TAU | BDO
TECH ACADEMY
CYBER | ENGINEERING | DATA | AI

קורס מבוא לסייבר ואבטחת מידע בשילוב בינה מלאכותית

הכשרה מקצועית לעבודה בתחום אבטחת סייבר שתוביל אותך לעבודה בחברות הפיננסים וההיי-טק המובילות בישראל!

בעידן הדיגיטלי המתפתח במהירות, אבטחת מידע וסייבר הפכו לנושאים קריטיים עבור ארגונים ופרטים כאחד. קורס זה, המוצע על ידי TAU BDO Tech Academy, מספק מבוא מקיף ומעשי לעולם אבטחת המידע והסייבר, תוך שילוב חדשני של כלי בינה מלאכותית.

במהלך 30 מפגשים אינטנסיביים, המשתתפים ירכשו הבנה מעמיקה של עקרונות אבטחת המידע, החל מיסודות תקשורת המחשבים ועד לטכניקות מתקדמות של זיהוי ומניעת איומי סייבר. הקורס משלב באופן ייחודי למידה תיאורטית עם התנסות מעשית, כולל עבודה עם כלים מקצועיים, הקמת מעבדות וירטואליות, ושימוש בטכנולוגיות מתקדמות כמו Docker וAI.

בוגרי הקורס יצוידו בידע וכלים פרקטיים הנדרשים בשוק העבודה העכשווי, כולל הבנה מעמיקה של מערכות אבטחה, יכולת זיהוי וניתוח איומים, והתמודדות עם אתגרי אבטחת המידע המודרניים. התוכנית מיועדת הן למתחילים המעוניינים לבנות קריירה בתחום והן לאנשי מקצוע המבקשים להרחיב את הידע שלהם בעולם הסייבר המתפתח.

הזדמנויות תעסוקה

בוגרי הקורס יכולים להשתלב במגוון תפקידי כניסה בתחום הסייבר ואבטחת המידע. התפקיד הטבעי ביותר הוא אנליסט SOC (מרכז אבטחת מידע), תפקיד שמקבל הכשרה מעמיקה בקורס ומאפשר לבוגרים להתחיל את דרכם בניטור וטיפול באירועי אבטחה. בנוסף, הבוגרים יכולים להשתלב כבודקי חדירות מתחילים, מומחי תמיכה באבטחת מידע, או מיישמי אבטחת מידע בארגונים. הקורס מקנה גם בסיס ידע חזק שמאפשר, עם צבירת ניסיון, להתקדם לתפקידים בכירים יותר כמו חוקרי אבטחת מידע, יועצי סייבר, או מומחי אבטחת מידע בתחומים מתקדמים כמו אבטחת AIואבטחת ענן.

TAU | BDO
TECH ACADEMY
CYBER | ENGINEERING | DATA | AI

קורס מבוא לסייבר ואבטחת מידע בשילוב בינה מלאכותית

הכשרה מקצועית לעבודה בתחום ניתוח נתונים שתוביל אותך לעבודה בחברות הפיננסים וההיי-טק המובילות בישראל!

למי המסלול מתאים

- המסלול מתאים לכל מי שמעוניין לרכוש מקצוע מתקדם ונדרש ודריסת רגל בתחום אבטחת הסייבר
- הקורס לא דורש ידע מוקדם ופונה לאנשים ללא רקע מקצועי בתחום

בסיום הקורס תדעו :

- ✓ לזהות ולנתח איומי סייבר בזמן אמת ולהגיב אליהם באופן מקצועי במסגרת עבודתם כאנליסטים במרכזי SOC.
- ✓ להקים ולתחזק סביבות עבודה מאובטחות תוך שימוש בכלי וירטואליזציה וקונטיינרים.
- ✓ לבצע בדיקות חדירות בסיסיות לאתרי אינטרנט ומערכות מידע תוך שימוש בכלים מקצועיים
- ✓ לנתח ולחקור אירועי אבטחה באמצעות כלי SIEM וטכניקות forensicsבסיסיות.
- ✓ לזהות ולהתמודד עם מתקפות פישינג, נוזקות ואיומים שונים על מערכות מחשוב ורשתות.
- ✓ ליישם מדיניות אבטחת מידע וציות בארגון תוך הבנת עקרונות Zero Trust ואבטחה מרובדת.
- ✓ לשלב כלי בינה מלאכותית בתהליכי זיהוי איומים והגנה על מערכות מידע.

