת מכרז זה, על הספק להציע ולתמוך בתצורה אשר תשמור על עצמאות כל מוסד בקביעת מדיניות מוסדית וברמת מידור התואמת את מערכת ההרשאות המוסדית.

מערכת SIEM רבת-ישויות (Multi-Tenancy) תאפשר איסוף מידע ואירועים ממערכות מידע ומתשתית אבטחת מידע של המוסדות, וכן אירועים נוספים המגיעים ממערכות אבטחה הנמצאות במחב"א. לכל מוסד תוקם ישות (Tenant) עצמאית עם גישה מלאה לאנשי המוסד המורשים בלבד. לצוות CSOC וצוות סייבר במחב"א תהיה גישה לכלל האירועים במערכת, אלא אם מוסד כלשהו יחליט אחרת.

באחריות הספק לתכנן תשתית SIEM לתמיכה בכמות האירועים של כל מוסד וכן להקים ולתחזק את התשתית על מערכות או תשתיות ענן שיסופקו על ידי מחב"א. על ההצעה לכלול מענה

טכנולוגי לגיבויים ולהתאוששות מקריסת המערכת המרכזית, כמו גם מענה לשמירת אירועים ישנים (Retention) בארכיון המותקן במערך אחסון זול.

תשתית המערכת תהיה בתצורת HA, ללא SPOF. עבור תצורת SaaS השירות יכלול פתרון המשכיות. עבור מערכת מנוהלת תוקם מערכת חלופית בתצורת Active-Passive וללא צורך ברישוי נוסף. העבודה הכלולה בהקמת מערכת הגיבוי במסגרת פרויקט ההקמה באחריות הספק, באחריות המזמין הקצאה של משאבי התשתית הנדרשים.

2.1.1 מערכת SIEM מרכזית לאיסוף לוגים

מערכת SIEM מרכזית תוקם בענן בשירות SaaS או בבעלות מחב"א. במקרה של בעלות מחב"א היא תותקן על גבי תשתית פרטית ברשת מחב"א או בענן ציבורי.

בכל מוסד יותקן מאגד (Collector) אחד או יותר אשר יזרים אירועים באופן מאובטח למערכת SIEM מרכזית. גישת המוסדות השונים למערכת SIEM תהיה ממודרת, כאשר כל מוסד יחשף **רק** לאירועים הרלוונטיים לאותו מוסד. הספק יהיה אחראי לחבר את מערך CSOC המוצע למערכת SIEM ולהפיק תוצרים נדרשים לכל מוסד בהתאם.

באחריות הספק לתכנן את תשתית SIEM לתמיכה בכמות אירועי כל מוסד וכן להקים ולתחזק תשתית על מערכות שיירכשו על ידי מחב"א או שירות IaaS באחריות כוללת של הספק.

על המערכת המוצעת לעמוד בדרישות אבטחת המידע המופיעות במפרט, בכל הקשור למנגנוני הזדהות (OTP ו- SAML), אבטוח התקשורת של משתמשים אל המערכת (TLS) ואבטחת תעבורה בין שרתי איסוף למערכת המרכזית.

הרשאות – מערך ההרשאות במערכת יהיה על בסיס ה"צורך לדעת". על המערכת לתמוך בהגדרת מספר תפקידים בעלי הרשאות שונות. לדוגמא: מנהל תשתיות, מנהל אבטחת מידע, מנהל מערכת תפעולי, אנליסט ועוד. יישום הרשאות יוגדר לכלל רכיבי המערכת. משתמש לא יקבל הרשאה שאינה מוגדרת בתפקידו.

הצפנה – 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 הצפנה ברשת.

ניהול המערכת – ניתן יהיה להגדיר שניהול המערכת יבוצע מעמדות מוגדרות מראש תוך זיהוי והצפנה של התווך. על הספק לפרט מהם פרוטוקולי הניהול.

בקרה – המערכת תתעד ותאפשר בקרה על כלל פעילויות הניהול שיבוצעו עליה – כדוגמת זיהוי, שינוי הגדרות, עדכונים וכו'. המערכת תתעד את כל האירועים ותרשום לוג מפורט. על הלוג להיחתם או להיות מוגן מפני שינוי נתונים מרגע שנרשמו. רישום לוג יהיה מוגן משינוי, נגיש וקריא למערכות חיצוניות. על המערכת עצמה לאפשר לשלוח אירועים (באמצעות דוא"ל או SMS) ולהציגם, אם אירע אירוע על המערכת המרכזית ו/או בסיס הנתונים.

הקשחות – על המערכת להיות מוקשחת בהתאמה למדיניות המזמין. ההקשחה חלה הן על מערכות ההפעלה והן על בסיס הנתונים.

2.2 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.

2.2.1 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	Y		

#	דרישה	הקמה	OoB Y/N	פיתוח Y/N
	הינה לאיסוף אירועים, הרי שבסיס הנתונים המרכזי של המערכת יכלול איסוף ראיות ותיעוד אירועי אבטחה			
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	Y		

#	דרישה	הקמה	OoB Y/N	פיתוח Y/N
	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.			
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				

2.2.2 דרישות תצורה

א. 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:

ב. 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

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

מענה המציע:

2.2.3 ניהול מידע במערכת

א. לוג במקורות מידע - קיימים מספר רב ומגוון של מקורות מידע ברשתות המוסדות. בכל מקורות המידע למעט אפליקציות – באחריות הספק להגדיר את דרישות הלוג במקור המידע ולאסוף את הלוג למערכת האיסוף. אם לא מוגדר לוג במערכת והמזמין יבחר להגדירו במקור המידע בעצמו, על הספק להגדיר למזמין מהו הלוג הנדרש או האירועים הנדרשים לניטור וכיצד להגדירם במערכת. בנוסף, הספק יידרש להבהיר למזמין לפני היישום את כלל השלכות כתיבת לוג במקור מידע.

ב. Rules/התראות/תרחישים - יוגדרו Rules והתראות לכל אחד ממקורות המידע והאפליקציות. ה- Rules יכולים להיות פשוטים או תרחישים מורכבים הכוללים כללי קורלציה\אגרגציה של מספר אירועים. הגדרת Rule כוללת זיהוי רשומה בלוג, קבלת הרשומה במערכת, הגדרת ה- Rule במערכת ובדיקת התראת ה-Rule. Rules שלא ייבדקו ע"י הספק – לא יעברו בדיקות קבלה.

ג. טיוב אירועים – לאחר הגדרת כל האירועים יבוצע שלב טיוב אירועים במערכת:

- טיוב ע"י הספק – הספק יטייב אירועים במערכת בכדי להוריד אירועים חלקיים/לא תורמים מידע/תקולים, לרבות קבלת מספר רב של אירועים ממקור ייעודי.
- טיוב ע"י המוסד – המוסד יחליט אם להוריד/להוסיף/ לחדד Rules במערכת. שלב זה יבוצע לאחר תחילת העבודה על כלל המערכות.

2.2.4 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'.

א. **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?

ב. **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.

ג. **תהליך שדרוג מערכת** - על המציע לפרט ברמה כללית את תהליך שדרוג המערכת, שלבים, השלכות.

ד. **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:

2.3 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:

א. האם מערכת SIEM תומכת OoB באיסוף מידע של מקור המידע?

ב. יכולות סינון אירועים ברמת נקודת קצה.

ג. אילו גרסאות מקור מידע נתמכות על ידי היצרן? אם אין תמיכת יצרן בגרסה עדכנית של מקור המידע, יש לפרט מועד מתוכנן לתמיכה כזו.

ד. 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:

ה. כיצד יבוצע איסוף מידע (פרוטוקולים, תצורת קישור חד/דו כיוונית, גורם יוזם)?

ו. האם קיימת תמיכה בהסתרת מידע פרטי (כמו ת.ז., שדה סיסמא וכו') ואי העברתו למערכת?

ז. מהם ביצועי המערכת לכל אחת משיטות איסוף מידע? לציין עומסים שבהם המערכת תעמוד.

מענה המציע לסעיפים ה'- ז' :

לאחר שלב ההקמה ניתן יהיה להוסיף מקורות חדשים ולגרוע מקורות מידע קיימים.

להלן קטגוריות מקורות המידע

2.3.1 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:

2.3.2 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:

2.3.3 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:

2.3.4 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:

2.3.5 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:

2.3.6 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:

2.3.7 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:

2.3.8 רשימת מקורות מידע

- הספק נדרש לתמוך בכל גרסאות התוכנה המותקנות במוסדות.
- הספק אינו מחויב לתמוך בגרסאות אשר אינן נתמכות על ידי היצרן ומוגדרות כ- EOL.
- המציע יציין יכולת תמיכה במערכות מדף ומוצרי קוד פתוח.
- המציע יפרט בנספח 2.3.8 את יכולותיו לאיסוף מידע ממקורות המידע השונים המפורטים בנספח.

מענה המציע : יש למלא את נספח 2.3.8

2.4 מסכי מערכת SIEM

א. כל המסכים המתוארים בהמשך יהיו בכפוף לאפיון משתמשים והרשאות שמופיע בסעיף היבטי אבטחת מידע 2.13.

ב. בכוונת המזמין להגדיר את כל מסכי המערכת באמצעות תפריטי מערכת ויכולות התאמה והטמעה שקיימים בה.

ג. המזמין ישאף לאחידות בממשקי משתמש, על מנת לייעל תהליכי עבודה ב- CSOC ותחזוקת מערכת SIEM.

2.4.1 מסכים נדרשים

א. מסכי מערכת בסיסיים יאופיינו ויוגדרו בהתאמה לתהליכי עבודה של כל מוסד. המסכים המרכזיים הנדרשים הינם: מסך כניסה למערכת, מסך מרכזי ראשי, מסך אירועים, מסך תגובה, מסך תחקור, מסך דוחות, מסך בקרה/מנהלים.

ב. המערכת המוצעת תספק מנגנון הרשאות מפורט, וממשק מתאים עבורו, המאפשר להגדיר הרשאות צפייה וכתיבה פרטניות למשתמש או לקבוצת משתמשים, לכל מסך ולכל פונקצייה במערכת.

ג. ממשק הרשאות ינוהל ע"י מנהל אבטחת מידע מוסדי ו/או מי מטעמו.

ד. 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	

מערכת SIEM/SOC - מסכים נדרשים	מענה המציע
מסך פירוט אירוע	
מסך תחקור אירוע	
מסך דו"חות וסטטיסטיקות	
מסך Knowledge base	

2.4.2 מסך כניסה למערכת – מערכת ה-SIEM

הזדהות למערכת SIEM תתאפשר באמצעות אחד משני מנגנוני הזדהות: SAML מול מערכת הזדהות של המוסד או OTP מבוסס SMS או Google Authenticator. המערכת תצטרך לתמוך בשלושת המנגנונים, כאשר כל מוסד יבחר את דרך ההזדהות בה ישתמש.

2.4.3 מסך מרכזי – מערכת SIEM

במסך הראשי במערכת יוצגו אירועים שמקורם בתשתיות, המסך יחולק לשלושה חלקים:

חלק ראשון – אירועי אבטחת מידע – חלק בו יוצגו אירועי אבטחת מידע ארגוניים על בסיס חיתוך זמן ורמת חומרת אירוע. הנחות יסוד בהצגת אירועים במסך:

א. יקבעו עד 4 רמות חומרה לסיווג אירועים, שמהם יגזרו רמות אסקלציה של המוסד.

ב. יוצגו רק אירועים ברמה גבוהה מרמה שתקבע (יתאפשר לקבוע לכל מוסד רמה ייחודית).

ג. לאחר חריגה מ-SLA שיקבע לרמת חומרה של אירוע, תועלה רמת החומרה של האירוע ברמה אחת ויועלה האירוע בחיתוך תצוגת האירועים.

ד. לאחר חריגה מ- SLA לטיפול באירוע יועבר מייל\SMS למנהל אבטחת מידע על אי טיפול באירוע, שיכלול ת כלל המידע על האירוע: תאריך וזמן, שם אירוע (לפי הסכמות מוגדרות מראש), מקור מידע עליו בוצע האירוע, רמת חומרה, כתובת/מקור מידע שביצע את האירוע.

ה. לחיצה על אירוע תפתח מסך נוסף (שלא במקום מסך קיים), עם פרטים נוספים על האירוע בהתאם לכל מקור מידע. אפיון יבוצע במהלך היישום.

ו. במקביל לקבלת מידע, ניתן יהיה להחליט על ביצוע פעולה/תגובה ראשונית לאירוע: פתיחת אירוע במסך אירועים או סגירת/הורדת אירוע ממסך ראשי, ללא תיעוד במסך אירועים.

ז. אם יוחלט על פתיחת אירוע במסך אירועים, האירוע יועבר מחלק ראשון של המסך לחלק שני. אם יוחלט על הורדת אירוע ממסך, האירוע יעלם מיידית. יודגש כי אין צורך ב- Refresh למסך.

חלק שני – סטטוס אירועים מטופלים – אירועים שנפתח עבורם אירוע במסך אירועים. בחלק שני יוצגו כלל האירועים שהבקר פתח בגינם אירוע במסך אירועים. האירועים יוצגו בהתאם לחומרה ולזמן פתיחת אירוע.

חלק שלישי – תפריט/סרגל כלים - באמצעותו ניתן יהיה לפנות לשאר מסכי המערכת, כדוגמת מסך אירועים מלא וכד'.

2.4.4 מסך אירועים

כיוון שמסך ראשי מציג אירועים רק בעלי חומרה/תעדוף מרמה מסוימת, יש לאפשר גם גישה לכל האירועים. מסך אירועים זה יחולק בשלושה אופנים (בהתאם להחלטה שתתקבל באפיון מפורט):

- אופן ראשון – הצגת כל האירועים בחיתוך רמת חומרה/ תעדוף וזמן קבלת אירוע.
- אופן שני – הצגת אירועים בהתאם למקור מידע בחיתוך רמת חומרה/תעדוף וזמן קבלת אירוע.
- אופן שלישי – הצגת אירועים בהתאם לסביבת עבודה שתוגדר – קרי הצגת כלל מקורות מידע קיימים באותה סביבה בחיתוך רמת חומרה/תעדוף וזמן קבלת אירוע.

ממסך אירועים ניתן יהיה לבצע את הפעולות הבאות:

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

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

- שם אירוע
- חומרת אירוע
- תאריך אירוע ושעה
- מספר אירוע – ייחודי לרמת SIEM
- גורם מעדכן
- גורם מטפל

2.4.5 מסך פירוט אירוע

לחיצה כפולה על אירוע או על לחצן ימני יאפשרו קבלת מידע מפורט על אירוע. נדרש לקבל את כלל המידע המתאפשר מלוג המערכת.

במסך זה יוצג מידע רלוונטי בהתאמה לדרישות המוסד. מידע שאינו רלוונטי יוסתר או שיורד מהמסך, כך שהמסך לא יכלול שדות ריקים ו/או לא קריאים.

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 עבודה בה התרחש האירוע
מקור מידע	מקור מידע שעליו חל האירוע: שם מחשב / מערכת וכו'
שם שרת	שם שרת/מערכת עליו בוצע האירוע
כתובת IP	כתובת IP של מקור מידע

חומרת אירוע	חומרת האירוע
גורם מבצע	גורם שביצע את האירוע כגון משתמש/שרת
תיאור האירוע	הסבר על מהות האירוע, השלכות וכו'
אגרגציה\קורלציה	שילוב של מספר אירועים יחד
Rule במערכת	Rule במערכת אשר העלה את האירוע

מסך תגובה לאירוע הינו מסך שבאמצעותו יטפלו באירועי אבטחה, הן אלה המגיעים מ-SIEM/SOC והן אירועי אבטחה תפעוליים.

המסך יכיל חלק אינפורמטיבי שיאפשר קבלת מידע ממערכת SIEM/SOC שתעביר נתונים מלאים על האירוע. יתקבל כלל המידע על האירוע, על מערכות קשורות, אנשי קשר שנדרש ליידע וכו'.

במהלך ההטמעה יבוצע אפיון מפורט של המסך, שיכיל לפחות את הפרטים הבאים:

- פרטים בסיסיים של האירוע
- סטאטוס טיפול באירוע - חיתוך של משימות נדרשות לביצוע אל מול ביצוע בפועל.
- הסבר מילולי על האירוע
- פירוט האירוע - מידע המתקבל מ-SIEM/SOC שמכיל את כל הפרטים על האירוע.
- מיקום האירוע.
- מידע - פרטים על משתמש/מבצע פעולה/גורם, ככל שניתן לקבל הרחבה מעץ משתמשים ארגוני.
- תגובות לאירוע - מנהליות / טכנולוגיות.
- הערות לגבי האירוע.
- אנשי קשר - גורמים רלוונטיים לאירוע/ למקור מידע/ סביבת עבודה - שנדרש לידע אותם. תהיה אפשרות לשלוח מייל ליחידים ו/או לקבוצות, עם כל פרטי האירוע.
- תאריך ושעת סיום אירוע. לאחר סגירת אירוע אין אפשרות לפתוח אותו.

2.4.6 מסך תחקיר אירוע

תחקיר אירוע שיבוצע על ידי אנשי CSOC, מנהל אבטחת מידע או מי מטעמו. תחקיר יהיה ברמת מוסד כאשר רק למוסד הרלוונטי לאירוע ולמחב"א תהיה גישה לתחקיר. אירועים גלובליים ברמת מספר מוסדות יפתחו על מחב"א שבאחריותו להעביר פרטים ונתונים רלוונטיים לכלל המוסדות או רק לאלה המעורבים באירוע, על פי החלטתו.

דרישות בסיסיות לתחקיר:

- לכל תחקיר יוקצה מספר מזהה חד ערכי.
- ניתן יהיה לפתוח תחקיר לאחר שגורם מבצע סגר תחקיר, אם נדרשות השלמות. אם יפתח תחקיר נוסף המבוסס על אירוע קודם, ניתן יהיה לאחד את התחקירים לכלל אירוע אחד.
- כלל הפרטים של האירוע יופיעו כשדות ללא שינוי.
- מסך תחקיר אירוע יתחלק לשלושה:

א. סרגל תחקירים - שבאמצעותו ניתן יהיה לחפש תחקיר קיים.

ב. השלמת תחקיר - שדות מלאים בתחקיר יוגדרו במהלך האפיון המפורט.

ג. הסקת מסקנות - גורם מטפל/מתחקר ישלים התייחסות לאירוע (למשל, למה אירע האירוע) וכן פעילויות נוספות שיש לבצע להמשך הטיפול וזאת במטרה לאפשר סגירת האירוע ולהמשיך לטפל ו/או לבצע פעילות מונעת.

2.4.7 מסך דו"חות וסטטיסטיקות

- דו"ח אוטומטי - ייווצר ברגע סגירת אירוע שבו ישלח סטאטוס "סגור". על המערכת ליצור PDF ולחתום דיגיטלית על התחקיר. דו"חות תחקירים ישמרו בספריה ייעודית/כספת ולא תינתן גישה לשינוי התחקיר אלא לקריאה בלבד.
- דו"חות סטטיסטיים של אירועים בחיתוך - טווח רמת חומרה מול סטאטוס טיפול באירוע.
  דו"חות שוטפים של מוקד - כלל הדוחות שיוגדרו להוצאה על בסיס יומי/שבועי/חודשי/רבעוני ושנתי.
- תחקירי אירוע - שתי רמות של תחקירי אירוע - תחקירים אוטומטיים ותחקירים רוחביים.
- סטטיסטיקות - כלל הסטטיסטיקות שיידרשו הן ממערכת SIEM/SOC, כדוגמת כמות אירועים למקור מידע מסוים בזמן נתון שיבחר בפילוג של שמות משתמשים.
- דו"ח סטאטוס אירועים - אירועים פתוחים אל מול מצב טיפול באירוע. הדוח יוצג בחיתוך רמת חומרה/תעדוף אירוע אל מול מצב טיפול.

2.4.8 מסך ניהול הידע (Knowledge base)

- מסך ניהול ידע הינו מסך שישמש את אנשי המוסד הרשאים לגשת למערכת ואת אנשי SOC.
- 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.
- 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.
- המציע נדרש לצרף צילומי מסך המדגימים את כל אחד מהמסכים עם ציון סוג המסך בכל צילום.

מענה המציע: צירוף מסכי ניהול ידע כנדרש.

2.5 שירותים שוטפים למערכת SIEM

2.5.1 כללי

א. הספק אחראי לשירותי תפעול ותחזוקה שוטפים לאורך כל תקופת ההתקשרות, כהגדרתם בסעיף 0.2 הגדרות וכמפורט בסעיף 2.5.2. הספק יהיה אחראי לתקינות המערכות שסופקו על ידו ולמתן תמיכה למערכות אלו, לרבות טיפול בכל רכיב תקול במערכת.

ב. על הספק לרכוש עבור מחב"א שירות תחזוקת יצרן לכלל מוצרי התוכנה הכלולים בהצעתו למשך כל תקופת ההתקשרות. השירות יכלול לפחות טיפול בתקלות וקבלת גרסאות.

ג. טיפול מרחוק - לכל מוסד מדיניות ייחודית למתן גישה מרחוק לספקים. לכן טיפול מרחוק יתאפשר בהתאם למדיניות כל מוסד.

ד. על הספק לספק שירות ותחזוקה באתרי הלקוח לרכיבים המותקנים באתר הלקוח ולבעיות/ תקלות בממשקי איסוף הנתונים.

ה. הספק יקשר את צוותי אבטחת מידע של מחב"א והמוסדות לרשימות תפוצה (Mailing List) של יצרן SIEM לקבלת מידע אודות נושאי תפעול שוטפים – עדכוני גרסאות, חדשות ספק/יצרן, טלאי אבטחת מידע, יכולות חדשות של המוצר וכו'.

ו. השירות יכסה את כלל מרכיבי המערכת, כולל חלקים שפותחו ע"י הספק.

ז. בנוסף, עבור חלופת SIEM מנוהל:

- תשתית המערכת תסופק על ידי הספק אם כשירות בתצורת IaaS ואם ברכש חד פעמי להקמה פרטית.
- מחב"א שומר לעצמו אפשרות להריץ את מערכת SIEM מעל תשתית פרטית אשר תמוקם ברשת מחב"א ללא צורך ליציאה לרשת האינטרנט. הספק נדרש להציע תשתית מתאימה בהתאם לתצורה הנדרשת. במידה ותופעל אופציה זו מחב"א שומר לעצמו זכות לרכישה חלקית אם בכלל של תשתית זו, ובלבד שלספק יעמדו כל התשתיות הנדרשות להתקנת המערכת ולמתן השירותים. שירותים שוטפים.
- שירות IaaS, עבור מרכיבי תשתית מערכת SIEM ומתן כלל השירותים על פי המפרט, יכלול לרבות ולא רק: מערכות הפעלה, בסיסי נתונים, שטחי אחסון, יתירות.

2.5.2 תפעול ותחזוקה שוטפים

להלן פעילויות נדרשות מהספק במסגרת תפעול ותחזוקת מערכת SIEM:

א. התקנת עדכוני תוכנה, התאמת תוכנה בהתאם לשינויים במקורות מידע, תיקון תקלות במערכת והתאמה לשפה הרלוונטית.

ב. טיפול מונע - לכל מוצר יבוצע טיפול מונע לפי הוראות יצרן המערכת. אחת לשנה הספק יבצע ביקורת למערכת לבדיקת אפקטבייות הטיפול המונע. בסיום סבב הביקורת יגיש הספק למזמין דו"ח ביקורת עם סיכום ממצאים, פעולות שבוצעו והמלצות לשיפור הטיפול המונע.

ג. הספק יתעד כל תקלה במערכת תקלות, במטרה ללמוד ולהפיק לקחים לעתיד, וכן ינהל על כל קריאה בקרת SLA כמפורט בסעיף 3.1.

ד. נדרשת הגעה לפי צורך לאתר המזמין לביצוע תמיכה ותחזוקה לרכיבים הכלולים במערכת.

ה. הספק ידאג לביצוע גיבויים למידע ערכי, עפ"י החלטת כל מוסד, במערכות ולשחזור נתונים בהתאם לתצורה שתוצע על ידו ותאושר ע"י מחב"א וכל מוסד.

ו. בסיס נתונים במערכת – בשל בקשת המזמין לשמור רק מידע ערכי על המציע לבצע באופן שוטף טיוב של בסיס הנתונים במספר היבטים:

- שמירת אירועים שיוגדרו ע"י המוסד במקרה שמבוצע איסוף של כלל הלוג מהמערכות - לאחר הגעת המידע למערכת, הספק יריץ שגרות אשר ינקו את הלוג ממידע "לא רלוונטי" מבחינת המוסד.
- הודעות שגיאה/ התראות חלקיות – אם יגיע מידע לא "שלם" בלוג, יריץ הספק שגרה אשר תמחק ו/או תעביר אירועים אלו לבסיס נתונים אחר.

ז. אם יצרן SIEM יתעכב בהתאמת גרסה עבור מקור מידע הכלול בוונילה של המערכת, הרי שעל ספק לתת מענה חלופי/זמני לניטור, באופן שלא תיגרם חשיפה של מערכות קריטיות.

ח. אם מוסד כלשהו ירכוש מערכת ו/או יפתח יישום שאינו כלול בכיסוי מערכת SIEM, על הספק לכלול את המערכת/היישום בשירות SIEM-CSOC וזאת תוך חודש מקבלת הבקשה והמידע הטכני הנדרש לכיסוי של המערכת/היישום.

ט. להגדיר עד 150 Rules ועד 45 תרחישים חדשים לשנה עבור כלל המערכות המקושרות ל-SIEM על פי דרישת מחב"א. Rules ותרחישים חדשים שיוגדרו במוסד אחד לא יחשבו כ-Rules חדשים עבור מוסדות אחרים ולכן לא יכללו בספירה זו. אם בשנה מסוימת לא תנוצל מלוא כמות ה- Rules והתרחישים לעיל, הרי שהכמות שלא נוצלה תועבר לשנת השירות הבאה, מעבר לכמות השוטפת הרגילה לעיל.

להלן דוגמאות לכללים לספירת Rules ותרחישים במערכת:

- התאמת Rule או תרחיש למוסד, דוגמת מרחבי כתובות, שמות שרתים ומשתני סביבה, לא ייחשבו כ- Rule או תרחיש חדש.
- התאמת Rule או תרחיש לגרסה חדשה של מערכת מנוטרת לא תיחשב כ- Rule או תרחיש חדש. (למשל Rule הכולל בדיקה מול AD בגרסה חדשה במוסד מסויים ובגרסה AD ישנה במוסד אחר, אלא אם הגרסה לא נתמכת יותר על ידי יצרן התוכנה).
- אימוץ תרחיש מורכב שרץ במוסד א', תוך כדי הפשטתו, לא ייחשב כתרחיש חדש. למשל, תרחיש מורכב מ- 4 חוקים והוחלט לאמצו במוסד אחר, תוך אי התחשבות/השמטה של 2 חוקים מתוך ה- 4.

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.

2.6 שו"שים במערכת SIEM

מעבר לכלול בשירותים השוטפים כמתואר בסעיף 2.5 לעיל, למחב"א תישמר הזכות להזמין שירותים נוספים על בסיס מחירון שירותים ושעות המופיע בפרק התמורה. להלן דוגמאות לשו"שים אפשריים:

א. תוספת Rules ותרחישים (מעבר לכמות הכלולה במסגרת התחזוקה השוטפת).

ב. הוספה ו/או גריעה של מקורות מידע ל/ממערכת SIEM.

ג. הקמת ממשקים למערכות אבטחת מידע משיקות.

2.7 שירותים שוטפים CSOC

להלן דרישות לשירותי CSOC שוטפים באחריות הספק.

מוקד CSOC - על הספק לאייש מוקד בתמהיל מומחים, הכולל בקרי קו ראשון וכן אנליסטים בעלי התמחות והסמכות בתחום אבטחת מידע ובעלי ראיה רוחבית, שביכולתם להציע דרכי טיפול אפקטיביים לאירועים ולסייע למוסדות במיסוד פעילות פרו-אקטיבית בתחום.

באחריות מוקד CSOC לספק את השירותים הבאים:

א. בקרת ניטור אירועים בזמן אמת באמצעות מערכת SIEM ודיווח למוסדות על בסיס חומרת אירוע.

ב. דיווח אירועי אבטחת מידע, יצירת קשר עם גורם רלוונטי במוסד ודיווח תוכן האירוע.

ג. ניהול אירועי אבטחת מידע בהתאם למדיניות המוסד.

ד. שירותי אנליסט בהתאם להגדרות SOW ו- SLA, כחלק מהשירות השוטף. תוצרי עבודת אנליסט עבור מוסד מסוים ישמשו במידת האפשר את כלל המוסדות.

ה. ניתוח ותחקור מלא של אירועי אבטחת מידע בתאימות למשפחת תקני ISO27001 ומסגרת ITIL. דוח ראשוני של התחקיר יוגש תוך 2 ימי עבודה מהתרחשות האירוע.

ו. תחקיר יבוצע על ידי אנליסט בשיתוף מנהל אבטחת מידע מוסדי או מי מטעמו. התחקיר יהיה ברמת המוסד הנוגע לאירוע ורק לו תהיה גישה לתחקיר. התחקיר יחתם על ידי אנליסט מטעם הספק שהיה שותף לתחקיר.

ז. אירועים גלובליים ברמת מספר מוסדות יקבלו תעדוף גבוה וינוהלו מול מחב״א. באחריות מחב״א להעביר פרטים ונתונים רלוונטיים לכלל המוסדות או רק לאלה המעורבים באירוע, על פי החלטתו ובאישור המוסדות המעורבים, לצורך פעילות מונעת והפגת (mitigation) האירוע.

ח. שליחת התראות (SMS/WhatsApp/Mail) לצוות אבטחת מידע מוסדי ולצוות סייבר מחב״א.

ט. העברת המלצות לדרכי תגובה לאירוע.

י. אנליסט שטח - על מנת לבצע תחקיר לאירועים שלא ניתן לבצעם מחצר הספק, על הספק לשלוח אנליסט לחצר המוסד/ות וזאת בתיאום עם מנהלי אבטחת מידע של המוסדות.

יא. קישור למידע מודיעיני מגורמים חיצוניים ובכללם דיווחים והתראות ממטה הסייבר הלאומי וממחב״א.

יב. בדיקת זמינות המערכת ותקינות זרימת האירועים מהמקורות השונים.

יג. אספקת דוחות עיתיים, לרבות דוח מנהלים חודשי ודוח סיכום תחקיר אירועים שבועי.

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.

2.8 שו״שים בשירות CSOC

מעבר לכלול בשירותים השוטפים כמתואר בסעיף 2.7 לעיל, למחב״א תישמר הזכות להזמין שירותים נוספים על בסיס מחירון שירותים ושעות המופיע בפרק התמורה. להלן דוגמאות לשו״שים אפשריים:

א. צוות התערבות לשירות IR (Incident Response) באתר הלקוח. שירות שמטרתו לסייע למוסד במימוש דרכי תגובה לאירוע אבטחת מידע, על בסיס מחיר מומחה ליום עבודה. השירות יוזמן על ידי המוסד בהתאם למחירון בהצעת הספק.

ב. שירותי אנליסט, מעבר לכלול בשירותים השוטפים.

ג. מבחני חדירה/מבדקי חוסן למערכות ויישומים.

ד. סקר אבטחת מידע למערכת.

ה. סקרי סיכונים.

2.9 היקפים עומסים וביצועים

2.9.1 ביצועים

על המערכת לספק ביצועים מתאימים לדרישות אבטחת מידע כדלקמן:

- קצב הכנסת אירועים מהמערכות השונות לבסיס הנתונים של המערכת לא יעלה על 15 שניות, על מנת למנוע איבוד נתונים.
- תצוגת אירוע לא תעלה על 5 שניות מזמן קבלת האירוע בבסיס הנתונים.

2.9.2 היקפים ועומסים

א. על מערכת SIEM מרכזית המסופקת לעמוד בעומס של 90,000 אירועים בממוצע לשנייה (EPS). הנחת יסוד לתכנון הקיבולת היא הצטרפות של 6 מוסדות לשירות במהלך השנה הראשונה להקמת המערכת. במידה ובמסגרת השלמת נספח ז' להסכם יתברר אחרת תבוצע התאמה של הקיבולת לכמות המוסדות בפועל.

ב. ההתאמה תבוצע על בסיס אומדן ממוצע למוסד של כ- 15,000 אירועים בשנייה וכמות של 1,500 flows, עם שיאים של עד 300%. פוטנציאל גידול ל- 25,000 אירועים לשנייה בממוצע למוסד.

ג. **הרחבת המערכת** - תצורת מערכת SIEM תתמוך ברישום וניהול של לפחות 150,000 אירועים בממוצע בשנייה. יכולת זו תתמך ע"י המערכת המסופקת מלכתחילה או באמצעות גידול/שדרוג שיבוצע בשטח ללא צורך בהשבתת המערכת. אם יתברר כי המערכת אינה עומדת בתנאי זה, על הספק יהיה לשדרג או להחליף את המערכת על חשבונו כך שתעמוד בדרישה זו.

ד. עבור חלופת SaaS ההיקפים והעומסים יהיו בהתאם לשימושיות ובשקיפות למזמין.

ה. 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

2.9.3 מעבר משכירות לרישוי קבוע ב SIEM מנוהל

לאור אי הוודאות בקביעת היקף העומסים, רישוי מערכת SIEM ינוהל עפ"י המנגנון הבא:

א. בשנה ראשונה יותקן במערכת רישוי התומך בהיקף המחושב עפ"י מכפלת כמות מוסדות בפועל ב- 15,000 EPS ממוצע. בשנה זו יקלטו המוסדות במערכת, ניטורים יטויבו ושגרת הניטור תתייצב. מחב"א תשלם בשנה זו דמי שכירות חודשיים לרישוי בהתאם לצריכת EPS ממוצעת בפועל.

