



מסלול הכשרה מחשוב וסייבר

סילבוס

200 ש"א

www.bluetech-ed.co.il



מבנה הקורס

מסלול הכשרה מחשוב וסייבר

בלוטק אדיוקיישן - מומחים בהכשרה מקצועית של אוכלוסיות בעלות פוטנציאל טכנולוגי ומוטיבציה להשתלב בתחום ההייטק, באמצעות תכניות ייעודיות וליווי מקצועי ואישי צמוד ומשלבים אותם בתפקידי מפתח בחברות גדולות במשק עם מעל 25 שנות ניסיון.

למי אנחנו פונים?

- לבוגרי קורסים והכשרות טכנולוגיות שמחפשים השמה ויציבות.
- למועמדים ללא רקע טכנולוגי המעוניינים בהסבה להייטק.
- לחברות הזקוקות לגיוס עובדים איכותיים ומקצועיים לתקופת זמן ארוכה.
- לארגונים המעוניינים לשדרג את הידע המקצועי של עובדיהם בתחומי הטכנולוגיה השונים.

למה בלוטק?

אנחנו מאמינים שהמוטיבציה, האוריינטציה להכשרה הטכנולוגית והמשמעת העצמית שלכם הן המפתח להצלחה ונעשה הכל כדי לספק לכם את הכלים והליווי הטובים ביותר הן בהכשרה והן בהשמה. אנו פועלים מתוך מטרה להשיג הצלחה מוכחת עבורכם ועבור הארגונים איתם אנו עובדים. לא מניע אותנו רווח כלכלי בלבד אלא תהליך הכשרה והשמה איכותי ומקצועי.

רוצים להיכנס לעולם הסייבר?
לפתח עוד יותר מיומנויות קיימות?
להתקדם בקריירה? זה הזמן!
הדרישה לאנשי מקצוע רק עולה.

שפע משרות מחכות לכם בתעשיית אבטחת הסייבר שצומחת במהירות והיא צפויה להמשיך לצמוח בשנים הקרובות. עד 2027, שוק אבטחת הסייבר צפוי להתרחב בקצב צמיחה שנתי ממוצע של 13.37%. זוהי תקופה מצוינת להשתלב ולהתפתח בתחום המחשוב והסייבר!

מנחי ההכשרה:

צוות מקצועי מומחה בהדרכה ובעשייה טכנולוגית מזה שנים רבות. תכני הקורס נשענים על ניסיון רב בהדרכות צבאיות וביטחוניות בחיל המודיעין הישראלי, כמו גם בתעשיית ההייטק האזרחית.

למי ההכשרה מתאימה?

מסלול ההכשרה של בלוטק אדיוקיישן הוא מסלול מקיף, מקצועי ואיכותי, המיועד לאלו שרוצים ללמוד את כל מה שנדרש כדי להשתלב בתפקידי תמיכה וניהול טכני של מערכות מחשוב.

דרישות:

12 שנות לימוד.

מבנה הקורס

מסלול הכשרה מחשוב וסייבר

במהלך ההכשרה תלמדו לתפעל מערכות SOC מסוגים שונים כולל:

- סוגי הפריצות ומהותן.
- ארכיטקטורות אבטחת מידע בארגונים שונים.
- אירועי חירום ומצבי שגרה של המערכות.
- ניתוח והבנת אירוע.
- תפקוד והפעלת מערכות נדרשות עם חשש או קיום של אירוע סייבר.
- הפעלת בעלי תפקידים שונים לתפעול האירוע.
- סוגי אירועים והתמודדות עימם ועוד.

מיומנויות מובילות שתלמדו:

- הקניית ידע ומיומנויות מעשיות בתחומי: מערכות הפעלה, רשתות מחשבים, אבטחת מידע ותכנות, על מנת לאפשר לבוגרי המסלול לעבוד בתפקידי תמיכה וניהול טכני של מערכות מחשוב.
- הבנה של עקרונות ופרוטוקולים בסיסיים - בתקשורת מחשבים, ויכולת ניתוח תעבורת רשת.
- לימוד השפה PYTHON וכן פיתוח יכולות תכנות בסיסיות.
- הקניית ידע בתחום אבטחת מידע והגנת סייבר - החל ממודעות לאיומים וכלה בהיכרות עם כלי הגנה מתקדמים.
- פיתוח מיומנויות עבודה בצוות ויכולת תפעול מרכזי SOC להגנת סייבר.
- שילוב של לימודים עיוניים ותרגול מעשי בסביבות מחשוב ורשת אמיתיות.

בסיום הקורס:

- הסטודנטים ישלטו הן בעולמות הגיוס והן בעולמות הטכנולוגיים הרלוונטיים.
- קבלת תעודת סיום מקצועית של Blue-Tech Education.
- צוות ההשמה של בלוטק אדיוקיישן יסייע לסטודנטים למצוא עבודה בתחום (אם ירצו).

DNS

מבנה הקורס

מסלול הכשרה מחשוב וסייבר

תקשורת מחשבים

- מודלי תקשורת
- כתובות IP ו SUBNETTING
- פרוטוקולי תקשורת ופורטים
- הפרוטוקולים TCP ו UDP
- פרוטוקול DNS
- פרוטוקול DHCP
- פרוטוקול HTTP
- ניתוח תעבורה באמצעות WIRESHARK
- מערכת ההפעלה LINUX
- מבוא למערכות LINUX
- עבודה באמצעות הטרמינל
- ניהול קבצים ותיקיות
- ניהול משתמשים והרשאות
- חיפוש קבצים ותוכנות
- כתיבת סקריפטים פשוטים ב-.BASH



PYTHON

- מבוא לשפת פייתון
- סוגי מידע ומשתנים
- שיטות קלט ופלט מידע
- תנאים ושליטה ברצף
- לולאות
- רשימות ומאגרי מידע
- תקשורת בשפת פייתון.



יסודות תקשורת

- מבוא לחומרה ותוכנה
- וירטואליזציה
- מערכת ההפעלה WINDOWS
- מבוא לרשתות מחשבים
- מבוא לשרתים
- התקנת שרת מסוג WINDOWS
- הגדרת DOMAIN CONTROLLER
- הגדרה וניהול DIRECTORY ACTIVE
- הקמה וניהול אובייקטים בשרת
- הקמה וניהול שרת DNS
- הקמה וניהול שרת DHCP
- הגדרת וניהול חוקי GPO.



סייבר הגנתי

- מבוא למתקפות ואיומי סייבר
- שיטות ומתודולוגיות הגנת סייבר
- ניטור מערכות ואתרים
- מבוא למערכות הגנת סייבר
- חומת אש
- מניעת חדירות ע"י IDPS
- הגנת DDOS
- הגנה אפליקטיבית - WAF
- תגובה וניהול אירועי סייבר
- מערכת ה SIEM
- צוות ה SOC.