****

**משרד הביטחון**

**קול קורא**

**ענף טכנולוגיות סייבר במינהל למחקר ופיתוח אמצעי לחימה ותשתיות טכנולוגיות (מפא"ת) מזמין בזאת מוסדות מחקר, חברות וגופים טכנולוגיים להגיש הצעות ורעיונות למחקר ופיתוח שיתרמו לנושאי הסייבר הבאים:**

1. **וירטואליזציה מאובטחת**
2. **הפרדת סביבות**
3. **Trusted computing**
4. **אימות פורמאלי של לוגיקה/קוד בהיבטי אבטחת מידע (verification)**
5. **פיתוח מאובטח – מתודולוגיות וטכנולוגיות (כלליות) להגברת החוסן של מערכות IT, מחקרים ממוקדים בטכניקות וטכנולוגיות להטמעה מאובטחת של טכנולוגיות נפוצות**
6. **ערפול קוד, חיסון קוד**
7. **ניתוח קוד אוטומטי למציאת חולשות/פגיעויות**
8. **ייצור מאגרי נתונים (datasets) לצורכי בדיקות אבטחה, עיבוד וניתוח**
9. **הגנה על ציוד רשת/תקשורת**
10. **הגנה על מערכות משובצות מחשב (embedded systems)**
11. **הגנה על מערכות סקאדה**
12. **הגנה על רשתות מידע אלחוטיות**
13. **יכולת התאוששות מהירה לאחר פגיעה**
14. **אבטחת קישוריות בין רשתות, יכולות העברת קבצים, מסמכים ומידע באופן ממוכן ובטוח בין גופים ורשתות בסיווגים שונים**
15. **טכנולוגיות privacy לאבטחה ומניעת דלף מידע**
16. **יכולת לבצע פעולות בדיקה ממוכנות על מידע מבלי לפגוע בפרטיות המידע**
17. **הצפנה הומומורפית**
18. **הגנה פרו-אקטיבית**
19. **אבטחה בחומרה (כגון TPM וכו')**
20. **בדיקת חדירות רשת/מערכת באופן אוטומטי, בדיקה אוטומטית של מערכות גילוי והגנה**
21. **יכולות טכנולוגיות להתמודדות עם הנדסה חברתית**
22. **יכולות לבדיקה, תרגול ואימון של גופי הגנה, מנטרים וחוקרים. כלים להגברת מודעות משתמשים**
23. **סימולציה של רשתות למטרות הגנה, סימולציה של פעילות משתמש, "משתמש אוטומטי"**
24. **שמירה על זמינות מידע**
25. **אמצעי שליטה, בקרה והכלת אירועים**
26. **השמדת מידע ומחיקת מידע באופן מאובטח (באופן שלא ניתן לשחזור)**
27. **Watermarking**
28. **זיהוי סטגנוגרפיה**
29. **כלי סינון תעבורת רשת וקבצים**
30. **חקירה אוטומטית של מדיה דיגיטלית וקבצים למציאת פוגענים וסימני תקיפה**
31. **אנליזה אוטומטית של זיכרון המחשב למציאת פוגענים וסימני תקיפה**
32. **"צילום" / העתקת זיכרון המחשב (RAM) באופן אוטנטי וברמת סמך גבוהה**
33. **יכולות קטלוג אוטומטי של פוגענים למשפחות וקבוצות דומות**
34. **התגוננות מפני פוגענים ברמת firmware**
35. **ניצול/שימוש ביכולות וטכניקות התקפיות למטרות הגנתיות**
36. **זיהוי התנהגות משתמשים חשודה, התנהגות המצביעה על כוונות עוינות (כגון ריגול)**
37. **יכולת חיסון אוטומטית בהינתן חולשה או פוגען**
38. **יכולת הכלה וטיהור אוטומטית בהינתן פוגען**
39. **יכולת ממוכנת למציאת קשרים והסקת תובנות מתקדמות בהינתן מידע על תוקפים/תקיפות (מודיעין, ממצאי חקירות, תעבורות מוקלטות, אתרים עוינים, קצות חוט, הפוגענים עצמם וכו')**
40. **יכולות ניתוח לוגים**
41. **מעקב אחר פעולות בהרשאות גבוהות**
42. **הונאת התוקף**
43. **יכולות גילוי והתראה מוקדמים בשלב איסוף המידע לפני תקיפה**
44. **גילוי תקיפות והתמודדות עם דואר אלקטרוני וצרופות**
45. **גילוי תקיפות בגלישה לאתרים (אתרים/לינקים עוינים)**
46. **גילוי והתמודדות עם איומי man in the middle בתעבורה**
47. **מערכות ניטור ארגוניות להתמודדות עם APT**
48. **התמודדות עם תקיפות וחולשות לא מוכרות (zero day)**
49. **Honeypots, רעיונות למלכודות ופיתיונות עבור תוקפים**
50. **גילוי והתמודדות עם תקיפות על smartphones**
51. **גילוי והתמודדות עם דלף מידע**
52. **יישום anomaly detection לצורכי הגנה, לזיהוי קוד עוין בתקשורת ובתחנות הקצה**
53. **זיהוי והתמודדות עם שיטות תקיפה המנצלות טכנולוגיות הסתרה, קידוד, התממה והצפנה למניעת גילוי**
54. **זיהוי מקורות תקיפה**
55. **זיהוי וניתוח פעילות ממוחשבת שמקורה במשתמשים לעומת מכונה (הבדלה בין התנהגות אנושית ל-"רובוטית")**
56. **גילוי והתמודדות עם ערוצי צד המשמשים לתקיפה**
57. **זיהוי הטמנות בתוכנה**
58. **זיהוי הטמנות בחומרה, זיהוי משדרים**
59. **זיכוי חומרה**
60. **אמצעי אבטחת שרשרת אספקה**
61. **טכנולוגיות ויכולות שיתוף מידע בין ארגונים שמאפשרות סטנדרטיזציה, שיתוף מידע אבטחתי ערכי ואנונימיזציה של מידע רגיש**
62. **רעיונות והצעות נוספות בתחום הסייבר**

ההצעה נדרשת לכלול תכולות מחקר ו/או פיתוח המבוסס על רעיון יצירתי/מקורי המספק מענה לאחד מהנושאים שצוינו לעיל. יש לוודא שאין מחקר או מוצר קיים המתבסס על אותו רעיון. רעיון יכול להתבסס על מוצרים קיימים בתנאי שעצם הרעיון הוא שימוש ייחודי/מקורי במוצרים או ביכולות קיימות כדי לספק מענה יצירתי/חדשני לאחד הנושאים המוזכרים לעיל.

ליצירת קשר ראשוני נא לשלוח את הטופס המצורף לכתובת הדוא"ל:
[Mafat\_cyber@mod.gov.il](http://www.removed.url)
או להשאיר הודעה בטלפון 03-6975358
יש להשאיר פרטי איש קשר (שם, טלפונים וכתובות דוא"ל) וכן את פרטי הגוף הפונה

**ההצעות הרלוונטיות יזכו למימון בהתאם לצרכי המשרד**

**קדימות תינתן לפניות שיוגשו עד לתאריך 30/04/2013**

**טופס פנייה להגשת הצעות**

|  |  |
| --- | --- |
| גוף פונה |  |
| שם איש קשר |  |
| תפקיד |  |
| כתובת דוא"ל |  |
| טלפון 1 |  |
| טלפון 2 |  |
| מהות הנושא (במשפט) |  |