ב. לאחר שנה ראשונה, תבוצע מדידה רבעונית של EPS ממוצע שתוצאותיה ישמשו בסיס לרישוי קבוע. בהתאם לעלות רישוי קבוע, מחב"א יחליט עפ"י שיקול דעתו אם להמשיך בשכירות רישוי חודשית או לעבור לרישוי קבוע, עפ"י המחירים הכלולים בהצעת הספק.

ג. החלפת רישוי, ככל שתבוצע, תעשה ללא צורך בהתקנה מחדש של המערכת ותוך זמן השבתה מזערי של פעולת איסוף המידע וניתוחו.

2.10 Big Data של מערכת SIEM

מערכת SIEM מוצעת נדרשת לביצועים מקובלים לחיפוש בעולם BIG DATA. נדרש ששאילתה המבוצעת על כ- 150 מיליון אירועים תחזיר נתונים בפרק זמן של עד 5 שניות. המוסד המזמין יהיה רשאי לדרוש תצוגת יכולת המוכיחה ביצועים עפ"י הנדרש בסעיף זה.

2.11 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:

2.12 נהלי עבודה

במהלך הפרויקט יכין הספק נהלים והוראות עבודה פנימיים לתפעול שוטף בשפה העברית ובמבנה נוהל התואם למשפחת תקני ISO27001. כל הנהלים ייכללו במסגרת תיק תפעול, שיכיל את כל ההנחיות הדרושות לתפעול השוטף של המערכת - עדכונים ושדרוגים, מעקב אחר שרתים, טיפול בתקלות, גורמים אליהם יש לפנות במקרה של תקלות וכד'.

להלן פירוט נהלים נדרשים:

א. נוהל תפעול יומי של פונקצית SOC - חיות מערכת, בדיקות בסיסיות, החלפת משמרת וכו.

ב. נוהל מוסדי לניהול אירועי אבט"מ, בהתאם למדיניות המוסד.

ג. נוהל טיפול בתקלה במערכת SIEM, הגדרת שלבים בסיסים לביצוע בעת תקלה.

ד. נוהל טיפול במצב בו סוכן לא מתפקד/אין איסוף מידע מצד Client.

ה. נוהל טיפול במצב בו שרת איסוף אינו מתפקד.

ו. נוהל מעבר לאתר גיבוי טכנולוגי.

ז. נוהל הוספת מקור מידע למערכת.

ח. נוהל הגדרת חוקים במערכת.

ט. נוהל הגדרת דו"ח.

2.13 היבטי אבטחת מידע

מידע קיים ברשתות המזמינה הינו מידע רגיש בהיבט של צנעת הפרט וסודיות עסקית. בהתאם לכך נדרש יישום אבטחת מידע במערכת ומידור מלא של המידע בין המוסדות הכלולים בשירות. למעט מאפיינים חיוניים למניעת/זיהוי/טיפול באירוע אבטחת מידע **לא יועבר מידע בין המוסדות** אלא באישור המוסד שהוא בעל המידע או באמצעות מחב"א.

א. גישת משתמשים למערכת תהיה בפרוטוקולים מאובטחים בלבד (TLS), SAML מול מערכת הזדהות של המוסד ו- OTP מבוסס Google Authenticator/SMS. על הפתרון לתמוך בשתי האפשרויות כאשר כל מוסד יבחר את הפתרון המתאים עבורו.

ב. ניהול הרשאות גישה למערכת ולישויות השונות יהיה על בסיס עיקרון הגישה המינימלית הנדרשת לבצע את המשימה, תוך הקפדה על מידור מלא בין המוסדות.

ג. הזרמת אירועים ממערכות מידע ואבטחת מידע במוסדות תעשה בתווך מאובטח ומוצפן ומכתובות קבועות שיוקצו על ידי המוסדות.

ד. גישת משתמשים למערכת תהיה למורשים בלבד ובאישור המוסד, הן לאנשי מוסדות ומחב"א והן בצד הספק.

ה. העברת מידע לגורמי צד שלישי, ובכללם גורמי אכיפת חוק ו\או גורמי ממשל כדוגמת מערך הסייבר, דורשת אישור מפורש של מחב"א ו\או המוסד טרם ביצוע הפעולה. העברת מידע על פי חוק ובכללו על פי צו בית משפט, תדווח למחב"א, אלא אם קיים צו איסור פרסום המונע את העברת הבקשה למחב"א.

ו. בפתרון SIEM מנוהל:

1. לא תינתן גישה לכל גורם צד שלישי כלשהו למערכת SIEM/SOC שלא באישור מחב"א בכתב, תוך ציון מדויק וברור של צורך ונתונים אליהם יש צורך לגשת, אם לצורך פתרון בעיה במערכת SIEM או לניתוח מידע שעלה מהמערכת.
2. בפתרון מנוהל הכנסת שינויים במערכת SIEM או תשתית SOC הנלווית אליה תעשה על ידי בעלי תפקידים מוגדרים ומורשים על ידי הספק ומחב"א בלבד. כל פעילות שהיא חריגה להקמת מערכת SIEM או תפעולה השוטף תדווח ותקבל את אישור מחב"א טרם ביצוע הפעילות.

ז. בפתרון SIEM בתצורת SaaS:

1. לא תינתן גישה לכל גורם צד שלישי כלשהו למחיצת Tenant של המוסד שלא באישור המוסד בכתב, תוך ציון מדוייק וברור של הצורך והמידע אליו יש לגשת.
2. בפתרון SaaS הכנסת שינויים ברמת Tenant תעשה אך ורק באישור המוסד מראש ובכתב, תוך כדי ציון מדוייק של השינוי, הסיבה לשינוי, השפעתו והסיכונים הכרוכים בביצוע או באי ביצוע השינוי.

2.14 תיעוד המערכת

2.14.1 תכולת תיק תפעול

- הסבר על מערכות ורכיבים
- אפיון ועיצוב הטמעת הפתרון

- אופן התקנת רכיבים וקבצי התקנה על מנת לאפשר שחזור התקנה ללא צורך ברכיבים נוספים
- הגדרות
- נהלי התקנה, תחזוקה, תפעול וטיפול מונע
- פרטי ספקים נותני שירות
- ספרות מלאה על כל רכיבי הציוד והתוכנה
- תהליכים וניהול ידע
- כל חומר עזר נוסף לצורך תחזוקה וטיפול במערכת.

2.14.2 שימושיות ותחזוקה

- תיק התפעול ייבנה ויתוחזק על ידי הספק.
- תיק התפעול יהיה זמין לכלל משתמשי המערכת (בהתאם לסיווגם וצרכיהם) במיקום מרכזי במערכת תומכת לניהול תוכן.
- תיק התפעול והידע שבו הינם רכושו של המזמין.

2.15 הדרכה

הספק יעביר טרום כניסה לייצור 10 ימי הדרכה לצוותי תפעול המערכת במחב״א ובמוסדות. ההדרכה תכלול הצגה בסיסית של המוצר, כיצד לבצע שינויים במערכת, הגדרות אבטחת מידע, תפעול ותחזוקה שוטפים למערכת – גיבויים, שרידות, תפעול מערכת ברמת משתמש, הפקה וניתוח דוחות אירועים, טיפול באירועי אבטחת מידע, טיפול בתקלות, ביצוע בדיקות בסיסיות למערכת וכו'.

ההדרכה תבוצע במתקן מחב״א על Test Tenant שיוקם במערכת SIEM לצורך הדרכות, גרסאות חדשות וקליטת חוקים.

טרום שדרוג גרסה עיקרית (Major) של מערכת SIEM יקויים יום הדרכה עבור משתמשי המערכת.

הדרכות נוספות בתקופת השירות השוטף יבוצעו לפי דרישה וישולמו בנפרד בהתאם לתעריפון.

2.16 בקרת תצורה

הספק יקים סביבת Test שנועדה להדרכות, לקליטת גרסאות חדשות של Connectors וכן לצורך בדיקה מקדימה של חוקים ותרחישים. סביבה זו תהיה נגישה לכלל המוסדות ותנוהל ידי הספק ומחב״א. כמות EPS ומשאבים שסביבת Test תצרוך לא ילקחו בחשבון בעת בדיקת שימושיות בפועל לצורך תשלום בגין רישוי SIEM ושירותי CSOC .

3. רמת שירות

3.0 חלונות שירות

3.0.1 חלון שירות למערכת SIEM ולשירות IaaS

- חלון שירות לפעילות איסוף וניטור של מערכת SIEM בתצורת SaaS הנו 7*24.

- חלון שירות מאוייש לתקלה רגילה בימים א'-ה' 8:00-17:00, ביום ו' 8:00-13:00. במקרה של מענה קולי, חזרה ללקוח תוך 60 דקות לכל היותר. במקרה של מענה קולי, זמן Open של כרטיס תקלה לצורך חישוב SLA הנו מועד השארת ההודעה במענה הקולי.
- חלון שירות לתקלה משביתה ימים א'-ה' 8:00-20:00, יום ו' מ- 8:00 ועד שעה לפני כניסת שבת. במקרה של מענה קולי, חזרה ללקוח תוך 15 דקות לכל היותר. במקרה של מענה קולי, זמן Open של כרטיס תקלה לצורך חישוב SLA הנו מועד השארת ההודעה במענה הקולי.
- חלון שירות לתקלה משביתה רוחבית 7*24 מלבד יום כיפור. במקרה של מענה קולי, חזרה ללקוח תוך 15 דקות לכל היותר. זמן Open לצורך חישוב SLA הנו זמן השיחה הראשונה.

3.0.2 חלון שירות לפעילות ניטור אירועים ב-CSOC

שירות CSOC ייתן מענה 364X7X24 (למעט יום כיפור), כאשר כל מוסד יוכל להזמין חלון זמן ייחודי עבורו לפי הפירוט הבא:

- חלון שירות בשעות עבודה: 09:00–17:00 בימי עבודה ראשון עד חמישי.
- חלון שירות מחוץ לשעות עבודה: 17:00-09:00 בימי עבודה ובסופי שבוע.
- 7X24
- 6X24, ללא שבתות ומועדי ישראל

3.1 רמת שירות

#	שם המדד	שירות	פירוט	תקופת ניתוח	פיצוי מוסכם
.1	משך טיפול בתקלה	SIEM	תקלות לפי סיווג: משביתה רוחבית, משביתה, רגילה	רבעון	עבור KPI משך חזרה לשירות בתלות בסיווג התקלה
.2	כיסוי מקורות המידע	SIEM	כל ההתאמות הנדרשות באמצעי האיסוף	חצי שנה	לכל שבירת SLA
.3	זמינות שירותים	SaaS IaaS CSOC	שיעור זמן בחלון שירות בו התשתיות זמינות למתן שירות	חצי שנה	
.4	תחקיר אירוע	CSOC	משך זמן להגשת דוחות	חצי שנה	
.5	תחקיר אירוע	CSOC	לקונה מהותית של פונקציית CSOC	חצי שנה	שבוע עבודה של אנליסט

א. פיצוי מוסכם בגין אי עמידה ברמת שירות יחושב על יחידות שלמות של חריגה.

ב. חישוב פיצוי מוסכם יבוצע בהתאם לעומק אי העמידה ולפי כמות יחידות חריגה.

3.1.1 משך טיפול בתקלה

#	תקלה	מענה ראשוני בתוך/ תחילת טיפול	אבחון מ Open	חזרה לשירות מ Open	יחידת חריגה	עלות ליחידת חריגה (₪)
1	משביתה רוחבית – משביתה לפחות 4 מקורות מידע או לפחות 3 מוסדות	30 דקות	שעתיים	6 שעות	שעתיים	5,000

2	משביתה	1 שעה	Next Day	1 י״ע	4 שעות	2,500
3	רגילה	Next Day		2 י״ע	1 י״ע	1,000

א. משך מדידה עבור מענה ראשוני מזמן פתיחת תקלה (Open) ועד מעבר לסטאטוס בטיפול.

ב. משך מדידה עבור אבחון מזמן פתיחת תקלה ועד אספקת מידע ללקוח הכולל אבחון ראשוני ופירוט לגבי המשך טיפול.

ג. משך מדידה עבור חזרה לשירות מזמן פתיחת תקלה ועד סטאטוס Resolved.

ד. רמת שירות נדרשת 95% מכלל האוכלוסייה.

ה. פיצוי מוסכם בגין אי עמידה ברמת השירות יחושב בגין יחידות שלמות של חריגה.

ו. דוגמא:

- במשך רבעון ארעו 10 תקלות משביתות. 8 מהם נפתרו במסגרת משך זמן של יום עבודה.
- רמת שירות בפועל עבור KPI תקלה משביתה הנה 80%, ולכן יש שבירת SLA.
- יש 2 אירועים בגינם יש אי עמידה ב– SLA, משך יום עבודה עבור תקלה משביתה על פי חלון שירות נדרש הנו 12 שעות. משכי חזרה לשירות במסגרת חלון שירות שנמדד עבור תקלות אלו הנם 18 ו- 23 שעות.
- תקלה שמשך פתרונה עמד על 18 שעות, חרגה ביחידת חריגה בודדת ולכן מושת עליה פיצוי מוסכם של 2,500 ₪.
- תקלה שמשך פתרונה עמד על 23 שעות, חרגה ב– 2 יחידות חריגה ולכן מושת עליה פיצוי מוסכם של 5,000 ₪.
- סך הכל פיצוי מוסכם לרבעון בגין אי עמידה ברמת שירות עבור מדד משך טיפול בתקלה 7,500 ₪.

3.1.2 כיסוי מקורות מידע

#	אמצעי איסוף עבור מקור המידע	התאמה נדרשת בימי עבודה	יחידת חריגה בימי עבודה	עלות ליחידת חריגה ב ₪	
.1	קיים ופותח על ידי הספק	5	2	2,000	
.2	קיים וההתאמה כלולה בוונילה של מערכת ה - SIEM	1	1	2,000	
.3	קיים וההתאמה לא כלולה בוונילה של מערכת ה - SIEM	10	3	2,000	
.4	חדש אשר כלול בוונילה של מערכת - SIEM	3	1	2,000	
.5	חדש ולא כלול בוונילה של מערכת ה- SIEM	20	3	2,000	

א. ספירת ימי עבודה מקבלת הבקשה והמידע הנדרש לביצוע ההתאמה.

ב. רמת שירות נדרשת הנה עבור 100% מהאוכלוסייה.

ג. דוגמא:

- במשך חצי השנה התווספו 5 מקורות מידע אשר לא היו כלולות בוונילה של מערכת ה-SIEM.

- עבור 2 מקורות מידע זמן ההתאמה נמשך למעלה מ-20 ימים, לכן יש אי עמידה ברמת שירות ואירוע של פיצוי מוסכם.
- מקור מידע אחד הותאם במשך של 22 ימי עבודה, אי עמידה ביעד בחריגה של 2 י״ע, החריגה קטנה מיחידת חריגה ולכן בעבורות אין פיצוי מוסכם.
- מקור מידע שני הותאם תוך 30 ימי עבודה, חריגה של 10 י״ע המהווים 3 יחידות חריגה שלמות, ולכן גובה הפיצוי המוסכם בגין אי עמידה במדד כיסוי מקורות מידע הנו 6,000 ₪.

3.1.3 זמינות שירותים

#	שירות	רמת שירות	יחידת חריגה בדקות	עלות ליחידת חריגה ב ₪
.1	SIEM - SaaS	99.9%	30	5,000
.2	IaaS ל SIEM מנוהל	99.9%	30	5,000
.3	CSOC	99%	30	5,000

א. זמינות שירות עבור CSOC תמדד באחוזים במסגרת חלון השירות של שירות הנמדד.

ב. זמינות שירות עבור SIEM תמדד באחוזים במסגרת של 7*24.

ג. חלון שירות 7*24 לשירות SIEM, בחצי שנה יש כ 4368 שעות שירות, עבור זמינות של 99.9% זמן השבתה מותר הנו כ- 4.4 שעות שהם 280 דקות. הפסקות שירות של עד 10 דקות לא יכללו בצבירה הכוללת ובתנאי שמשך הפער ביניהם יהיה גדול מ 24 שעות.

ד. דוגמא - במשך תקופת מדידה סה״כ זמן השבתת שירות עבור שירות SIEM בתצורת SaaS הצטבר ל- 6 שעות (360 דקות). הפער בין זמן השבתה מותר לאי זמינות בפועל הנו 80 דקות, גדול מיחידת חריגה ולכן יש אירוע פיצוי מוסכם. החריגה היא של 2 יחידות שלמות של יחידות חריגה ולכן סכום הפיצוי עומד על 10,000 ₪.

3.1.4 תחקירי אירוע

#	נושא	רמת שירות	יחידת חריגה בימי עבודה	עלות ליחידת חריגה ב ₪
.1	דוח ראשוני	95%	1	1,000
.2	דוח סיכום	95%	2	1,000
.3	לקונה	100%		

א. לאירוע אבטחת מידע יקוים תחקיר, כאשר דוח ראשוני שלו יוגש ללקוח בתוך 48 שעות.

