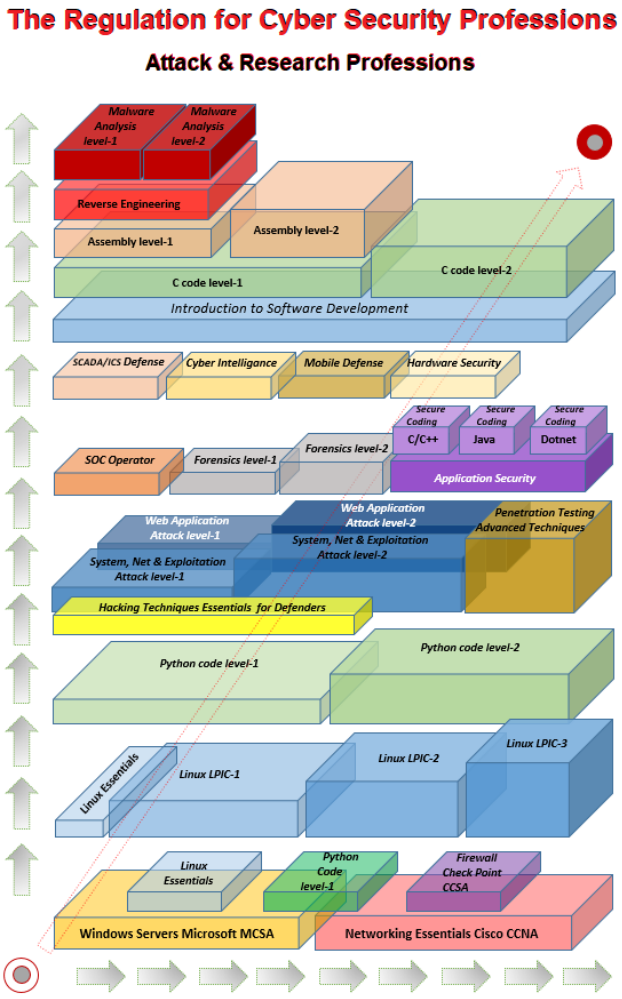
REVERSE ENGINEERING & MALWARE ANALYSIS



See
cyber security college

להיות מקצוען MALWARE ANALYSIS

התמחות Malware Analysis היא מהבכירות ומהיוקרתיות בעולם הסייבר.

בתכנית מתקדמת זו, נלמד כיצד לנתח נוזקות הן באמצעות הנדסה לאחור והן באמצעות ניתוח ההתנהגות של הנוזקה. לאחר ניתוח הנדסה לאחור של הנוזקה, נצלול אל הטכניקות השונות בהן נוזקה משתמשת כדי להסתיר את עצמה והן וכדי לפגוע במשתמשים. נלמד כיצד ניתן לגלות את הטכניקות הללו, הן באמצעות ניתוח הקוד באופן סטטי והן באמצעות ניתוח דינמי ע"י שימוש בכלים מתאימים.

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד כְּפִי שָׁרַק שִׁיא סֶקְיוּריטִי יוֹדַעַת לְלַמֵּד, עִם הַלֵּב.

Reverse Engineering & Malware Analysis level-2

אודות המכללה

מכללת See Security הנה מכללה **בינלאומית** התמחותית **למקצועות הסייבר**, אחת מ 7 -מכללות מסוגה בעולם ועוסקת בלעדית בתחום זה בכל זמנה, תוך שימוש במתודולוגית הדרכה שנבנתה עבור גורמים ממלכתיים.

המכללה מייצאת את תכניות הלימודים לכל רחבי העולם באמצעות המותג *See Security International* ובאמצעות גופי סייבר ישראליים ידועי-שם העוסקים ביצוא בטחוני. מנהל הקבוצה שבה משולבת המכללה, מר אבי ויסמן, הינו ממובילי ענף הסייבר, יועץ לממשלת ישראל בנושא "אסדרת מקצועות הגנת הסייבר בישראל", פרשן בערוצי השידור בארץ ובחו"ל, מקימו של הפורום הלאומי לאבטחת מידע IFIS יחד עם האלוף במיל' וראש המל"ל לשעבר, יעקב עמידרור, מנכ"ל משותף בחברה להשמת כוח אדם בענף הסייבר *SeeHR*, בחברה לייעוץ *Cyber See Consulting*, בחברה לפתרונות Managed SEIM/SOC בשם *See Events* ובמכללה הבינלאומית לסייבר *See Security College International*.

אודות אסדרת מקצועות הסייבר בישראל: הרשות הלאומית להגנת סייבר

הרשות אשר פועלת במסגרת משרד ראש הממשלה כיחידה עצמאית, החליטה להפעיל אסדרה (רגולציה) מחייבת בנושא הגדרתם של המקצועות השונים בעולם הסייבר, ומפעילה המלצות ברורות בנוגע לתכני הידע לכל מקצוע. התמחות Malware Analysis היא מהבכירות ומהיוקרתיות בעולם הסייבר.

