Cyber Battle Royale – מלא סילבוס

קורס סייבר לנוער (כיתות ז׳ ומעלה) הכנה להסמכה הבינלאומית **LPI Security Essentials 020-100**

24 יחידות לימוד



הקדמה לקורס

קורס **Cyber Battle Royale** מציג לתלמידים את עולם אבטחת המידע בצורה חווייתית, עדכנית ומעשירה. התוכנית משלבת ידע תיאורטי רחב מעולם הסייבר לצד התנסות מעשית, סימולציות, קרבות Blue vs Red ותרגולים מקוונים.

התלמידים ייחשפו לאיומים, מתקפות, הגנות, עבודה עם מערכות הפעלה, רשתות, ניהול הרשאות, הצפנה, DFIR ו-SIEM — תוך הכנה מלאה להסמכת **LPI Security Essentials (020-100)**.

הערה חשובה:

יחידת לימוד אינה בהכרח שוות־ערך למפגש. מפגש יכול להכיל מספר יחידות לימוד, ויחידת לימוד יכולה להתפרס על פני מספר מפגשים — בהתאם למתכונת הקורס.

רציונל הקורס

העולם הדיגיטלי שבו אנו חיים מתבסס על תקשורת, מערכות מידע ושירותים מקוונים, ולכן התמודדות עם איומי סייבר הפכה למיומנות נדרשת לכל תלמיד, עובד וארגון. קורס *Cyber Battle Royale* נועד להקנות לתלמידים הכשרה מעמיקה, עדכנית וחווייתית בתחום אבטחת המידע — בשילוב תרגולים מעשיים, סימולציות, ניתוחי אירועים וחשיבה התקפית־הגנתית. הקורס מותאם לבני נוער ללא רקע קודם, ומטרתו לפתוח עבורם דלת לעולם המקצועי של הסייבר תוך ביסוס הבנה תיאורטית ומעשית כאחד.

התוכנית בנויה בהתאם לדרישות ההסמכה הבינלאומית

LPI Security Essentials (020-100)

ומאפשרת לתלמידים לרכוש את כל הידע הנדרש כדי להיבחן בהצלחה - החל ממושגי יסוד באבטחת מידע ועד הבנה תפעולית של מערכות, רשתות, ניהול הרשאות, הצפנה, SIEM ותגובה לאירועים.

עקרונות פדגוגיים ומבנה הלמידה

הקורס משלב בין ארבעה צירי למידה מרכזיים:

העמקה תיאורטית

הכרת מושגי יסוד, מודלים, מתודולוגיות ותקנים בתחום הסייבר.

תרגול מעשי

עבודה עם כלים אמיתיים, אתרי סימולציה, ניתוחי לוגים, ופתרון אתגרי סייבר במערכת מעבדות מקצועית (IronScale).

למידה חווייתית

תרגילי Blue vs Red, משחקי חשיבה, חקירות דיגיטליות ופריסת תרחישי אירוע.

הכשרה להסמכה

יישום תכני ההכנה לבחינת LPI כחלק אינטגרלי מהקורס.

הערה ארגונית:

יחידת לימוד אינה בהכרח מפגש. מפגש עשוי לכלול מספר יחידות לימוד, ויחידת לימוד עשויה להתפרס על פני שניים או יותר מפגשים – בהתאם למתכונת הקורס (קורס שנתי, מחנה קיץ, האצה וכדומה).

מטרות הקורס

מטרות־על

1. להקנות יסודות תיאורטיים ומעשיים בעולם אבטחת המידע והסייבר.
2. לפתח חשיבה אנליטית, ביקורתית וגמישה באמצעות התנסות מעשית ועבודה מדורגת.
3. להכין את התלמידים בצורה מיטבית למבחן ההסמכה הבינלאומי LPI Security Essentials.
4. לבסס התנהגות דיגיטלית אחראית, מודעות לאיומים, ואתיקה בעידן המידע.
5. לאפשר לתלמידים לגלות יכולות והעדפות מקצועיות לקראת המשך דרכם בתחומי הטכנולוגיה.

יעדי למידה (Learning Outcomes)

בסיום הקורס התלמידים יוכלו:

יעדים תיאורטיים

- להגדיר ולהסביר מושגי יסוד באבטחת מידע וברשתות.
- לזהות סוגי תוקפים, איומים ונוזקות ולהבין את מאפייניהם.
- לתאר מודלים של תקיפה (Kill Chain) ומודלים של הגנה (Defense-in-Depth).
- להבין את עקרונות IAM, מדיניות אבטחת מידע ופרקטיקות ארגוניות.

