אאוץ! פברואר 2022

עלון המודעות החודשי לביטחון עבורך

כל אחד יכול להתחיל קריירה בתחום אבטחת סייבר

סקירה כללית

אנו קוראים על אירועי סייבר בחדשות כמעט כל יום כאשר ארגונים וממשלות ברחבי העולם ממשיכים להיפגע מתוכנות כופר, הונאות והתקפות סייבר. יש ביקוש עצום לאנשים שהוכשרו באבטחת מידע וסייבר כדי לסייע בהגנה מפני האיומים ההולכים וגדלים. למעשה, מחקרים עדכניים מעריכים כי יש כמעט 3 מיליון משרות פנויות בתחום אבטחת סייבר ברחבי העולם.

האם שקלת קריירה כמומחה אבטחת מידע וסייבר? זהו תחום מהיר ודינאמי עם מספר עצום של התמחויות מעניינות לבחירה. תפקידים אלה כוללים תחומים כמו חקירת ראיות, מודעות והדרכה, אבטחת תחנות משתמשים, תשתית קריטית, תגובה לאירועים, כתיבת קוד מאובטח ומדיניות. קריירה בתחום אבטחת סייבר מאפשרת לך לעבוד כמעט בכל מקום בעולם, עם מגוון הטבות והזדמנות לחולל שינוי אמיתי.

האם אני צריך תואר במדעי המחשב?

בהחלט לא. לרבים מאנשי המקצוע הטובים ביותר בתחום אבטחת המידע יש רקע לא טכני. המפתח הוא תשוקה ללמוד; ברגע שאתה מבין איך טכנולוגיות עובדות (ונפרצות), אתה יכול לאבטח אותן טוב יותר. אבטחת מידע וסייבר כל כך מרגשת כי אתה יכול להתחיל ללמוד בקצב שלך, בנוחות שלך וסביבה הביתית שלך.

איך אני מתחיל?

התחל לחקור נושאים שונים כדי לגלות את תחומי העניין שלך. לעתים קרובות אתה יכול להתחיל רק עם המחשבים או המכשירים שיש לך בבית.

- **קוד**: למד את היסודות של תכנות. **Python, HTML** או **JavaScript** הם כולם שפות טובות להתחיל. תשקול שימוש באתר הדרכה מקוון או תשיג ספר תכנות למתחילים.
- **תשתיות**: למד את היסודות של ניהול מערכת הפעלה, כגון לינוקס או חלונות. אם אתה באמת רוצה להתבלט, התמחה בשימוש בממשק שורת הפקודה (**CLI**) וסקריפטים.
- **אפליקציות**: למד כיצד להגדיר, להפעיל ולתחזק יישומים, כגון שרתי אינטרנט.
- **תקשורת**: גלה כיצד מחשבים ומכשירים מדברים זה עם זה על ידי לכידה וניתוח של תעבורת רשת. זה יכול להיות כיף גדול מכיוון שהבית שלך הוא ככל הנראה כבר סביבה מרושתת עם כל מיני מכשירים המחוברים אליו.
- **טכנולוגיות ענן**: למד כיצד פועלים שירותי ענן והדרכים השונות שניתן למנף אותם.

הקם מעבדה משלך בבית. אתה יכול להשתמש במשאבי ענן מקוונים, כגון AWS של אמזון או Azure של מיקרוסופט. או שאתה יכול ליצור מערכות הפעלה וירטואליות מרובות באותו מחשב פיזי עם שירותי וירטואליזציה. אם אתה רוצה לעבוד ישירות עם חומרה, רכוש מחשבים פשוטים וזולים כמו רסברי פי או ארדואינו. לאחר שתתקין ותפעיל את המערכות שלך, התחל לשחק איתן ולמד כל מה שאתה יכול על קביעת התצורה והאופטימיזציה שלהן, או התחל לתכנת וליצור קוד במערכות אלו. אין דרך נכונה או לא נכונה להתחיל, פשוט לכו בעקבות תחומי העיניין שהכי מעניין אתכם.

דרך מצוינת נוספת להתחיל היא להיפגש ולעבוד עם אחרים בתחום אבטחת הסייבר. שקול להשתתף בכנס אבטחת מידע וסייבר מקומי או בכנס וירטואלי כגון Bsides או SANS New2Cyber. החלק הקשה ביותר הוא למצוא את האירוע או את המפגש הראשון. לאחר שתשתתף, התחבר למשתתפים אחרים והגדל את הרשת המקצועית שלך.

אפשרויות נוספות ללימוד אבטחת מידע וסייבר כוללות סרטונים מיוטיוב , האזנה לפודקאסטים, ביקור בפורומים מקוונים, הרשמה לבלוגים של אנשי אבטחה, או השתתפות באירועי Capture the Flag מקוונים (CTF). בסופו של דבר, אל תיתן להשבלה או לרקע שלך לעבב אותך. תשוקה ללמוד ולעזור לאחרים, כמו גם היכולת "לחשוב מחוץ לקופסה" הן תכונות מפתח. ברגע שתתחיל לפתח את הכישורים הטכניים שלך ולהיפגש עם אחרים, ההזדמנויות יגיעו.

עורכת אורחת

לודרינה צ'רן (@hexplates) היא עו"ד אבטחת מידע הראשית ב-Cybereason, המניעה חדשנות ופיתוח של שיטות עבודה מומלצות הקשורות לתקני אבטחת סייבר ולמדיניות. היא גם מדריכה מוסמכת במכון SANS, שם היא עוזרת לאנשי אבטחת מידע לקדם את ההבנה הבסיסית שלהם בזיהוי פלילי דיגיטלי ותגובה לאירועים (DFIR).

משאבים

כנסי אבטחת מידע Bsides: http://www.securitybsides.com/
נשים בתחום הסייבר: https://www.wicys.org/
רשימת השמעה ביוטיוב של New2Cyber: https://youtube.com/playlist?list=PLtgaAEEmVe6BQkZiJC5nIk9xx74QTGtsZ
אקדמיות הסייבר של SANS: https://www.sans.org/scholarship-academies/
SANS Cyber Aces: https://www.cyberaces.org/
פודקאסטים של אבטחת מידע וסייבר: https://www.sans.org/blog/cybersecurity-podcast-roundup/

תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר