משרד ראש הממשלה
מערך הסייבר הלאומי

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

29 מרץ 2018
יג' ניסן תשע"ח

הנדון: <u>מענה לשאלות הבהרה - בנוגע לפניה מוקדמת של מערך הסייבר הלאומי לקבלת מידע למערכת סנסורים מבוזרים להגנה לאומית מפני איומי סייבר</u>

1. בהמשך לפניה המוקדמת של מערך הסייבר הלאומי, לקבלת מידע בנוגע לנושא שבנדון, להלן מענה לשאלות הבהרה שהוגשו:

מס'	סעיף	שאלות הבהרה	מענה לשאלות ההבהרה
1	יעדים ומטרות סילוק איומי סייבר (תת סעיף 1)	איך מתבצעת התקשורת בין מטה הסייבר לאתרי היעד?	התקשורת בין מערכת הבית לסנסורים באתרי היעד תבוצע בערוץ Out of Band מוצפן מסחרית.
2		מה ההגדרה של אתר יעד (ארגון ממשלתי, אתר אינטרנט וכו')?	אתר יעד הינו רשת IT של ארגון כלשהו בישראל, ממשלתי או אחר. נפח התעבורה יכול לנוע בין מגות בודדות למאות מגות ביט לשניה.
3		מהם הערוצים (דואר, גלישה וכו') בהם נדרשת ההגנה?	ההגנה נדרשת ברמת כלל פרוטוקולי התקשורת הסטנדרטיים של רשת IT.
4		האם הפתרון לאתרי היעד מיועד גם לסביבה הפנימית שלו או רק ליציאה ל – WAN?	כפי שמצוין ב-RFI, הפתרון מיועד לאזור שמחוץ לפרימטר של הארגון, ולא לסביבה הפנימית.
5		האם נדרשת פתיחה של תעבורה מוצפנת?	לא.
6	אפיון על של המערכת, תת סעיף 7	למה נדרש לעשות rollback (מדיניות, חוקה הגדרות)?	נדרשת יכולת Rollback לטובת התמודדות עם מקרים של תקלות, שבהן נרצה לשחזר תצורה קודמת של הגדרות ו/או חוקה ו/או מדיניות.
7	אפיון על של המערכת, כללי	האם ניתן לשלב שני מוצרים על מנת לענות על המענה?	אין מניעה, אולם יש לשים לב שהסנסורים יותקנו באתרים של צד ג' ולכן יש חשיבות רבה ל"חתימה" נמוכה (Footprint).
8	אפיון על של המערכת, סעיף 4	בנוגע לדרישה לגמישות ברמת יכולת מערך הסייבר הלאומי לשלב בסנסור קוד/רכיב תוכנה, הן מוצר צד ג' והן פיתוח ייעודי של המערך, כחלק ממימוש תפיסת הניטור - האם הכוונה להתקנה על המוצר המוצע? או התממשקות של תוכנה צד ג' ל-API של המוצר המוצע?	הכוונה לייצר יכולת להריץ/לממשק כלי תוכנה חיצוניים, בין עם מסחריים או כאלה שנכתבו ע"י מערך הסייבר, **כחלק מהסנסור** שיושב באתר (ראו גם את תשובתנו לשאלה מס' 7).
9	אפיון על של המערכת, סעיף 8	בנוגע לדרישה ליכולת ליצור הודעה שיקבל משתמש בגוף המנוטר, כאשר הסנסור חוסם תעבורה כלשהי שרלוונטית אליו - האם התעבורה הרלוונטית מנותבת גם ע"י	ההודעות תועברנה לצוות אבטחת המידע של הגוף באמצעות התרעה למערכת ה-SIEM/SOC של הארגון ו/או באמצעות מערכת שיתוף מידע של מערך הסייבר הלאומי.

מס'	סעיף	שאלות הבהרה	מענה לשאלות ההבהרה
		Proxy ו-Mail Relay?	

בברכה,

כפיר ישראל
רמ"ח סנסורים וכלים
מערך הסייבר הלאומי