MALWARE ANALYST

LEVEL-1

"לנתח" MALWARE.

הבנת עקרונות הפעולה של נוזקה, משמעה, הסקת מסקנות לגבי יכולת הפועלה, ההפצה, והפגיעה שלה.

בתכנית זו המבוססת בעיקר על התנסות, נלמד את העקרונות הבסיסיים מבנה נוזקה, דרכי פעולתה, נבין מה מתרחש "מאחורי הקלעים", ונלמד כיצד לזהותן.

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד כְּפִי שָׁרַק שֵׁיא סָקְיוּרִיטִי יוֹדַעַת לְלַמֵּד, עִם הַלֵּב.

Malware Analysis level-1

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 (לצד האלוף במיל' וראש המל"ל לשעבר, יעקב עמידרור), מנכ"ל משותף בחברה להשמת כוח אדם בענף הסייבר *SeeHR*, בחברה לייעוץ הגנת סייבר *See Secure Consulting*, בחברה לפתרונות Managed SEIM/SOC בשם See *Events* ובמכללה הבינלאומית לסייבר *See Security College International*.

אודות אסדרת מקצועות הסייבר בישראל: מערך הסייבר הלאומי

המערך אשר פועל במסגרת משרד ראש הממשלה כיחידה עצמאית, החליט להפעיל אסדרה (רגולציה) מחייבת בנושא הגדרתם של המקצועות השונים בעולם הסייבר, ומפעיל המלצות ברורות בנוגע לתכני הידע לכל מקצוע. חלק ממקצועות הסייבר דורשים הבנת סביבת ה- SOC.

אודות התכנית ללימודי Malware Analysis

לאורך שנים רבות, בעלי נטייה לסקרנות ביקשו להבין כיצד נוזקות פועלות "מבפנים". עולם הנוזקות מגוון, ובהן: Ransomware, סוסים טרויאנים ווריאציות שלהם.

בתכנית זו נלמד כיצד לנתח נוזקות, מה הן המתודולוגיות וכלי העזר המשמשים לשם כך, ומהן הטכניקות.

קהל יעד

לבעלי עניין להתפתח בתחום המחקרי של הגנת סייבר.

- IT security professionals.
- SoC analysts.
- Digital Forensics experts.
- Others with the passion and eagerness to discover and learn new topics.

מטרת התכנית

- בסיום התכנית תהיה לבוגרים הבנה מעמיקה בנושאי הנדסה לאחור: כלים, טכניקות ומתודולוגיה.
- תשתית לתכניות מתקדמות יותר בתחום: Reverse Engineering and Malware Analysis.

תנאי קבלה

- Basic understanding of networking: TCP/IP, Routing, Forwarding.
- Reading and understanding code.
- Basic understanding of Windows Server and Linux Shell commands.
- Basic understanding of well-known protocols such as HTTP/HTTPS, DNS, SMTP, FTP, SSH.
- PC/MAC with Intel i5/i7/i9 CPU, 16GB of RAM and an SSD storage.
- Local administrator account is must.
- VMware Workstation/Fusion installed.

מתכונת הלימודים

משך התוכנית כ- 35 שעות במתכונת של 7 מפגשי ערב או בוקר בני 5 שעות אקדמיות. הלימודים מתקיימים במתכונת פרונטלית עם אפשרות לצד תמיכה הדדית בקבוצת WhatsApp. המסלול נפתח כ-3 פעמים בשנה.

חובות אקדמיות

- קיימת חובת נוכחות ב-90% מהמפגשים.
- קיימת חובת עמידה בדרישות סיום (עבודה או מבחן).

- בנושאים הטכניים: תרגול (Hands-on) בכיתה (מעבדה).

זכאות לתעודה והסמכות בינלאומיות

לעומדים בדרישות, תוענק תעודה מטעם See-Security.

מי שאינם עומדים בדרישות, יהיו זכאים לתעודת השתתפות.

הערות

- פתיחת התכנית מותנית בכמות של 15 נרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- המכללה מביאה לידיעת הנרשמים והסטודנטים כי ייתכנו שינויים במערך התכנית, במועדי הלימוד והבחינות או בכל נושא אחר. הודעה על שינוי תימסר למשתתפים.
- תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.
- משימות קריאה מהווים חובה לימודית, ובכללם, ספרי הקורס וחומרי הלימוד האחרים.

למידע נוסף / פגישת יעוץ

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

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

<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 _____

תכנית לימודים

Lesson 1 - Virology Intro

- Virology
- Analysis Techniques
- Build a Lab

Lesson 2 - Malware Analysis Basics

- Static Malware Analysis
- Dynamic Malware Analysis
- Sysinternals

Lesson 3 - Advanced Functionalities

- Understand PE Headers
- Know DLL files imports and exports
- Mutex & Entropy

Lesson 4 - Emails CTF lab

- Email analysis
- True types
- "Email to crisis" Drill

Lesson 5 - Deep dive investigations

- Catch me if u can
- Twit Drill

Lesson 6 - Threat Hunting - Find the malwares

- Analyze USB
- Malware analysis APT

Lesson 7 - Final Exam + Hands-On Test