

קורס סייבר ואבטחת מידע - אנליסט SOC

AI CONCEPT



**הכנה למבחני ההסמכה
הבינלאומיים:**

Linux Professional Institute - Linux Essentials
CompTIA - Cybersecurity Analyst (CySA+)
EC-Council - Certified SOC Analyst (CSA)

ראש תחום מקצועי:
יקי בן ניסן

ICS 
המרכז הארצי ללימודים

רקע על ראש התחום:

יקי בן ניסן - מנהל מקצועית את הקורס, והינו הבעלים של חברת ייעוץ בתחום אבטחת מידע וכן מרצה מבוקש בתחום רשתות ואבטחת מידע בסייבר למעלה מ-20 שנה. לצידו מובילים את התוכנית סגל מרצים מקצועיים, בעלי ניסיון וותק רב שנים בתעשייה. נותן שירותים למוסד, לשב"כ ולחברות מובילות בארץ ובעולם.

כללי

תחומי הסייבר ואבטחת המידע מתרחבים בכל יום וזאת בשל האיומים ההולכים וגוברים. אחד המקצועות שצמחו מתוך צרכי האבטחה הוא אנליסט אבטחת מידע וסייבר.

תוכנית הקורס

הקורס כולל ספרות מקורית בעברית וחומר לימוד רשמי באנגלית של Cisco Network Academy



מה צריך לדעת אנליסט אבטחת מידע?

דרישות התפקיד הם היכרות מעמיקה עם מערכות הפעלה, מערכות תקשורת, ידע באבטחת מידע וידע בתקיפה.

שכר בתחום:

כמה מרוויחים מומחי סייבר ואבטחת מידע?

מומחה אבטחת מידע Malware analyst

0-1 שנים 12,000-16,000 ₪

3-5 שנים 21,000-27,000 ₪

דרג ניהולי 28,000-35,000 ₪

על-פי טבלאות השכר המפורסמות ברשת

מה תפקידו של אנליסט אבטחת מידע?

מרכז ניטור האבטחה בארגון (SOC – Security Operating Center) זהו מרכז הניטור והבקרה של אבטחת המידע בארגון. בדרך כלל מרכז זה פעיל במתכונת רציפה במשך כל שעות היממה ובכל ימות השנה במטרה לספק הגנה בלתי פוסקת לנכסי המידע של הארגון. במרכז זה פועלים כל בעלי התפקידים בתחום אבטחת המידע בארגון כולל האנליסטים שלו.

תפקידו של אנליסט אבטחת מידע מתמקד בהגנה על המידע הארגוני מפני סיכונים האורבים לו מחוץ לארגון, ניטור אבטחת הרשת הפנימית בארגון ובדיקת חריגות של מחלקה מסוימת או של הארגון כולו.

הכנה להסמכות בינלאומיות

Linux Professional Institute - Linux Essentials

CompTIA - Cybersecurity Analyst (CySA+)

EC-Council - Certified SOC Analyst (CSA)



דרישות סף:

נדרש יכולת קריאת טקסט באנגלית ברמה סבירה.
רצוי אך לא חובה ידע קודם במחשבים.

קהל יעד:

הקורס מיועד לאנשים ללא רקע בתחום ההייטק, לבעלי רקע בסיסי במחשבים ולאנשי IT, המבקשים להשתלב בתחום אבטחת המידע והסייבר או לעבור הסבה מקצועית לתחום זה.

מה לומדים?

קורס סייבר ואבטחת מידע

מודול 1 -

יסודות רשתות תקשורת

- כיצד התקן מזוהה ברשת
- בדיקת קישוריות ברשת (ICMP)
- מושגי יסוד ברשתות
- Address Resolution Protocol
- כתובות מסוג IPv4
- מודל OSI
- TCP-IP Ports & Protocols
- כיצד מבצעים ניתור לרשת באמצעות Wireshark

מודול 2 -

הגדרת ציוד תקשורת ואבטחת הרשת מפני תוקפים

- Basic IOS Configuration
- הגדרת שרת DHCP
- הגדרת ניתוב סטטי וניתוב דינמי (OSPF)
- הגדרת NAT
- Virtual LAN (VLAN)
- Access Control Lists
- Port Security

מודול 3 -

מערכות הפעלה -

Windows Server 2022

- התקנת שרת כמכונה וירטואלית בסביבה וירטואלית
- התקנת וניהול Active Directory
- יצירה וניהול של משתמשים וקבוצות
- ניהול הרשאות גישה ושיתוף תיקיות
- הקשחת סביבת העבודה באמצעות Group Policy

מודול 4 - מערכות הפעלה -

Linux

- היסטוריה של לינוקס
- The Shell - Linux Command Lin
- ניהול קבצים
- Archive and Compression
- טיפול בקבצי טקסט ובפלט
- ניהול חשבונות משתמשים וקבוצות
- ניהול הרשאות גישה

מודל 5 - הגנת סייבר

- מונחים בעולם אבטחת מידע
- תקיפה (הסתכלות בעיני התוקף)
- CIA - Confidentiality, Integrity, and Availability
- Security Operations Center (SOC)
- Firewall Technologies and IPS-IDS
- Incident Response
- תחקור אירועים

מודל 6 - סייבר התקפי

- Cyber Kill Chain
- סוגי תקיפות
- סוגי תוכנות זדוניות
- NMAP
- Vulnerability Scanning
- Cyber Threat Intelligence
- Penetration Testing
- סייבר התקפי
- התקפה תשתיתית
- התקפה אפליקטיבית



למען הסר ספק, מובהר כי המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכניות הלימודים, היקף שעות הלימוד, סגל המדריכים, ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

קורס מסתיים במעבר בהצלחה על המבחן המסכם, הגשת כל הפרויקטים ואחוז נוכחות בשיעורים > 80%

הגשה למבחנים חיצוניים כרוכה בעלות של אגרת בחינה
ותשלום ישירות למעבירי הבחינה החיצונית
בחינה פנימית במכללה וקבלת תעודה מהמכללה – ללא עלות

דוגמאות לתעודות גמר בסיום הקורס ו\או בסיום בחינה חיצונית בהצלחה:

