



WHITE - HAT LTD

PROACTIVE CYBER INTELLIGENCE & THREAT HUNTING

הצעת מחיר

לביצוע סקר אבטחת מידע,
בדיקות קונפיגורציה
ומבדק חדירה

במשרד המשפטים



לכבוד,

מר חן מיכאלי - חב' ליאקום

הנדון: הצעת מחיר לביצוע סקר אבטחת מידע בדיקות קונפיגורציה ובדיקות חדירה למערכת טלפוניה במשרד המשפטים

שלום רב,

1. כללי

במסגרת היות חברת כובע לבן ספק שירותי ייעוץ אבטחת מידע והגנת סייבר במשרד המשפטים, ובהמשך לפנייתכם ולבקשתכם, אנו מתכבדים להגיש הצעת מחיר לחברת ליאקום, לביצוע סקר אבטחת מידע, בדיקות קונפיגורציה ובדיקות חדירה למערכת טלפוניה במשרד המשפטים.

2. אודות החברה

חברת כובע לבן בע"מ הינה חברת סייבר אזרחית, מובילה וייחודית, נוסדה ב – 2013, ממוקמת במרכז תל אביב ומעסיקה למעלה מ - 70 מומחים מהשורה הראשונה, בתחומי אבטחת המידע והגנת הסייבר השונים.

החברה מעניקה ללקוחותיה מענה הגנתי מקיף, הכולל שירותי ייעוץ בתחומים שונים ומגוונים - החל משירותי ניהול סיכונים, סקרי אבטחת מידע, לוח טכנולוגי אסטרטגי במדיניות ונוהלי אבטחת מידע ארגוניים, מענה לרגולציה והסמכות לתקני אבטחת מידע, בדיקות חדירות (Penetration Test), איסוף מודיעין סייבר איכותי, ניתוח, עיבוד ומחקר המידע, מתן מענה לאירועי סייבר (Incident Response), פיתוח מתודולוגיות תקיפה לצרכי הגנה וטיפול מערכות ההגנה של לקוחות החברה. לחברה דסק סייבר המאויש 24/7, ע"י האקרים מומחים, הפועלים אקטיבית לטובת איסוף מידע איכותי, שעיקרו רובו ממוקד ולא מידע ממקורות Open source. בשירותיה בישראל, חברת כובע לבן בע"מ הינה חברה ייחודית, נתון אשר בא לידי ביטוי בעצם תפישת ומתודולוגיית ההגנה שלה - "האקרים כנגד האקרים".

תפישה Proactive Cyber Defense הינה אחת מהתמחויות החברה ומספקת ללקוחותיה שירותי Cyber Intelligence and Threat Hunting.

לעובדי החברה ומנהליה, אשר רבים מהם יוצאי היחידות הטכנולוגיות בצבא, ניסיון מודיעיני מחד והתקפי מאידך והיא מנצלת ידע זה לטובת הגנה וטיפול בסוגיות סייבר, אשר אינן מקבלות מענה בשיטות ההגנה הקלאסיות בעולם אבטחת המידע, שהרי, מוצרי אבטחת מידע לבדם, אינם מספקים מענה הולם לדינמיות ההולכת וגוברת של ההתקפות הנהוגות היום ובוודאי לא לקראת המחר, פתרונות אבטחת מידע לבדם מספקות מענה לאירועים שהיו נכונים לפני כ - 8 שנים ומעלה. שירותי הסייבר של WHITE-HAT מאפשרים לארגונים להתגונן פרואקטיבית במגוון תחומים שונים ולזהות את פוטנציאל הנזק עוד בהתהוותו.

3. רשימה חלקית של ארגונים, שותפים לדרך:

התפישה החדשנית והמתקדמת הביאו את החברה לביצוע מוצלח במגוון רחב מאוד של פרויקטים



מורכבים בתחום אבטחת מידע המסורתי והגנת סייבר מתקדמת וייחודית, בארגונים גדולים, בארץ ובעולם:

- **משרדי וגופי הממשלה:** משרד המשפטים, משרד הבריאות, משרד החקלאות - באמצעות מערך הסייבר הלאומי, רשות מקרקעי ישראל, רשות האוכלוסין וההגירה, משרד התקשורת, משרד התחבורה, מינהל התכנון, המשרד לביטחון פנים.
- **בנקאות:** בנק הפועלים, בנק לאומי, בנק דיסקונט, הבנק הבינלאומי, בנק מזרחי, בנק ירושלים.
- **חברות ביטוח, שוק ההון וקופות חולים:** הראל, הפניקס, מנורה, מגדל, כלל ביטוח, איילון, ביטוח ישיר, שלמה ביטוח, הכשרה-חברה לביטוח, AIG, אלטשולר שחם, מכבי שירותי בריאות.
- **חברות אשראי:** ויזה כאל, ישראלכרט, MAX.
- **הייטק ותעשייה:** אל-על, תעשיה אווירית, איילקס מדיקל, Playtech, My Heritage, כייל, FOX, ועוד.

