## מערך הסייבר הלאומי

# פניה מוקדמת לקבלת מידע (RFI)

# מס' 0305/2023

# בנושא: מערכת Continuous Controls Monitoring (CCM)

**מאי 2023**

# פנייה מוקדמת לקבלת מידע (RFI) בנושא:
# מערכת Continuous Controls Monitoring (CCM)

## 1. רקע ומטרת הפנייה

1.1 ארגונים רבים עושים שימוש במגוון רחב של כלי הגנה על נכסים, מידע וסביבת ה-IT שלהם. ניטור רציף ואימות כי כלל הכלים מוגדרים ומיושמים בצורה נכונה – אם ע"פ הגדרות היצרן, אם בהתאם לדרכי פעולה מומלצות או בהתאמה לצרכי הארגון – הם פעולות מורכבות הדורשות זמן רב.

1.2 ארגונים נדרשים לעמוד באוסף רגולציות ותקני אבטחה (ISO, NIST, PCI,CIS) ונדרש מאמץ רב לאיסוף וניתוח המידע משלל הכלים והמערכות הפרוסים בארגון במטרה להעריך את מידת העמידה (Compliance) בתקנים אלו.

1.3 ארגונים זקוקים לשיטות וכלים יעילים להערכת חומרת הסיכון ולתעדוף הטיפול בפערי אבטחה של הנכסים הקריטיים המעורבים בתהליכים העסקיים שלהם והם משקיעים תקציבים רבים ברכש טכנולוגיות חדשות ופתרונות הגנה כנגד איומים מתהווים אך מתקשים לגבש תמונת מצב שלמה ועדכנית של מצב החוסן בארגונם.

1.4 לאור המפורט לעיל מעוניין מערך הסייבר הלאומי לקבל מידע בנושא מערכות CCM (Continuous Controls Monitoring) שהן מוצר טכנולוגי המנטר באופן רציף את מידת העמידה בבקרות ההגנה של הארגון.

1.5 המוצר מתחבר לכלי ניהול ההגנה השונים הפרושים בארגון, כגון: AD, FW, EDR, WAF, Vulnerability Management (VM), וכן לכלי ניהול תשתיות התקשורת והמערכות בארגון, מנטר כל כלי בתחומו, אוסף מכל כלי הגדרות וסטטוסים ומפיק ציון משוקלל לרמת העמידה בתורת הגנה, תקן או רגולציה, מציג מגמות ומתריע על חריגות. המוצר צריך להיות בעל יכולת התמודדות עם ארגונים רבים מסוגים שונים ואוסף נרחב של כלי הגנה.

## 2 כללי

2.1 פנייה זו הינה פנייה מוקדמת **לקבלת מידע** בהתאם לתקנה 14א לתקנות חובת המכרזים, תשנ"ג – 1993. אין בה כדי ליצור מחויבות כלשהי כלפי מי מהמשיבים ו/או לראות בה התקשרות משום סוג. הפנייה נועדה לקבלת מידע בלבד ובעקבותיה ישקול המערך את המשך פעולותיו בהתאם לשיקולים מקצועיים ועניינים.

2.2 אם וככל שיתקיים מכרז או הליך רכש אחר בעתיד, יהא רשאי המערך לשנות או להוסיף תנאים ודרישות, הכל לפי שיקול דעתו המקצועי ובהתאם לצרכיו.

2.3 המערך יהא רשאי לעשות שימוש במידע שיימסר לו במענה לפנייה זו, ולספק לא יהיו טענות בגין זכויות יוצרים.

2.4 מענה לפנייה זו לא יהווה תנאי להשתתפות במכרז, אם וככל שייערך בעקבותיה, ולא יקנה יתרון במכרז למי שנענה לפנייה רק בשל כך שנענה לה, ולא יחייב שיתופו במכרז או התקשרות עמו בכל דרך אחרת.

2.5 ניתן לעיין ולהוריד את המסמכים המלאים של הבקשה לקבלת מידע באתר האינטרנט של מנהל הרכש הממשלתי בכתובת: https://www.mr.gov.il/Pages/HomePage.aspx או באתר האינטרנט של מערך הסייבר הלאומי בכתובת: http://cyber.gov.il.

