



פנייה מוקדמת לקבלת מידע למערכת מבוססת סנסורים מבוזרים להגנה לאומית מפני איומי סייבר עבור מערך הסייבר הלאומי

מרץ 2018

מסמך זה הינו רכוש מדינת ישראל. כל הזכויות שמורות למדינת ישראל (C). המידע הכלול בו לא יפורסם, לא ישוכפל ולא יעשה בו שימוש מלא או חלקי לכל מטרה שהיא מלבד מענה על פנייה זו.



פניה מוקדמת לקבלת מידע (RFI) למערכת מבוססת סנסורים מבוזרים להגנה לאומית

מפני איומי סייבר עבור מערך הסייבר הלאומי

רקע

מערך הסייבר הלאומי (להלן – המערך) מופקד על מכלול הפעולות למניעה, לנטרול, לחקירה ולהתמודדות עם איומי סייבר ואירועי סייבר וצמצום השפעתם והנזק הנגרם מהם, וזאת בטרם התרחשותם, במהלכם ולאחריהם.

על מנת לספק מענה הגנתי פרואקטיבי נדרשת פלטפורמת הגנה לאומית, המבוססת על טכנולוגיות מתקדמות לזיהוי ולסילוק איומי סייבר בראיה מדינתית, בדגש על גופים שהינם תשתיות קריטיות (לפי התוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשמ"ח-1998). הפלטפורמה תאפשר הגנה ברמת Prevention ו-Detection מפני תקיפות סייבר על בסיס מודיעין מדינתי, אלגוריתמים לזיהוי אנומליות ואינדיקטורים ייעודיים. המערך מבקש לקבל מידע על רכיבים ומערכות המקיימות את כלל היעדים והמטרות המפורטים.

יעדים ומטרות

1. **סילוק איומי סייבר** – הגנה על גופים באמצעות אמולציה לזיהוי איומים ואכיפת מודיעין סייבר עדכני בכל אתר יעד, תוך הפעלת יכולות Sandboxing וסינון של קבצים ותעבורת נתונים זדוניים ברשת.
2. **מודיעין איומים** – אספקת הזנות (Feeds) מודיעיניות ציבוריות ופרטיות, הניתנות להתאמה עבור כל אתר מוגן, וכן ניטור מרכזי של אירועי אבטחה שסוכלו לצורך ניתוח מעמיק וממוקד. בנוסף, נדרשת אינטראופרביליות (שיתוף ותאימות) מודיעינית תוך שימוש בפרוטוקולים סטנדרטיים כגון STIX/TAXII.
3. **יכולת לאומית לניטור וזיהוי תקיפות סייבר** בגופים – יצירת פלטפורמת ניטור לאומית, שתאפשר לחוקרים ולאנליסטים במערך הסייבר הלאומי לסקור ולבדוק כיווני חקירה שונים מבלי לשבש את תעבורת הנתונים במערכות הייצור של הגופים המונחים.
4. **גמישות** – אכיפת מאפייני אבטחה שונים ע"פ ישות יחידה ו/או קובץ ישויות, תוך מתן מענה לדרישות אבטחה שונות מהרמה הסקטוריאלית ועד לקישור מוגן בודד.
5. **פרטיות וסודיות מידע רגיש** – הגנה על פרטיות או סודיות מידע עסקי של הישויות לפי צורך, באמצעות צמצום איסוף, שמירה או מיסוך תכנים פרטיים או רגישים אחרים מרשומות אירועי האבטחה ויצירת חיץ בין תצוגות יומן אירועים ודוחות האבטחה.
6. **יכולת הרחבה** – יצירת מערכת הניתנת להרחבה ע"י צורך במטרה לתמוך בכמות גדולה של נקודות ניטור וסילוק.
7. **קלות פריסה ותחזוקה** – על נקודות האכיפה לתמוך ביכולות Plug&Play במטרה לאפשר פריסה מהירה ותחזוקה קלה.



