יסודות יישומיים ואבטחת סייבר מתקדמת – InfoSec

קורס מתקדם לסטודנטים ומקצועני הייטק המעניק ידע עיוני ויישומי בתחום אבטחת המידע והגנת סייבר בארגונים. המשתתפים ילמדו את עקרונות התשתיות, הגנה על נקודות קצה, ניהול זהויות והרשאות, אבטחת רשתות וחומות אש, לצד יסודות ההצפנה ותשתיות PKI.

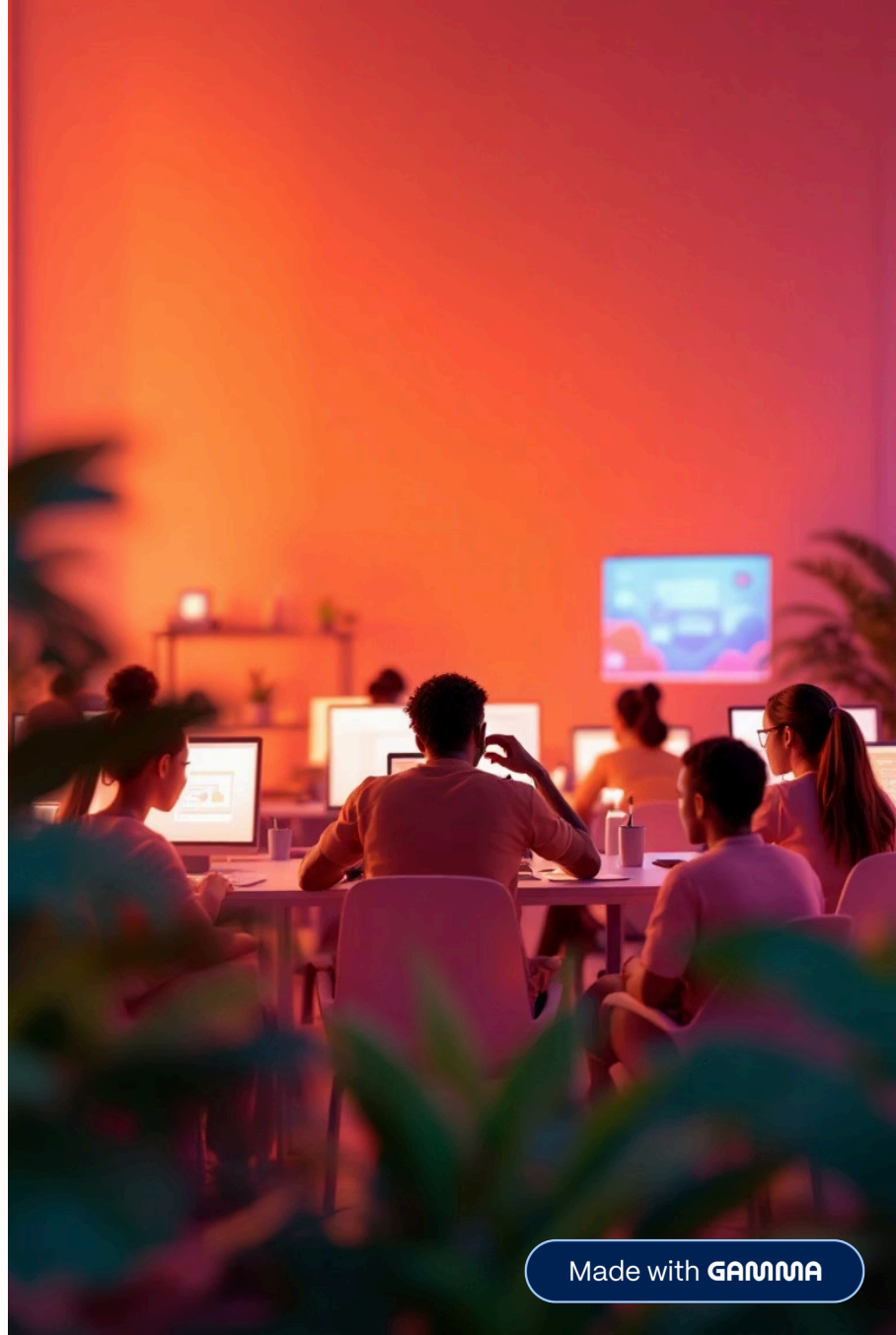
מבנה הקורס וייעדים אקדמיים

יעדי למידה

- הבנה עמוקה של עקרונות אבטחת מידע
- יכולת יישום מעשי של פתרונות אבטחה
- ניתוח איומים וניהול סיכונים
- הכנה למקצוע בתחום הסייבר

גישה פדגוגית

שילוב ייחודי של תיאוריה ופרקטיקה עם דגש על כלים וטכנולוגיות מובילים מהתעשייה. הקורס מבוסס על למידה חווייתית עם בדיקות מעבדה וסימולציות.



יחידה 1: מבוא לאבטחת מידע ותשתיות

01

היכרות עם InfoSec

מהי אבטחת מידע, סקירת תשתיות קריטיות בארגון, הכרת סביבת העבודה הטכנולוגית ויעדי הקורס.

02

מודל OSI וניתוח תעבורה

שכבות המודל, פרוטוקולים מרכזיים (Telnet, ICMP), עבודה מעשית עם Wireshark לניתוח פאקטים ברשת.

03

הגנת נקודות קצה

עקרונות הגנת תחנות קצה, זיהוי וחסימת תוכנות זדוניות, יישום Host Firewall ופתרונות ארגוניים.

הגנת נקודות קצה ופתרונות McAfee

טכנולוגיות הגנה מתקדמות