2.6 להלן טבלת ריכוז התאריכים לפנייה זו:

| הפעילות | תאריך | שעה |
|---|---|---|
| מועד פרסום הפנייה | 15.5.23 | 14:00 |
| המועד האחרון להמצאת שאלות הבהרה מן הספקים | 29.5.23 | 12:00 |
| מועד המענה של המשרד לשאלות ההבהרה | 7.6.23 | 12:00 |
| המועד האחרון להגשת מענים | 15.6.23 | 12:00 |

## 3 מושגי יסוד

3.1 מערכת CCM (Continuous Controls Monitoring) - מוצר טכנולוגי המנטר באופן רציף את מידת העמידה בבקרות ההגנה של הארגון.

## 4 מפרט דרישות

במסגרת RFI זה מבקש מערך הסייבר הלאומי (להלן: "**המערך**") לקבל מידע על אודות מערכות שמספקות מענה כמפורט להלן.

יובהר כי הפתרון המבוקש נועד להשתלב בארגונים בעלי מאפיינים שונים במשק (תשתיות, גופי תעשייה ועוד), בהתאם לצרכים ומאפייני הארגון ולהתאים לחיבור לרכיבים מסוגים שונים- רכיבי OT, IT, IOT וכו.

### 4.1 המשיב יפרט בדבר יכולות המוצר / המערכת בהתייחס להיבטים הבאים:

4.1.1 האם השירות הינו SaaS?

4.1.1.1 האם למציע קיימת יכולת להפעיל את השירות על-בסיס תשתיות הענן שנבחרו במכרז "נימבוס" (מכרז מרכזי 01-2020 לאספקת שירותי ענן על גבי פלטפורמה ציבורית עבור משרדי הממשלה ויחידות הסמך), AWS או GCP והאם המציע יכול להקים מרכז נתונים ב-Region הישראלי של תשתיות הענן שנבחרו במכרז "נימבוס" על-מנת לספק את השירות ממנו?

4.1.1.2 במידה והתשובה הינה שלילית, כמה זמן יידרש על-מנת להקים את השירות כמתואר לעיל?

4.1.1.3 ניתן להתרשם מדרישות הממשלה בהיבטי הגנה בסייבר, פרטיות, תנאי שימוש, אחסון ועיבוד מידע וכן דרישות נוספות בהיבטי אבטחת מידע ביחס לעבודה בענן, אשר הפתרון המוצע נדרש לעמוד בהן, בהתאם לפירוט הקיים במכרז המרכזי להוספת שירותים לשוק הדיגיטלי הממשלתי בענן, אשר נערך במסגרת פרויקט נימבוס ומסמכיו מפורסמים באתר מינהל הרכש בקישור הבא:

https://mr.gov.il/ilgstorefront/he/p/4000553566

4.1.1.4 מערכת ה-CCM (Continuous Controls Monitoring) תבדוק באופן אוטומטי ורציף את תקינות הגדרות ובקרות הגנת הסייבר (Cybersecurity Controls) המיושמות בארגונים המנוטרים.

4.1.1.5 בחינת קיום פגיעויות מוכרות ברכיבי תוכנה או מערכת כגון CVE's.

4.1.1.6 המערכת תכיל באופן מובנה (built-in) הגדרות הגנה בסייבר מומלצות בהתאם לתקנים מקובלים בשוק כגון NIST, ISO-27001 וכן הגדרות יצרן ו/או דרכי פעולה מומלצות (Best Practices).

4.1.1.7 המערכת תאפשר למשתמש לעדכן (להוסיף, לשנות או לבטל) את הגדרות ההגנה המוזכרות לעיל לפי מדיניות ההגנה שאותה הוא מעוניין ליישם ולמדוד.

