

24 באוגוסט 2008

## הנדון : אינדקס קורסים - תוכניות לימודים

שלום רב,

להלן מידע אודות תוכניות הלימודים העומדות לרשותכם במסגרת הפורום הישראלי לאבטחת מידע, מועדי הלימודים ואופן ההצטרפות לפורום.

הלימודים נמשכים במשך שנה, על-בסיס מפגש חד-חודשי, במרכז הארץ, בכיתות לימוד פרונטליות וכוללים הדגמות מקצועיות. "תהליכי מכירות" אסורים מעבר להצגה עצמית מטעם המרצה. לימוד "מוצרים" – על-בסיס החלטתו הבלעדית של מנהל הקורס.

מידע מלא אודות המועדים הנוספים לכל קבוצה יפורסמו בהמשך.

### 1 מבוא - קבוצות הלימוד:

מנהל הקורס	יום קבוע ופתיחה	קבוצת לימוד
ג'קי אלטל	ה' 18/9/08	1.1 קבוצת Penetration Testing
יעקב פטרושקה	ג' 16/9/08	1.2 קבוצת GISO Functions & IT Security Department Management & Auditing
ארז מטולה	א' 14/9/08	1.3 קבוצת Application & DB Security
אופיר ליבר	ב' 15/9/08	1.4 קבוצת Frauds Prevention
ליאור ברש	ד' 17/9/08	1.5 קבוצת Security Tools & Technologies
בקרוב	בקרוב	1.6 קבוצת Infrastructure Security

- הפורום שומר לעצמו את הזכות המלאה לבצע שינויים במועדי המפגשים, בתכולתם ובמרצה, על-בסיס זמירותם.
- תכני הלימודים הנם מקצועיים. חומר הלימוד מבוסס שקפי PDF.
- המפגשים, אחת לחודש, בשעות 18:00 עד 20:00.

Information Security

מומחה באחד התחומים? מעוניין להרצות? אנא, פנה אל איתי ינובסקי: 052-6002745, [yanovski.itay@il.zim.com](mailto:yanovski.itay@il.zim.com)

### 2 הצטרפות והשתתפות בלימודים:

- 2.1 מילוי טופס הצטרפות לפורום הישראלי לאבטחת מידע המצ"ב, לרבות פרטי העדפת התנדבות (חובה), ומשלוחו בפקס: 03-6345345.
- 2.2 מסירת פרטי כרטיס אשראי לתשלום למזכירת הפורום: דורית שאול, בטלפון: 03-7731001, או הבאת המחאה לפקודת "איל"א" מסומנת "למוטב בלבד" למפגש הראשון (תנאי כניסה).
- 2.3 לשאינם מעוניינים בחברות בפורום הלאומי/ישראלי: תשלום בסך 50 שח למפגש בודד בהמחאה/ מזומן במועד המפגש (לא קיים הסדר זיכוי להצטרפות מאוחרת).