יעדים טכנולוגיים־מעשיים

- להפעיל פקודות בסיס במערכות Windows ו-Linux.
- לבצע סריקות רשת בסיסיות (Recon ו-Port Scanning).
- להשתמש בכלי OSINT לאיסוף מידע גלוי.
- לנתח לוגים, לזהות אנומליות ולבצע חקירת אירוע ראשונית (DFIR).
- להגדיר ולבחון מנגנוני אבטחה בסיסיים ברשת, בתחנה ובמערכת Web.
- ליישם עקרונות הצפנה וגיבוב ברמה בסיסית.

יעדים מתודולוגיים

- לבצע עבודת צוות בתרחישי Red Team מול Blue Team.
- להפיק דוחות אבטחה ותחקירי אירוע ברמה בסיסית.
- לפתח הרגלי חשיבה התקפית־הגנתית, יכולת ניתוח וסדר־פעולה.

קהל יעד ודרישות

דרישות מחשוב

- מחשב אישי עם חיבור לאינטרנט ודפדפן.
- שימוש בכלים חינמיים אונליין: OSINT, DNS Lookup, Hashing וכד'.
- גישה למערכת אתגרי הסייבר והמעבדות: **Cyber Arena / IronScale**.

קהל יעד

בני נוער מכיתות ז' ומעלה, מכל הרמות — כולל תלמידים ללא רקע קודם במדעי המחשב או סייבר.

דרישות קדם

- אין צורך בידע קודם.
- שליטה בסיסית באנגלית רמה של קריאת ממשקי משתמש וכלים טכנולוגיים.

יחידות הלימוד: יחידות 1-6

01

מבוא לעולם הסייבר | Introduction to Cyber Security

יחידה זו מהווה את שער הכניסה לעולם הסייבר. התלמידים מכירים את מושגי היסוד באבטחת מידע, מודלים בסיסיים כמו CIA Triad ומי הם התוקפים העיקריים בעולם הדיגיטלי. הבסיס התיאורטי כאן יוצר מסגרת ראשונית להבנת מהו סייבר ולמה הוא חשוב.

תתי־נושאים: CIA Triad, Threat Landscape, מבנה בחינת LPI.

מעבדות אונליין: סימולציית CIA, בדיקת זליגת מידע (haveibeenpwned)

LPI Domain: 1.1 Security Concepts

02

שחקני איום וחשיבה תקפית־הגנתית | Threat Actors & Offensive-Defensive Thinking

יחידה זו מפתחת אצל התלמידים הבנה של שחקני האיום – החל מתוקפים חובבנים ועד קבוצות מדינתיות. התלמידים לומדים כיצד תוקף מתכנן תקיפה וכיצד צוות הגנה מתמודד איתה לאורך מחזור החיים של מתקפה (Kill Chain).

מעבדות אונליין: ניתוח תקיפות גלובליות (Digital Attack Map), OSINT ראשוני על גורם דמיוני

LPI Domain: 1.2 Threat Actors

03

מודיעין סייבר ו-OSINT | Cyber Intelligence & OSINT

יחידה זו עוסקת באחד השלבים הראשונים במתקפות סייבר – איסוף מידע גלוי. התלמידים לומדים כיצד מאתרים מידע על ארגונים, דומיינים ומשתמשים תוך שימוש בכלים פתוחים. היחידה בונה בסיס חזק לשלב ה־Recon העתידי.

מעבדות אונליין: Whois Lookup, VirusTotal Domain Search, Google Dorking (בטוח ומוגבל)

LPI Domain: 2.3 Reconnaissance

04

הנדסה חברתית ופישינג | Social Engineering & Phishing

ביחידה זו התלמידים מבינים שהאדם הוא נקודת הכשל המרכזית. התלמידים מנתחים מתקפות פישינג, זיופי כתובות, מתקפות Spoofing ולומדים לזהות מניפולציה דיגיטלית.

מעבדות אונליין: Google Phishing Quiz, ניתוח כתובת URL

LPI Domain: 2.2 Social Engineering

05

נוזקות ומתקפות זדוניות | Malware & Malicious Software

התלמידים נחשפים לעולם הנוזקות – כופרות, תולעים, Botnets ועוד. היחידה מסבירה איך נוזקות פועלות, מהן טכניקות הפצה וכיצד ניתן לזהותן בשלב מוקדם.