4.1.1.8 ממשקי ניהול

4.1.1.8.1 ממשק ניהול של קבוצת ארגונים – ממשק המאפשר צפייה, הגדרה ועדכון של בקרות ומערכות מנוטרות עבור קבוצה של ארגונים

4.1.1.8.2 ממשק ניהול עבור ארגון – ממשק המאפשר צפייה, הגדרה ועדכון של בקרות ומערכות מנוטרות עבור ארגון יחיד

4.1.1.8.3 המערכת תכיל ממשקים (למשל, APIs) לניטור מוצרי הגנה וניהול IT ו/או ICS (OT) נפוצים, השייכים למשפחות המוצר הבאות לפחות. המשיב יפרט את המערכות הרלוונטיות בכל אחת מן המשפחות הבאות:

4.1.1.8.3.1 Asset Management / Identity Management

לדוגמה: Microsoft Active Directory, BigFix, SCCM

4.1.1.8.3.2 Firewall

לדוגמה: Checkpoint, Fortinet, Cisco, Palo Alto

4.1.1.8.3.3 IPS (Intrusion Prevention Systems)

לדוגמה: TrendMicro, Cisco

4.1.1.8.3.4 AV & EPP/EDR

לדוגמה: VMware Carbon Black, Symantec, McAfee

4.1.1.8.3.5 Email Gateway

לדוגמה: Microsoft, Symantec, TrendMicro

4.1.1.8.3.6 Virtualization

לדוגמה: VMware vCenter, Microsoft Hyper-V

4.1.1.8.3.7 Patch Management

לדוגמה: HCL BIGFIX, Microsoft WSUS

4.1.1.8.3.8 Vulnerability Management / Assessment

לדוגמה: Rapid 7, Tenable

4.1.1.8.3.9 Vulnerabilities Scanners & BAS (Breach and Attack Simulation)

לדוגמה: Rapid 7, Nessus, Skybox, Pentera

4.1.1.8.3.10 WAF & Load Balancer

לדוגמה: F5, Imperva

4.1.1.8.3.11 NAC

לדוגמה: Forescout, Portnox

4.1.1.8.3.12 VPN

לדוגמה: PulseSecure, Fortinet

4.1.1.8.3.13 Network Management / Network

רכיבי רשת שונים (נתבים, מתגים ועוד)

4.1.1.8.3.14 DB

לדוגמה: MySQL, SQL Server, MongoDB

4.1.1.8.3.15 Cloud

לדוגמה: Azure, AWS, GCP

4.1.1.8.3.16 Storage

לדוגמה: Dell EMC , NetApp , Veeam

4.1.1.8.3.17 Legacy Systems

לדוגמה: Lotus Notes ,Net and Oracle ,SAP

4.1.1.8.3.18 OT-IDS

לדוגמה: Checkpoint ,Splunk ,Fortinet, Tenable OT

4.1.1.8.4 ניטור המערכות השונות יתבצע באופן שאינו פוגע או פוגם בביצוע המערכות הנבדקות. הניטור יתבסס על ייבוא/איסוף נתונים מהמערכות באמצעות ממשק API או ייצוא באמצעות פקודות לגיטימיות של הגדרות המערכות הנבדקות.

4.1.1.8.5 התאמה של הממשקים לעיל, ללא שינוי קוד, באמצעות קונפיגורציה.

4.1.1.8.6 הוספת ממשקים חדשים (SDK).

4.1.1.8.7 תצוגות באמצעות פורטל המערכת ו/או דו"חות:

4.1.1.8.7.1 הצגת נתונים באופן רציף ובזמן אמת.

4.1.1.8.7.2 תמונת מצב ההגנה (Cybersecurity Posture), כולל ציון סיכון משוקלל בהתחשב בחומרה / חשיבות של הבקרות המנוטרות, לכל הארגון ובחלוקה למשפחות המוצר המנוטרות (לפי הרשימה לעיל).

4.1.1.8.7.2.1 הפעילות התקינה של המערכות המנוטרות.

4.1.1.8.7.2.2 יישום בקרות הגנת הסייבר במערכות אלה בהתאם לתקן שנבחר כבסיס לניטור.

4.1.1.8.7.2.3 פירוט המסביר את מהות הבקרה, השפעתה על רמת ההגנה של המערכת והאופן הנכון ליישמה או ליישום בקרה מפצה.

4.1.1.8.7.2.4 ציון ודירוג של חומרת וחשיבות כל בקרה על בסיס המלצות יצרן מקובלות או תקן חומרה מקובל אחר כבסיס להתאמה (Compliance).

4.1.1.8.7.2.5 הצבעה על פערים והמלצות לתיקון ושיפור המצב הקיים.