### 3 מפרט תוכניות הלימוד:

<p><b>ב קבוצת CISO Functions &amp; IT Security Department Management &amp; Auditing</b></p> <p><b>מידע כללי:</b></p> <p><u>מועד:</u> בימי ג', החל מיום ג' 16/9/08.</p> <p><u>מנהל הקורס:</u> יעקב פטרושקה.</p> <p><u>מרצים:</u> יעקב פטרושקה, איציק כוכב, אלון פלקסר, גלעד ירון, אופיר זילביגר, איתי ינובסקי, דני וישליצקי, שוקי פרייס, עמיר דויד, רוא"ח זאב אילברט.</p> <p><u>רקע מומלץ:</u> אבטחת מידע / ביקורת מערכות מידע / משפט.</p> <p><u>מיקום:</u> יפורסם בהמשך לנרשמים בלבד (מרכז הארץ).</p> <p><b>תכנית הלימודים:</b></p> <ol style="list-style-type: none"> <li>עקרונות בסיסיים באבטחת מידע (Generally Accepted Information Security Principles)</li> <li>מבוא להערכת סיכונים</li> <li>מבוא להערכת וניהול סיכונים</li> <li>תכנית אבטחת המידע כפונקציה של הארכיטקטורה, מדיניות ובקורות ותהליכים באבטחת מידע</li> <li>אבטחת מידע כתהליך – תהליכים באבטחת מידע</li> <li>בשלות תהליכים באבטחת מידע ובשלות התוכנית</li> <li>מסמך מדיניות ארגונית לאבטחת מידע</li> <li>ניהול לוגים ומערכות EISM</li> <li>ניהול תגובה לאירועי אבטחת מידע</li> <li>תקציב אבטחת מידע והקצאת משאבים</li> <li>מדדים להצלחה ומדידת יעילות התכנית</li> <li>ביקורת מערכות מידע</li> </ol>	<p><b>א קבוצת לימוד Penetration Testing</b></p> <p><b>מידע כללי:</b></p> <p><u>מועד:</u> בימי ה', החל מיום ה' 18/9/08.</p> <p><u>מנהל הקורס:</u> ג'קי אלטל.</p> <p><u>מרצים:</u> ג'קי אלטל, דודי ממון, ארז מטולה, זאב שניידר, יונתן בוקובזה, יורם כהנא, מיכה בורד.</p> <p><u>רקע מומלץ:</u> רשתות / פיתוח.</p> <p><u>מיקום:</u> יפורסם בהמשך לנרשמים בלבד (מרכז הארץ).</p> <p><b>תכנית הלימודים:</b></p> <ol style="list-style-type: none"> <li>מבוא להאקנינג, סרטון הדגמה (תקציר הקורס)</li> <li>שימוש בכלי בדיקה/תקיפה (Live-CD) לינוקס (שימוש מתקדם ב-backtrack)</li> <li>איסוף מידע פאסיבי מרשת האינטרנט - Passive Reconnaissance</li> <li>איסוף מידע (אקטיבי) שימוש באתרים ובכלי חיפוש מידע ברשת</li> <li>חיפוש מתקדם בגוגל (גוגל ככלי איסוף מידע/תקיפה) - GOOGLE Hacking</li> <li>Sniffers, Port Scanners</li> <li>התקפות ברשת המקומית. MITM</li> <li>מציאת פגיעויות וכתובת קוד שינצל אותן- Buffer overflow</li> <li>התקפות צד לקוח</li> <li>הזרקת קוד עניין לשרתי INJECTION SQL -WEB</li> <li>TUNNELING SSH</li> <li>TROJAN/ROOTKITS</li> </ol>
<p><b>ד קבוצת Frauds Prevention</b></p> <p><b>מידע כללי:</b></p> <p><u>מועד:</u> בימי ב', החל מיום ב' 15/9/08.</p> <p><u>מנהל הקורס:</u> אופיר ליבר.</p> <p><u>מרצים:</u> אופיר ליבר, אריאל פיסצקי, איתי הורוביץ, משה רובינשטיין, אייל שרון, ליאור ישראלי, מירב ורד.</p> <p><u>רקע מומלץ:</u> פרטים בקרוב.</p> <p><u>מיקום:</u> יפורסם בהמשך לנרשמים בלבד (מרכז הארץ).</p> <p><b>תכנית הלימודים:</b></p> <ol style="list-style-type: none"> <li>הקמת מערך מהימנות עובדים בארגון והונאות עובדים- אופיר ליבר</li> <li>מבדקי מהימנות</li> <li>דרישות אבטחת כרטיסי אשראי</li> <li>הונאות כרטיסי אשראי</li> <li>אירועי אבטחת מידע בחברות – שלב ההוכחות.</li> <li>הונאות טלפוניה</li> </ol>	<p><b>ג קבוצת Application Security</b></p> <p><b>מידע כללי:</b></p> <p><u>מועד:</u> בימי א', החל מיום א' 14/9/08.</p> <p><u>מנהל הקורס:</u> ארז מטולה.</p> <p><u>מרצים:</u> ארז מטולה, מתי סימן, ירון חקון, אבי דוגלן, עמית קורן, רן אדלר.</p> <p><u>רקע מומלץ:</u> פיתוח / אבטחת מידע.</p> <p><u>מיקום:</u> יפורסם בהמשך לנרשמים בלבד (מרכז הארץ).</p> <p><b>תכנית הלימודים:</b></p> <ol style="list-style-type: none"> <li>מבוא לאבטחת אפליקציות (תקציר הקורס)</li> <li>מתקפות אפליקטיביות</li> <li>ביצוע בדיקות קוד (code review)</li> <li>עקרונות לכתיבת קוד מאובטח</li> <li>ביצוע בדיקות חוסן אפליקטיביות (application penetration testing)</li> <li>ניהול תהליכי פיתוח לפי מודל SDL (Secure)</li> </ol>

<p>Socials engineering (7) (8) שיעורים 8-12 – פרטים בקרוב.</p>	<p>(Development Life Cycle) (7) אוטנטיקציה וניהול הרשאות נכון (8) קריפטוגרפיה (9) אבטחת SOA ו web services (10) אבטחת תשתיות האפליקציה (11) אבטחת בסיסי נתונים (12) רגולציות והשפעתן על תהליכי הפיתוח</p>
<p><b>ו קבוצת לימוד Infrastructure Security</b> <b>מידע כללי:</b> <b>מועד:</b> <b>פרטים בקרוב.</b> <b>תכנית הלימודים:</b> (1) <b>פרטים בקרוב.</b></p>	<p><b>ה קבוצת Security Tools &amp; Technologies</b> <b>מידע כללי:</b> <b>מועד:</b> בימי ד', החל ד' 17/9/08. <b>מנהל הקורס:</b> ליאור ברש. <b>מרצים:</b> ליאור ברש, ישי ורטהיימר. <b>רקע מומלץ:</b> ניהול רשתות. <b>מיקום:</b> יפורסם בהמשך לנרשמים בלבד (מרכז הארץ). <b>תכנית הלימודים:</b> Thinking security technologies: Technology (1) Environment Defined Cryptography (2) Access control (3) Perimeter protection: Firewalls, Proxy (4) Architectures Remote Access: Virtual Private Networking (5) Detection and response: IDS \ IPS (6) Anti-malware technologies – Viruses, Worms, (7) Trojans, Spyware Physical and Wireless security (8) Risk management: Assets Management, Patch (9) Management, Vulnerability Management SIM - Security Information Management (10) BCP/DRP in a nutshell (11) Microsoft server 2003: Active Directory, IIS, (12) Exchange, WSUS, MS-CA, IP-Sec, RMS</p>

בברכה,

דורית שאול,  
מזכירת הפורום  
03-7731001  
[ila@ila.org.il](mailto:ila@ila.org.il)

אבי ויסמן,  
יו"ר הפורום  
03-6122831, 054-5222305  
[avi@nisf.org.il](mailto:avi@nisf.org.il)

איתי ינובסקי, ס' יו"ר הפורום  
ראש ועדת הכשרה מקצועית  
052-6002745  
[yanovski.itay@il.zim.com](mailto:yanovski.itay@il.zim.com)