ITSAFE

Cyber Security Trainings

מסלול

אנליסט SOC היברידי

CYSOURCE

ISRAEL CYBER ALLIANCE

מסלול

אנליסט SOC היברידי

SOC (מרכז ניטור פעולות אבטחה) הוא מרכז אבטחת מידע ייעודי שמנטר, מזהה ומגיב לאירועי סייבר.
SOC כתפיסה הוא "לב ליבה" של הארגון, ולמעשה הוא הגוף הראשון שיחווה אירוע סייבר בארגון

המשימה העיקרית של **אנליסט SOC** היא לזהות ולנטר אירועים בזמן אמת, ולבצע חקירה ראשונית ועמוקה יותר על מנת לספק מאפייני זיהוי לאיום.

SOC יכול להיות החל מבקר או אנליסט אחד בודד שמבקר ומנטר אחר האירועים למרכז גדול המונה מספר רב של בקרים ואנליסטים. כאמור, המטרה העיקרית שלו היא פיקוח אחר רשתות, מערכות, התקני קצה ומשאבים רגישים אשר יכולים להיפגע ע"י תוקף מבחינה תדמיתית, עסקית ואף לפגוע בנכסי הארגון בצורה משמעותית.

מסלול **אנליסט SOC** הינו מסלול אשר מותאם לחסרי רקע המעוניינים להשתלב בתעשיית הסייבר **כאנליסטי SOC**
מסלול זה כולל 4 קורסים,שני קורסי ליבה **לינוקס Lpi Essentials, תקשורת נתונים CCNA**
ושני קורסי התמחות:
אנליסט SOC עם הכנה להסמכה בינלאומית **QRadar IBM Certified Associate Analyst**
ואיש צוות תגובה וטיפול באירועים **Incident Response Level 1**

ברוכים הבאים לפלטפורמת ITSAFE
מבית CYSOURCE

אז מי **אנחנו?**

CYSOURCE פועלת על מנת לפתח ולאתר את כוח האדם האיכותי ביותר בעידן הדיגיטלי על ידי שימוש בטכנולוגיות בינה מלאכותית (AI) ופלטפורמת SaaS מתקדמת אשר תומכת בלמידה בשלל שפות.

CYSOURCE מכשירה ומפתחת כוח אדם על ידי הידע שנצבר מהשטח, לסייסורס מחלקת תקיפה ומחקר אקטיבית אשר פועלת בגזרות הסייבר ההגנתי\ההתקפי ומהידע הנצבר בשטח נבנות ההכשרות שלנו על גבי פלטפורמת הלמידה.

הפלטפורמה שלנו הוקמה על מנת לתת מענה לחוסר כוח אדם בתעשיית הסייבר ולהנגיש מקצועות סייבר טכנולוגיים מתקדמים ולשלבם לעבודה בהייטק.
פלטפורמת ההכשרות החדשנית מאפשרת ללמוד ממגוון מומחים מוכרים בקהילת הסייבר.
ב **ITSAFE** למדו אלפי תלמידים ורבים הושמו לחברות סייבר מובילות.

אצלנו תלמידים לומדים
ובסוף עובדים!

ITSAFE
Cyber Security Trainings

בוגרים מספרים

חתמתי היום חוזה בחברת EY בתור גוניור PT.
רוצה להגיד תודה ענקית למכללת ITSafe על חומר מדויק שמכין אותך בצורה הכי טובה לעולם הסייבר.

הקורסים מועברים על ידי מרצים בעלי שם וידע מטורף.
יש מתרגלים העוזרים לכולם בכול שעה וזמן.
לקחת תלמיד בלי ניסיון והבאתו לשוק העבודה בתור PT פשוט מטורף בעייני, האמת שחשבתי אפילו בלתי אפשרי.

כל קורס מלווה בפרויקט מסכם, שזה מדהים לפי דעתי.
המכללה מכינה אותך בלי ידע, לידע מתקדם מאוד.
המכללה מעדכנת כל הזמן את הקורסים בהתאם לתעשייה.
המכללה עורכת ראיונות עבודה דמו על ידי בודקי חוסן כדי לבחון את ההתאמה לאחר הקורסים.

