קורס Information Security Tools & Technologies

יועץ אקדמי: מר אבי ויסמן *

תוכנית לימוד בת 40 שעות לימוד לבעלי רקע של תשתיות טכנולוגיות, למפתחים או לעוסקים במערכות מידע המעוניינים בהיכרות עם טכנולוגיות אבטחת מידע בראייה הנדסית-ניהולית.

מבוא

קורס InfoSec Tools & Technologies נבנה כקורס סקירה אודות טכנולוגיות נפוצות בעולם הגנת המידע, בראייה תכנונית הנדסית, ולא כקורס יישום כלים (התקנה ותחזוקה). הקורס ממוקד בפן זה, לצד קורסים ממוקדים נוספים כגון: קורס תכנון אבטחה, קורס תקיפת מערכות, קורס ניהול, ארגון ושיטות ניהול אבטחה, וקורס ממשל אבטחת מידע.

מטרת התכנית

לספק סקירה מקיפה על כלים קנייניים טיפוסיים, או כלים המהווים חלק ממערכת מלאה, בראיית של מהנדס/מנהל.

קהל היעד

בעלי רקע בתחומי ה- IT ופיתוח תכנה, ובפרט פרוטוקולי תקשורת, מערכות הפעלה Windows ו- Linux, אבטחת מידע ו- Hacking.

מתכונת הלימודים

משך התכנית כ- 40 שעות אקדמיות או 60 שעות אקדמיות, לארגונים כקורס בלעדי - במתכונת של לימודי יום (09:00 עד 16:00), ולבודדים – כקורס ערב (השתלבות במסלול קיים לצורכי קורס זה).

עלות התכנית

יש לפנות להנהלת המכללה.

זכאות לתעודה

- קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחן סיום, בציון 70 לפחות.
- תיעוד: בוגרי הקורס אשר יעמדו במבחן הסיום בציון 70 לכל הפחות, יזכו מטעם מכללת See Security בתעודת בוגר קורס:

Information Security Tools & Technologies

ה ע ר ו ת :

- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- דמי ההרשמה ומבחנים חיצוניים כלשהם אינם כלולים בשכר הלימוד.
- המכללה מביאה לידיעת הנרשמים והתלמידים כי ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.
- רשימת תת הנושאים, עומקם ורוחבם עשויה להשתנות בהתאם לשליטת התלמידים בחומר.

לכל מידע נוסף או לתיאום ראיון אישי או פגישת יעוץ:

מידע מינהלי: אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com

יועץ אקדמי: אבי ויסמן : 054-5222305, avi@see-security.com

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

מתודולוגיה: מקצועות אבטחת מידע ותחומי אבטחת מידע

הקורס נבנה על-בסיס פדגוגי ודידקטי ואוריינטציה פרקטית בפיקוח אקדמי, במדרג של בעלי תארים (רמות שונות), והכרה בארגונים בעלי אתיקה דומה (ISC2, ISACA, GIAC, ISSA, SII). תשומת לב ניכרת ניתנת לדגשים הנהוגים בישראל (הפורום הישראלי לאבטחת מידע IFIS).

המתודולוגיה המתוארת מתבססת על רשימת כל המקצועות התעסוקתיים המקובלים בתעשיית אבטחת המידע ולוחמת המידע, ומולם – כל תחומי הידע הקיימים בעולם זה.

מהמטריצה נגזר הידע הנדרש לכל מקצוע, ומכאן - נגזרים מסלולי הלימוד והקורסים, היקפיהם ומיקודם. מטריצה זו של הפורום הישראלי לאבטחת מידע מהווה עמוד שידרה למתודולוגיית הלימודים של See Security.

מקצועות והתמחויות בעולם אבטחת המידע (מודגשים המקצועות הנפוצים יותר)

1. מינהלן אבטחת מידע - **ISAD** - Information Security Administrator
2. מיישם מערכות אבטחת מידע - **ISSI** - Information Systems Security Integrator
3. מהנדס אבטחת מידע - **ISSE** - Information Security Systems Engineer
4. מנהל אבטחת מידע יח' המחשב - **ISSO** - Information Systems Security Officer
5. מנהל אבטחת מידע ארגוני - **CISO** - Chief Information Security Officer
6. מבקר אבטחת מידע - **ISA** – Information Security Auditor

התמחויות (מומחה תחומי באבטחת מידע - Information Security Expert – ISE)

A מומחה ניטור אירועי אבטחה - Information Security Incident Expert - ISIE
B מומחה בדיקות חדירות - Testing Information Security Penetration Expert - ISPTE
C מומחה חקירות למערכות מידע - Forensics Information Systems Expert - ISFE
D מומחה אבטחה פיזית למערכות מידע - Physical Security Information Systems Expert - ISSPE
E מומחה אבטחת יישומים ופיתוח - Security Application Development Expert - ADSE
F מנהל פרויקט למערכות אבטחת מידע - Information Security Systems Project Manager - ISSPM

עולמות ידע (תחומים) בעולם אבטחת המידע

העולמות השונים המהווים יחד "אבטחת מידע" או "הגנת מידע", מפורטים להלן. לכל אחד מהעולמות, ניתן להתייחס מאחת מהדיסציפלינות הבאות:

א. זוית הראייה של מיישם (הפן הטכני של התקנה ותחזוקה).
ב. זוית הראייה של מהנדס/ארכיטקט (פן התכנון המרחבי).
ג. זוית הראייה של מנהל אבטחת המידע הארגוני (משימות, נהלים ותהליכים).

1. עולם אבטחת תשתיות מחשוב (מערכת הפעלה, תקשורת, אלחוטית, ניידים, קוד ואפליקציה, Web)
2. עולם הכלים והטכנולוגיות (FW, IDS, IPS, PKI, VPN, Anti's, Spofer, Scanner, Biometrics…)
3. עולם התקיפה והלוחמה הקיברנטית (Hacking & Cyber Warfare)
4. עולם ממשל אבטחת המידע (Governance: Laws, Regulations, Standards & Business needs)
5. עולם הניהול והאו"ש של יחידת אבטחת מידע (משימות, תהליכים, תיאור התפקיד)

* עולם האבטחה הפיזית – לא נכלל במתודולוגיה, אך נושק לעולם אבטחת המידע ואף חופף לו בהיבטים אחדים, בהגנה ובהתקפה.

תוכנית הלימודים

1. **Certificate and Security Overview**

- Certificate overview
- Information Security Matrix
- Security Overview
- Information Security Risk Management & Prioritize Approach
- Security Plan and Preparation

2. **Methods of Information Security (The Technical Landscape)**

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-Repudiation

3. **Threats**

- Definition
- Threat Classification
- Threat Model
- Threat agents
- Threat Communities
- Threat Analysis
- Threat Management

4. **Vulnerabilities**

- Definition
- Vulnerabilities Classification
- Vulnerabilities Causes
- CVE & CVSS

5. **Controls**

- Definition
- Preventive
- Detective
- Corrective
- Common Countermeasures

6. **Attack and Defense Techniques**

- Defense Models
- Defense in Depth
- ISSE
- Common Criteria

7. **Cryptography**

- Introduction to cryptography
- Classic cryptography to Modern Cryptography
- Basics of Modern Cryptography
- Symmetric Key Algorithms
- Block Ciphers Modes of Operation
- Stream ciphers
- Key Management
- Public Key Cryptography
- Message Integrity and Authentication Controls
- Public Key Infrastructure
- Installing Configuring & Maintaining Certification Authorities
- Configuring, Deploying & Maintaining Certificates, EFS

8. **Identity and Access Management**

- Access Control
- What is Access control
- Identification and authentication (I&A)
- Authorization and AC Models
- Centralized Access Control Methodologies
- The IDM Paradigm
- IAM process
- Identity Management Systems

9. Smart Cards/Tokens Security and Applications

- Smart Cards
- Tokens
- Biometric

10. Software Security

- OWASP
- WASC
- Application Threats and Attacks
- SDLC

11. Database Security

- Access Control
- Auditing
- Authentication
- Encryption
- Integrity Controls
- Database Activity Monitoring (DAM)

12. Secured Network Architecture

- Network Secure Design
- Secured Network Components
- Enclave defined,
- The need for Perimeter Protection,
- Router security
- Firewalls
- VPN Technology
- NAC

13. Physical Security

- Standards
- Environmental design
- Mechanical, Electronic and Procedural Access Control
- Intrusion Detection
- Video Monitoring

14. Wireless Security

- Wireless Technologies
- Wireless Encryption Methods
- Vulnerabilities & Countermeasures

15. DLP

- Data Leakage prevention techniques and implementation

16. Cloud Computing Security

- Cloud computing definitions and technologies.
- Designing and implementing security policies for cloud computing
- Monitoring cloud computing security.
- Defense techniques

17. Mobile Security

- Mobile Device Management (MDM)

18. Detection and Response

- The Need for Detection Systems
- IDPS Systems Capabilities
- Implementation & Management
- Security Information & Event Management
- Log Retention And Management
- Organizing a SIEM Project

19. Social Networks

- Sociology
- Social Network analysis
- Social Network as a Business
- Biology and Social Networks
- Business Information Analysis

20. Cyber Warfare

- Tools and Techniques
- Information Operation
- Non-Military

דף רישום ללימודים בעמוד הבא

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

לכבוד
המכללה לאבטחת מידע וללוחמת מידע
שיא סקיוריטי טכנולוג'יז בע"מ
רמת-גן – פקס : 03-6122593

נא לרשום אותי לתוכנית הלימודים ברמת גן

קורס Information Security Tools & Technologies

פרטים אישיים:

שם משפחה _____ שם פרטי _____ ת.ז._____ שנת לידה _____

כתובת פרטית _____.

טל' בבית: _____ טל' נייד_____פקס_____ .

כתובת E –mail _____.

מקום עבודה:

שם החברה_____טל' _____ תפקיד_____.

לתשלום (נא סמן בחירתך):

☐ 400 ₪ - דמי רישום (חובה בכל מקרה) ☐ _____ ₪ - מקדמה (בגובה 10% משכר הלימוד)

☐ שכר לימוד בסך _____₪

☐ מצ"ב שיק מס' _____ע"ס _____ ₪ (ניתן לשלם עד _____תשלומים בהמחאות דחויות)

(את ההמחאות יש לרשום לפקודת שיא סקיוריטי בע"מ)

☐ מצ"ב מכתב התחייבות המעסיק, אם הינך ממומן על ידו. (1) יודפס ע"ג נייר לוגו (2) בציון מספר ח.פ של החברה, (3) לתשלום שוטף + 30 ממועד הפתיחה לכל היותר)

☐ נא לחייב כרטיס אשראי ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

☐ בתשלום אחד

☐ ב- _____ תשלומים (עד 18 תשלומים בקרדיט).

☐ ב- _____תשלומים ללא ריבית.

שם בעל הכרטיס _____ ת.ז. בעל הכרטיס _____תא' לידה של בעל הכרטיס _____.

כתובת בעל הכרטיס, המעודכנת בחברת האשראי _____.

טלפון בעל הכרטיס, המעודכן בחב' כרטיסי האשראי _____ .

שם בנק+סניף הבנק בו מנוהל חשבון כרטיס האשראי _____ .

- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכון וSee Security.
- דמי ההרשמה אינם כלולים בשכר הלימוד.
- יש לוודא כי התשלומים יסתיימו עד למועד סיום הקורס.

תאריך: _____ חתימה: _____.

שיא א. סקיוריטי טכנולוג'י בע"מ	ח.פ: 513431403	ספק משהב"ט: 83/168200