מכרז מספר : 97945 בינמשרדי

מס' המשרה : 81119532
תואר המשרה : מנהל/ת יחידת סייבר מגזר התקשורת 1 - משרות.
היחידה : משנה למנכ"ל ומנהל מינהל הנדסה
המקום : תל אביב - יפו
המשרד : משרד התקשורת
הדרגה : דרגה 41 - 43 דירוג 11 מח"ר או
דרגה 41 - 43 דירוג 12 מהנדסים.
חלקיות : 100 אחוז

תאור התפקיד :
אחריות כוללת לניהול הגנת הסייבר במגזר התקשורת בסביבה הרשתית (סב"ר).
גיבוש, אפיון ומימוש תפיסות, שיטות, מתודולוגיות, מדיניות ונהלים להגנת הסייבר במגזר.
הובלה וגיבוש של הוראות לאסדרה ותקינה בתחום הסייבר במגזר.
הובלת ובקרת תהליכים של ניהול סיכונים בהגנת הסייבר במגזר.
הובלה ואחריות על תהליכי הנחיה וסיוע בביצוע פיקוח, בקרה ואכיפת המדיניות בתחום הגנת הסייבר.
הגדרת המתודולוגיות והתהליכים הארגוניים להגנה על בסב"ר.
אחריות להקמה, עיצוב ושדרוג מרכז קברניטי המגזרי (מק"מ / SOC) על מנת לאפשר ביצוע בקרה, פיקוח ואכיפה יעילה.
פיתוח מתודולוגיות וטכנולוגיות לתפעול הגנת הסייבר במערכות המק"מ.
אחריות לקיום תחזוקה שוטפת של מערכות הגנת הסייבר במק"מ.
אחריות לקיום תהליך הזנת מקורות ידע טכנולוגי ותפעולי למערכות המק"מ.
הובלת תהליך מיצוי מידע וגיבוש תמונת מצב לאומית במערכות המק"מ.
אבטחת שרשרת האספקה, המשכיות עסקית, התאוששות מאסון וניתוח השפעות עסקיות על המגזר.
גיבוש תוכנית עבודה שנתית בתחום הגנת הסייבר המגזרית.
ניהול צוות העובדים (בתחום ההנחיה, מעבדה וכו'), וניהול מקצועי של צוות המק"מ .
ביצוע פעולות נוספות בהתאם לצורך ובהתאם לדרישת הממונה.
דרישות המשרה:
דרישות סף:
****
השכלה:

השכלה אקדמית (תואר ראשון) בתחומים הבאים (תחום מקצועי עיקרי/ משני/ התמחות/שילוב בין תארים): מדעי המחשב / מערכות מידע / הנדסת תוכנה / הנדסת

מחשבים/הנדסת אלקטרוניקה / הנדסת תקשורת / הנדסת תעשיה וניהול/מתמטיקה/הנדסת חשמל/פיסיקה.

או

תואר אקדמי אחר ובנוסף תואר שני במינהל עסקים עם התמחות במערכות מידע או תואר שני בניהול טכנולוגיית המידע.

או

תואר אקדמי אחר או הנדסאי/ת טכנאי/ת מוסמכ/ת (רצוי בוגר/ת מגמת מחשבים/ טכנולוגיה) ובנוסף, הכשרות/ הסמכות* מקצועיות בהגנת סייבר בהיקף משמעותי (300 שעות במצטבר) שיוכרו על ידי מערך הסייבר הלאומי.

או

בוגר/ת יחידה טכנולוגית בצה"ל (ממר"ם, 8200 , תקשוב ויחידות מקבילות) ו/או בראמ"ם/ ו/ או במערך הסייבר הלאומי ובלבד שקיבל/ה הסמכה בקורס ייעודי בתחום הסייבר ועסק/ה בתחום הסייבר במשך שנתיים לפחות.

ניסיון:

בעלי/ות תואר ראשון או בוגר/ת יחידה טכנולוגית - 5 שנות ניסיון*

לבעלי/ות תואר שני - 4 שנות ניסיון*

***נדרש ניסיון בלפחות ארבעה תחומים או יותר מבין התחומים הבאים, כאשר חובה שאחד מהם יהיה ניסיון בסעיפים 1 או 2:**

1. ניסיון בתקינה ואסדרה ישראלית ובין-לאומית בנושאי הגנת סייבר ואבטחת מידע, כגון: סדרת ISO 27000, , PCI DSS, SOX באזל, סדרת 800 של NIST, ISO IEC 62443 ,31000 ,HIPAA הוראות רגולטוריות בתחום הגנת הסייבר.