ב. לאחר הגשת דוח ראשוני יקבע במשותף תאריך יעד להגשת דוח סיכום.

ג. אם בתחקיר יתברר באופן חד משמעי שאירוע אבטחת מידע נגרם בשל לקונה של פונקצית CSOC או שנגרם למי מהמוסדות נזק כתוצאה ישירה של חוסר תפקוד או לקונה של CSOC, אזי במקרה זה יהיה המוסד/ות הנפגע/ים זכאי/ם לשירות אנליסט של פונקצית CSOC בהיקף של שבוע עבודה, מעבר לשירות השוטף

3.2 מערכת מדידת ובקרת רמת השירות

א. הספק נדרש להקים מערכת מדידה ובקרת רמת השירות על מנת תמוך בדרישות בסעיפים 3.1. לעיל. ו- 4.3.4.

ב. מערכת בקרת השירות תכלול DashBoard ברמת עדכניות של 24 שעות לסטאטוס מדדי השירות, ניתן יהיה לבצע Drill Down לרמת ה- KPI הבודד ולהחזר את האירועים אשר בגינם יש סיכון לשבירת SLA.

ג. לו"ז להקמת מערכת רמת השירות מפורט בסעיף שלבי הקמת המערכת 4.2.1.

ד. תחילת עבודה עם המערכת החל ברבעון ראשון של סבב הקמה ראשוני של 2 מוסדות, במסגרת רבעון זה תבוצע מדידה ראשונית, המערכת תותאם ותיוצב, כאשר מנגנוני הפיצוי המוסכם לא יופעלו בפועל.

ה. החל מרבעון שני לתחילת השירות מערכת המדידה תופעל באופן מלא כולל מנגנון הפיצוי המוסכם בגין אי עמידה ברמת השירות.

ו. לצורכי בקרה ואכיפת רמת השירות יוגש ללקוח דוח חודשי של מדדי רמת השירות, כאשר ניתוח המדדים מהיבט עמידה/אי עמידה ברמת השירות והפעלת פיצוי מוסכם יבוצע בהתאם לתקופת ניתוח של כל מדד.

4. מימוש והקמה

4.0 כללי

העבודה על מערכת SIEM וקישורי מקורות מידע למערכת מרכזית תבוצע באתרי המוסדות ובאתר המזמין בשיתוף אנשי המוסד. הספק יידרש להגיע לכל אחד מאתרי המוסד הרלוונטיים. האחריות המלאה ללוגיסטיקה, אמצעי תקשורת, אמצעי תחבורה ותובלה וארגון העבודה יהיו של הספק.

4.1 תפקידי מפתח

4.1.1 מנהל פרויקט הקמה

א. **אחריות**

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

ב. **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.

ג. **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	

4.1.2 מנהל שירות CSOC

א. **אחריות -** ניהול מרכז שירות **CSOC**.

ב. **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.

ג. **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	

4.1.3 אנליסט

א. אחריות –אנליסט עבור מחב"א והמוסדות.

ב. **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.

ג. **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	

4.1.4 בקרי CSOC

א. 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.

ב. **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.

ג. **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
.1				
.2				
.3				
.4				
.5				

4.1.5 ארכיטקט

א. **אחריות – ארכיטקט מערכת SIEM.**

ב. **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.

ג. **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	

4.1.6 מיישם SIEM

א. **אחריות** – מיישם מערכת SIEM.

ב. **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.

ג. **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	

4.2 הקמת מערכת SIEM

א. הנחת היסוד היא שבשנה הראשונה למתן השירות יצטרפו למערכת 6 מוסדות.

ב. יש לתכנן קליטת המוסדות לשירות ב- 3 סבבים של 2 מוסדות בכל סבב. מועד תחילת הסבבים הסבבים יהיו בהפרשים של כ- 3 חודשים ולכן תיווצר מקביליות בין הסבבים.

במידה ויתברר במסגרת השלמת נספח ז' לחוזה שמספר המוסדות אשר יכללו בשירות יהיה שונה תבוצע התאמה מבוססת על דרישות המוסדות, ובתנאי שכל סבב לא יכיל יותר מ- 2 מוסדות ללא הסכמת הספק.

ג. טבלה בסעיף 4.2.1 מתייחסת הן לפתרון על בסיס SIEM מנוהל והן פתרון על בסיס SIEM בתצורת SaaS. למעט ההתאמות הבאות שאינן כלולות בחלופת ה SaaS:

- אין צורך באספקת תשתית, הספק נדרש לתכנן קיבולת לכל Tenant ולהקצות בהתאם לכך משאבים. התקנה מתוחמת רק לשרתי ביניים ושרתי איסוף בחצרי המזמין.
- אין צורך בהתקנת תשתית ומערכת SIEM מרכזית.

4.2.1 פרויקט הקמה – שלבים ולו"ז

שלב	תיאור	פעילויות ותוצרים עיקריים	אישור	מועד סיום בחודשים	הערות
.1	אפיון ארכיטקטורת המוצר וממשקי משתמש וכתבי כמויות על פי דרישת מחב"א ואופן התחברות המוסדות	פגישות לימוד ארכיטקטורה קיימת ודרישות לקוח		ARO + 2	ARO – מועד חתימה בפועל
		תוכנית עבודה לפרויקט ההקמה ברמה רוחבית	מחב"א		בתום שלב זה כל המשאבים הנדרשים להקמת המערכת יהיו זמינים
		עיצוב ארכיטקטוני למערכת לפי חלופת ה- SIEM שנבחרה	מחבא+מוסד		
		אספקת תשתיות המערכת	מחב"א		
		LLD למערכות והשירותים הכלולים בשירות	מחבא+מוסד		
		לימוד מקורות מידע ואפליקציות המצוינות בנספח 2.3.8			
.2	הקמת תשתית, התקנת המוצר בקונפיגורציה בסיסית והתאמתו לדרישות המזמין	הקמת תשתית מערכת SIEM	מחב"א	ARO+ 4	בתום שלב זה המערכת תהיה מוכנה ברמה הרוחבית וניתן יהיה להתחיל לבצע את פרויקטי הצטרפות המוסדות לשירות
		התקנת מערכת SIEM	מחב"א		
		התאמות רוחביות במערכת ה-SIEM בהתאם ל- LLD	מחב"א		
		הקמת Tenant Test וחיבורו למקורות מידע	מחב"א + מוסד		
		קישור המערכת למרכז CSOC בתאימות לסעיף 4.4	מחב"א		
		בדיקות מסירה כולל בדיקת עומסים	ארכיטקט מערכת SIEM ומנהל שירות CSOC		
		סבב בדיקות קבלה	מחבא+ מוסד		
		הדרכה + תיעוד	מחב"א + מוסד		
.3	הקמת Tenant סבב ראשון: 2 מוסדות. תהליך לכל מקור מידע: עיצוב תצורת קישור מקור מידע למערכת מרכזית, קישור טכנולוגי של מקור מידע, בניית פרסר/ממשק למקור מידע (אם לא קיים),	תוכנית עבודה עבור הסבב	מוסד	ARO + 8	קישור מקורות מידע תשתיתיים, יישומיים ותקשורתיים בהתאם לסדר עדיפות מוסד, כולל בניית חוקים ודוחות מתאימים
		LLD	מוסד		
		הקמת ה- Tenant לכל מוסד, התקנת Collector וחיבור מקורות מידע ברמת וונילה	מוסד		
		הוספת מקורות מידע, התאמת ניטורים, הטמעת Rules, תרחישים וקורלציות	מוסד		

	הגדרת Rules רלוונטיים, בחינת ישימות החוקים	אתראות בדיקת ישימות Rules ואתראות כולל מול מערך CSOC	מוסד		
		מבחני מסירה מערכת SIEM ל מוסדות סבב ראשון כולל בדיקת עומסים	ארכיטקט SIEM, מנהל שירות CSOC.		
		מבחני קבלה מערכת SIEM למוסדות סבב ראשון	מוסד		
		הכנת הוראות עבודה, התאמת תהליכים והדרכת CSOC	מוסד		הקמת מערכת ניהול אירועים ברמה מוסדית, חיבור מערכי התראות, מסרים והסלמה של CSOC, כולל נוהל תגובת אירוע
		הדרכות למערכת SIEM ולתהליכי עבודה עם CSOC ומסירת תיעוד מערכת.	מוסד		בתום שלב זה יתחיל השירות עבור מערכות SIEM ו- CSOC
		כניסה לפעילות מבצעית של פונקצית CSOC	מוסד		
		תקופת הרצה – כוונון המערכת וטיפול צמוד בבעיות.	מוסד		תקופה זו תסתיים לאחר ריצה של חודש ימים ללא תקלה משביתה במערכת
4.	הקמת Tenant סבב שני : 2 מוסדות נוספים	כמו בסבב ראשון	כמו בסבב ראשון	ARO + 11	כמו בסבב ראשון
5.	הקמת Tenant סבב אחרון : 2 מוסדות נוספים	כמו בסבב ראשון	כמו בסבב ראשון	ARO + 13	כמו בסבב ראשון
6.	הקמת מערכת רמת ובקרת השירות	LLD לכלל המערכת	מחב"א + מוסד	ARO + 3	בתום שלב זה תופעל מערכת רמת ובקרת השירות על כל מרכיביה
		יישום המערכת במסגרת מערכת ניהול הקריאות והמערכות המודדות (תפעולי)	מחב"א + מוסד	ARO + 5	
		בדיקות מסירה וקבלה למרכיבי המערכת הממומשים במערכת ניהול קריאות	מחב"א + מוסד	ARO + 6	
		יישום מערכת מרכזית ברמת ניתוח המדד, החלטה לגבי עמידה/אי עמידה וחישוב פיצוי מוסכם	מחב"א + מוסד	ARO + 7	
		בדיקות מסירה וקבלה למרכיבי המערכת הממומשים במערכת ניהול קריאות	מחב"א + מוסד	ARO + 8	
		הרצה לרבעון ראשון ללא הפעלת פיצוי מוסכם	מחב"א + מוסד	ARO + 11	
7.	סיום הטמעה	בחינת אירועים חוצי מוסד	מוסד + מחב"א	ARO + 15	נועד עבור תיקוף ארכיטקטורה וקיבולת של המערכת
		בדיקות עומסים			
		בחינת קיבולת			
8.	מדידת EPS לרישוי קבוע	בהתאם לסעיף 2.9.3	מחב"א	ARO +18	

- כל דחייה מעבר לזמן זה דורשת אישור בכתב של מנהל אבטחת מידע של המוסד ומנהל הפרויקט מטעם המזמין.
- צפוי שבמהלך הפרויקט יתווספו מקורות מידע חדשים. הצדדים ידנו ביניהם בהשלכות של תוספת המקורות על לוח הזמנים והעלות. החלטה אם לכלול את המקורות החדשים כבר ביישום המקורי או לדחותן למימוש מתום היישום נתונה למוסד.
- על מערכות המחשוב במוסד המזמין להיות זמינות 24 שעות, 7 ימים בשבוע. התקנת והטמעת המערכת לא תפגע בעבודה שוטפת של המוסד אל מול מערכות פנימיות. אם תידרש הפרעה או השבתת פעילות של אחת המערכות, הרי שהיא תהא מינימלית ותתוזמן מראש, בכדי לתת לספק חלון זמן מתאים לביצוע הפעילות.

4.2.2 ניהול הפרויקט

א. מיידית עם הזכייה ימנה הספק מנהל פרויקט לתחילת עבודה מיידית.

ב. ניהול סיכונים - מנהל הפרויקט ינהל סיכונים לאורך כל שלבי הפרויקט. ישיבות ניהול הסיכונים יבוצעו במסגרת סטאטוס ניהול הפרויקט לפחות אחת לשבועיים.

ג. במהלך ההטמעה יתקיימו פגישות טכניות תקופתיות לעדכון סטטוס שלבים שבוצעו ושלבים הבאים וכן לפתרון בעיות.

ד. 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 :

ה. התקנות ברשת מוסד/מחב"א דורשות תיאום מראש עם כלל הגורמים הרלוונטיים, התקנה שלא תתואם מראש תידחה עד לסיום התיאום.

ו. התקנות על מערכות ייצור יתבצעו אך ורק לאחר קבלת אישור מנהל תשתיות של המוסד ועל הספק להיערך לכך בהתאם. על הספק ללמוד את אילוצי המוסדות השונים לפני בנית תכנית עבודה מפורטת.

ז. לפני כל התקנה תתקיים פגישה עם מנהל התשתיות של המוסד או מי שימונה על ידו למשימה, במטרה להבהיר את משמעות ההתקנה, כיצד היא עלולה להשפיע על תהליכי עבודה או על פעילותן של מערכות מחשוב של המוסד, הסבר על התקנות, סיכונים, דרכים ונהלים לטיפול בבעיות אפשריות וכו'.

ח. בשלב הטמעה יקבעו ישיבות דו שבועיות של הספק ונציגיו עם נציגי המזמין להפקת לקחים. הספק מחויב להיות נוכח בישיבות אלה וכן לקחת בהן חלק פעיל. לאחר מעבר לשגרה יקבעו פגישות אלה בהתאם לצורך (לפחות אחת לרבעון).

ט. באחריות הספק לבצע בדיקות מסירה של המערכת לפני ביצוע בדיקות קבלה של המזמין. בדיקות שיתבצעו ע"י הספק יכללו: בדיקות תפעוליות לכלל עבודת המערכת, בדיקות חוקים שהוגדרו, בדיקות ביצועים ועומסים.

י. אישור המערכת על ידי המזמין מותנה בעמידה בבדיקות קבלה שיבוצעו על ידו ושיכללו: בדיקות תפעוליות, בדיקות הגדרה במערכת, בדיקות ביצועים ועומסים והקשחת מערכת

4.2.3 תכניות עבודה לפרויקט הקמה

א. תכניות העבודה תבנה בהתאם לשלבי הפרויקט המתוארים בסעיף 4.2.1.

ב. תכנית עבודה תכיל גאנט עבור כל השלבים המוצעים.

ג. על הספק להפריד בתכנית העבודה בין פעילויות שבאחריותו לבין פעילויות שידרשו מהמזמין (כדוגמת פעולות הכנה וכו')

ד. הפעילויות להלן מפורטות כבסיס לתכנית. הספק נדרש להתייחס אליהן ולכלול אותן בתכנית שתוצע על ידו, כך שלו"ז סיום שלבים יהיה בהתאמה.

ה. מועד סיום בחודשים המופיעים בטבלה לעיל הנו מקסימלי. הספק הזוכה, בעת הכנת תוכנית העבודה, רשאי להציע משך קצר יותר. ניתן להציע משך לפי סבבים.

4.3 מנגנוני ניהול ובקרה

4.3.1 איכות ובקרה

המוסד או מחב"א רשאים לבצע בקרה שוטפת של העבודה שתבוצע ע"י הספק ולדרוש כל מידע רלוונטי. הספק מחויב לתקן תקלות שיעלו בבקרה. הספק ימסור דוח התקדמות מפורט אחת לשבועיים בשלב ההקמה וכן תתקיים פגישת עבודה בינו לבין מנהלת הפרויקט, בה ילובנו בעיות, ידונו מהלכים שבוצעו ויתואמו מהלכים עתידיים. לדוחות התקדמות יצורפו תרשימי גאנט מפורטים שישקפו סטאטוס עדכני של הפרויקט ביחס לתכנון.

4.3.2 ועדת היגוי עליונה

עם תחילת הפרויקט תוקם ועדת היגוי עליונה בראשות מנכ"ל מחב"א ובהשתתפות נציגים בכירים של המוסדות, מנכ"ל הספק ונציגים נוספים לפי צורך.

ועדת היגוי עליונה תתכנס אחת לחצי שנה ובנוסף לפי צורך, ותפקידיה העיקריים יהיו.

- בקרה תקופתית על עמידה ביעדי המערכת.
- ניהול סיכוני על למערכת.
- אישור תקציב ושינויים מהותיים בהיקפי התקשרות וכן החלטה על הארכת שירות או היפרדות
- כתובת להסלמה למקרה של אי הסכמה ברמת ועדת היגוי תפעולית.

4.3.3 ועדת היגוי תפעולית

עם תחילת הפרויקט תוקם ועדת היגוי תפעולית בראשות נציג מחב"א ובהשתתפות נציגי המוסדות, סמנכ"ל הספק, מנהל הפרויקט מטעם הספק, מנהל פונקצית CSOC ומנהל שירות SIEM מטעם הספק, ונציגים נוספים לפי הצורך.