מעבדות אונליין: ניתוח Hash של קובץ חשוד, תצוגת כופרה תיאורטית

LPI Domain: 2.2.2 Malware

06

יסודות רשתות – חלק א׳ | Network Fundamentals – Part 1

יחידה זו מציגה את יסודות הרשת: כתובות IP, Subnet, פורטים, פרוטוקולי TCP/UDP. זוהי תשתית קריטית לכל ידע עתידי בסייבר.

מעבדות אונליין: dnschecker.org, Ping / Traceroute Online

LPI Domain: 3 – Network Basics

יחידות הלימוד: יחידות 7-12

01

יסודות רשתות – חלק ב׳ | Network Fundamentals – Part 2

היחידה מתמקדת בפרוטוקולי Web מרכזיים: HTTP, HTTPS, DNS Resolver וקשרי שרת־לקוח. התלמידים לומדים לבחון תעבורה ולזהות בעיות בסיסיות.

מעבדות אונליין: Developer Tools → Network, בדיקת HTTPS ב־SSL Labs

LPI Domain: 3 – Protocols & Services

02

אבטחת רשתות | Network Security

ביחידה זו התלמידים לומדים על שכבות ההגנה ברשת – Firewall, IDS/IPS, VPN. הנושאים מהווים את תשתית ההגנה הקריטית של כל ארגון.

מעבדות אונליין: בדיקת פורטים (yougetsignal.com), SSL Analyzer

מעבדות IronScale: Creating Network-Based Firewall, Snort Detections and Analysis

LPI Domain: 3.3 Network Security

03

יסודות Web ואבטחת Web | Web Fundamentals & Web Security

היחידה מציגה לתלמידים כיצד מובנה אתר אינטרנט, מהו HTTP Request/Response, מהן חולשות Web נפוצות וכיצד לבדוק תקינות בסיסית של יישום Web.

מעבדות אונליין: ניתוח HTTP Request/Response, Cookie & Session Exploration

מעבדות IronScale: Detecting XSS in WordPress, File Inclusion Assessment

LPI Domain: 2.3 Web Weaknesses

04

יסודות Windows | Windows Fundamentals

יחידה תפעולית־מערכתית שמלמדת את עקרונות העבודה עם Windows: מערכת קבצים, NTFS, ממשק ניהול, תהליכים ושירותים.

מעבדות אונליין: בדיקות הרשאות NTFS בסיסיות

מעבדות IronScale: Basic Windows Commands, Processes with Task Manager

LPI Domain: 3.4 Host Security

05

הקשחת Windows | Windows Hardening

יחידה זו מלמדת כיצד להפוך את Windows למאובטח יותר — עדכונים, Anti-Malware, מדיניות סיסמאות, הרשאות ותצורות הגנה.

מעבדות אונליין: ניתוח תצורת Windows Defender

מעבדות IronScale: Hardening My Operating System, Audit Policies

LPI Domain: 3.4 Host Security

06

יסודות Linux | Linux Fundamentals

יחידה מקיפה הבונה יכולת בסיסית בעבודה עם טרמינל, הרשאות, מבנה מערכת ופקודות ליבה.

מעבדות אונליין: WebVM / JSLinux – פקודות בסיס

מעבדות IronScale: Basic Linux Commands, Linux CLI

LPI Domain: 3.4 Host Security

יחידות הלימוד: יחידות 13-18

01

הקשחת Linux וניהול לוגים | Linux Hardening & Logs

היחידה מכסה הרשאות, שירותים וניתוח לוגים במערכות לינוקס — מיומנות קריטית בתפקידים תפעוליים ואבטחתיים.

מעבדות אונליין: שינוי הרשאות + הפעלת שירותים

מעבדות IronScale: Hardening My Operating System (Linux), Inspecting Linux Logs

LPI Domain: 3.4 Host Security

02

ניהול זהויות והרשאות (IAM) | Identity & Access Management

היחידה עוסקת במנגנון בקרת הגישה: משתמשים, קבוצות, הרשאות ותפקידי מערכת. זהו בסיס לכל ארכיטקטורת אבטחה.

מעבדות אונליין: סימולציית הרשאות (Google Docs Permissions)

מעבדות IronScale: Creating & Managing AD Objects, User Password Policies

LPI Domain: 4 – IAM

03

אימות וסיסמאות | Authentication & Password Security

יחידה זו עוסקת בפרקטיקות אבטחה בסיסיות — סיסמאות חזקות, Brute Force (קונספטואלית), MFA ו־SSO.

