Hacker.U
מזניקים אותך לקריירה בהייטק

היערכות הגנת סייבר לאיומים קוואנטיים
(Quantum Cyber Readiness)

העולם הטכנולוגי עומד בפני מהפכה. מחשוב קוואנטי מביא עמו הזדמנויות אדירות, אך גם איום קיומי על מערכות ההצפנה הקלאסיות המגינות כיום על המידע הרגיש ביותר בארגון. קורס זה מעניק למנהלי אבטחת מידע ומובילים טכנולוגיים את הידע הקריטי והכלים המעשיים להיערכות ליום שבו ההצפנות ייפרצו. הקורס מתמקד בשיטת "Harvest Now, Decrypt Later" (איסוף מידע כעת ופענוח בעתיד) , סוקר את הרגולציות החדשות (NIST 2030) , ומספק מתודולוגיה סדורה לבניית תוכנית פעולה ארגונית למעבר ל-Post-Quantum Cryptography (PQC).

פרטי הקורס

משך הקורס
30 שעות אקדמיות.

רמת מיומנות
רמה מקצועית / ניהולית.

קטגוריה
סייבר ואבטחת מידע, ניהול סיכונים, אסטרטגיה טכנולוגית.

קהל היעד

הקורס מיועד לבעלי תפקידים בארגונים המחזיקים במידע רגיש ונדרשים לעמוד ברגולציה מחמירה (פיננסים, בריאות, תשתיות קריטיות, ממשל).

- **מנהלי אבטחת מידע (CISO) ומנהלי סיכונים (GRC).**
- **צוותי IT וארכיטקטי מערכת בכירים.**
- **מבקרים פנימיים ודירקטורים הנדרשים להבנת הסיכון העסקי.**

דרישות קדם

הקורס מיועד לאנשי מקצוע בעלי רקע בניהול אבטחת מידע או תשתיות IT.

- **היכרות עם עולמות הסייבר וניהול סיכונים.**
- **הבנה בסיסית בתשתיות הצפנה (PKI, SSL/TLS) - יתרון.**
- **אנגלית ברמה טכנית.**

מי מוביל את ההכשרה?

ההכשרה נבנתה בשיתוף עם חברת PQCLayer - חברת סייבר אמריקאית
המספקת פלטפורמה לניהול סיכונים קריפטוגרפיים והערכות לאיומים קוואנטים.

שבי דגן

שותף מייסד ו-CTO ב-PQCLayer,
מומחה לאבטחת מידע בעידן הקוונטי

האיום הקוואנטי כבר אינו תרחיש עתידי רחוק, אלא אתגר ניהולי מיידי. השאלה איננה 'אם' ההצפנות ייפרצו, אלא האם הארגון שלכם ייתפס מוכן ברגע האמת. אני מודע לכך שעבור מנהלי אבטחה, היערכות קוואנטית נתפסת לעיתים כמסע מורכב ומתיש. מטרתנו ב-PQCLayer היא לשנות בדיוק את המשוואה הזו: לקחת נושא שנתפס כתיאורטי ומאיים, ולהפוך אותו לתוכנית עבודה סדורה, מדידה ואופרטיבית. בקורס זה לא רק נלמד על הסיכון – אלא נטמיע את המתודולוגיה שתהפוך את ההגנה הקוואנטית לחלק בלתי נפרד, ופשוט ליישום, בליבת האבטחה הארגונית שלכם.

מבנה התוכנית

MODULE 01

המהפכה הקוואנטית והאיום המתהווה

הבנת הבסיס הטכנולוגי והסיבה לדחיפות העסקית כבר היום.

- **מבוא למחשוב קוואנטי:** מה הופך אותו לשונה ממחשוב קלאסי וכיצד הוא מאיים על הצפנות RSA ו-ECC.
- **ציר הזמן הטכנולוגי:** סקירת התקדמות טכנולוגית ולוחות זמנים צפויים לשבירת ההצפנות.
- **למה עכשיו?** הבנת איום ה- "Harvest Now, Decrypt Later" והסיכון למידע הנאגר כיום.
- **עלויות ומשמעויות:** עלות אי-היערכות מול עלות היערכות מוקדמת.

MODULE 02

רגולציה, תקינה וניהול סיכונים

מיפוי הנוף הרגולטורי המתגבש וההשלכות על הארגון.

- **הנחיות הרגולטור (NIST):** הכרת הסטנדרטים המתהווים ודרישות המוכנות לשנת 2030.
- **תאימות בינלאומית:** השפעות המעבר הקוואנטי על עמידה בתקני GDPR, HIPAA, PCI-DSS.
- **עמדת גופי העל:** התייחסות של CISA, ENISA ורגולטורים מובילים בעולם.

MODULE 03

בניית תוכנית פעולה מעשית (Action Plan)

יציאה מהקורס עם "פלייבוק" (Playbook) וצ'ק-ליסט ליישום מיידי בארגון.

- **מיפוי נכסים (Discovery):** איתור נכסים קריטיים ונתונים רגישים הדורשים הגנה קוואנטית.
- **זיהוי פערים (Gap Analysis):** ניתוח מנגנוני ההצפנה הקיימים ורמת הפגיעות שלהם.
- **בניית Roadmap:** תכנון המעבר לפתרונות Post-Quantum Cryptography (PQC).
- **מדיניות Crypto Agility:** קביעת נהלים המאפשרים החלפה מהירה של אלגוריתמים בעת הצורך.

MODULE 04

ניהול, בקרה וכלים טכנולוגיים

כיצד לנהל את האירוע ברמת ההנהלה והדירקטוריון, ושימוש בכלים מתקדמים.

- **היבטי ניהול:** איך להציג את האיום לדירקטוריון ולבנות Case כלכלי להשקעה.
- **ביקורת ובקרה:** שאלון ביקורת יישומי לבדיקת מוכנות הארגון (Readiness Assessment).
- **חדשנות וכלים:** סקירת כלים לניהול Crypto Posture, והיכרות עם פתרונות (כגון PQCLayer).
- **צעדים מעשיים למחר בבוקר:** שילוב PQC ב-Risk Register והתחלת POC עם אלגוריתמים חדשים (Kyber, Dilithium).