ועדת היגוי תפעולית תתכנס אחת לשבועיים בתקופת פרויקט ההקמה ואחת לחודש בשוטף, ותפקידיה העיקריים יהיו:

- אישור תכנית עבודה,
- מעקב החלטות מול ביצוע
- מעקב שוטף על שלבי פרויקט ההקמה וכן על הפעילות השוטפת

- הקצאת ובקרת משאבים: הוספה וגריעה של מקורות מידע, בנק חוקים ותרחישים, משאבי אנוש,
- בקרת עמידה ב- SLA
- ניהול סיכונים.
- כתובת להסלמה למקרה של אי הסכמה בין צוותי הפרויקט.

4.3.4 ניהול שוטף

לאחר מעבר לייצור והפעלת המערכת יוגדרו מול מחב"א 2 פונקציות ניהוליות מטעם הספק:

- מנהל CSOC עבור כלל שירותי CSOC. המנהל ישמש כ- SPOC לשירות CSOC מול אחראי אבטחת מידע במוסד ומול מחב"א.
- מנהל מערכת SIEM עבור כלל שירותי SIEM. המנהל ישמש כ- SPOC לשירותי SIEM מול מנהל שירות SIEM במחב"א ומול ממונה SIEM במוסד.

☜ *אפשר שהפונקציות יאוישו על ידי אותו אדם.*

הספק יתנהל בשקיפות מול מחב"א והמוסדות. לצורך כך יעמיד הספק לשימוש מרחוק של מחב"א ונציגי המוסדות פורטל לניהול השירות שיכלול את הפונקציונאליות הבאה:

א. תצוגת מדדי שירות הכלולים בסעיף 3.1 ברמת שעונים עם יכולת ל Drill Down לכל מדד. ניתן יהיה לצפות בתצוגה בחתך Tenant או בחתך כלל המוסדות, לפי הרשאה ולפי הרשאה.

ב. דוחות שימושיות בשירותים ברמת Tenant וכלל מערכת SIEM לפי המרכיבים הבאים: צריכת EPS, שימושיות של פרסרים/מקורות מידע, שימושיות ב- Rules/תרחישים, שו"שים - ביצוע מול הזמנות.

ג. דוחות שימושיות בשירות CSOC – דוח ממצאי CSOC כולל המלצות וסטאטוס ביצוע, דוח זמינות פונקצית CSOC, תחקירים בביצוע וארכיון, יתרת פעילות הכלולה במסגרת התמורה השוטפת, שו"שים - ביצוע מול הזמנות.

ד. דוחות לחישוב פיצוי מוסכם על בסיס כללי, מוסדי, מדד ותקופה.

ה. יכולת הפקה עצמית של דוחות ממערכת ניהול שירות על בסיס תקלות/בקשות שירות לפי חתכים של סוגי תקלות/בקשות, זמנים, אוכלוסייה, סטאטוסים וכיו"ב.

4.4 הכשרת פונקציית CSOC

על הספק לבצע את הפעילויות הבאות, טרום תחילת אספקת שירותי CSOC:

א. קבלת מידע והדרכה מטעם המוסד להכרת עקרונות מדיניות אבטחת המידע המוסדי, שגרת פעילות, ארכיטקטורה של מערכות אבטחת המידע במוסד, מערכות מידע עיקריות וסיכונים עיקריים ברמה המוסדית. הדרכה זו תהיה בהיקף של לפחות חצי יום למוסד וחובת השתתפות תחול על כל נותני השירותים מטעם הספק.

ב. הכנת הוראת עבודה פנימית לנוהל תגובת אירוע מוסדי במסגרת פעילות CSOC. הוראת העבודה תהיה ברמת כל מוסד ותאושר על ידי ממונה אבטחת מידע של המוסד.

ג. הגדרת תפקידים ואחריות ואיוש בתיאום עם המוסד.

ד. איסוף ותיעוד כל מידע נדרש למתן שירות CSOC בשוטף (כגון טלפונים ואמצעי תקשורת לאנשי מפתח, זמנים מיוחדים, Known Problems).

ה. פתיחת חשבונות וקבלת הרשאות תפעוליות ברמת Tenant במערכת SIEM מרכזית.

4.5 היפרדות

4.5.1 כללי

א. מחב"א ו/או מוסד רשאים להיפרד מהשירות מכל סיבה שהיא באופן מלא או חלקי: משירות CSOC בלבד או משירות SIEM באופן חלקי או מלא בכל אחת מתצורות IaaS, SaaS או תשתית.

ב. מחב"א רשאי להיפרד משירות CSOC ולהמשיך לצרוך שירותי SIEM ולהיפך - להיפרד משירותי SIEM ולהמשיך לצרוך שירות CSOC.

ג. כל מוסד רשאי להיפרד ברמת Tenant שלו מכלל השירות, משירות CSOC בלבד או משירות SIEM בלבד.

ד. היפרדות חלקית משירות ברמת מחב"א או מוסד לא תשנה את רמת השירות שלה מחויב הספק או את אופן חישוב עלות השירותים שנותרו. כלומר, מחירוני הספק המשמשים לקביעת עלות השירותים לא ישתנו בעקבות היפרדות כלשהיא.

ה. למען הסר ספק, היפרדות אינה כרוכה בתשלום נוסף כלשהו מצד המזמין, למעט צריכת שירות של Read Only עבור Data היסטורית בתצורת SaaS.

4.5.2 היפרדות מחב"א משירות SIEM מנוהל

א. על היפרדות מטעמי נוחות מחב"א יודיע לספק לפחות שלושה חודשים מראש.

ב. ניתן יהיה להסב את חוזה תחזוקת יצרן למזמין או לספק חלופי אחר.

ג. כל התאמות ופיתוחים שבוצעו במערכת SIEM יועברו לרשות המזמין, כולל קוד עבור Parsers יעודיים, ככל שפותחו.

ד. הספק יעביר ידע ככל שיידרש לנציגי המזמין בכל היבטי מערכת SIEM.

ה. חשבונות יעודיים של ספק מערכת SIEM יוקפאו או יועברו לנציגי המזמין.

ו. ספק SIEM ישלים משימות שו"שים שהיו בביצוע ברמת חוקים/תרחישים/עדכון והוספת Connectors, אלא אם המזמין יחליט להפסיקן ולהעביר את המשימה לספק אחר. במקרה כזה הספק נדרש לשתף פעולה ולחפוף את הספק חדש בהשלמת המשימה.

4.5.3 היפרדות מוסד משירות SIEM מנוהל

א. כל התאמות ופיתוחים ברמת Tenant יועמדו לרשות ושימוש המוסד, ככל שיחליט לישם אותם במערכת SIEM חדשה. היישום יהיה באחריות המוסד בלבד.

ב. המוסד יהיה רשאי לקבל את חלקו היחסי ברישוי SIEM, במקרה של תצורה מקומית בבעלות מחב"א. משמעות הדבר היא שספק SIEM ידרש לפצל את הרישוי בין מחב"א למוסד. אם המערכת מותקנת עם רישוי קבוע הרי שיש לבטל רישוי קיים ולהנפיק 2 רישיונות חדשים.

ג. Tenant של מוסד יעבור לתצורת Read Only ויעמוד לרשות המוסד לתקופה של חצי שנה לצורך אחזור מידע היסטורי.

4.5.4 היפרדות משירות SaaS

א. הספק יעביר לכל מוסד מידע האגור במערכת והמשוייך למוסד, כך שיהיה מוסכם על המוסד, ברמה של מבנה קבצי נתונים (למשל פורמט מערכת גיבוי קיימת במוסד) ואופן העברה (למשל העתקה של Disk 2 Disk) ומועדים.

ב. הספק יעביר לכל מוסד כל Meta Data רלוונטית ששרתה את המוסד ברמת Tenant, לרבות ולא רק: חוקים, תסריטים, תחקירים ושגרות שירות, כך שאם המוסד יבחר להמשיך לעבוד עם אותו מוצר SIEM הרי שניתן יהיה לבצע Import למידע ולשמר את ההשקעה.

ג. הספק יאפשר לכל מוסד אופציה לשמירת מידע למשך של עד 6 חודשים ממועד ההיפרדות, ברמה של Read Only לצורך אחזור וניוד הדרגתי של המידע.

ד. עם סיום השימוש במערכת (כולל תקופת אופציה של Read Only) ימחק הספק את נתוני המוסד ממערכת SIEM (Online וארכיון), כך שלא ניתן יהיה לשחזר אותם בשום צורה.

ה. במקביל לנתונים אגורים במערכת SIEM, הספק יימחק כל נתוני מוסד המצויים במערכותיו לרבות ולא רק: מערכות ניהול שירות (ניהול קריאות, מערכת מדידה, פורטל שירות), מערכות BI ו Big Data וכיו"ב.

ו. הודעת היפרדות מטעמי נוחות תינתן לספק לפחות 90 יום מראש ובכתב.

ז. הודעת היפרדות עקב אי עמידת הספק בהסכם תינתן לספק מראש ובכתב. המזמין יקבע את מועד הפסקת השירות בפועל, שאפשר שיקבע באופן מיידי, הכול בהתאם לשיקולי המוסד.

4.5.5 היפרדות משירות IaaS

א. ספק שירותי SIEM נדרש לנייד את מערכת SIEM מתשתית בשירות IaaS לתשתית חלופית.

ב. פרויקט ניוד לתשתית IaaS חדשה או לתשתית מחב"א יבוצע באחריות מלאה של ספק SIEM.

ג. ניוד מערכת SIEM מתשתית IaaS לתשתית חלופית לא תהיה כרוכה בתוספת תשלום בגין רישוי, כלומר ניתן יהיה לנייד רישוי קיים או לקבל מהיצרן רישוי חדש בהיקף דומה, ללא תוספת עלות.

ד. אחת ל- 5 שנות התקשרות לשירותי SIEM, רשאית מחב"א לדרוש מהספק במסגרת התמורה השוטפת לנייד את מערכת SIEM לתשתית חלופית (IaaS אחר או On Premise).

ה. התנתקות משירות IaaS ומעבר לתשתית חלופית תבוצע לאחר מבחני קבלה מטעם מחב"א וספק שירותי CSOC ובדיקת עומסים מטעם מחב"א.

ו. התנתקות משירות IaaS לא תשפיע על שירותי SIEM ו CSOC של הספק.

ז. לאחר היפרדות משירות IaaS באמצעות הספק, האחריות לאספקה תקינה ושוטפת של תשתית מערכת SIEM תהא על מחב"א. למען הסר ספק, תשתית זו כוללת: מערכת הפעלה בהתאם לדרישת יצרן מערכת SIEM, תצורה בסיסית בהתאם להיקפים שנמדדו בעת היפרדות והתאמות נדרשות כתוצאה מגידול/קיטון בפעילות, בסיס נתונים כפי שנדרש ע"י יצרן מערכת SIEM, מערך אחסון תואם לנפחים, לדרישות ביצועים ויתירות המערכת.

ח. מיד עם היפרדות משירות זה יבוטל מדד זמינות IaaS מול הספק.

ט. מעבר לתשתית חדשה יבוצע כך שיידרשו מינימום שינויים במערכת ובהגדרות סביבה ואבטחת מידע. לדוגמא: כתובת IP ושם DNS של שרתי מערכת יישמרו, לא יעלה צורך בשינוי/עדכון חוקי FW וכו'.

4.5.6 היפרדות מחב"א משירות CSOC

א. על היפרדות הנובעת מטעמי נוחות תינתן הודעה לספק לפחות 90 ימים מראש.

ב. הספק ינתק קשר VPN בינו לבין מערכת SIEM של מחב"א.

ג. הספק ימחק ממערכותיו כל מידע הנוגע למחב"א והמוסדות בהתאם להנחיה שיקבל.

ד. הספק יבצע חפיפה עם נציג מחב"א ונציג של כל מוסד לצורך רציפות פונקצית SOC ברמת המוסדות בפרט וכן ברמת מחב"א.

5. עלות

5.0 כללי

5.0.1 מרכיבי תמורה

סעיף	סעיף משנה	מרכיב תמורה
5.1		**SIEM בחלופת SaaS**
	5.1.1	הקמת SIEM בחלופת SaaS
	5.1.2	שירות שוטף SIEM בחלופת SaaS
	5.1.3	שו"שים SIEM בחלופת SaaS
5.2		**SIEM בחלופה מנוהלת**
	5.2.1	רכש מערכת SIEM בחלופה מנוהלת
	5.2.2	רכש תשתית SIEM בחלופה מנוהלת
	5.2.3	הקמת מערכת SIEM בחלופה מנוהלת
	5.2.4	שירות שוטף ושו"שים SIEM בחלופה מנוהלת
5.3		**שירותי CSOC**
	5.3.1	שירותי CSOC שוטפים
	5.3.2	שו"שים בשירותי CSOC

בנוגע לחלופות SIEM, המציע נדרש להציע אחת מהאפשרויות הבאות:

1. SIEM בחלופת SaaS – המציע ימלא את כל סעיפי 5.1
2. SIEM בחלופה מנוהלת – המציע ימלא את כל סעיפי 5.2
3. הצעה בגין שתי החלופות לעיל – המציע ימלא את כל סעיפי 5.1 ו- 5.2

5.0.2 הצמדה למחירון יצרן מוצר/ספק שירות

מוצרים או שירותים מסוימים הנקובים בדולר יהיו צמודים אחת לשנה למחירון יצרן מוצר/ספק שירות, ובהתאם לשיעור הנחה הנקוב בהצעה. מדובר ב:

1. שירותי SIEM בחלופת SaaS
2. רישוי SIEM במערכת מנוהלת
3. מערכת מנוהלת בתצורת IaaS

עבור כל מוצר או שירות יש לציין את שיעור ההנחה של הרכיב ממחירון עדכני של היצרן/ספק. יש לציין את סוג ושם כל מחירון עליו מתבססת ההצעה וכן לינק למחירון באינטרנט, ככל שקיים.

הצמדה תבוצע בפעם הראשונה לאחר 18 חודש ממועד הגשת ההצעה ולאחר מכן בתדירות שנתית.

המחירים החדשים יחושבו ע"י הפעלת שיעור הנחה מוצע על מחיר מחירון מעודכן למועד ההצמדה.

לדוגמה:

שיעור הנחה בהצעת הספק לשירות SIEM בחלופת SaaS לחודש למערכת בהיקף של 50,000 EPS בממוצע לחודש עד 60 מקורות מידע שונים הנו 60%.

- מחיר המחירון לשירות בעת הגשת ההצעה הנו 10,000$ לחודש.

☜ *מחיר המחושב בהצעת הספק עבור השירות לאחר הפעלת שיעור הנחה הנו 4,000$.*

- מחיר המחירון המעודכן בעת חישוב ההצמדה הנו 8,000$ לחודש.

☜ *מחיר המעודכן לאחר הפעלה של שיעור הנחה בהצעת הספק במחיר השירות המעודכן הנו 3,200$.*

5.0.3 אופן התשלום

א. כל המחירים שיהיו נקובים בהצעה יהיו סופיים, ויכללו את כל מרכיבי העלות, מסים (למעט מע"מ), היטלים או תוספות אחרות, לרבות כל תשלום מסוג כלשהו לצד שלישי בגין תמלוגים ו/או זכויות שימוש.

ב. מחירים יהיו נקובים בשקלים או ב- $ ארצות הברית, עפ"י המופיע בתיאור מרכיבי התמורה. תמורה דולרית תומר ביום הוצאת החשבונית לש"ח על בסיס שער דולר יציג עדכני ארצות הברית כפי שמפורסם על ידי בנק ישראל.

ג. אופן חיוב בגין שירותים שוטפים – חשבון יוגש עד העשירי לחודש בגין החודש החולף. החשבון יוגש למחב"א עם פירוט של כל מוסד/ Tenant. מחב"א יאשר בתוך חמישה ימי עבודה את החשבון או יגיש הסתייגויותיו. לאחר אישור סופי של החשבון על ידי מחב"א, יגיש הספק חשבונית לתשלום, כולל פירוט נלווה של כל מוסד/ Tenant.

ד. התשלום לספק יבוצע על בסיס שוטף + 60 ימים.

ה. **הצמדה**

כל הסכומים הנקובים ב- ₪, לרבות תעריפי שעה, וכן סכומי הפיצוי המוסכם המופיעים בנספח רמת שירות, יוצמדו למדד המחירים לצרכן, אחת לשנה, בהתאם לכללים הבאים:

- מדד הבסיס הנו המדד הידוע במועד האחרון להגשת ההצעות.
- המדד הקובע הראשון יהיה תום השנה הראשונה ממועד תחילת השירות, והמדדים הקובעים לאחריה יהיו בתום כל אחת משנות השירות הבאות.
- ההצמדה תחושב עפ"י היחס שבין המדד הקובע האחרון לבין מדד הבסיס, כשיחס זה מוכפל ב 75%.

כל הסכומים הנקובים ב- $ ארצות הברית יוצמדו לפי המתואר בסעיף 5.0.2 לעיל.

5.1 SIEM בחלופת SaaS

5.1.1 הקמת SIEM בחלופת SaaS

תמורה עבור הקמת מערכת SIEM, עפ"י המתואר בסעיף 4.2.

להלן טבלת אבני דרך לתשלום בגין הקמת המערכת:

א. אבן דרך ראשונה הנה כללית לכל המוסדות ותשולם בסכום אחד, ללא תלות בכמות מוסדות שיצטרפו.