התקנה ותצורה בסיסית של מערכות הגנה, ניהול הרשאות משתמשים, ניתוח Audit Logs והקשחת תחנות עבודה. דגש מיוחד על הבנת התקפות מתקדמות וטכניקות הגנה.

- זיהוי והסרת תוכנות זדוניות
- ניהול מדיניות אבטחה ארגונית
- ניטור פעילות חשודה במערכת

מניעת זליגת מידע - DLP

עקרונות וארכיטקטורת DLP, דוגמאות יישום בסביבה ארגונית באמצעות McAfee DLP להגנה על נתונים רגישים.

יחידה 2: ניהול זהויות והרשאות

Active Directory

מבנה ותפקיד Active Directory בארגון, ניהול קבוצות והרשאות משתמשים, שימוש מתקדם ב־Group Policy לאכיפת מדיניות אבטחה.

הרשאות מועדפות - PAM

הצגת מערכת CyberArk כפתרון מוביל בתחום, רכיבי PSM לניהול סשנים מועדפים ו־PTA לניתוח איומים בהרשאות מועדפות.

מערכת CyberArk ויישומים מעשיים

ניתוח איומים - PTA

טכנולוגיה מתקדמת לזיהוי התנהגויות חריגות של משתמשים מועדפים, שימוש באלגוריתמי למידת מכונה לזיהוי איומים פנימיים ואנליטיקה התנהגותית.

ניהול סשנים מועדפים - PSM

מערכת לניהול וניטור גישה של משתמשים מועדפים למערכות קריטיות. הקורס יכלול התקנה, תצורה וניתוח לוגים למטרות ביקורת ואבטחה.

יחידה 3: אבטחת רשתות ופרוטוקולים

פרוטוקולי רשת קריטיים

מושג הפורטים, TCP ו־UDP הבדלים מהותיים בין IP Protocol, הלוגיים והשפעתם הישירה על תקשורת ברשת והיבטי האבטחה.