4.1.1.8.7.2.6 עדכון התקן המשמש כבסיס להתאמה (Compliance).

4.1.1.8.7.2.7 שינויים בתמונת ההגנה לאורך זמן, כולל התרעות על חריגה מהתנהגות מצופה, של הארגון כולו, של משפחת מוצרים או של מוצר מסוים.

4.1.1.8.7.2.8 תמיכה בהצגה של תמונות המצב לעיל באופן סיכומי במספר היררכיות:

4.1.1.8.7.2.8.1 ברמת ארגון ועבור מבנים ארגוניים מורכבים (Multi-site, International, etc.).

4.1.1.8.7.2.8.2 תמונת מצב מגזרית המורכבת משקלול התמונות של הארגונים המנוטרים המרכיבים אותו.

4.1.1.8.7.2.8.3 תמונת מצב לאומית המורכבת משקלול סך הארגונים המנוטרים.

4.1.1.8.7.2.9 תמיכה בהצגת תמונת המצב לעיל, בהיררכיות שונות, לבעלי עניין שונים ובכלל זה: גוף התפעול (SOC/NOC), מנהל תשתיות ה-IT, ה-CISO, מנהל הסיכונים (Risk Officer), מנחה של ארגון / מגזר במערך הסייבר הלאומי, תמונת מצב לאומית (סך הארגונים המנוטרים).

4.1.1.8.7.2.10 למערכת יכולת לבצע סינון נתונים והצגה של תוצאות הבדיקה לפי סוג המערכת הנבדקת, שם הארגון / רשת וכן חלוקות מותאמות אישית כגון מספר ארגונים אשר הלקוח המרכזי (מערך הסייבר הלאומי) משייך לאותה קבוצה.

4.1.1.8.7.2.11 המערכת תאפשר הפקת דוחות בפורמטים שונים ומקובלים כגון PDF, Word ,Csv.

4.1.1.8.7.2.12 המערכת תאפשר יכולת בניית תבנית של בקרות בהתאם לאפיון הלקוח המרכזי. יש לפרט בנוגע להשפעת בניית תבנית מותאמת ללקוח על הדו"חות, סינון הנתונים ועוד.

4.1.1.9 ניהול משתמשים והרשאות לפי תפקיד (RBAC) כולל התייחסות לסוגי המשתמשים השונים (מנהל-על / Admin, מנהל קבוצת ארגונים, נציג ארגון מנוטר), להיררכיות התצוגה השונות (כפי שצוינו לעיל) ויכולת הגדרת הצפייה במידע ע"פ הרשאות.

4.1.1.10 יכולת התאמת המערכת לארגונים שונים – גודל, סיווג (בלמ"ס, מסווגת, תפעולי) ומבנה רשתות – מבודלות / פתוחות.

4.1.1.11 הגדרות המערכות הנבדקות תשמרנה באופן מוגן / מוצפן במערכת הבדיקה או לחילופין לא תשמרנה כלל ותנותחנה על-ידי מערכת ה- CCM בתצורת Online.

4.1.1.12 למערכת יכולת פרישה רחבה במספר ארגונים ורשתות, של סוכני איסוף ויכולת העברת הנתונים הנאספים לשרת מרכזי לניתוח.

4.1.1.13 העברת הנתונים בין סוכני האיסוף לשרת המרכזי תבוצע באופן מוגן ומוצפן מפני האזנה והתערבות.

4.1.1.14 השרת המרכזי של ניתוח הנתונים יותקן בסביבה מאובטחת On Prem ו/או בספק ענן לפי דרישת הלקוח המרכזי, באחד משני ספקי הענן זוכי מכרז נימבוס.

4.1.1.15 נדרש כי השרת המרכזי יאפשר שמירת הנתונים שינותחו באופן מוגן ומוצפן .

4.1.1.16 נדרש כי השרת המרכזי ינוהל על-ידי הלקוח המרכזי או ע"י לקוח אחר מטעמו (למשל, יחידה מגזרית) באופן מלא תוך שליטה בהרשאות הגישה וכי לספק תהיה גישה לטובת תמיכה בלבד תחת בקרה ובידיעת הלקוח המרכזי.