2. ניסיון מוכח בתחום ה- GRC (Governance, Risk management and Compliance):

א. ממשל הגנת סייבר (Governance) – ניהול הגנת סייבר ברמת הארגון, מבנים ארגוניים תומכים, מימוש מדיניות הגנת סייבר ארגונית, בעלי תפקידים, תקצוב, שליטה ובקרה ארגונית, הקצאת משאבים, מחויבות הנהלה ודירקטוריון.

ב. ניהול סיכונים (Risk management) – מתודולוגיות ניהול סיכונים (כגון מתודולוגיית COSO), סוגי סיכונים, זיהוי הסיכונים, ניתוח הסיכונים, השפעת הסיכונים על הארגון, דרכי התמודדות, סיכונים שיוריים.

ג. תאימות (Compliance) – תאימות לדרישות חוק, רגולציה, תקינה, חוזים, מדיניות ונהלים ארגוניים, דרישות פנים ארגוניות וחוץ ארגוניות (כגון דרישות לקוח).

3. ניסיון בעבודה ע"פ תפיסות וגישות בהגנת סייבר: מעגלי הגנה, Defense in Depth (DiD), No single point of failure, Least privilege, Need to know

הלימה בין רמת הגנה לרמת סיווג (כולל אבחנה בין סיווג למידור), מימוש בקרות מפצות כמנגנון משלים.

4. ניסיון בליווי הקמה/ הפעלה/ תחזוקה מערכת הגנת סייבר ארגונית בסביבה הרשתית: הגדרת
היעדים, הגדרת נכסי המידע / המערכות החיוניות, זיהוי וניהול הסיכונים, הגדרת תהליכי טיפול ומניעה, הגדרת ובחירת הבקרות הנדרשות, מיקוד בתהליכי עבודה אפקטיביים, שילוב ההגנה כחלק מהתהליכים הארגוניים, הנעת תהליכי לימוד, הפקת לקחים ושיפור.

5. ניסיון בביצוע ביקורת (security monitoring) בתחום הגנת סייבר בסביבה הרשתית:
בקרות טכנולוגיות ומתודולוגיות נדרשות, וכן הכנת וליווי ארגונים למבדקי תאימות לתקינה.

6. ניסיון בתכנון מענה טכנולוגי תשתיתי וארכיטקטורה להגנת סייבר בסביבה רשתית.

7. ניסיון בעבודה על מוצרי הגנה בסביבה הרשתית והשוואה בין מוצרים.

כישורים ונתונים רצויים:

==========

ניסיון בליווי פרויקטים בהיבטי הגנת סייבר: שילוב נושאי ההגנה במכלול מחזור החיים של מערכות ממוחשבות (SDLC).
ניסיון והכרות טכנולוגית ורגולטורית עם מגזר התקשורת נייח, נייד, ISP.
ניסיון באבטחת מרכיבי שרשרת האספקה.
ניסיון עם תהליכים בהמשכיות עסקית (BCP), התאוששות מאסון (DRP) וניתוח השפעות עסקיות (BIA).
היכרות בסיסית של שיטות ותהליכים לפיתוח קוד מאובטח (Secure Coding).
היכרות בסיסית ומושגים ב forensics
היכרות בסיסית עם תהליכי מודיעין סייבר
ידיעת השפה האנגלית כדי קריאת חומר מקצועי
היכרות עם תחום התקשוב הממשלתי / ציבורי
יכולת גבוהה בפיתוח קשרים בינאישיים ובעל/ת כושר שכנוע/ כריזמטיות
כושר למידה עצמית וכושר ביטוי בכתב ובע"פ.
תודעת שירות גבוהה, אסרטיביות, עצמאות, יכולת עמידה מול קהל.