ב. הסכומים הכלולים באבני דרך 2-4 מיועדים לכסות את הקמת מערכת SIEM עבור 6 מוסדות שעפ"י הערכת מחב"א יצטרפו בשנה ראשונה. התשלום בפועל לספק יהיה בהתאם למספר

המוסדות שיצטרפו בפועל לשירות. כלומר, אם כמות המוסדות בפועל תהיה שונה מ- 6, תותאם עלות הקמה בגין שורות 2-4 בטבלה שלהלן בהתאם ליחס שבין מספר המוסדות ל- 6.

ג. לאחר עמידת כל אחד מהמוסדות באבני דרך 2-4, הספק יהיה זכאי לתשלום בגין 1/6 מאבן דרך.

ד. עלות תוספת מוסד שעשוי להצטרף בהמשך לשירות תהיה לכל היותר שישית מהמחירים הנקובים בשורות 2-4 של הטבלה.

#	תיחום/תוצר	גורם מאשר	הפניה לתוכנית עבודה בסעיף 4.2.1	%	מחיר בש"ח ללא מע"מ
1.	הקמת מערכת SIEM ברמה רוחבית	מחב"א	שלב 2 - תת שלב "סבב בדיקות קבלה"	30%	
2.	קישור 20 מקורות מידע עבור כ"א מ- 6 המוסדות הכלולים בפרויקט ההקמה	מחב"א ומוסדות	שלבים 3-5 תת שלב "הוספת מקורות מידע"	30%	
3.	עמידה במבחני קבלה עבור 6 מוסדות	מוסדות	שלבים 3-5 תת שלב "מבחני קבלה מערכת SIEM"	15%	
4.	מערכת SIEM מותאמת ומטוייבת ל- 6 מוסדות כך שמיום העברה לייצור ובמשך חודש רצוף לא התרחשה תקלה משביתה.	מוסדות	שלבים 3-5 תת שלב "תקופת הרצה"	25%	
5.	**סה"כ הקמת מערכת SIEM**			100%	

5.1.2 שירות שוטף SIEM בחלופת SaaS

תשלום חודשי שוטף לשירות SIEM בתצורת SaaS יכלול את כל הפעילויות בסעיף 2.5. התשלום יחל לאחר שלב הקמה 3 – "כניסה לפעילות מבצעית של פונקצית CSOC" של כל מוסד. תשלום יתבסס על כמות EPS בפועל לכל Tenant.

המחיר יוצמד בהתאם למנגנון המתואר בסעיף 5.0.2.

א. יש להציע מערכת SIEM בתצורת SaaS עבור ההיקפים הבאים:

- היקף של 50,000 EPS בממוצע חודשי, ואשר כוללת לפחות 60 מקורות מידע שונים.
- היקף של 90,000 EPS בממוצע חודשי, ואשר כוללת לפחות 80 מקורות מידע שונים.
- היקף של 150,000 EPS בממוצע חודשי, ואשר כוללת לפחות 100 מקורות מידע שונים.

ב. המחיר בפועל לשירות SIEM בתצורת SaaS יתבסס על מדידת שימוש ממוצע חודשי של EPS בפועל. המחיר יהיה יחסי למחיר הנקוב בסעיף א'. כאשר החישוב היחסי יבוצע מול הדרגה הגבוהה הקרובה לממוצע בפועל, למעט עבור ערכים של למעלה מ- 150,000 EPS שיחושבו מול המחיר של 150,000.

ג. הסבר ודוגמאות:

- במדידה שבוצעה בחודש ראשון לשירות, השימוש בפועל היה 44,000 EPS. לכן יש לבצע חישוב יחסי מול מחיר מערכת של 50,000 EPS.

- במדידה שבוצעה בחודש 45 לשירות עלה שהשימוש בפועל היה 120,000 EPS. לכן יש לבצע חישוב יחסי מול מחיר מערכת של 150,000 EPS.

ד. טבלת כמויות

☜ *כמות חודשי השירות בגין כל סוג שירות שלהלן נועדה לצורך השוואת עלות והלקוח אינו מתחייב לרכש בהיקף כלשהו.*

- יש לפרט את שם מוצר מערכת ה- SIEM, שם יצרן המערכת, שם ספק נותן השירות, כתובת מלאה של אתר השירות.
- לצורך השוואת הצעות הוגדר תסריט אשר מחלק את 60 חודשי ההתקשרות כך שבחצי השנה הראשונה מערכת ה- SIEM תהיה בהיקף של 50,000 EPS, במשך 3 שנים שלאחר מכן בהיקף של 90,000 EPS, ובשנה וחצי האחרונות להתקשרות בהיקף של 150,000 EPS. התשלום בפועל יהיה על בסיס שימושיות בפועל של כל מוסד.

#	סוג שירות	מחיר מחירון ב $ ארה"ב ללא מע"מ	שיעור הנחה	עלות $ ארה"ב ללא מע"מ, לאחר הנחה	בפועל חודשי שירות ל- 5 שנים	סה"כ עלות לכמות מבוקשת ב $ ארה"ב ללא מע"מ
.1	שירות SIEM לחודש למערכת בהיקף 50,000 EPS בממוצע לחודש, עד 60 מקורות מידע שונים				6	
.2	שירות SIEM לחודש למערכת בהיקף 90,000 EPS בממוצע לחודש, עד 80 מקורות מידע שונים				36	
.3	שירות SIEM לחודש למערכת בהיקף 150,000 EPS בממוצע לחודש, עד 100 מקורות מידע שונים				18	
.4	סה"כ לשירות SIEM ל- 5 שנים					
.5	שירות SIEM לחודש ברמה של Read Only לאחזור Data היסטורי בלבד ל- Tenant בודד, למימוש לאחר היפרדות				12	

5.1.3 שו"שים SIEM בחלופת SaaS

א. מימוש שו"ש יעשה רק לאחר ניצול מלא של תכולת השירותים השוטפים.

ב. הזמנת לקוח לבנק שעות תכלול היקף של 200 שעות, בעוד התשלום בפועל יעשה בהתאם לכמות שתנוצל מדי חודש.

#	שירות	עלות בש"ח ללא מע"מ	כמות לשנה	סה"כ עלות לכמות המבוקשת בש"ח ללא מע"מ
.1	כתיבת 10 תרחישים נוספים מעבר לכמות הכלולה בשוטף		4	

.2	בנק של 200 שעות לשירותים שאינם כלולים במסגרת השירות השוטף		2	
.3	יום הדרכה למפעילי מערכת במוסדות		6	
.4	סה"כ שירות SIEM שנתי להשוואת עלויות			

5.2 SIEM בחלופה מנוהלת

5.2.1 רכש מערכת SIEM בחלופה מנוהלת

א. יש להציע מערכת SIEM מנוהלת אשר תתמוך בלפחות EPS 90,000 בממוצע.

ב. בהתאם לאמור בסעיף 2.9.3 – מעבר משכירות לרישוי קבוע, המציע ינקוב בטבלה שלהלן במחיר EPS 90,000 הן לשכירות חודשית והן למחיר חד פעמי בעבור רישוי קבוע שישרת את הלקוח ללא הגבלת זמן.

ג. המחיר שישלם הלקוח בפועל בגין רישוי בשכירות ו/או רישוי קבוע יתבסס על מחיר יחסי בין כמות EPS בפועל למול המחיר הנקוב בטבלה להלן בגין מחיר EPS 90,000.

ד. רכש תחזוקת יצרן שנתית תחושב על פי הכפלת שיעור תחזוקה שנתית על מחיר רכישת הפריט בפועל (המחיר לאחר הנחה ולא מחיר מחירון). שיעור תחזוקה ממחיר הרכישה יהיה תקף לכל תקופת ההתקשרות.

ה. המחיר יוצמד בהתאם למנגנון המתואר בסעיף 5.0.2.

ו. טבלת כמויות

#	פריט	מחיר מחירון $ ארה"ב ללא מע"מ	% הנחה	עלות $ ארה"ב ללא מע"מ, לאחר הנחה	#	סה"כ עלות כמות מבוקשת ב- $ ארה"ב ללא מע"מ	שיעור תחזוקה שנתית
.1	רישוי SIEM בשכירות לחודש בהיקף EPS 90,000				15		
.2	רישוי קבוע למערכת SIEM בהיקף EPS 90,000				1		

5.2.2 רכש תשתית SIEM בחלופת מנוהלת

בחלופת שירות SIEM מנוהל המזמין יחליט אם לממש את תשתית המערכת באמצעות שירות IaaS או על ידי רכש תשתית אשר תותקן ע"י הספק במתחם הלקוח במד-1 או באתר אחר.

5.2.2.1 שירות IaaS

א. תשלום לשירות IaaS יתחיל מיום התקנת מערכת SIEM.

ב. תשלום בפועל בגין השירות יהיה על בסיס כמות EPS בממוצע לחודש.

ג. המחיר יקבע באופן יחסי אל מול מחיר נקוב למערכת של EPS 90,000.

ד. המחיר יוצמד בהתאם למנגנון המתואר בסעיף 5.0.2.

ה. יש לפרט את שם ספק נותן השירות, כתובת מלאה של אתר השירות.

#	פריט	מחיר מחירון $ ארה"ב ללא מע"מ	שיעור הנחה	עלות $ ארה"ב ללא מע"מ, לאחר הנחה	# לשנה	סה"כ עלות לכמות מבוקשת ב- $ ארה"ב ללא מע"מ
1	שירות חודשי IaaS למערכת SIEM בהיקף 90,000 EPS בממוצע לחודש				12	

5.2.2.2 רכש תשתית

א. המציע נדרש להציע חלופה על בסיס יחידות נפרדות שורות 1-4 בטבלה או חלופת Unified שורות 6-7 בטבלה. ניתן להציע את 2 הפתרונות. לצורך חישוב TCO תלקח ההצעה הזולה יותר.

ב. בעת המימוש בפועל ייבחר הפתרון, אשר יחד עם עלות אירוח וסביבה שיסופקו על ידי הלקוח, ייתן מענה מיטבי למזמין על בסיס איכות/תועלת.

ג. המציע נדרש להוסיף בשורה 4 פריטים נוספים הנדרשים לצורך קבלת פתרון שלם. יודגש שאם יתברר במהלך פרויקט ההקמה שנדרשים פריטי תשתית נוספים להקמת שירות SIEM, אזי פריטים אילו יסופקו על ידי על הספק בהתאם להיקף הנדרש ועל חשבונו.

#	פריט	עלות יחידה ₪ ללא מע"מ, לאחר הנחה, כולל התקנה ו- 3 שנות אחריות	#	סה"כ עלות לכמות ₪ ללא מע"מ	תחזוקה שנתית לכל הכמות ₪ מעבר ל- 3 שנות אחריות
.1	שרתים פיזיים				
.2	מערך אחסון מהיר כנדרש ל 90,000 EPS ל-12 חודשים ואחסון פחות מהיר ל- 4 שנים נוספות		2		
.3	מתג לקישור מערך אחסון לשרתים		1		
.4	חומרה ופריטים נוספים להקמת המערכת				
.5	סה"כ			שורות 1-4	שורות 1-4
.6	פתרון Unified עבור שורות 1-4 לעיל		1		
.7	מערך אחסון נוסף כנדרש ל 90,000 EPS (לצורך גיבוי ורפליקציה של מידע)		1		
.8	סה"כ			שורות 6-7	שורות 6-7

5.2.3 הקמת מערכת SIEM בחלופה מנוהלת

תמורה עבור הקמת מערכת SIEM, עפ"י המתואר בסעיף 4.2.

להלן טבלת אבני דרך לתשלום בגין הקמת המערכת:

א. אבן דרך ראשונה הנה כללית לכל המוסדות ותשולם בסכום אחד, ללא תלות בכמות מוסדות שיצטרפו.

ב. הסכומים הכלולים באבני דרך 2-4 מיועדים לכסות את הקמת מערכת SIEM עבור 6 מוסדות שעפ"י הערכת מחב"א יצטרפו בשנה ראשונה. התשלום בפועל לספק יהיה בהתאם למספר המוסדות שיצטרפו בפועל לשירות. כלומר, אם כמות המוסדות בפועל תהיה שונה מ- 6, תותאם עלות הקמה בגין שורות 2-4 בטבלה שלהלן בהתאם ליחס שבין מספר המוסדות ל- 6.

ג. לאחר עמידת כל אחד מהמוסדות באבני דרך 2-4, הספק יהיה זכאי לתשלום בגין 1/6 מאבן דרך.

ד. עלות תוספת מוסד שעשוי להצטרף בהמשך לשירות תהיה לכל היותר שישית מהמחירים הנקובים בשורות 2-4 של הטבלה.

#	תיחום/תוצר	גורם מאשר	הפניה לתוכנית עבודה בסעיף 4.2.1	%	מחיר בש"ח ללא מע"מ
.1	הקמת מערכת SIEM ברמה רוחבית	מחב"א	שלב 2 תת שלב סבב בדיקות קבלה	30%	
.2	קישור 20 מקורות מידע עבור כ"א מ- 6 המוסדות הכלולים בפרויקט ההקמה	מחב"א ומוסדות	שלבים 3-5 תת שלב הוספת מקורות מידע	30%	
.3	עמידה במבחני קבלה עבור 6 מוסדות	מוסדות	שלבים 3-5 תת שלב מבחני קבלה מערכת SIEM	15%	
.4	מערכת SIEM מותאמת ומטוייבת ל- 6 מוסדות כך שמיום העברה לייצור ובמשך חודש רצוף לא התרחשה תקלה משביתה.	מוסדות	שלבים 3-5 תת שלב תקופת הרצה	25%	
.5	**סה"כ הקמת מערכת SIEM**			100%	

5.2.4 שירות שוטף ושו"שים SIEM בחלופת מנוהלת

תשלום חודשי שוטף לשירות SIEM בחלופה מנוהלת יכלול את כל הפעילויות בסעיף 2.5. התשלום יחל לאחר שלב הקמה 3 – "כניסה לפעילות מבצעית של פונקצית CSOC" של כל מוסד. תשלום יתבסס על כמות EPS בפועל לכל Tenant.

א. מימוש שו"ש יעשה רק לאחר ניצול מלא של תכולת השירותים השוטפים.

ב. הזמנת לקוח לבנק שעות תכלול היקף של 200 שעות, בעוד התשלום בפועל יעשה בהתאם לכמות שתנוצל מדי חודש.

#	שירות	סוג	עלות בש"ח ללא מע"מ	כמות לשנה	סה"כ עלות לכמות מבוקשת בש"ח ללא מע"מ
.1	תחזוקה ותפעול שוטפים למערכת לחודש, ללא תחזוקת יצרן (הכלולה בטבלה (5.2.1)	שוטף		12	
.2	חיבור 10 מקורות מידע נוספים למערכת מעבר לכמות הכלולה בשוטף	שו"ש		4	

.3	כתיבת 10 תרחישים נוספים מעבר לכמות הכלולה בשוטף	שו"ש		4	
.4	שעת עבודה ארכיטקט מערכת	שו"ש		50	
.5	שעת עבודה מיישם מערכת	שו"ש		150	
.6	בנק של 200 שעות לשירותים שאינם כלולים במסגרת השירות השוטף	שו"ש		2	
.7	יום הדרכה למפעילי מערכת במוסדות	שו"ש		6	
.8	סה"כ שירות SIEM שנתי להשוואת עלויות				

5.3 שירותי מערכת CSOC

תשלום חודשי שוטף עבור שירותי CSOC יכלול את כל הפעילויות בסעיפים 2.7 ו- 2.8. התשלום יחל עם כניסה למבצעיות של פונקצית CSOC ברמה של כל מוסד.

הטבלאות שלהלן נועדו לצורך השוואת עלות ההצעות למשך שנת שירות. התשלום בפועל יתבסס על כמות EPS במערכת SIEM לכל Tenant, בהתאם לדוגמה בסעיף 5.3.3.

5.3.1 שירות שוטף

תשלום בפועל יחושב עפ"י מחיר שירותים לפי חלון שירות בטבלה שלהלן, שיותאם באופן יחסי לכמות EPS בפועל לכל אחד מחלונות השירות.