אביב וינוגרצקי
בודק חוסן EY

רוצים לדבר עם אביב?
חפשו אותו בלינקדאין:
Aviv Vinograzki

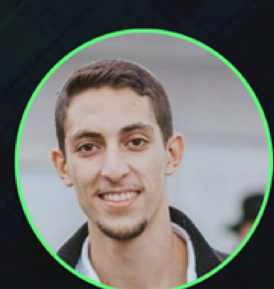
ITSAFE
Cyber Security Trainings

בוגרים מספרים

מגיל צעיר רציתי לעבוד בתחום, בתור ילד הייתי סקריפט קיד ותמיד אהבתי ורציתי ללמוד האקינג. ברגע הראשון אחרי שגזרתי חוגר חיפשתי איך אני משתלב בתחום בצורה הכי מקצועית שיש.
חקרתי ובדקתי מלא כיוונים קורסים פרונטליים וגם מקוונים.
הגעתי ל ITsafe ממודעה שקפצה לי בפייסבוק, שלחתי את הסילבוס של הקורס לחבר שעבד בתחום והוא אמר שזה נראה ממש טוב.
התלבטתי עם עוד קורס במקום אחר, אבל ב"ה עשיתי את ההחלטה הנכונה, חבר שלי שלקח את הקורס במכללה השניה והצטער על זה.

- החומר מועבר בצורה ברורה, מ0 ל 100 עם תמיכה בכל שאלה ותקלה.
- החומר מוכוון כולו להאקינג, ככה שתקבלו ערך מוסף.
- אפשר לחזור בכל רגע נתון שזה בונוס ענק.
- יש תרגולים ומעבדות לאורך הקורסים.
- קהילת תלמידים תותחים שתמיד עוזרים וכיף גם סתם לדבר איתם.
- והכי חשוב, עם עבודה קשה, בסוף יש גם עבודה.

בזכות ITsafe אני התקבלתי לעבודה בחברת Comsec בתור Web PT



אלדר שיביץ
בודק חוסן בחברת ComSec

רוצים לדבר עם אלדר?
חפשו אותו בלינקדאין:
Eldar Shayeviz

ITSAFE
Cyber Security Trainings

בוגרים מספרים

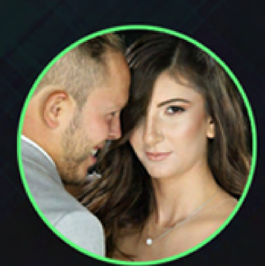
בקצרה (והכי חשוב!) - בזכות הקורס של ITSAFE והידע שצברתי בו התקבלתי לעבודה בתחום ה PT

עכשיו לפירוט - חיפשתי דרך להרחיב את הידע וללמוד בצורה טובה את תחום ה PT וראיתי את הקורס של ITSAFE,

חיפשתי חוות דעת של אנשים ויצרתי איתם קשר בשביל לקבל יותר מידע על איך הולך הקורס והאם הוא באמת טוב כמו שאומרים, והופתעתי לגלות שהקורס באמת נותן את הידע הדרוש בשביל למצוא עבודה בתחום ומעבר.

בנוסף, גם מבחינת המחיר, הקורסים מאוד משתלמים, ולמרות שהם מוקלטים (שלדעתי זה יתרון), יש קבוצות טלגרם שאפשר לדבר עם המרצים ולקבל תשובה על כל שאלה במהירות.

לדוגמא, קורס ה Web PT מתחלק ל 2 מה שבאמת מסביר לעומק איך האתר בנוי ואיך לחפש בו חולשות.
ממליצה בחום!



ענת אזולאי
בודקת חוסן בחברת EY

רוצים לדבר עם ענת?
חפשו אותה בלינקדאין:
Anat Azulay

70 שיעורים
11 שעות תוכן
מעבדות תירגול
30 שעות מעבדה

לינוקס Essentials

1. היכרות עם לינוקס

- ליונס טורבאלדס
- מהו OpenSource
- סוגי רשיונות בקוד פתוח
- סוגי מערכות לינוקס
- התקנת מערכת הפעלה
- Kali linux
- Ubuntu
- תוכנות נפוצות במערכת ההפעלה
- ניהול חבילות והתקנת תוכנות
- חנות האפליקציות והפקודה Apt