מעבדות אונליין: Password Strength Checker, הפעלת MFA חשבון אמיתי

מעבדות IronScale: Account Lockout Simulation, Password Cracking (Demo)

LPI Domain: 4 – Authentication

04

הצפנה וגיבוב – יסודות | Encryption & Hashing Fundamentals

יחידה זו מסבירה כיצד מגנים על מידע באמצעות הצפנה סימטרית ו-Hashing — כולל שימושים יומיומיים כמו שמירת סיסמאות.

מעבדות אונליין: Hash Generator, Base64 Encoding/Decoding

מעבדות IronScale: Hash Cracking (Demo), File Encryption Basics

LPI Domain: 1.3 Encryption

05

הצפנה א־סימטרית ו־TLS | Asymmetric Encryption & TLS

התלמידים לומדים על Public/Private Keys, תעודות דיגיטליות, חתימות וטכנולוגיית TLS/HTTPS.

מעבדות אונליין: בדיקת HTTPS Certificate, Certificate Chain Inspection

מעבדות IronScale: SSL/TLS Inspection, Certificate Chain Exploration

LPI Domain: Encryption & Network Security

06

סריקות רשת ו־Recon טכני | Network Scanning & Technical Recon

התלמידים מבצעים מיפוי פעיל של רשתות: פורטים, שירותים, Banners וזיהוי פוטנציאל תקיפה.

מעבדות אונליין: Nmap Online, PortQuiz

מעבדות IronScale: Nmap Port Scanning, Service Enumeration

LPI Domain: 2.3 Network Attacks

יחידות הלימוד: יחידות 19-24

01

חולשות, CVE ו־Exploits | Vulnerabilities & Exploits (Conceptual)

יחידה זו מסבירה כיצד חולשות נוצרות, איך מתעדים אותן (CVE) ומה ההבדל בין חולשה לניצול.

מעבדות אונליין: CVE Details, בדיקת CVSS Score

מעבדות IronScale: Types of XSS, SQL Injection Playground

LPI Domain: 2.3.2 Exploits

02

ניטור, לוגים ו־SIEM | Monitoring, Logs & SIEM

יחידה זו עוסקת בקריאת לוגים, זיהוי חריגות, הבנת מבנה אירוע וזיהוי מוקדם של תקיפה.

מעבדות אונליין: Developer Tools → Console Logs

מעבדות IronScale: Analyzing Logs Using Splunk, SIEM Integration with Apache Logs

LPI Domain: 3.6 Monitoring

03

Incident Response וחקירה | Incident Response & DFIR Basics

יחידה מקיפה על תהליך התגובה לאירוע: זיהוי, עצירה, חקירה ושחזור.

מעבדות אונליין: בניית ציר זמן אירוע, תחקיר טקסטואלי

מעבדות IronScale: Windows Event Viewer Investigation, DFIR Considerations

LPI Domain: 3.6 IR

04

IoT ואבטחת רשת ביתית | IoT & Home Network Security

היחידה מציגה איומים על מכשירים חכמים, נתבים ביתיים, מצלמות ועוד — עולם שמוכר לתלמידים וקרוב לחייהם.

מעבדות אונליין: Explore Shodan (קריאה בלבד), זיהוי התקנים ברשת ביתית

מעבדות IronScale: Network Authentication, IoT Device Enumeration

LPI Domain: 2.4 IoT Risks

05

ניהול סיכונים, הגנת מידע ומדיניות | Risk Management, Data Protection & Policies

יחידה זו משלבת ניהול סיכונים, גיבוי וניהול מידע, ותפיסות של מדיניות אבטחת מידע ברמה ארגונית.

מעבדות אונליין: Risk Matrix Exercise, תרגול הרשאות בענן

מעבדות IronScale: Recovering Deleted Files, Handling Local Security Policies

LPI Domain: 1.4, 5.4, 5.5

06

סימולציית מבחן וגמר הקורס | Final Exam Simulation & Cyber Battle Royale

יחידה מסכמת הכוללת סימולציית מבחן מלאה, קרב סייבר בין קבוצות (Blue vs Red) וחקירת DFIR מסכמת.

מעבדות אונליין: סימולציית מבחן LPI, תחקיר Red/Blue

מעבדות IronScale: Crack it Like a Boss, Process Investigation, Detecting XSS in WordPress, Splunk Investigation & Dashboarding

LPI: All Domains

מבנה הקורס המלא

הקורס מורכב מ־**24 יחידות לימוד** המכסות את כל תחומי אבטחת המידע הנדרשים להסמכת LPI Security Essentials.