הערה:

=====

****ניתן להתייחס לניסיון גם לפני קבלת התואר.**
*****בהתאם לחוק ההנדסאים והטכנאים המוסמכים, התשע"ג - 2012, ובתיאום בין נציבות שירות המדינה לבין הארגון היציג של הסתדרות ההנדסאים והטכנאים, הנדסאי/ת או טכנאי/ת מוסמכ/ת, הרשומ/ה בפנקס ההנדסאים והטכנאים המוסמכים, רשאי/ת להתמודד במכרזים בדירוג האקדמאים בהם נקבעה דרישה להשכלה אקדמית כללית.**
במקרה זה הניסיון הנדרש מטכנאי/ת מוסמכ/ת הוא של 7 שנים בתחומים המפורטים

לעיל, ומהנדסאי/ת של 6 שנים בתחומים המפורטים לעיל.
בעל תעודת הנדסאי/ת או טכנאי/ת מוסמכ/ת אשר ייבחר למשרה ידורג בדירוג המנהלי.
עובד/ת מתוך שירות המדינה אשר דורג/ה זה מכבר בדירוג ההנדסאים או הטכנאים רשאי/ת לשמר את דירוגו/ה המקצועי.
נדרש סיווג בטחוני סודי ביותר.

הערות:

יוער כי בהתאם להחלטת ממשלה מספר 1661 מיום 13.05.2007 ותחיקונה בהחלטה מספר 1605 מיום 18.05.2014, יש לבצע מעבר של היחידות הארציות של משרדי הממשלה לעיר ירושלים עד לחודש מאי 2008.
כל מקום בו מפורט תאור התפקיד בלשון זכר,הכוונה גם ללשון נקבה וכן להפך מועמדים למשרה זו עשויים להיבחן במבחני כישורים כלליים והתנהגותיים.
ראה/י הסברים והנחיות למועמדים שייבחנו .
המכרז הבין-משרדי מיועד לעובדי מדינה שהתמנו לשירות כדין לפי חוק המינויים.
עובד המגיש מועמדות למכרז בין-משרדי יצרף לבקשה אישור זכאות להשתתף במכרז בין-משרדי ושתי הערכות עובד תקופתיות של השנתיים האחרונות.
במידה שלא בוצעו הערכות עובד יש לצרף אישור על כך מאגף משאבי אנוש במשרד.
המכרז פורסם ביום : י' באייר, תשפ"ב (11/05/2022)
היום האחרון להגשת בקשות למכרז זה הוא : כד' באייר, תשפ"ב (25/05/2022)

בקשות למכרז זה יש להגיש באמצעות מערכת הגיוס האלקטרונית (הגשת מועמדות שאינה מקוונת תתאפשר במקרים חריגים ובהתאם לכללים שנקבעו-במקרה זה יש להגיש המועמדות והטפסים הנלווים למשרד הרלוונטי.)

על המועמדים המגישים בקשה יש למלא את טופס" שאלון המועמד "המקוון ולצרף תעודות השכלה ממוסד להשכלה גבוהה המוכר על ידי המועצה להשכלה גבוהה או המקביל לה בארץ בה נרכש ואושר כשקול לתואר מהתארים האקדמיים הנהוגים בישראל על ידי האגף להערכת תארים מחו"ל ,כל זאת על פי דרישות ההשכלה הנדרשות במכרז.

בנוסף יש להמציא העתקים מאושרים ומסמכים הדרושים לאימות הפרטים שנרשמו בטופס" שאלון המועמד "המקוון ,כולל אישורי העסקה ממקומות עבודה קודמים הרלוונטיים לתפקיד המבוקש תוך ציון של היקף המשרה ותיאור תמציתי של תוכן התפקיד וכן על כל עניין הקשור בהתאמה למשרה.

במידה ונשלחה דרישה להמצאת מסמכים נוספים הרי שהמועמדות תיבדק רק אם יתקבלו המסמכים תוך 5 ימים מתאריך הוצאת המכתב ובו בקשה להשלמת מסמכים חסרים ,אחרת תראה המועמדות כמבוטלת.

בקשות שתגענה לאחר התאריך האמור לא תובאנה בחשבון.

במידה ותוך שבועיים מהמועד האחרון להגשת מועמדות לא קבלת הודעה על המשך ההליכים במכרז עליך לפנות למרכז השירות האינטרנטי באמצעות מערכת הגיוס האלקטרונית.