2. עבודה בסיסית בסביבת לינוקס

- פקודות שימושיות
- מניפולציה של קלט ופלט
- תהליכי סריקה וזיהוי פגיעויות
- חיפושי U Wildcard ו- Globaling
- ביטוי רגולרי והפקודה grep

3. מערכת הקבצים בלינוקס

- מערכת הקבצים HSF
- מיפוי קבצים Mount
- הגדרת משתנה סביבתי
- הגדרת הסביבה
- לינקים Hard and Symbolic
- פקודות חיפוש
- דחיסת קבצים

4. פיתוח בסיסי ב BASH

- סוגי כתבנים בלינוקס
- עבודה עם Vim
- מבוא לפיתוח בשפת Bash
- קלט,פלט ומשתנים
- תנאים
- פונקציות

5. תהליכים לוגים ואיתחול מערכת

- סוגי כתבנים בלינוקס
- עבודה עם Vim
- מבוא לפיתוח בשפת Bash
- קלט,פלט ומשתנים
- תנאים
- פונקציות

הידעת ?

90% מהשרתים בעולם
הינם שרתי לינוקס

6. תקשורת ושירותי רשת

- בדיקת תקשורת בין עמדות ברשת
- ניתוח תעבורת רשת
- שירותי רשת מוכרים וחיוניים
- DNS
- DHCP
- SSH
- כתובות עמדות ברשת ומושגים
- IP
- Gateway
- Netmask
- הגדרת כתובת רשת
- הגדרת DNS
- הגדרת Gateway Default

6. משתמשים והרשאות

- יצירת משתמשים וקבוצות.
- ניהול משתמשים במערכת.
- מבנה קובץ /Etc/Passwd
- הרשאות וקבצים.
- הרשאות מיוחדות.
- פרופיל המשתמש.
- מסכות.
- הרשאות מתקדמות.

94 שיעורים

13 שעות תוכן

מעבדות תירגול

110 שעות מעבדה

CCNA

Routing & Switching

1. היכרות עם עולם התקשורת

- סטנדרטים בתקשורת.
- מודל TCP/IP.
- מודל ISO.
- TCP/UDP.
- חבילות מידע ומבנה ה-Packet.
- כתובות Mac Address.
- כתובות IP.
- ציוד תקשורת.
- היכרות עם סוגי רשתות.
- הגדרת סביבת המעבדה.

2. עבודה עם מתגים

- מצבי גישה.
- פקודות כלליות להגדרת המתג.
- ARP Table
- Mac Address Table
- בדיקת תקשורת ברשת.
- הגדרת סיסמא ופריצת סיסמא
- ניהול מתג מרוחק
- חלוקה לוגית של הרשת VLAN
- תקשורת ברשת מבוססת מתגים.
- Native Vlan
- Trunk & DTP
- VTP
- Spanning Tree
- Rapid Spanning Tree
- IIDP & CDP
- EtherChannel

3. עבודה עם נתבים ברשת

- כתובות IP.
- חישוב כתובת IP על פי מסכת רשת.
- כתובות פרטיות ופומביות.
- VSLM
- ממשק וירטואלי לתקשורת בין VLAN's
- הגדרת נתב.
- DHCP
- WLC ו-LAP בעולמות ה-WiFi
- הגדרת רשת אלחוטית WiFi
- פרוטוקולי ניתוב.
- EIGRP
- OSPF
- שיפור ביצועי רשת באמצעות HSRP

4. שירותי רשת ואבטחת רשת

- NAT
- SYSLOG
- SSH
- התקפות על מתגים.
- התקפות על שירותי רשת.
- שימוש ב Access List.
- עבודה עם Port Security.
- כיצד לאבטח את הרשת.