24

יחידות לימוד

6

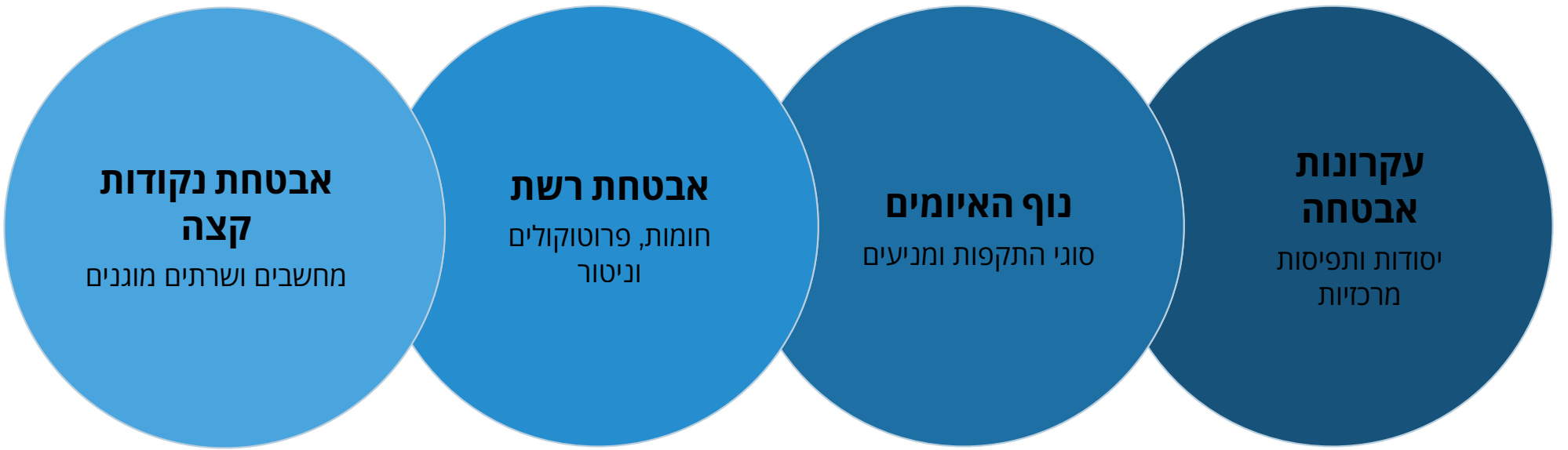
תחומי ליבה

100%

כיסוי מבחן LPI



תחומי הליבה של הקורס



הקורס מכסה שישה תחומי ליבה מרכזיים המשתלבים זה בזה ליצירת הבנה מקיפה של עולם אבטחת המידע. כל תחום בנוי על הקודם ומוביל לבא אחריו, תוך יצירת מסלול למידה הדרגתי ומעמיק.

מסלול הלמידה והתקדמות

שלב 1: יסודות

יחידות 1-6: מושגי יסוד, איומים, OSINT, הנדסה חברתית ויסודות רשתות

שלב 2: אבטחת מערכות

יחידות 7-13: אבטחת רשתות, Web, Windows, Linux והקשחת מערכות

שלב 3: זהויות והצפנה

יחידות 14-17: IAM, אימות, הצפנה סימטרית וא-סימטרית

שלב 4: תקיפה וחקירה

יחידות 18-21: סריקות, חולשות, ניטור ותגובה לאירועים

שלב 5: התמחות וסיכום

יחידות 22-24: IoT, ניהול סיכונים וסימולציית מבחן מלאה

כל שלב בנוי על הידע שנרכש בשלב הקודם, ומאפשר התקדמות הדרגתית מיסודות תיאורטיים ועד יישום מעשי מתקדם.

סיכום והמשך דרך



קורס **Cyber Battle Royale** מציע מסלול למידה מקיף, מעשיר ומאתגר לבני נוער המעוניינים להיכנס לעולם אבטחת המידע.

הקורס משלב:

- **תיאוריה מעמיקה** – כל מושגי היסוד והמודלים הנדרשים
- **תרגול מעשי** – מעבדות אונליין ו-IronScale
- **חוויה אמיתית** – קרבות Blue vs Red וחקירות DFIR
- **הכנה מלאה** – להסמכת LPI Security Essentials 020-100

בסיום הקורס, התלמידים יהיו מוכנים להיבחן בהצלחה ולהמשיך את דרכם המקצועית בעולם הסייבר.