אפיון על של המערכת

המערכת תתבסס על מרכיבי קצה (סנסורים) פיזיים או וירטואליים במתקני הגופים המונחים, אשר יותקנו בחיבור In-Line ו/או TAP Mode מחוץ לפרימטר של הארגון. סנסורים אלה יהיו שקופים ככל הניתן לפעילות הגוף המנוטר ולא ייצרו עומס תקשורתי, תפעולי או תחזוקתי על הגוף.

הסנסורים שיוצעו במסגרת RFI זה נדרשים לעמוד בתנאים הבאים:

1. התקנה פשוטה, ברמת Plug&Play.
2. התמודדות עם Load Balancing בקווי התקשורת של הגוף המנוטר.
3. זיהוי אנומליות ונתונים זדוניים בתעבורת הרשת על בסיס IOCs ו-Yara Rules, מינוף יכולות כגון Antivirus, Sandboxing, IPS ואמולציית איומים ברמת המעבד.
4. גמישות ברמת יכולת מערך הסייבר הלאומי לשלב בסנסור קוד/רכיב תוכנה, הן מוצר צד ג' והן פיתוח ייעודי של המערך, כחלק ממימוש תפיסת הניטור וה- Incident Response.
5. Fail Open ברמת תוכנה וחומרה, שיאפשר Bypass אוטומטי וימנע מהסנסור להפוך לנקודת כשל יחידה ברשת של הגוף המנוטר.
6. מתן חיווי על הצלחה/כישלון של הפצת/עדכון אינדיקטורים לסנסורים.
7. יכולת לבצע Rollback לתצורה קודמת על בסיס Time Stamp.
8. יכולת ליצור הודעה שיקבל משתמש בגוף המנוטר, כאשר הסנסור חוסם תעבורה כלשהי שרלוונטית אליו.
9. ניהול, שליטה ובקרה על הסנסורים יתאפשר בערוץ Out Of Band.
10. מיסוך לוגים ושדות בממשק הניהול לטובת הגנה על פרטיות המידע.
11. ממשק חד-כיווני לשליחת התראות/לוגים מהסנסור ל-SIEM של הגוף המנוטר.
12. יכולת להגדיר מדיניות שונה לאזורים שונים בארגון המנוטר (לדוגמה – הגדרת מוד Detection בסגמנט אחד ומוד Prevention בסגמנט שני).
13. יכולת לתקשר מול NOC קיים של מערך הסייבר הלאומי בפרוטוקולים סטנדרטיים, כגון SNMP, SSH וכד'.

המערכת תאפשר פעילות בלוח זמנים מיידי של המערך באירועי סייבר בגופים המנוטרים, באמצעות הפצה של אינדיקטורים וחוקים (כגון YARA) "פרטיים" ברמה הקרובה לזמן אמת ובקנה מידה רחב, במספר שיטות:

1. ממשק משתמש לשליטה/הזנה ידנית של מזהי אבטחה לאיתור ולסילוק איומים.
2. API מודיעיני עבור כלי צד שלישי, לרבות מאגר המודיעין של המערך (נדרש ממשק דו-כיווני שיאפשר העשרה של המאגר, למשל בפרוטוקול STIX/TAXII).



הגשת מענה לפנייה זו

1. יודגש כי פנייה זו הינה פנייה מוקדמת לקבלת מידע בלבד. פנייה זו אינה בבחינת הזמנה להציע הצעות ואינה חלק מהליכי מכרז, לפיכך 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 פעולותיה בהתאם לשיקולים מקצועיים וענייניים.
2. המערך שומר לעצמו את הזכות להשתמש במידע אשר יתקבל בעקבות פנייה זו לצורך הרכבת רשימת ספקים פוטנציאליים, הכל לפי שיקול דעתה הבלעדי.
3. אם וככל שיתקיים מכרז בעתיד, יהא רשאי המערך לשנות או להוסיף תנאים ודרישות, הכל לפי שיקול דעתה המקצועי ובהתאם לצרכיה.
4. המערך שומר לעצמו את הזכות לפנות, ככל שיידרש, למי שענה על פנייה זו בבקשה להשלמת מידע והבהרות, להצגת מצגות והדגמות, לביצוע פיילוט, לביקור באתרי הלקוחות ובאתרים של מי שענה לפנייה זו.
5. המערך יהא רשאי לעשות שימוש במידע שיימסר במענה לפנייה זו, ולספק לא יהיו טענות בגין זכויות יוצרים.
6. 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.
7. המענה לפנייה יהיה בהיקף כולל של עד 50 עמודים המציגים את המענה. בנוסף על כך ניתן לצרף נספחים ומפרטים טכניים ללא הגבלת היקף.
8. במסגרת המענה יש להתייחס להיבטים הבאים:
 - א. אופן העמידה של המערכת ביעדים ובמטרות לעיל.
 - ב. אופן העמידה של המערכת באיפיון העל שתואר לעיל.
 - ג. ניסיון מבצעי של המערכת בישראל ובעולם.
 - ד. ניסיון מבצעי של המציע.
 - ה. תוכנית הפיתוח של המערכת.
 - ו. אינטראופרוביליות של הפתרון למול מערכות קיימות.
 - ז. תמיכה ותחזוקה.
 - ח. היבטים כלכליים.
9. מסמכי הבקשה לקבלת מידע זמינים 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>.
10. מענים/הצעות לבקשה לקבלת מידע יש להגיש בעותק דיגיטלי עד לתאריך 15.04.18 בשעה 14:00. יש לתאם את הגשת המענה עם גבי שירלי היגאני בדואר אלקטרוני cyber-michrazim@pmo.gov.il טלפון: 03-7450854, 03-7450883 (להלן: " איש הקשר"). על הפונה לוודא קבלת מסמכי המערך.
11. בראש המענה ירשם: " פניה מוקדמת לקבלת מידע (RFI) למערכת מבוססת סנסורים מבוזרים להגנה לאומית מפני איומי סייבר עבור מערך הסייבר הלאומי".
12. ספק המעוניין להגיש מענה כאמור יציג תשובה למענה המתייחסת לסעיפים המופיעים לעיל.



13. ספקים רשאים להפנות את שאלותיהם לאיש הקשר עד ליום 25.03.18 בשעה 12:00. על הספק לוודא ששאלותיו הגיעו בשלמות לאיש הקשר.
14. מענה לשאלות והבהרות יינתן עד תאריך 29.03.18 על ידי המערך באמצעות העברה לאיש הקשר בחברה.
15. למען הסר ספק, מובהר בזאת כי שאלות הבהרה ותשובות שיינתנו להן עד למועד הקבוע לכך בסעיף 14 לעיל, יפורסמו באתר האינטרנט של מנהל הרכש הממשלתי ובאתר האינטרנט של מערך הסייבר הלאומי, בכתובות המפורטות בסעיף 9 לעיל.

א. פרטי הספק בטבלה הבאה:

מס"ד	המידע המבוקש	המענה
1	שם הספק	
2	כתובת הספק	
3	מס' טלפון	
4	מס' פקס	
5	שם איש הקשר לבקשה	
6	מס' טלפון של איש הקשר	
7	כתובת דואר אלקטרוני של איש הקשר	

הצגה פרונטלית של המענה ובדיקות התכנות של המענה

לאחר בחינת המענים, המזמין שומר לעצמו את הזכות להזמין את כל מי שנענה לפניה זו להציג את השירותים בפני צוות מקצועי מטעמו במיקום ובמועד שיקבע המזמין.

במסגרת הצגת המענה, נדרש להתייחס לכל המתואר במסגרת פניה זו. ולשאלות שיוצגו על ידי הצוות המקצועי מטעם המזמין.

כמו כן, במידת הצורך, המזמין שומר לעצמו את הזכות לבצע בדיקות התכנות (POC) של השירותים באתר הלקוח (המזמינים) לתקופה של עד כשלושה חודשים לצורך בדיקות התאמת השירותים לדרישות הפונקציונליות.