

ITSAFE

POWERED BY CYSOURCE

מסלול אנליסט SOC



CYSOURCE

מסלול אנליסט סוק

SOC (מרכז בקרה וניטור אירועי אבטחת מידע) הוא מרכז אבטחת מידע יעודי שמנטר, מזהה ומגיב לאירועי סייבר, SOC כתפיסה הוא "לב ליבו" של הארגון, ולמעשה הוא הגוף הראשון שיחווה אירוע סייבר.

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

SOC יכול להיות החל מבקר או אנליסט אחד בודד שמבקר ומנטר אחר האירועים ועד למרכז גדול המונה מספר גדול יותר של בקרים ואנליסטים. המטרה העיקרית שלו היא פיקוח אחר רשתות, מערכות, התקני קצה ומשאבים רגישים אשר יכולים להיפגע ע"י תקיפה.

מסלול **אנליסט SOC** הינו מסלול אשר מותאם לחסרי רקע המעוניינים להשתלב בתעשיית הסייבר כאנליסטים, המסלול כולל 3 שלבים המכילים את כל הידע הנדרש על מנת לעסוק במקצוע.

המסלול שלנו, עובד!

שימו לב לעדויות של תלמידים מהפייסבוק שלנו

Nitai Moshe January 26 recommends ITSafe powered by CySource.

הי חברים, שמח לבשר כי התקבלתי לעבודה בחברת IPV בתור בודק חוסן תשתית. רוצה למצוא את הרגע הזה להכיר תודה למכללת ITSafe, ובפרט לשי, ולכל הצוות שעזר ותמך והיה שם בשבילי. תודה על החומר הלימודי שהעברתם ברמה הכי גבוהה שיש, מגוון מסורף של מעבדות, קורסים עשירים, קבוצות חרטל, ומתרגלים תותחים. שיטת הלימוד היחידית, המותאמת לקצב הלימדה שלי, אפשרה לי למצוא את הזמן בצורה האופטימלית גם בשעות הקטנות של הלילה. ההכשרה הזאת העניקה לי את הידע לעבור את הראיונות ולהתבלט בצורה הכי טובה שאפשר. תודה על הזמן שהקדשתי לי בהכנה לשוק העבודה, בראיונות חרטל, וכן סיוע במציאת עבודה. ההכשרה הזאת העניקה לי את הידע לעבור את הראיונות ולהתבלט בצורה הכי טובה שאפשר. תודה על היותכם המכללה הכי טובה שיש, ואם שוב הייתי צריך לבחור, ללא ספק הייתי בוחר בה מחוץ!! וכמובן למנהל המכללה Shai Alfasi על הדאגה והאכפתיות על הסיוע בהשמה על המענה האישי לחודעות ושאלות ועל כיהול המכללה ללימודי סייבר הכי טובה במדינה!

Michal Rotenberg March 14 recommends ITSafe powered by CySource.

ממליצה מאוד על מכללת ITSafe, השיעורים מועברים על ידי מרצים בעלי שם עולמי וברמה הכי גבוה שיש, המסלול מקצועי, מפורט ומתאים למתחילים וגם למתקדמים בתחום! הקורס כולל אלפי שעות מוקלטות, מעבדות ייחודיות לחרטל, סימולציות לראיונות עבודה ומתרגלים שזמינים לכל שאלה. אני עשיתי את המסלול של בודקת חוסן ומצאתי עבודה כמעט ללא מאמץ בזכותם! תודה רבה לכם ITSafe

Maor Cohen November 16, 2022 recommends ITSafe powered by CySource.

מנסיון שלי עם מכללות אחרות (שנחשבות המובילות בשוק), אף אחת לא מגיעה לרמה של ITSafe. רמת החומר הלימודי - הכי גבוהה שיש, הספרים מסודרים מאוד גם לאנשים שלא יודעים לפתוח תיקייה במחשב. ממשיך המערכת מאוד מסודר קל לתפעול ומכון ללימדה מסודרת. הצוות - האנשים המובילים והמקצוענים ביותר, ידעו להוביל אותי לכוון ולעזור להגיע למטרות המקצועיות וחרבה מעבר לכך! תמיכה - תשתית של עשרות מתרגלים שנותנים מענה בכל שעה שלא תהיה גם בשעות הקטנות של הלילה. השמה - אחרי שסיימתי את הלימודים (כחצי שנה) המכללה דאגה לתת לי לעשות 2 סימולציות לראיונות עם אנשי מקצוע בתחום לפני שאגיע לראיונות בחברות. בזכות ההכוונה והמסלול הייחודי הצלחתי להשיג כמעט ללא מאמץ להתקבל לחברת EY שהיא אחת החברות הגדולות והאיכותיות לתפקיד Penetration Tester.

Daniel Abay January 3 recommends ITSafe powered by CySource.