4.1.1.17 בנוסף למענה המבוקש כמפורט לעיל, המשיבים רשאים להציג יכולות ושירותים נוספים ו/או משתלבים וכן תפיסה ורעיונות קיימים ועתידיים.

4.1.2 **<u>המשיב יפרט בדבר פרטי החברה המשיבה:</u>**

4.1.2.1 האם החברה המשיבה היא החברה המפתחת את המוצר/המערכת והבעלים שלו/ה?

4.1.2.2 האם ההטמעה והתמיכה במוצר/במערכת ניתנות ישירות ע"י החברה המשיבה? אם לא, מי מספק את ההטמעה והתמיכה?

4.1.2.3 האם לחברה המשיבה יש מרכז פיתוח ו/או תמיכה בישראל?

4.1.2.4 כמה לקוחות משלמים קיימים למוצר/מערכת?

4.1.2.5 האם חלק מהלקוחות המצוינים לעיל הם לקוחות פיננסיים ו/או ממשלתיים? אם כן, כמה והאם בישראל? במשך כמה שנים?

4.1.2.6 כמה זמן נמצא/ת המוצר/המערכת בשוק, בשימוש של הלקוחות המשלמים המפורטים לעיל, בארץ ובעולם?

4.1.2.7 מהו מודל התמחור, תוך התייחסות לתכולת רישיון לשימוש במערכת:

4.1.2.7.1 כמה ואלו כלים נכללים ברישיון למשתמש?

4.1.2.7.2 כמה ארגונים נכללים ברישיון למשתמש?

4.1.2.7.3 האם קיימות מדרגות תמחור עבור כמויות שונות של רישיונות למשתמשים?

4.1.2.7.4 האם קיימים שירותים נוספים, שלא כלולים ברישיון, ומה מחירם?

4.1.2.8 במידה והתשובה לאחד משני הסעיפים, הנוגעים להפעלת השירות על-בסיס זוכות מכרז "נימבוס" ומרכז נתונים ב-Region הישראלי, לפחות, הינה שלילית, מהי העלות למימוש הפעלת השירות באופן זה? במידה ונושא זה יהווה תנאי לאספקת השירות למשרדי ממשלה בישראל, מהו הפתרון המוצע ע"י המשיב?

4.1.2.9 כיצד מתומחרות שעות פיתוח בהתייחס למשימות ייעודיות ולפרוייקטים שלמים?

4.1.2.10 כיצד מתומחרות שעות Professional Services (PS)?

4.1.2.11 האם ניתן לתמחר פרוייקט התממשקות למערכות ולפורטלים חיצוניים לשירות ע"פ דרישות הלקוח ומה מנגנון התמחור?

4.1.2.12 האם ניתן לתמחר פרוייקט פיתוח ע"פ דרישות הלקוח ומה מנגנון התמחור?

4.1.3 האם קיימים מסמכים המפרטים תנאי שימוש בשירות ותנאי התקשרות? אם כן, נא לצרפם.

4.1.3.1 המשיב רשאי להוסיף כל מידע רלוונטי נוסף בהקשרים אלה.

## 5 המענה המבוקש

על ההצעות לתת מענה המתייחס לכל אחת מהדרישות המפורטות בסעיף 4 לעיל, ובכלל זה לכלול התייחסות לנושאים הבאים:

5.1 עבור כל ההצעות:

5.1.1 הצגת יכולות כמפורט בסעיף 4.

5.1.2 היצע פתרונות עם יכולת התאמה לארגונים שונים – גודל, סיווג (בלמ"ס, מסווגת, תפעולי) ומבנה רשתות פתוח / סגור.

5.1.3 קלות התקנה, תפעול ועדכון.

5.1.4 הצעות או רעיונות בדבר הקמת התשתיות, הכלים או המערכות הנדרשות למימוש הדרישות מהמערכת המוצעת.

5.1.5 בנוסף למענה המבוקש כמפורט לעיל, המשיבים רשאים להציג גם תפיסה ורעיונות קיימים ועתידיים וכן שירותים נוספים המרחיבים את המענה הכולל.