אודות התכנית ללימודי Malware Analysis

מנתח פוגעני סייבר (Cyber Security Malware Analyst) CSMA משתמש בכלים המאפשרים לזהות טכניקות ידועות, ובדיקה של מערכת ההפעלה ומרכיביה, כדי להתמודד עם תוכנות זדוניות מתקדמות במיוחד. כלים קיימים מספקים חלק מהתובנות המבוקשות של תוכנות זדוניות פשוטות, אך הם מוגבלים ביכולתם לזהות וריאנטים חדשים.

בתכנית מתקדמת זו, נלמד כיצד לנתח נוזקות הן באמצעות הנדסה לאחור והן באמצעות ניתוח ההתנהגות של הנוזקה. לאחר ניתוח הנדסה לאחור של הנוזקה, נצלול אל הטכניקות השונות בהן נוזקה משתמשת כדי להסתיר את עצמה והן וכדי לפגוע במשתמשים. נלמד כיצד ניתן לגלות את הטכניקות הללו, הן באמצעות ניתוח הקוד באופן סטטי והן באמצעות ניתוח דינמי ע"י שימוש בכלים מתאימים.

קהל יעד

לבעלי עניין להתפתח בתחום ההנדסה לאחור או לפתח כישורי ניתוח נוזקות.

מטרת התכנית

- בסיום התכנית תהיה לבוגרים יכולות גבוהות של הנדסה לאחור, וטכניקות מתקדמות של נוזקות, על מנת להבין את יכולות ההתפשטות של פוגענים.

תנאי קבלה

בוגרי תכנית "Reverse Engineering level-1" או הוכחת ידע שקול ערך.

עלות

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

מתכונת הלימודים

משך התוכנית כ- 80 שעות במתכונת של 20 מפגשי ערב. הלימודים מתקיימים בקמפוס See Security ברמת-גן (צמוד לתחנת רכבת מרכז). המסלול נפתח פעמיים בשנה.

חובות אקדמיות

- קיימת חובת נוכחות ב-80% מהמפגשים.
- בנושאים הטכניים - תרגול (Hands-on) בכיתה (מעבדה).

זכאות לתעודה והסמכות בינלאומיות

לעומדים בדרישות, תונפק תעודה מטעם See-Security.

הערות

- פתיחת התכנית מותנית בכמות של 10 נרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- ייתכנו שינויים במערך התכנית, במועדי הלימוד והבחינות או בכל נושא אחר. הודעה על שינוי תימסר למשתתפים.

למידע נוסף / פגישת יעוץ

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

יעוץ אקדמי: אבי ויסמן, 03-5799555, 054-5222305,
avi@see-security.com

תכנית לימודים:

חלק א': הנדסה לאחור של טכניקות נוזקה מבוססות VM

- טכניקות ליצירת malware – מעבדה
- ניתוח מצבי malware
- ריצה והתמדה (persistence) של נוזקה
- קידודים נפוצים שנוזקות משתמשות בהם – צופן קיסר, Base64, Crypto , דחיסה, אובפוסקציה
- כיצד malware מפענח (decode) את עצמו
- איך debugger עובד
- כיצד malware פורס (unpack) את עצמו לאחר הדחיסה
- תקשורת החוצה – מציאת "חללית האם", C&C ואינדיקטורים נוספים
- ניתוח DLL
- טכניקות אנטי-ניתוח (מניעת הניתוח) ע"י הנוזקה – Anti-Debug, Anti-VM, Anti-Sandbox
- ניתוח Shellcode
- ניתוח מסכם של Ransomware מודרני

חלק ב': נושאים מתקדמים בהנדסה לאחור: טכניקות Rootkits מבוססי VM

- קבצי הרצה המכילים סוסים טרויאניים – עקרונות
- Hook (לכידה בזמן ריצה) מסוג inline
- Hook על ה- Interrupt Descriptor Table
- Hooking על ה- System Call Table
- Hooking על ה- Interrupt Descriptor Table
- Hooking על ה- Kernel Object ומניפולציה עליו
- Hooking על ה- IO Request Packet
- החבאת תהליכים, קבצים ופורטים פתוחים ע"י הנוזקה
- שינוי וזיהום ה- Master Boot Record

<u>הצהרת תלמיד בלימודי Malware Analysis</u>

הריני מאשר בזאת כי קיבלתי דף מידע זה, הבנתי את תכנו והסכמתי לתנאים המפורטים בו.

שם הנרשם: _____ תאריך: _____ חתימה _____