לכל מי שעדיין לא יודע, אחד המקומות הכי טובים בארץ ללמודי סייבר זה ITSafe! כל החומר הלימודי מועבר ברמה הכי מקצועית מאנשים שנמצאים בתעשייה, עם מרצים ואנשי צוות הכי טובים בשוק!! אני אישית עשיתי את המסלול של הבודק חוסן ITSafe ומצאתי עבודה בזכותם, ממליץ ממליץ! 🔥



מבוא והיכרות עם תקשורת | 2 שעות תוכן | מבחן

1. היכרות והבנה בסיסית של מהי רשת

- עקרונות תקשורת בסיסיים
- חוקי תקשורת בסיסיים
- סוגי רשתות:
 - PAN
 - LAN
 - WLAN
 - CAN
 - WAN
- היכרות עם Client Server
- היכרות עם Peer2Peer
- היכרות עם פרוטוקולי תקשורת ותפקידם
 - Web Protocol
 - SMTP protocol
 - FTP protocol
- מודל שבע השכבות (OSI)
 - שכבת האפליקציה
 - שכבת הפרזנטציה
 - שכבת הסשן
 - שכבת התעבורה
 - שכבת הרשת
 - שכבת המידע
 - שכבה פיזית

2. היכרות עם ציודי תקשורת

- HUB
- Switch
- Router

3. היכרות עם מודל TCP/IP

- פרוטוקולי TCP/UDP
- היכרות עם פורטים
- היכרות עם סוקטים



לינוקס Essentials | 7.5 שעות תוכן | 25 שעות תירגול | מבחן

4. שירותים ולוגים

- היכרות עם Apache2
- היכרות עם Nginx
- Nginx & Apache2 Reverse Proxy
- UFW
- FTP
- SSH
- SCP
- Auth Log
- Access Log

5. תקשורת ופקודות

Troubleshooting

- Network Identification
- החלפת כתובת IP זמנית
- היכרות עם DHCP
- קביעת כתובת IP סטטית
- היכרות עם DNS
- עבודה עם Netstat
- Ps & Top
- Kill
- Df & Du
- עבודה עם Tcpdump

6. הרשאות, משתמשים וקבוצות

- מבוא להרשאות, משתמשים וקבוצות
- יצירת משתמשים וסוגי משתמשים
- היכרות והבנה של קובץ passwd
- היכרות והבנה של קובץ shadow
- היכרות עם sudo
- היכרות עם קבוצות
- יצירת קבוצות
- הוספת משתמשים לקבוצות
- היכרות עם הרשאות
- Chown & Chmod
- הרשאות נומריות
- מבחן קורס

1. מבוא ללינוקס

- דברי פתיחה ודגשים ללמידה
- ההיסטוריה של לינוקס
- היכרות עם הפצות לינוקס
- מבוא לוירטואליזציה
- הכנה לוירטואליזציה
- ישום וירטואליזציה עם VirtualBox
- התקנת סביבת Ubuntu Server
- עזרי למידה

2. פקודות ועבודה בסיסית

- היכרות עם Linux Shell
- פקודות ניווט
- פקודות Listing
- עבודה עם ספריות
- עבודה עם כתבנים
- אופרטורים
- פקודות חיפוש
- עבודה עם grep
- התקנת חבילות בלינוקס
- פקודות דחיסה וארכיון
- Wildcard & Globbing

3. מערכת הקבצים של לינוקס

- היכרות עם FHS
- root
- bin
- etc
- sbin
- usr
- var
- dev
- lib
- mnt
- opt
- proc
- Environment Variable
- Hard Links & Soft Links
- introduction to bash scripting



תקשורת רשתות CCNA | 13 שעות תוכן | 110 שעות תירגול | פרויקט גמר

1. היכרות עם עולם התקשורת

- סטנדרטים בתקשורת
- מודל TCP/IP
- מודל ISO
- UDP/TCP
- מבנה חבילות מידע
- כתובות MAC Address
- כתובות IP
- ציודי תקשורת
- סוגי רשתות
- הגדרת סביבת מעבדה

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
- WiFi - WLC בעולמות LAP
- הגדרת רשת אלחוטית WiFi
- פרוטוקולי ניתוב
- EIGRP
- OSPF
- שיפור ביצועי רשת באמצעות HSRP

4. שירותי רשת ואבטחה

- NAT
- SYSLOG
- SSH
- התקפות על מתגים
- התקפות על שירותי רשת
- שימוש ב Access List
- עבודה עם Port Security
- אבטחה ברשת

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



אנליסט סוק | 10 שעות תוכן | 100 שעות תירגול | פרויקט גמר

7. SOC Analyst - Labs

- :Lab 1
 - IBM Wincollect Installation On Dedicated Server
- :Lab 2
 - Qradar - Custom Log Activity
- :Lab 3
 - Qradar - Parsing Fields From Payload
- :Lab 4
 - Qradar - Custom Building Block
- :Lab 5
 - Qradar - Custom Rules
- :Lab 6
 - Qradar - Reference Lists
- :Lab 7
 - Sysmon
- :Lab 8
 - Find The Suspicious Log
- :Lab 9
 - Threat intelligence With Qradar

4. SIME/SOC Fundamentals

- Organization Monitoring
- SOC Fundamentals
- The Adaptive Security Architectures
- Cyber Security Components And Vendors
- SIEM Introduction
- Qradar SIEM Introdoction
- 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

- Qradar Log Activity
- Windows sysinternals
- Windows Sysmon
- Cyber Attack Summary
- Log Analysis
- Threat Intelligence
- SOAR Concept

1. היכרות עם סביבות ווינדוס

- Inroduction to virtualization
- VirtualBox Installation
- Virtualization Networking
- Deploy a virtual machine
- Windows Server2016 installation
- Domain Controller
- DC Pre configurations
- AD DS installation on DC
- Windows 10 Client installation
- Virtualization and Windows10 client
- Client domain join
- DHCP Service
- DHCP deployment
- IP ranges
- IP Reservations
- DNS record types
- DNS Zones
- Creating and managing domain users
- Creatubg and managing domain groups
- Creating and managing GPO's

2. אבני יסוד בהגנה

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

3. היכרות עם צד תוקף

- Layer II cyber attacks
- Layer III cyber attacks
- Various cyber attacks types
- Cyber Kill Chain
- IOC's



ITSAFE

POWERED BY CYSOURCE

www.ITSafe.co.il