## 6 אופן הגשת שאלות הבהרה ומענה לפנייה זו

6.1 איש קשר

איש/אשת הקשר מטעם המערך בנוגע לפנייה זו הוא/היא שרון בוסידן, טל' 072-3388578 דוא"ל cyber-michrazim@cyber.gov.il.

6.2 שאלות הבהרה

6.2.1 שאלות הבהרה בנוגע לפנייה זו יש להגיש בכתב בלבד, לא יאוחר מהמועד האחרון להמצאת שאלות הבהרה כמפורט בטבלה שבסעיף 2.6, לאיש/אשת הקשר בדוא"ל cyber-michrazim@cyber.gov.il. על הספק לוודא ששאלותיו הגיעו בשלמות לאיש/אשת הקשר, בטל' 072-3388578.

6.2.2 המערך שומר לעצמו את הזכות לנהל סבב אחד או יותר של שאלות הבהרה בהתאם לשיקול דעתו הבלעדי.

6.2.3 שאלות ההבהרה יוגשו בשפה העברית, במבנה הבא:

| מספר הסעיף בפנייה | פירוט השאלה |
|---|---|
| | |
| | |

6.2.4 מענה לשאלות ההבהרה יועבר על ידי המערך אל הפונים, וכן יפורסם באתר האינטרנט של מינהל הרכש הממשלתי ושל מערך הסייבר הלאומי בכתובות המפורטות בסעיף 2.5 לעיל. מובהר כי תשובות ההבהרה ינוסחו באופן שאינו חושף את זהות השואלים.

6.3 <u>הגשת מענה לפנייה</u>

6.3.1 המענה לפנייה יהיה **<u>בשפה העברית או האנגלית</u>**, בהיקף כולל של עד 50 עמודים המציגים את המענה. בנוסף על כך ניתן לצרף נספחים ומפרטים טכניים ללא הגבלת היקף.

6.3.2 את המענה לבקשה לקבלת מידע יש להגיש בעותק דיגיטלי עד למועד האחרון להגשת מענים המפורט בטבלה שבסעיף 2.6 לעיל באמצעות תיבת דוא"ל Cyber-Michrazim@cyber.gov.il. ולוודא אישור קבלה בטל' 072-3388578. בנושא הדוא"ל יירשם: "פניה מוקדמת לקבלת מידע (RFI) בנושא מערכת Continuous Controls Monitoring (CCM)".

6.3.3 המערך רשאי לדחות את המועד האחרון להגשת מענה לפי שיקול דעתו הבלעדי. הודעה על כך תישלח לכל מי שהשיב לפנייה, וכן תפורסם באתר האינטרנט של מינהל הרכש הממשלתי ושל המערך בכתובות המפורטות בסעיף 2.5 לעיל. בהודעה יצוין המועד החדש להגשת המענים.

6.3.4 במסגרת המענה יפורטו פרטי המשיב:

| מס"ד | המידע המבוקש | מענה |
|---|---|---|
| 1 | שם המשיב | |
| 2 | כתובת המשיב | |
| 3 | מס' טלפון | |
| 5 | שם איש קשר מטעם המשיב | |
| 6 | מס' טלפון של איש הקשר | |
| 7 | כתובת דואר אלקטרוני של איש הקשר | |

## 7 <u>בדיקת המענה</u>

7.1 המערך שומר לעצמו את הזכות לפנות, ככל שיידרש, למשיבים לפנייה זו בבקשה להשלמת מידע והבהרות, להצגת מצגות והדגמות, לביקור באתרי הלקוחות ובאתרים של מי שהשיב לפנייה זו, בהתאם לשיקול דעתו של המערך.

7.2 במסגרת בחינת המענים, המערך שומר לעצמו את הזכות להזמין את כל מי שנענה לפניה, להציג את הפתרון המוצע על-ידו בפני צוות מקצועי מטעמו במיקום ובמועד שיקבע המערך.

7.3 במסגרת בחינת המענים, המערך שומר לעצמו את הזכות להזמין את המציעים לקיים פיילוט שמשכו עד חודשיים. יובהר כי המערך שומר לעצמו את הזכות להזמין רק חלק מהמציעים לקיום פיילוט כאמור, בהתאם לשיקול דעתו הבלעדי, בהתאם לצרכיו ויכולותיו של המערך וזמינות המציעים.