#	שירותים לפי חלון שירות	מחיר ליחידה ב- ₪ ללא מע"מ	כמות לשנה	סה"כ עלות
.1	שירות שוטף חודשי עבור מערכת בהיקף של EPS 60,000 לחלון שירות בשעות העבודה		12	
.2	שירות שוטף חודשי עבור מערכת בהיקף של EPS 10,000 לחלון שירות מחוץ לשעות העבודה		3	
.3	שירות שוטף חודשי עבור מערכת בהיקף של EPS 15,000 לחלון שירות של 24*7		12	
.4	שירות שוטף חודשי עבור מערכת בהיקף של EPS 15,000 לחלון שירות של 24*6		12	
.5	סה"כ שירות CSOC שנתי שוטף			

5.3.2 שו"שים

#	שירות	מחיר ליחידה ב- ₪ ללא מע"מ	כמות	סה"כ עלות
.1	אנליסט בהיקף של יום עבודה מעבר לנדרש ב- SOW וב- SLA		18	

.2	אנליסט בהיקף של שבוע עבודה ברצף מעבר לנדרש ב- SOW וב- SLA.		3	
.3	תוספת אנליסט בהיקף של חצי משרה לחודש מעבר לנדרש ב- SOW וב- SLA		6	
.4	תוספת אנליסט בהיקף של משרה מלאה לחודש מעבר לנדרש ב- SOW וב- SLA		4	
.5	שירות IR בהיקף של יום עבודה בחצר הלקוח (מעבר לנדרש בסעיף 2.7),		6	
.6	מבחן חדירה למערכת מידע		2	
.7	סקר אבטחת מידע למערכת קטנה		2	
.8	סקר אבטחת מידע למערכת בינונית		2	
.9	סקר אבטחת מידע למערכת גדולה		2	
.10	סקר סיכוני אבטחת מידע למוסד		2	
.11	סה"כ שירות CSOC שנתי שושים			

5.3.3 דוגמה לעלות בפועל לשירות CSOC

חישוב התמורה בפועל יעשה אחת לחודש בהתאם לצריכת EPS בפועל של כל מוסד ומוסד בנפרד בגין החודש החולף, להלן דוגמא:

#	שם מוסד	חלון שירות נבחר	EPS	סה"כ EPS לחלון שירות	סה"כ עלות
.1	מוסד1	שעות עבודה	13000	62,000	מחיר עלות ל- 60,000 לחלון שירות שעות עבודה <מחולק> 60 < כפול > 62.
.2	מוסד2	שעות עבודה	14000		
.3	מוסד3	שעות עבודה	15000		
.4	מוסד4	שעות עבודה	20000		
.5	מוסד5	24*7	15000	27000	מחיר עלות ל- 15,000 לחלון שירות 24*7 < מחולק> 15 < כפול > 27.
.6	מוסד6	24*7	12000		
.7	מוסד7	24*6	8000	8000	מחיר עלות ל- 15,000 לחלון שירות 24*6 < מחולק> 15 < כפול > 8.
.8	מוסד8	מחוץ לשעות עבודה	5000	5000	מחיר עלות ל- 10,000 לחלון מחוץ לשעות העבודה < מחולק> 10 < כפול > 5.

5.4 השוואת הצעות

א. הטבלאות להלן הנן סיכומיות בהתבסס על טבלאות עלות קודמות, ומטרתן ליצור TCO לצורך השוואת עלות כוללת.

ב. יחושב TCO נפרד לחלופת SaaS ולחלופת מערכת מנוהלת. אם בהצעת הספק הזוכה ייכללו 2 חלופות, מחב"א יהיה רשאי להתנייד בין החלופות במשך כל תקופת ההתקשרות.

ג. המחיר הכולל בטבלאות אינו מעיד על היקף ההתקשרות ו/או על תקציבים המיועדים לשירותים אלו.

ד. נתוני עמודת עלות יועתקו מטבלת המקור שבסעיף המתאים.

5.4.1 TCO לחלופת SaaS

#	מרכיב תמורה	סעיף	עלות	גורם מכפיל	סכום בש"ח ללא מע"מ
.1	הקמת מערכת SIEM	5.1.1 שורה 5		1	
.2	שירות שוטף SIEM	5.1.2 שורה 4		שער $ ארה"ב יציג	
.3	ש"ושים מערכת SIEM 5 שנים	5.1.3 שורה 4		5	
.4	אופציה לשירות Read Only לאחר היפרדות משירות SIEM	5.1.2 שורה 5		שער $ ארה"ב יציג	
.5	שירות שוטף מערכת CSOC 5 שנים	5.3.1 שורה 5		5	
.6	שו"שים לשירות CSOC 5 שנים	5.3.2 שורה 11		5	
	TCO לצורך השוואת הצעות				

5.4.2 TCO לחלופת SIEM מנוהל

#	מרכיב תמורה	סעיף	עלות	גורם מכפיל	סכום כולל בש"ח ללא מע"מ
.1	שכירות רישוי מערכת SIEM למשך של 15 חודשים	5.2.1 שורה 1		שער $ ארה"ב יציג	
.2	רכש מערכת SIEM	5.2.1 שורה 2		שער $ ארה"ב יציג	
.3	שירות IaaS – 2 שנים	5.2.2.1 שורה 1		שער $ ארה"ב יציג < כפול> 2	
.4	רכש תשתית – 3 שנים	5.2.2.2 שורה 5 או 8 (הזול מבינהם)		1	
.5	הקמת מערכת SIEM	5.2.3 שורה 5		1	
.6	תחזוקת יצרן מערכת SIEM ל-3 שנים	5.2.1 שורה 2	שיעור מרכישה <כפול> עלות שורה 2	3 < כפול> שער $ ארה"ב יציג	
.7	שוטף וש"ושים מערכת SIEM ל-5 שנים	5.2.4 שורה 8		5	
.8	תחזוקת תשתית – שנתיים	5.2.2.2 שורה זהה לכניסה 4		2	
.9	שירות שוטף מערכת CSOC – 5 שנים	5.3.1 שורה 5		5	
.10	שו"שים לשירות CSOC – 5 שנים	5.3.2 שורה 11		5	
	TCO לצורך השוואת הצעות				

נספחי מנהלה

נספח 0.3.1 א' טופס הרשמה לקבלת מסמכי המכרז

שם התאגיד הנרשם למכרז: _____

המדינה בה התאגד התאגיד: _____

אנשי קשר מטעם התאגיד, המוסמכים לייצגו לצורך המכרז:

1. _____
2. _____

כתובת דואר למשלוח הודעות: _____

מספר טלפון: _____

מספר פקס: _____

כתובת דואר אלקטרוני: _____

ידוע לי כי אין בהעברת פרטי ההתקשרות כדי לפטור אותי מחובתי להתעדכן בהודעות והבהרות מטעם המזמין באמצעות אתר האינטרנט של המזמין.

חתימה של מורשה חתימה מטעם התאגיד וחותמת התאגיד

_____

נספח 0.3.3 גלופה להעברת שאלות ובקשות הבהרה

לכבוד,

מחב״א

להלן שאלות ובקשות הבהרה שיש לנו בקשר עם **״מכרז פומבי 01.2019 לאספקת ותחזוקת מערכת SIEM, וקבלת שירותי** CSOC״.

שם הספק	
מזהה הספק (ח.פ/ח.צ/ע.מ)	
כתובת דואר אלקטרוני	
שם איש הקשר אצל הספק	

המסמך	סעיף	פירוט השאלה/בקשת הבהרה

על החתום,

שם מלא	תאריך	חתימה

נספח 0.6.2 - שגיאה! מקור ההפניה לא נמצא.**מעמדו המשפטי של המציע**

א. צורת ההתאגדות של המציע (חברה / עמותה / שותפות / אחר) _____

ב. מספר מזהה (לפי הרישום במרשם הרלוונטי) _____

ג. המדינה בה התאגד המציע _____

ד. מורשי החתימה בשם המציע ותפקידם אצל המציע:

#	שם	ת.ז.	תפקיד בתאגיד	דוגמת חתימה

ה. צירוף מסמכים נדרשים (סמן ☑ במקום המיועד לכך אם צורף):

המסמך הנדרש	האם צורף? (סמן ☑)
אישור על רישום התאגיד	❒
נסח רישום תאגיד עדכני לשנת 2018	❒
אישור של עו"ד בדבר זהות מורשי החתימה אצל המציע	❒
אישור רואה חשבון כי עסקו של המציע הוא בשליטת אישה (ככל שרלוונטי)	❒

נספח 0.6.3 - עמידה בהוראות חוק עסקאות גופים ציבוריים ושמירה על דיני עבודה

א. **צירוף מסמכים נדרשים**

סמן ☑ במקום המיועד לכך אם צורף:

המסמך הנדרש	האם צורף? (סמן ☑)
אישור תקף על ניהול פנקסי חשבונות ורשומות לפי חוק עסקאות גופים ציבוריים	❒

ב. **תצהיר מאומת ע"י עו"ד בדבר היעדר הרשעות בעבירות לפי חוק עובדים זרים**

אני הח"מ _____ ת.ז. _____ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

הנני נותן תצהיר זה בשם _____ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך המכרז מספר 1/2019 לאספקת ותחזוקת מערכת SIEM ושירותי CSOC אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

בתצהירי זה, משמעותו של המונח "**בעל זיקה**" כהגדרתו בחוק עסקאות גופים ציבוריים התשל"ו-1976 (להלן: "**חוק עסקאות גופים ציבוריים**"). אני מאשר/ת כי הוסברה לי משמעותו של מונח זה וכי אני מבין/ה אותו.

משמעותו של המונח "**עבירה**" – עבירה לפי חוק עובדים זרים (איסור העסקה שלא כדין והבטחת תנאים הוגנים), התשנ"א-1991 או לפי חוק שכר מינימום התשמ"ז-1987, ולעניין עסקאות לקבלת שירות כהגדרתו בסעיף 2 לחוק להגברת האכיפה של דיני העבודה, התשע"ב-2011, גם עבירה על הוראות החיקוקים המנויות בתוספת השלישית לאותו חוק.

המציע הינו תאגיד הרשום בישראל.

(סמן ☑ במשבצת המתאימה)

❒ המציע ובעל זיקה אליו **לא הורשעו** ביותר משתי עבירות עד למועד האחרון להגשת ההצעות (להלן: "**מועד להגשה**") מטעם המציע בהתקשרות מספר 1/2019 לקבלת לאספקת ותחזוקת מערכת SIEM ושירותי CSOC .

❒ המציע או בעל זיקה אליו **הורשעו** בפסק דין ביותר משתי עבירות **וחלפה שנה אחת** לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

❒ המציע או בעל זיקה אליו **הורשעו** בפסק דין ביותר משתי עבירות **ולא חלפה שנה אחת** לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

_____	_____	_____
תאריך	שם	חתימה וחותמת

אישור עורך הדין

אני הח"מ _____, עו"ד מאשר/ת כי ביום _____ הופיע/ה בפני במשרדי אשר ברחוב _____ בישוב/עיר _____ מר/גב' _____ שזיהה/תה עצמו/ה על ידי ת.ז. _____ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

_____	_____	_____
תאריך	מספר רישיון	חתימה וחותמת

נספח 0.6.4 – תצהיר בדבר ניסיון המציע

לכבוד: מחב"א

הנדון: **מכרז פומבי 01.2019 לאספקת ותחזוקת מערכת SIEM, וקבלת שירותי** CSOC **(להלן - "המכרז")**

1. אני הח"מ, **<u>מורשה החתימה</u>** והמוסמך לתת תצהיר בשמה של חברת _____, המציעה במכרז (להלן – "המציע"):

שם מורשה החתימה	ת.ז	חותמת תאגיד	חתימה אישית	תאריך

2. לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר כדלקמן:

א. למציע ניסיון של לפחות שנתיים בהתקנה, תמיכה ותחזוקה של מערכת SIEM, מהם לפחות שנה במערכת המוצעת על ידו.

ב. המציע הנו יצרן או מפיץ מורשה של מערכת SIEM המוצעת.

ג. למציע ניסיון באספקת שירותי SIEM שעונים על כל התנאים שלהלן:

1. ניסיון באספקת שירותי SIEM לפחות ל- 5 לקוחות פעילים, מהם לפחות 3 בישראל.
2. לפחות ל- 3 לקוחות ניתן ביום הגשת ההצעה שירות באמצעות מערכת SIEM המיושמת בשיטת Multi Tenancy או בעלת פונקציונאליות דומה.
3. היקף הניטור ל- 3 לקוחות הנו לפחות 10,000 EPS בממוצע לכל לקוח במחצית האחרונה של שנת 2018.

ד. למציע, שכלל בהצעתו חלופת SaaS, יש לפחות 3 לקוחות כלולים ביום הגשת ההצעה בשירות SaaS של SIEM.

ה. ספק שירותי CSOC עומד בדרישות חוקי הגנת הפרטיות בישראל.

ו. למציע ניסיון באספקת שירותי SOC לפחות ל- 10 לקוחות פעילים, ובנוסף עונה על התנאים הבאים:

1. לפחות ל- 3 לקוחות פעילים ניתן שירות באמצעות פונקצית SOC המיושמת בשיטת Multi Tenancy או בעלת פונקציונאליות דומה.
2. היקף הניטור ל- 3 לקוחות הנו לפחות 10,000 EPS בשיא לכל לקוח במשך שנה עד ליום הגשת ההצעה.

3. להלן תיאור הניסיון להוכחת עמידה בתנאי סף 2 ג' לעיל. לצורך עמידה בתנאי סף זה, ניתן לראות בניסיון קבלני המשנה כניסיון המציע.

ס"ק 1: 5 לקוחות SIEM פעילים מהם לפחות 3 בישראל.

#	שם לקוח	ספק השירות	מדינה	שם איש קשר	פרטי התקשרות: טלפון וכתובת e-mail
1.			ישראל		

.2			ישראל		
.3			ישראל		
.4					
.5					

ס"ק 2 : 3 לקוחות SIEM פעילים בשירות בתצורת Multi Tenancy או דומה.

	שם לקוח	ספק השירות	שם איש קשר	פרטי התקשרות: טלפון וכתובת e-mail
.1				
.2				
.3				

ס"ק 3 : 3 לקוחות SIEM בהיקף ניטור של לפחות 10,000 EPS בממוצע במחצית האחרונה של 2018.

#	שם לקוח	ספק השירות	שם איש קשר	פרטי התקשרות: טלפון וכתובת e-mail
.1				
.2				
.3				

4. להלן תיאור הניסיון להכוחת עמידה בתנאי סף 2 ד' לעיל.לצורך עמידה בתנאי סף זה, ניתן לראות בניסיון קבלני המשנה כניסיון המציע.

ס"ק 3 : למציע אשר מציע חלופת SaaS: 3 לקוחות SIEM פעילים בשירות SaaS.

	שם לקוח	ספק השירות	שם איש קשר	פרטי התקשרות: טלפון וכתובת e-mail
.1				
.2				
.3				

5. להלן תיאור הניסיון להוכחת עמידה בתנאי הסף 2 ו' לעיל. לצורך עמידה בתנאי סף זה, ניתן לראות בניסיון קבלני המשנה כניסיון המציע.

10 לקוחות פעילים בשירות SOC.

#	שם לקוח	ספק השירות	שם איש קשר	פרטי התקשרות: טלפון וכתובת e-mail
.1				
.2				
.3				
.4				
.5				
.6				
.7				
.8				
.9				
.10				

ס"ק 1 : 3 לקוחות פעילים בשירות SOC בתצורת Multi Tenancy או דומה.

	שם לקוח	ספק השירות	שם איש קשר	פרטי התקשרות: טלפון וכתובת e-mail
.1				
.2				
.3				

ס"ק 2 : 3 לקוחות SOC בהיקף ניטור של לפחות בשיא 10,000 EPS בשנה האחרונה.

#	שם לקוח	ספק השירות	שם איש קשר	פרטי התקשרות: טלפון וכתובת e-mail
.1				
.2				
.3				

אישור עו"ד

הנני מאשר כי ביום _____ הופיע בפני, מר/גב' _____ נושא ת.ז. שמספרה _____, ולאחר שהזהרתיו/ה כי עליו/ה לומר את האמת וכי ת/יהיה צפוי/ה לעונשים הקבועים בחוק אם לא ת/יעשה כן, אישר/ה את נכונות הצהרתו/ה דלעיל וחתמ/ה עליה בפני.

_____ _____ _____

שם עו"ד כתובת טלפון

_____ _____ _____

תאריך מספר רישיון חתימה וחותמת

נספח 0.6.5 תצהיר בדבר היעדר ניגוד עניינים

שנערך ונחתם ב_____ ביום ____ בחודש _____ שנת_____

אני_____ הח"מ, נושא ת.ז. _____ נותן תצהירי זה בקשר **מכרז פומבי 01.2019 לאספקת ותחזוקת מערכת SIEM, וקבלת שירותי CSOC**.

הנני נותן תצהירי זה בשם תאגיד _____, שמספרו המזהה הוא _____ (להלן – המציע).

הנני מכהן במציע בתפקיד _____.

הנני מורשה חתימה במציע ויש בחתימתי כדי לחייב את המציע.

הואיל ומחב"א והמוסדות השותפים בו עשוי לקבל את השירותים/הטובין כהגדרתם להלן;

והואיל והנני עשוי להיות מועסק בקשר למתן השירותים/הספקת הטובין;

והואיל והנני עשוי להימצא במצב של ניגוד עניינים במסגרת מתן השירותים ולאחריו;

לפיכך הנני מתחייב כלפי מחב"א והמוסדותכדלקמן:

א. הגדרות

בהתחייבות זו תהיה למונחים הבאים המשמעות המופיעה לצידם:

"**השירותים/הטובין**" - אספקת ותחזוקת מערכת SIEM וקבלת שירותי CSOC.