חומות אש - תיאוריה ויישום

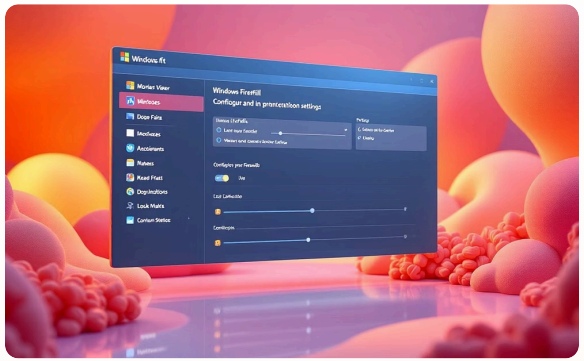
תפקידי Host Firewall לעומת Network Firewall, בניית חוקי Firewall מתקדמים, דוגמאות מעשיות ליישום (Windows Firewall, Azure Firewall).

הקורס יכלול מעבדות מעשיות לתצורת חומות אש בסביבות שונות ובדיקת יעילותן מול התקפות מדומות.

יישום מעשי של חומות אש

Azure Firewall

פתרון חומת אש מבוסס ענן, ניהול תעבורה בסביבות היברידיות, אינטגרציה עם שירותי Azure Security Center.



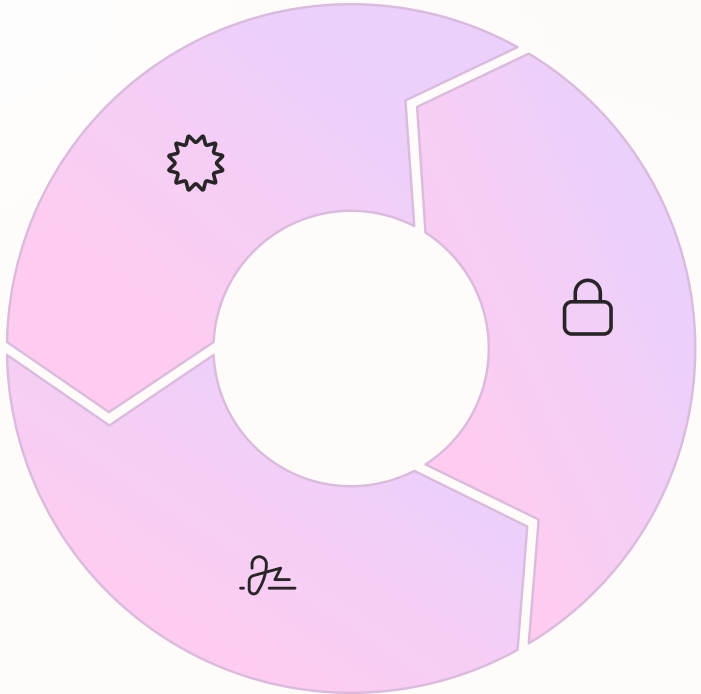
Windows Firewall

תצורת חוקי אבטחה ברמת המערכת, ניהול יוצאות ונכנסות של תעבורת נתונים, והתאמה לסביבת עבודה ארגונית.

יחידה 4: הצפנה ותעודות דיגיטליות

יסודות ההצפנה

מהות התעודה הדיגיטלית, הבדלים קריטיים בין הצפנה סימטרית לא־סימטרית (Public/Private Key).



תשתית PKI

ארכיטקטורה מלאה, תפקידי CA, RA, VA ותהליך הנפקה ואימות תעודות בסביבה ארגונית.

ניהול תעודות

חתימה דיגיטלית, Certificate Chain, שדות חשובים בתעודה, ניהול Certificate Store ואחסון מפתחות.

סיכום הקורס והכנה למקצוע

הישגי הקורס

- ידע מעשי באבטחת מערכות וארגונים
- הכרת כלים מובילים בתעשייה
- יכולת ניתוח איומים וסיכונים
- הבנה מעמיקה של תשתיות אבטחה

הזדמנויות קריירה

הקורס מכין את הסטודנטים לתפקידים במגוון תחומים: מנהל אבטחת מידע, מומחה SOC, יועץ אבטחה ארגונית, ומפתח פתרונות אבטחה.

מכללת Umbrelix - הכשרה מקצועית מתקדמת לעתיד הטכנולוגי שלכם