5. IPV6 ואוטומציה

- היכרות עם IPV6
- הגדרת רשת מבוססת IPV6
- הגדרת ניתוב ב-IPV6
- ביצוע פעולות באמצעות אוטומציות.
- הגדרת מתגים ונתבים בצורה מהירה.
- עבודה עם ממשק API
- עבודה עם JSON

55 שיעורים | 10 שעות תוכן

מעבדות תירגול | 100 שעות מעבדה

SOC Analyst

1. Windows Environments

- What is Virtualization
- VirtualBox installation
- Virtualization Networking
- Deploy a virtual machine
- Windows Server 2016 installation
- What is Domain Controller
- Pre configurations for Domain Controller
- AD DS installation on DC
- Windows 10 Client installation
- Virtualization and Windows 10 Lab Setup
- Client domain joining
- DHCP service
- DHCP deployment
- IP ranges
- IP reservations
- DNS record types
- DNS Zones
- Creating and managing domain users
- Creating and managing domain groups
- Creating and managing GPO’s

2. Cyber Security Fundamentals

- CIA Triad
- Risk Consideration
- Identity Threats
- Risk Assessment
- Risk Control
- AAA Security
- Hashing
- Cryptography And Encryption
- Website Security
- Malwares

3. Attacker & Hacking Methodology

- Layer II Cyber Attacks
- Layer III Cyber Attacks
- Various Cyber Attack Types
- Cyber Kill Chain
- IOC

4. SIEM/SOC Fundamentals

- Organization Monitoring
- Soc Fundamentals
- The Adaptive Security Architectures
- Cyber Security Components And Vendors
- SIEM Introduction
- Qradar Siem Introduction
- WinCollect Installtion
- Windows Audit

5. Qradar SIEM Hands-On

- QRadar Log Activity
- QRadar Log Source
- Qradar Console
- Qradar DSM & Parsing
- Qradar Building Block
- Qradar Rules
- Qradar Reference Lists

6. Forensics, Threat Intelligence & SOAR

- Windows Sysinternals
- Windows Sysmon Installation
- Cyber Attack Summary
- Logs Forensics
- Threat Intelligence
- SOAR Concept

7. SOC Analyst -Student Labs

- LAB 1 – IBM Wincollect Installation On Dedicated Server.
- LAB 2 – Qradar-Create Custom Log Activity
- LAB 3 -Qradar – Parsing Fields From Payload.
- LAB 4 – Qradar – Create Custom Building block.
- LAB 5 – Qradar – Create Custom Rules
- Lab 6 – Qradar – Create Rules With Reference Lists.
- Lab 7 – Windows Sysmon Installation
- Lab 8 – Find The Suspicious Log
- Lab 9 – Threat Intelligence With QRadar

התעודה הזו יכולה להיות **שלך!**

57 שיעורים
7 שעות תוכן

מעבדות תירגול
40 שעות מעבדה

1. Attack & Defense Methodolgy

- Introduction
- MITRE ATT&CK
- Cyber Kill Chain
- TACTICS, TECHNIQUES & PROCEDURES
- Incedint Responde Methodolgy
- Proactive Hunt
- Live Analysis
- Ioc's Vs Ioa's
- Know Your Process
- Virtualization and Windows 10 Lab Setup

2. Threats And Scoping

- Host & Network Based incidents
- Threats types
- Threat triage
- Operation system visabilty
- PS Transcription And User Sid

3. Endpoint Threat Artifects

- The Sysinternals suite
- Process explorer Deep Dive
- Persistnce with Autoruns
- Autoruns CommandLine
- Exercise Scenario – Red Line Malware
- Unsigned binary detection
- Operation detection procmon
- Procmon Beautifier
- Njrat exercise – Detection and Response
- Network activity views
- Detect Source Zone Identifier
- System Resource Utilization Monitor
- RDP Cacheing
- ActivitiesCache

4. Windows Logs Analysis

- Windows Event logs
- Event Logon Types
- Event Id's
- Event Log Capabilities Demo
- Investigation Scenario Exercise
- Evtx Over TimeLine Explorer
- Sysmon
- Event Hunting

5. Registry Threat Artifects

- Registry Structure
- Registry File Acquisition
- Registry Explorer
- Registry Points Of Interst
- RegistryASEPS
- UserAssist
- ShellBags
- Setupapi

7. Evidence Of Execution

- Jump Lists
- ShimCache
- AmCache

6. Networking Threat Analysis

- Working With Wireshark
- Wireshark Filters and Adaptations
- Wireshark Statistics
- DNS Analysis
- DHCP Analysis
- HTTP Analysis
- Attack Scenarios Exercies
- SMB & MS-RPC Analysis
- Attack Scenario Exam