"**עובד**" - כל אחד מעובדי המציע אשר באמצעותו יינתנו השירותים למזמין.

ב. הנני מצהיר ומתחייב שאין ולא יהיה לי, במהלך תקופת מתן השירותים, ובמהלך שלושה חודשים מתום תקופה זו, ניגוד עניינים מכל מין וסוג שהוא עם גורמים בעלי עניין בתחום נושא הפניה, למעט באם ועדת המכרזים אישרה בכתב, לאחר שהעובדות הוצגו בפניה, כי אין בעובדות אלו משום ניגוד עניינים או באם קיים ניגוד עניינים מדובר בניגוד עניינים שולי אשר אין בו השפעה על השירותים נשוא המכרז.

ג. הנני מצהיר ומתחייב שלא אפעל מטעם כל גורם שהוא בתחום השירותים נשוא מכרז זה, למעט מטעם המזמין, במהלך תקופת מתן השירותים בין הצדדים ושלושה חודשים לאחריה, אלא אם כן התקבל לכך אישור מראש ובכתב של המזמין.

ד. הנני מתחייב להודיע למזמין באופן מידי על כל נתון או מצב, שבשלם אני עלול להימצא במצב של ניגוד עניינים, מיד עם היוודע לי הנתון או המצב האמורים.

ה. הנני מצהיר ומתחייב לדווח מראש למזמין על כל כוונה שלי, להתקשר עם כל גורם כאמור בסעיפים ב-ג לעיל, בניגוד להתחייבויותיי בסעיפים אלו, ולפעול בהתאם להוראותיו בעניין. המזמין רשאי לא לאשר לי התקשרות כאמור או לתת הוראות אחרות שיבטיחו העדר ניגוד עניינים, והנני מתחייב כי אפעל בהתאם להוראות אלו, בהקשר זה.

זהו שמי, זו חתימתי ותוכן תצהירי אמת.

ולראיה באתי על החתום: _____

<u>אישור</u>

הנני מאשר כי ביום _____ הופיע בפני, מר/גב' _____ נושא ת.ז. שמספרה _____, ולאחר שהזהרתיו/ה כי עליו/ה לומר את האמת וכי ת/יהיה צפוי/ה לעונשים הקבועים בחוק אם לא ת/יעשה כן, אישר/ה את נכונות הצהרתו/ה דלעיל וחתמ/ה עליה בפני.

_____	_____	_____
שם עו"ד	כתובת	טלפון
_____	_____	_____
תאריך	מספר רישיון	חתימה וחותמת

נספח 0.6.6 תצהיר כללי

א. פרטי המציע

אני_____ החי"מ, נושא ת.ז. _____ נותן תצהירי זה בקשר **מכרז פומבי 01.2019 לאספקת ותחזוקת מערכת SIEM, וקבלת שירותי** CSOC.

הנני נותן תצהירי זה בשם תאגיד _____, שמספרו המזהה הוא _____ (להלן – המציע). התאגיד התאגד ב_____.

הנני מכהן במציע בתפקיד _____.

הנני מורשה חתימה במציע ויש בחתימתי כדי לחייב את המציע.

במציע קיימים מורשי חתימה נוספים שהם (שם, ת.ז.):

1. _____.
2. _____.
3. _____.

ב. הסכמה לדרישות המכרז

קראתי את כל תנאי **מכרז פומבי 01.2019 לאספקת ותחזוקת מערכת SIEM, וקבלת שירותי** CSOC ודרישותיו, הבנתי אותם ואני מתחייב בשם המציע ומטעמו כי המציע ימלא אחר כל התנאים והדרישות של המכרז, ההצעה וההסכם, בדייקנות, ביעילות, במומחיות ובמיומנות, לשביעות רצון עורך המכרז, ובמועדים אשר ייקבעו על ידו, והכל בכפוף להוראות מכרז זה וההסכם.

הנני מצהיר כי כל הנתונים המפורטים בהצעה למכרז נבדקו על ידי והם נכונים ומדויקים.

ג. הצהרה על שימוש בתוכנות מקוריות וזכויות קניין

הנני מצהיר כי המציע משתמש בתוכנות מחשב מקוריות בלבד.

הנני מצהיר כי המציע הוא בעל זכויות הקניין, זכויות הפטנטים, זכויות היוצרים והזכויות האחרות הגלומות בהצעתו (להלן ביחד - "זכויות הקניין") או שהמציע מורשה לעשות שימוש בזכויות הנ"ל, ולא קיימת מניעה משפטית כל שהיא להגיש הצעתו ולהתקשר לפיה עם עורך המכרז כמפורט במכרז.

המציע מתחייב לשפות ולפצות את עורך המכרז בגין נזקים כלשהם בשל תביעות צד ג' נגדו כתוצאה מהפרת זכויות קניין כלשהן בשל ההצעה או ההתקשרות של עורך המכרז.

ד. הצהרה בדבר אי תיאום הצעות במכרז

המחירים ו/או הכמויות אשר מופיעים בהצעה זו נקבעו על ידי התאגיד באופן עצמאי, ללא התייעצות, הסדר או קשר עם מציע אחר או עם מציע פוטנציאלי אחר (למעט קבלני המשנה אשר צויינו בהצעה).

המחירים ו/או הכמויות המופיעים בהצעה זו לא הוצגו בפני כל אדם או תאגיד אשר מציע הצעות במכרז זה או תאגיד אשר יש לו את הפוטנציאל להציע הצעות במכרז זה.

לא הייתי מעורב בניסיון להניא מתחרה אחר מלהגיש הצעות במכרז זה.

לא הייתי מעורב בניסיון לגרום למתחרה אחר להגיש הצעה גבוהה או נמוכה יותר מהצעתי זו.

לא הייתי מעורב בניסיון לגרום למתחרה להגיש הצעה בלתי תחרותית מכל סוג שהוא.

הצעה זו של התאגיד מוגשת בתום לב ולא נעשית בעקבות הסדר או דין ודברים עם מתחרה או מתחרה פוטנציאלי אחר במכרז זה.

יש לסמן ☑ במקום המתאים

❐ למיטב ידיעתי, התאגיד מציע ההצעה לא נמצא כרגע תחת חקירה בחשד לתיאום מכרז

אם כן, אנא פרט:

_____

_____

_____

אני מודע לכך כי העונש על תיאום מכרז יכול להגיע עד חמש שנות מאסר בפועל לפי סעיף 47א לחוק ההגבלים העסקיים, תשמ"ח-1988.

זהו שמי, זו חתימתי ותוכן תצהירי אמת.

_____

חתימה

<u>אישור לנספח תצהיר כללי</u>

הנני מאשר כי ביום _____ הופיע בפני, מר/גב' _____ נושא ת.ז. שמספרה _____, ולאחר שהזהרתי/ה כי עליו/ה לומר את האמת וכי י/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא י/תעשה כן, אישר/ה את נכונות הצהרתו/ה דלעיל וחתם/ה עליה בפני.

_____	_____	_____
שם עו"ד	כתובת	טלפון
_____	_____	_____
תאריך	מספר רישיון	חתימה וחותמת

נספח 0.6.7 - תצהיר בדבר העסקת אנשים עם מוגבלות

אני הח"מ _____ ת.ז. _____ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

הנני נותן תצהיר זה בשם _____ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך **מכרז פומבי 01.2019 לאספקת ותחזוקת מערכת SIEM, וקבלת שירותי** CSOC. אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

(סמן ☑ במשבצת המתאימה):

❒ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998 לא חלות על המציע.

❒ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998 חלות על המציע והוא מקיים אותן.

(במקרה שהוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998 **חלות על המציע** נדרש לסמן x במשבצת המתאימה):

❒ המציע מעסיק פחות מ-100 עובדים.

❒ המציע מעסיק 100 עובדים או יותר.

(במקרה שהמציע מעסיק 100 עובדים או יותר נדרש לסמן X במשבצת המתאימה):

❒ המציע מתחייב כי ככל שיזכה במכרז יפנה למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998, ובמקרה הצורך – לשם קבלת הנחיות בקשר ליישומן.

❒ המציע התחייב בעבר לפנות למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998, הוא פנה כאמור ואם קיבל הנחיות ליישום חובותיו **פעל ליישומן** (במקרה שהמציע התחייב בעבר לבצע פנייה זו ונעשתה עמו התקשרות שלגביה נתן התחייבות זו).

המציע מתחייב להעביר העתק מהתצהיר שמסר לפי פסקה זו למנהל הכללי של משרד העבודה הרווחה והשירותים החברתיים, בתוך 30 ימים ממועד ההתקשרות.

אישור עורך הדין

אני הח"מ _____, עו"ד מאשר/ת כי ביום _____ הופיע/ה בפני במשרדי אשר ברחוב _____ בישוב/עיר _____ מר/גב' _____ שזיהה/תה עצמו/ה על ידי ת.ז. _____ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

_____	_____	_____
תאריך	חותמת ומספר רישיון	חתימה

נספח 0.6.8 העדפת תוצרת הארץ

נספח 0.6.9 תצהיר בדבר זמינות מיידית

אני הח"מ _____ ת.ז. _____ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

הנני נותן תצהיר זה בשם _____ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך **מכרז פומבי 01.2019 לאספקת ותחזוקת מערכת SIEM, וקבלת שירותי** CSOC. אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

השירותים והמועמדים המוצעים מטעם המציע נשוא מכרז זה זמינים ויועמדו לרשות המזמין מיידית לאחר החתימה על הסכם זה.

המציע מתחייב כי המערכות והשירותים הכלולים בהצעה עומדים בדרישות הטכנולוגיות המפורטות במסגרת פנייה זו.

אישור עורך הדין

אני הח"מ _____, עו"ד מאשר/ת כי ביום _____ הופיע/ה בפני במשרדי אשר ברחוב _____ בישוב/עיר _____ מר/גב' _____ שזיהה/תה עצמו/ה על ידי ת.ז. _____ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

_____	_____	_____
תאריך	חותמת ומספר רישיון	חתימה

נספח 0.7 מפל – ניקוד איכות

#	סעיף	קריטריון	משקל סעיף/ משקל מוחלט
.1	**השירות**		70.0%
.2	SIM01	מערכת ה SIEM - תכלול מנגנון לבדיקת Rules קיימים, ו- Rules חדשים על DATA היסטורי הנמצא במערכת ברמת גישה on-line.	1.75%
.3	SIM02	מערכת ה SIEM - תכלול יכולת חיפוש אחר התרחשות של אירוע במוסד על סמך תבנית של אירוע אבטחת מידע שזוהה במוסד אחר המקושר למערכת	3.50%
.4	SIM03	מערכת ה SIEM - תכלול ממשקים למקורות מידע מודיעינים חיצוניים כדוגמת מערך הסייבר ותתמוך בפרוטוקולי תקשורת סטנדרטיים כדוגמת.stix/taxii	3.50%
.5	SIM08	תצורת איסוף נתונים ממקורות המידע השונים המפורטים בהמשך המסמך – דיאגרמה מלאה של איסוף הנתונים, פרוטוקולים, להיכן ירוכזו הנתונים, שרתי הביניים וכו.	5.25%
.6	SIM10	דרכי התממשקות	3.50%
.7	SIM11	בקרה על תהליך קבלת האירועים	3.50%
.8	SIM12	תיעדוף אירועים	1.75%
.9	SIM14, SIM15	מודולים נוספים	1.75%
.10	2.2.2	דרישות תצורה	3.50%
.11	2.2.4	תהליכים	3.50%
.12	2.3.8	מקורות מידע רוחביים	8.75%
.13	ס"ק ד' 2.4.1	מסכי המערכת	3.50%
.14	2.9.2	ביצועים, עומסים והיקפים	8.75%
.15	2.11	גיבויים ושרידות	3.50%
.16	2.5.2	משאבים לתחזוקת SIEM	7.00%
.17	2.7	משאבים לשירות CSOC	7.00%
.18	מימוש		20.0%
.19	4.1.2	מנהל שירות CSOC	5.00%
.20	4.1.3	צוות שירות - CSOC אנליסט	6.67%
.21	4.1.5	צוות - SIEM ארכיטקט מערכת SIEM	5.00%
.22	4.1.4	צוות השירות - בקרי קוו ראשון	1.67%
.23	4.1.6	צוות השירות - מיישם SIEM	1.67%
.24	**כללי**		10.0%
.25	1.3.1	Multi-Tenancy ולקוחות פעילים	2.00%
.26	1.3.1	מיקום אצל אנליסטים	2.00%
.27		התרשמות כללית – מענה המציע	3.00%
.28		התרשמות כללית – מצגת המציע	3.00%
.29		**סה"כ**	**100.0%**

ציון סף איכות מינימאלי: **75.0**

נספח 0.9 הסכם התקשרות

מצורף כמסמך נפרד

נספח 0.11 תבנית להגשת הצעה

מצורף כמסמך נפרד

נספח 2.3.8 רשימת מקורות מידע

להלן הנחיות למילוי נספח רשימת מקורות מידע.

- בעמודה OoB יש לציין "כן" באם מקור המידע נתמך ברמת הונילה של המערכת המוצעת (OoB), כך שניתן לאסוף מידע ממנו ולנטרו ללא צורך בהתאמה/פיתוח עבור מקור המידע. אחרת יש למלא "לא".
- עבור עמודה גרסאות נתמכות יש לפרט את גרסאות יצרן של מקור המידע הנתמכות על ידי המערכת המוצעת.
- בעמודת מענה המציע יש לפרט לגבי אופן איסוף וניטור מקור המידע כפי שמוצע, ובמקרים שאין תמיכה ברמת הונילה לפרט כיצד בכוונת המציע לכלול את מקור המידע במערכת.

#	מקור מידע	דרישות הפירוט	OoB	גרסאות נתמכות	מענה\הערות המציע
			כן/לא		
INT01	Active Directory	Microsoft AD			
INT02	מערכת שליטה ובקרה	HPOV			
INT03		Nagios			
INT04		Zabbix			
INT05		Solarwinds			
INT06	שרתי הפצת עדכוני אבטחת מידע.	תמיכה ב-WSUS וב- SCCM			
INT07	אנטי וירוס - תמיכה במערכת אנטי-וירוס ארגונית	Trend micro			
INT08		Kaspersky			
INT09		Symantec			
INT10		McAfee			
INT11	IPS	Mcafee			
INT12	EPO	McAfee			
INT13	DLP	Mcafee			
INT14	MDM	Citrix MDM / MAM system			
INT15	Firewall	Checkpoint			
INT16		Checkpoint with VS support			
INT17		Palo Alto			
INT18		Cisco ASA			
INT19		Fortigate			
INT20		Juniper - SRX			
INT21	Web Application Firewall & DB Firewall	Imperva			

			F5 LTM	Web Application Firewall & Load Balancer	*INT22*
			F5 ASM		*INT23*
			F5 APM		*INT24*
			Sentrigo	DB Firewall	*INT25*
			Guardium		*INT26*
			MS-SQL	Data Bases	*INT27*
			ORACLE		*INT28*
			SAP (S4HANA)		*INT29*
			MySQL		*INT30*
			CISCO WIFI Conroller	WiFi	*INT31*
			HP-Aruba		*INT32*
			SharePoint on Prem	שרתי אפליקציה	*INT33*
			SharePoint as a Service (365)		*INT34*
			VMware	סביבות וירטואליות	*INT35*
			Terminal Server		*INT36*
			Openstack		*INT37*
			Oracle Application	ERP	*INT38*
			SAP		*INT39*
			Commvault	גיבויים	*INT40*
			קמטק	בספות	*INT41*
			CyberArk		*INT42*
			CISCO	מתגים	*INT43*
			Juniper		*INT44*
			HP		*INT45*
			Microsoft 365	שירותי דואר	*INT46*
			& Google G-Suite		*INT47*
			Windows Server 2003/2008/2012	מערכות הפעלה לשרתים	*INT48*
			Linux		*INT49*
			Solaris		*INT50*
			Windows XP	מערכות הפעלה עמדות קצה	*INT51*
			Windows 7		*INT52*
			Win10		*INT53*
			גרסאות מגוונות של LINUX.		*INT54*
			Novell NetIQ	IDM	*INT55*
			Citrix Netscaler	App Delivary	*INT56*
			Cisco ISE	Identity Services	*INT57*
			Cisco ESA & SMA Iron Port	Mail Security	*INT58*
			Trend micro		*INT59*
			Blue coat Proxy SG	BlueCoat Suite	*INT60*
			Blue coat CAS		*INT61*
			Blue coat MAA		*INT62*
			Blue coat CASB		*INT63*
			Blue coat Analytics		*INT64*

			Portnox	NAC	*INT65*
			ezporoxy	Proxy שירותי	*INT66*
			Squid		*INT67*
			Nimsoft	Other	*INT68*
			Comsign Trust HSM signer1		*INT69*
			CA monitoring system		*INT70*
			RSA Authentication Manager		*INT71*
			Infoblox		*INT72*
			Meraki		*INT73*