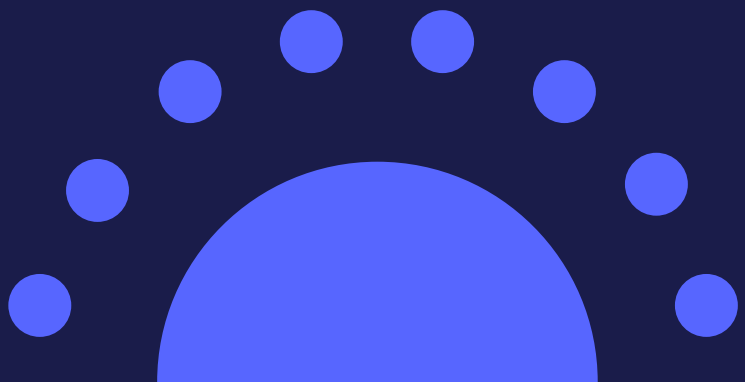
אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

THE INSTITUTE
Empowering Israel's future through AI

האקדמיה הטכנולוגית
של מערכת הביטחון
אתלס

AI Cyber Warfare

AI by Cyber ◗ Cyber by AI



רציונל

המרחב הדיגיטלי עובר שינוי עמוק בעקבות התקדמות הבינה המלאכותית.
גם עולם הסייבר לא חסין: AI משמש לפיתוח מתקפות מתקדמות, ומנגד גם מאפשר כלי הגנה, כגון: זיהוי אנומליות, חיזוי איומים והפעלה של מגנוני הגנה.
מערכות AI מסוגלות כיום לייצר קוד, לבצע ניתוח מודיעין, לנתח מתקפות בזמן אמת ולהפעיל להפעיל מערכות אוטונומיות. לימוד משולב של AI וסייבר אינו רק יתרון אלא הכרח מקצועי: פיתוח יכולות רב-מערכתיות בזירת הקרב הדיגיטלית.

הקונספט

קורס מתודולוגי מקצועי לגיבוש הבנה מעמיקה של שימושי סייבר בסביבת לחימה חדשה, באמצעות בסיס תיאורטי ותרגול אפקטיבי בסימולציות שונות.

מטרות הקורס

- יכולת לזהות ולנתח חולשות במערכות AI
- היכרות עם שיטות תקיפה מתקדמות על מודלים ומערכות מבוססות AI
- יישום AI לזיהוי איומים, אוטומציה של SOC וניהול אירועי סייבר
- פיתוח חשיבה כ-Architects של מערכות מורכבות
- הקורס מקנה כלים לניתוח מערכות מורכבות והטמעת פתרונות בסביבה ביטחונית.

מתודולוגיה

60% הרצאות ושיעורים פרונטליים – הבנת מודלים, טכנולוגיות ואיומים.
30% תרגול מעשי – תרגולים, סימולציות תקיפה והגנה, Playbook, ניתוח מערכות AI.
10% הפקת לקחים – תובנות ליישום בארגון.
התרגולים מתבצעים באמצעות כלי AI על מחשבי המשתתפים.

פרטים ליצירת קשר | office@atlastech.co.il

מפגש 1 AI משנה את זירת הסייבר

- Cyber by AI vs AI by Cyber
- מהפכת LLM
- AI כמכפיל כוח לתוקף
- AI כמכפיל כוח להגנה
- מגמות התקיפה בעולם
- תרגול – מיפוי מערכת ארגונית והערכת סיכונים בעולם ה-AI

מפגש 2 יסודות AI לעולם הסייבר

- Large Language Models
- Embeddings
- RAG
- AI Agents
- Guardrails
- תרגול – פירוק מערכת AI לרכיבים ארכיטקטוניים וזיהוי נקודות תקיפה.

מפגש 3 Threat Landscape בעידן ה-AI

- האצת מתקפות באמצעות AI
- Deepfake attacks
- קוד זדוני שנוצר ע"י מודלים
- אוטומציה של תקיפות
- תרגול – ניתוח מתקפות אמיתיות מהשנים האחרונות.

מפגש 4 AI by Cyber - תקיפת מערכות AI

- Prompt Injection
- Indirect Prompt Injection
- Data Leakage
- Tool Abuse
- Model Exploitation
- תרגול – תקיפה והגנה על AI assistant ארגוני.

מפגש 5 התקפות על מודלים ודאטה

- Data poisoning
- Model inversion
- Training attacks
- Supply chain attacks
- תרגול – סימולציית הרעלת מערכת ידע.

מפגש 6 אבטחת מערכות AI

- Threat modeling
- Monitoring
- Secret management
- Isolation architectures
- Guardrails
- תרגול – תכנון ארכיטקטורת הגנה למערכת AI.

מפגש 7 Cyber by AI – הגנה מבוססת AI

- AI-driven SOC
- Threat hunting
- AI copilots
- SOAR automation
- Human-in-the-loop
- תרגול – בניית Playbook להגנה באמצעות AI

מפגש 8 תרגיל מסכם – AI Cyber Battle

- **תרחיש** – מערכת AI מבצעית בארגון ביטחוני.
- **המשתתפים מתחלקים לקבוצות** – Red Team / Blue Team.
- **המשימות** – ניתוח Threat Model, תקיפה מבוקרת, בניית הגנה, הפקת לקחים.
- **התוצרים** – Threat model, רשימת בקרות, Playbook מבצעי.