4. רקע אודות המערכת

- 4.1. למשרד המשפטים יש מערכת טלפוניה של CISCO (נקראת שירליו). המערכת מותקנת במשרד 3 שנים. לפני שנתיים בוצע מבדק חוסן.
- 4.2. מרכזייה אחת (כמה שרתים), יש הקלטת שיחות רק במוקד, יש IVR אחד שיושב בכניסה, VOIPים, פקסים, webex, Jabber (SoftPhone על המחשבים) שרתי ניהול שלוחות, דוחות, מזכירה וכו'.
- 4.3. לא קיים SBC מול השרתים הפנימיים.
- 4.4. לא פתוחים בפרוטוקולי SIP ו-VOIP.
- 4.5. הפערים שנמצאו אמורים היו להיות מטופלים. המשרד מעוניין לבצע חוזר ולראות שהמצאים אכן תוקנו וכן לבדוק סעיפים נוספים.

5. תכולת הפעילות

- 5.1. סקר אבטחת מידע על המרכזייה.
- 5.2. ביצוע בדיקות קונפיגורציה לרכיבי המרכזייה (IVR, VOIP, Webex, Jabber, פנקודים, פקסים) ומיסקונפיגורציות של הרכיבים השונים.
- 5.3. עקיפת תפריטים, פתיחת תפריטי טכנאי וכו'.
- 5.4. תקיפת רכיב IVR.
- 5.5. ניסיון ביצוע Dial In לחדרי ישיבות מטלפונים חיצוניים.
- 5.6. ניסיון תקיפה בתוך הרשת - התחזות לטלפון לטובת גישה לרשת טלפוניה וביצוע האזנות, ניסיון גישה לממשקי ניהול.
- 5.7. מימוש פגיעויות של TFTP (משיכת קבצי קונפיגורציה משרתי מרכזייה, קריאה של תא קולי).
- 5.8. האזנה מתוך המחשב לתעבורה (דרך SpftPhone).



6. כ"א

6.1. חברת WHITE-HAT תעמיד את מר עידן קרן, סמנכ"ל פרויקטים כמנהל הפעילות. לעידן ניסיון ניהולי ומקצועי רב, בארגונים גדולים ומורכבים, כמנהל אבטחת מידע, כיועץ ומנהל סקרים על סוגיהם, לרבות סקרי סיכונים ומבדקי חדירה. לעידן ידע וניסיון רב שנים בהיבטי הרגולציה. עידן יהווה עבורכם SINGLE POINT OF CONTACT לכל תחומי הפעילות.

6.2. לטובת הפעילות, יוקצו מומחי אבטחת מידע מטעם חברת WHITE-HAT, מומחים בעלי ידע וניסיון בביצוע סקרי אבטחת מידע אפליקטיביים ותשתיתיים, בארגונים גדולים מאוד. היועצים מבצעים את הסקרים לפי מתודולוגיות ממוסדות ומתוקפות עפ"י דרישת הלקוח, כשאיכות התוצר עומדת לנגד עיניהם, יחד עם עמידה בלוח"זים נדרשים ודרישות הארגון. למותר לציין כי מאחורי ביצוע משימותיהם עומד מנהל הפעילות וידע וניסיון מצטבר של החברה בפעילויות דומות בארגונים בעלי מאפיינים טכנולוגיים תשתיתיים ואפליקטיביים, דומים למשרד המשפטים.

6.3. איש קשר:

כאיש קשר, חברת כובע לבן תעמיד לרשותכם, את עמית הרטמן, סמנכ"ל שיווק ומכירות, אשר יעמוד לרשות המשרד בכל דבר ועניין, מקצועי-טכנולוגי ושירותי כאחד.

7. להלן פירוט השעות שתידרשנה לביצוע הפעילות בחלוקה למשימות:

המשימה	כמות שעות למומחה מנוסה	כמות שעות למומחה בכיר
סקר אבטחת מידע	100	10
בדיקת קונפיגורציה	130	10
מבדק חדירה	130	10
מעבר על דו"ח עבר (עד 10 ממצאים)	25	
סה"כ שעות	385	30



8. עלות

- 8.1. בעבור ביצוע כלל הפעילות המפורטת, **תהא העלות 91,500 ₪.**
- 8.2. לעלות יתוסף מע"מ כחוק.
- 8.3. החיוב יבוצע עם הגשת טיוטת דו"ח מסכס.
- 8.4. תנאי התשלום: ש + 30.
- 8.5. תוקף ההצעה: 30 ימים מיום הוצאתה.

9. לסיכום:

אנחנו משוכנעים, כי היחודיות והמאפיינים הטכנולוגיים של חברת "כובע לבן", בשילוב עם הניסיון הנצבר, ההיכרות המעמיקה את משרד המשפטים, על ליבת העשייה שלו, מנהליו ועובדיו, שיתוף הפעולה בשנים האחרונות, האמון המקצועי ובעיקר המשאב האנושי הייחודי, יסייעו לביצוע איכותי של המשימה.

נשמח לסייע בכל שאלה ולהמשיך לשתף פעולה עם משרד המשפטים,

בכבוד רב,

עמית הרטמן, סמנכ"ל שיווק ומכירות
נייד: 054-6749462
כובע לבן בע"מ