המסלול להכשרת מפעילי מרכז SOC ותומכי Incident Response

see security colege

יועץ אקדמי: מר אבי ויסמן, מרצה ראשי: רפי רוסו

תוכנית ממוקדת לאוכלוסיות טכנולוגיות, לבעלי רקע במחשבים להבנה והכרת כלים בעולם הניטור ה-SOC והתגובה לאירועים.

(תאריכים בעמוד הראשי של המכללה)

מבוא

תוכנית הלימודים להכשרת אנשי SOC ותומכים בסביבת Incident Response הינה תוכנית מקורית ראשונה מסוגה אשר נבנתה בישראל. התחומים בהם עוסק הקורס הם נושאי הליבה הקריטיים בתחום הפעלת מוקדי ניטור סייבר וצוותי תגובה ראשוניים. בוגרי הקורס נדרשים ללמוד את רזי פעילות הליבה של תחום זה. בתוך כך, הם נדרשים להכיר את האספקטים התיאורטיים העומדים מאחורי תחום האחריות שלהם ואף את הפעולות האקטיביות אשר נידרש מהם לבצע עם היווצרות חשד לאירוע סייבר. באחריות איש הניטור להבין את ארכיטקטורת אבטחת המידע הארגונית שלו בשגרה. עם קרות אירוע, באחריותו: לזהות פעילות אנומלית ו/או זדונית במערך התקשוב הארגוני באמצעות כלי הניטור והבקרה; לנתח בקווים כלליים וראשוניים את מהות הפעילות והשלכותיה האפשריות; להכיל את האירוע תוך תחימתו; לספק תשתית בסיסית להתאוששות אחר סילוק.

מאפייני תוכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית / **טכנית** / **יישום**
שלב:	מתחילים / **מתקדמים**
רוחב:	**ממוקד** / רחב
עומק:	סוקר / **עמוק למחצה**
הסמכות:	SOC/IR Practitioner
שעות:	**48 שעות**
פתיחה:	**ראה בעמוד הראשי של המכללה**
מתכונת:	**12 מפגשים ערב**
תרגול בית:	לא קיים / **קיים בהיקף 120 שעות**

מטרת התוכנית

התוכנית נבנתה לצרכי ידע מעשי: הכשרת אנשי מקצוע המתעתדים לאייש מוקדי ניטור ובקרה (SIEM/SOC) ו/או לשמש כצוותי תגובה ראשוניים לאירועי אבטחת מידע (Incident Response).

קורס זה מספק את מרבית התשתית התיאורטית הנדרשת מגורמי הניטור ואף את הניסיון המעשי בכלים השונים אותם גורמי הניטור נדרשים להכיר ולהפעיל.

היכולת תירכש מתוך היכרות עם הטכנולוגיות, הטכניקות , והוראות העבודה הנהוגות (Best Practice) בתחומים אלו, יכולת זו תוקנה לתלמיד בתוכנית הלימודים בין השאר, באמצעות הרצאות, התנסויות ותרגול.

קהל יעד

בעלי ידע מתחום תשתיות התקשוב: תקשורת המחשבים והיכרות בסיסית עם עולם מערכות ההפעלה.

הסמכה

לעומדים בדרישות התוכנית, תוענק תעודה מטעם See-Security:

"מיישם מרכז בקרת סייבר מוסמך - Certified SOC Operator".

מי שאינם עומדים בדרישות, יהיו זכאים לתעודת השתתפות, ולהשלמת מחויבויותיהם (השתתפות חוזרת / עבודות ומשימות) ללא תשלום, לצורך קבלת ההסמכה.

הכרה

תוכנית הלימודים להכשרת אנשי SOC ותומכים בסביבת Incident Response, הינה הראשונה מסוגה בישראל, ונבנתה על-בסיס ההחלטות הרשמיות של המטה הקיברנטי הלאומי מינואר 2015 בנוגע לרשימת מקצועות הליבה באבטחת מידע וסייבר, ולצורך אספקת הביקוש לאנשי המקצוע המאיישים עמדות בקבוצת IR.