דרישות קבלה לקורס

- אנגלית ברמה בסיסית ויכולת תקשורת טובה
- זיקה חזקה לאינטרנט ומחשבים
- חדורי מוטיבציה לפתח קריירה כמומחי אבטחת סייבר
- יחסי אנוש בריאים ויכולת חשיבה אנליטית טובה

יש להגיע לקורס עם מחשבים ניידים אישיים

מתכונת הקורס

30 מפגשים, פעמיים בשבוע, 150 שעות אקדמיות

מיקום הקורס

ייקבע בהמשך

זכאות לתעודה

לעומדים בדרישות התכנית תוענק תעודה על הכשרת "Cyber Security"
מטעם TAU-BDO TECH ACADEMY

לייעוץ ללא התחייבות עם יועצי הלימודים שלנו :
info@tau-bdo.co.il | 03-9718800

TAU | BDO
TECH ACADEMY
CYBER | ENGINEERING | DATA | AI

קורס מבוא לסייבר ואבטחת מידע בשילוב בינה מלאכותית

סילבוס הקורס

פרקי לימוד	פירוט
מבוא לאבטחת מידע וסייבר	▪ הצורך באבטחת מידע וסייבר, מהי אבטחת סייבר? ▪ נתונים אישיים, נתונים ארגוניים, סודיות, שלמות וזמינות, ההשלכות של פריצות האבטחה ▪ הפרופיל של תוקף הסייבר, סוגי תוקפים, איומים פנימיים וחיצוניים, נושאים של חוק ואתיקה באבטחת סייבר ▪ סקירה של לוחמת סייבר והמטרה של הלוחמה ▪ מתקפות, מושגים וטכניקות ▪ הגנה על הנתונים והפרטיות ▪ הגנה על הארגון ▪ התקני אבטחה ▪ יישום מדיניות אבטח המידע בארגונים לפי הנחיות פיתוח תוכנה מאובטחת ▪ רשתות האינטרנט, הווב וה- Darknetוהשימושים בהן
יסודות תקשורת נתונים לסייבר ואבטחת מידע	• מבוא לעולם התקשורת ולימוד מושגי היסוד של תקשורת: מהי רשת האינטרנט, רשת WEB וגרסותיה ,מהן חבילות מידע (מנות מידע) ומהי רשת ממותגת מנות, ציוד ורכיבי תקשורת הנפוצים • צורות וסוגי חיבור לרשת: רשת LANורשת WAN ,קצב העברת הנתונים (מהירות) Bit Rate,רוחב פס Band Width, Throughput, כרטיס רשת ,NICמאפייני וסוגי כרטיסי רשת מעשיים • שיטות הפצת נתונים: Unicast , Multicast , Broadcast, Anycast • כתובת MAC, IPסוגיה וכלי עבודה להגדרה ובדיקות כתובות ,IP היכרות עם מושג ה- Subnetting, טכנולוגיית האתרנט • מודל OSI של 7 השכבות ומודל TCP/IP, האיומים האפשריים בשכבות השונות ושיטות התגוננות ,סקירה ותפקידים בסיסיים עבור ציוד התקשורת • הכרת פרוטוקולי תקשורת כולל סקירה לפרוטוקולים הנפוצים • מודל שרת-לקוח Client-Serverומודל עמית-לעמית Peer to Peer ומודל משולב • הגדרת תפקיד חבילת המידע Data Packetוהצגת מבנה חבילות , TCP , IP UDP • ניתוח תעבורה בעזרת תוכנת Wireshark • היכרות עם Cloud Computingוסוגי ענן

TAU | BDO
TECH ACADEMY
CYBER | ENGINEERING | DATA | AI

קורס מבוא לסייבר ואבטחת מידע בשילוב בינה מלאכותית

סילבוס הקורס

פרקי לימוד	פירוט
הכירות עם שרתים והכלים של Windows	• הכירות מהו מחשב מארח, Host תפקיד המארחים ברשת, שרת, Server הבנה מהו מחשב/תוכנת לקוח Client, שימוש בקובץ hostsשל Windows • הקמת שרתי, Webקבצים וכלי שליטה מרחוק על מחשב אישי, הקמת מעבדה ווירטואלית ע"י שימוש בתוכנת ה- Hypervisorהמובנית של, MS Hyper-V היכרות עם תוכנות ווירטואליזציה נוספות כגון VMwareאו Proxmox או Virtual Box • הכרות מהו hypervisor סוג 1 ו-2 ומה ההבדלים והשימושים שלהם • הקמת מכונות ווירטואלית של וינדוס כולל קונפיגורציה ושליטה בהן כולל גרסאות שונות של וינדוס וההבדלים ביניהן • היכרות עם WSL של וינדוס ויכולותיה לשילוב של מערכות ההפעלה לינוקס במכונת וינדוס • הדגמות ושימוש בשילוב של מערכות ההפעלה Windowsו- Linux, הכרות ושימוש בתוכנת Docker Desktop • הורדת images, של קונטיינרים השונים מ-Docker Hub • היכרות עם כלי שליטה מרחוק על מחשבים ושרתים, שימוש ב- Secure Shell (ssh)להתחבר לשרת מרוחק וכלי SCP-וSSH • היכרות עם מערכת הרשאות ומערכת קבצים של מערכות הפעלה השונות, ניהול הרשאות, כלי שורת הפקודה של וינדוס והסקריפטינג Powershell ו-Command Line
היכרות עם מערכת הפעלה Linux	• היכרות עם מערכת ההפעלה, Linux הפצות השונות כולל ייעודיות לעולם הסייבר • היכרות עם מערכת הקבצים והספריות של לינוקס, מערכת הרשאות של לינוקס ומשתמשי-על • היכרות ועבודה עם הרשאות הקבצים במערכות ההפעלה, Linuxלימוד פקודות נפוצות של לינוק • היכרות עם כלי שורת הפקודה של לינוקס shell, bashכתיבת סקריפטים ב- bashו-one-liner • היכרות עם עורכי קבצים בלינוקס, התקנות תוכנות במערכת ההפעלה של לינוקס • הגדרות רשת, DNSשימוש בקובץ hosts, עבודה עם Environment Variablesבלינוקס, שימוש בתוכנת Dockerבלינוקס והפעלת קונטיינרים • היכרות עם שרותי לינוקס נפוצים כגון DNS, Web server