תובל 30, רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593

www.see-security.com avi@see-security.com

המסלול להכשרת מפעילי מרכז SOC ותומכי Incident Response

תנאי קבלה

- רקע בסיסי בעולם רשתות התקשורת ומערכות ההפעלה. התלמיד נדרש להכיר סוגיות בסיסיות במערכות ההפעלה המקובלות היום, פרוטוקולי תקשורת ומודל TCP/IP.
- נכונות לעבודה עצמית מונחית (כ- 120 שעות לימוד ביתי).
- ראיון אישי.

מטלות תוכנית הלימודים

- קיימת חובת נוכחות בכל המפגשים.
- קיימת חובת עמידה בדרישות סיום (עבודה או מבחן).
- בנושאים הטכניים - תרגול (Hands-on) בכיתת מעבדת מחשבים.

מתכונת הלימודים

משך התכנית כ- 48 שעות, במתכונת של 12 מפגשי ערב (כ- 1.5 חודשים). הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח פעמיים בשנה.

עלות הלימודים

סך 9,000 ₪ + 400 ₪ דמי רישום (כולל מע"מ)

המרצים בתוכנית

על המרצים נמנים מובילי הענף, בהם מומחים מקצועיים המובילים בתחומם, ולרבות רפי רוסו, מומחה Incident Response.

מידע נוסף

- **מידע מינהלי:** אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com
- **יועץ אקדמי:** אבי ויסמן, 054-5222305, avi@see-security.com

תוכנית הלימודים (מקוצר)

Introduction to Incident Response

פרק הפתיחה של הקורס. תוכן השיעור חושף את התלמידים לעולם הניטור והבקרה והתגובה לאירועי אבטחת מידע. הפתיח התיאורטי יבסס את שלד ההתנהלות למול אירועי אבטחת מידע (בהתאם למתודולוגיה פורמאלית) תוך שימוש בנתוני אמת לצורך המחשה.

- **Definitions of "incident"**
- **Incident handling** (According to NIST)
  - Preparation; Detection and Analysis; Containment, Eradication and Recovery; Post Activity

Cyber Threats Categorization and Attack Vectors

הפרק עוסק בסקירת קטגוריות האיומים השונים וערוצי התקיפה המוכרים כיום. התלמידים יכירו את סוגי האיומים השונים עימם ארגונים נאלצים להתמודד בשגרת היומיום. בנוסף, התלמידים ייחשפו למגוון ערוצי התקיפה אותם יידרשו להכיר ולזהות בעת מילוי תפקידם בשגרה.

- **Definitions of 0day, vulnerability, exploits**
- **Malware types**
- **Threat Categories** (Spoofing, DDOS, Social Engineering, Common Web Attacks)
- **Attack Vectors** (Web, email, removable media, BYOD)

Network Architecture

במסגרת עבודתם השוטפת, תלמידים יידרשו להכיר את ארכיטקטורת הרשת של הארגון. מטרת הפרק הינה להציג לתלמידים ארכיטקטורות מקובלות. בנוסף, הפרק יציג לתלמידים שירותים שונים שארגונים נדרשים להגן עליהם תוך ניטורם ובקרתם.

- **Basic Network Architectures**
- **Enterprise IT Services**

Basic Network Infrastructure (DNS, DHCP); Web Servers; DB Servers; Security Systems.

המסלול להכשרת מפעילי מרכז SOC ותומכי Incident Response

Security Information and Event Management (SIEM)

עבודתו השגרתית של איש מערך SOC היא למול מערכות האיסוף, האגרגרציה והקורלציה אודות אירועי אבטחת מידע בארגון (קרי, מערך ה-SIEM). מטרת הפרק הינה לחשוף את התלמידים למערך ה-SIEM (תצורה, רכיבים, יישום ותפעול).