TAU | BDO
TECH ACADEMY
CYBER | ENGINEERING | DATA | AI

קורס מבוא לסייבר ואבטחת מידע בשילוב בינה מלאכותית

סילבוס הקורס

פרקי לימוד	פירוט
מבוא לפיתוח אתרי Web **ו- Web Penetration Testing**	• היכרות עם Web application technologies • לימוד HTML כולל HTML Tags השונים, CSS-ו Java Script • היכרות עם פרוטוקולים של HTTP גרסה 1, 2 ו-3 והעברת מידע ברשת • עבודה עם פרוטוקול TLS, סוגי תעודות ומנפיקי תעודות CA • היכרות עם כלי מניעת התקפות כגון Captcha-ו JS Challenge • הכירות בסיסית עם מושגים של Front-End, Back-End • בדיקות צד לקוח ובדיקות צד שרת וכלים כגון Postman, DevTools ועבודה עם API • בדיקות חדירות עם שרת פרוקסי של Burp Suite • היכרות עם בסיסי נתונים SQL & NO-SQL • היכרות והדגמת OWASP top 10 attacks • עבודה עם Wireshark וניתוח מידע.
היכרות עם תשתית הסייבר	• הזדהות ואימות משתמשים • היכרות עם גישת Zero Trust • מערכות חומת אש (FW- Access List) • סוגי נוזקות השונים ודרכי התמודדות • היכרות עם סוגי המתקפות • איסוף מידע ומודיעין ממקורות פתוחים: OSINT • היכרות עם מערכות IPS, IDS-ו WAF- • הבנת Zero-day attack • היכרות עם סוגים של VPN שימוש בשרות ה- VPN ושרתי ה-Proxy • המשך העבודה עם כלי ההקלטה וניתוח תעבורה Wireshark • קריפטוגרפיה וסוגי הצפנה הנפוצים • שימוש ברשתות אל חוטיות והסכנות שבהן • Windows and Linux Privilege Escalation

TAU | BDO
TECH ACADEMY
CYBER | ENGINEERING | DATA | AI

קורס מבוא לסייבר ואבטחת מידע בשילוב בינה מלאכותית

סילבוס הקורס

פרקי לימוד	פירוט
תפקיד של בקר/אנליסט SOC (SOC Analyst) ותגובה לאירועי סייבר	• היכרות עם תפקיד של SOC Analyst • היכרות עם Cyber security incident types and categories • היכרות עם Incident Response • היכרות עם כלי SIEM והפונקציות שלהם • היכרות עם Attack chain • עבודה עם איסוף וניתוח נתונים ולוגים של אירועי סייבר • היכרות עם סוגי לוגים של מערכות ענן • כלים אינטרנטיים לחקירות של וירוס/פישינג/כתובות זדוניות/סריקת דומיינים • העמקה של עולם הפישינג - איך מזהים, איך מדווחים • ניתוח התנהגויות חשודות - Windows, Linux & Network Forensics, Malware Analysis • היכרות עם Security monitoring
שימוש בלמידת מכונה וכלי בינה מלאכותית לזיהוי, ניצול פגיעות במערכות מחשב והגנה על מערכות ממתקפות סייבר	• היכרות עם בינה מלאכותית וכלי AI • היכרות והבנה של עקרונות ה- ML-וAI • שימוש בכלי AIלתכנון וייעול בדיקות חדירות • שימוש בכלי AIלכתיבת וניתוח דוחות של בדיקות חדירות.