- **SIEM Definitions and Features**
- **SIEM Components and Architecture** (Agents, Collectors, Archives)
- **SIEM Operations** (Rules, Events, Incidents, Queries, Reports, Intelligence)
- **SIEM Implementation**

Network Forensics

פרק זה פותח את השער המעשי בתחום בפני התלמידים בכך שהם נדרשים להכיר כלים טכניים ולהכיר את אופן השימוש שלהם במסגרת התגובה לאירועים. מדובר בשני מפגשים הכוללים היכרות עם כלי ניתוח אירועים ברשתות תקשורת.

- **Introduction to Wireshark** (elaboration of the OSI model) by emphasizing protocols from:
  - Application Layer; Transport Layer; Network; Link.
- **Network Artifacts Analysis** (Trojan traffic, DDOS traffic and Exploit kits traffic)

Microsoft Windows Artifacts

לאחר שהתלמידים נחשפו להתנהלות הטכנית מול רשתות התקשורת והתעבורה בה, הם ייחשפו להתנהלות הטכנית מול מערכות הפעלה. התלמידים יכירו את האובייקטים השונים במערכת ההפעלה Windows אותם הם נדרשים לחקור ולבחון במסגרת אירוע.

- **Introduction to Sys-Internals suite**
- **Introduction to PSTools**
- **Understanding Windows Artifacts** (Registry Keys, Event Log, Prefetch, Pagefile, Filesystems)
- **Introduction to Browser Forensics**

Introduction to Malware Analysis

הפרק מהווה מעין הקדמה ופתיח לתחום העצום של ניתוח נוזקות (Malware Analysis). התלמידים יכרו פרקטיקות נהוגות בכל הקשור להקמת תשתית חקירה וניתוח (מעבדת חקירות). בנוסף, התלמידים ייחשפו בצורה בסיסית לניתוחים סטאטיים ודינאמיים של נוזקות.

- **Introduction to Forensics Lab Construction and Accept Best Practices**
- **Introduction to Basic Static and Dynamic Malware Analysis Methodologies**

Introduction to Memory Forensics

בהמשך לחשיפת התלמידים לעולם ניתוח הנוזקות, הם ייחשפו גם לפעולות המקובלות בניתוח וחקירה של זיכרון המחשב. מכיוון שמידע רב נשמר (ונשאר) בזיכרון המחשב, התלמידים יכירו את הפעולות שיש לבצע על מנת לשמר מידע בזיכרון (ובמילים אחרות – ראיות לפעילות זדונית) ופעולות ניתוח בסיסיות

- **Introduction to Memory Dumping Tools**
- **Basic Usage of Memory Analysis** (Volatility)
- **Practical Simulations and Test Cases** (ZEUS, Stuxnet)

Final Exercise and Simulation

בסיום הקורס יקבלו התלמידים הזדמנות ליישם את הידע התיאורטי והמעשי שרכשו וזאת במסגרת מפגש שלם המיוחד במלואו לתרגול וסימולציה של אירועי אבטחת מידע. בתחילת המפגש התלמידים ייחשפו לחשד אודות אירוע אבטחת מידע מתגלגל והם יאלצו להגיב לאירוע זה באמצעות הכלים ומתודולוגיה שלמדו.

- **Predefined Security Incident** (Data Leakage, Malware Infection, etc.)
- **Summary**

הערות לתוכנית הלימודים

א. תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.

ב. משימות קריאה מהווים חובה לימודית, ובכללם, ספרי הקורס וחומרי הלימוד האחרים.

ג. נושאי טכנאות/יישום אבטחת מידע (התקנות ותחזוקה) לא כלולים בתוכנית הלימודים (ראה תוכנית מתחילים)

הערות מינהל

- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי ביה"ס.
- דמי ההרשמה ומבחנים חיצוניים כלשהם אינם כלולים בשכר הלימוד.
- ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.

תובל 30, רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com