CSRP

תגובות לאירועים

CYBER SCHOOL

מסלול הקורס

1. תגובות לאירועים (מבוא ל-DFIR)
2. רכישת נתונים
3. Windows Forensics
4. ניתוח זיכרון
5. Linux Forensics
6. Network Forensics
7. ניתוח זדוני
8. פרויקט גמר

CYBER SCHOOL

סקירה כללית

נלמד על DFIR, איך מתכננים DFIR, ועל התהליכים, כלים ושיטות שמיושמים בו. בנוסף, נלמד איך לתכנן נהלי תגובות לאירוע, מונחים בסיסיים של אבטחת מידע, ואיך להכין מעבדת Windows DFIR.

- מבוא ל-DFIR
- תכנון תגובות לאירוע
- התהליך של DFIR
- ערכת הכלים של DFIR
- תרחיש שימוש ב-DFIR
- סביבת DFIR
- תרחישי DFIR
- הגדרת נכסים
- שלישיית ה-CIA
- מרכז תפעול אבטחה
- תכנית תגובה לאירועים
- הכנה טכנית
- תכנית שיקום לאחר אסון
- תאימות GRC

CYBER SCHOOL

CYBER SCHOOL

שיעור 1

תגובה לאירועים

מבוא ל-DFIR

DFIR

DFIR – חקירת התקפת סייבר אחרי אירוע.

DF – ניתוח artifacts אחרי התקפת סייבר.

IR – ביצוע פעולות כאשר קורית פריצת אבטחה.

Digital Forensics

- חשיפת ואיסוף כל הנתונים האלקטרוניים, מבלי לשנות או לזהם אותם.
- שימור ראיות ובניית אירועי עבר מחדש.

CYBER SCHOOL

מה זה תגובה לאירועים (IR)?

ניהול והתמודדות נגד פריצת אבטחה או התקפה.

הפחתת הנזק והעלות של השיקום.

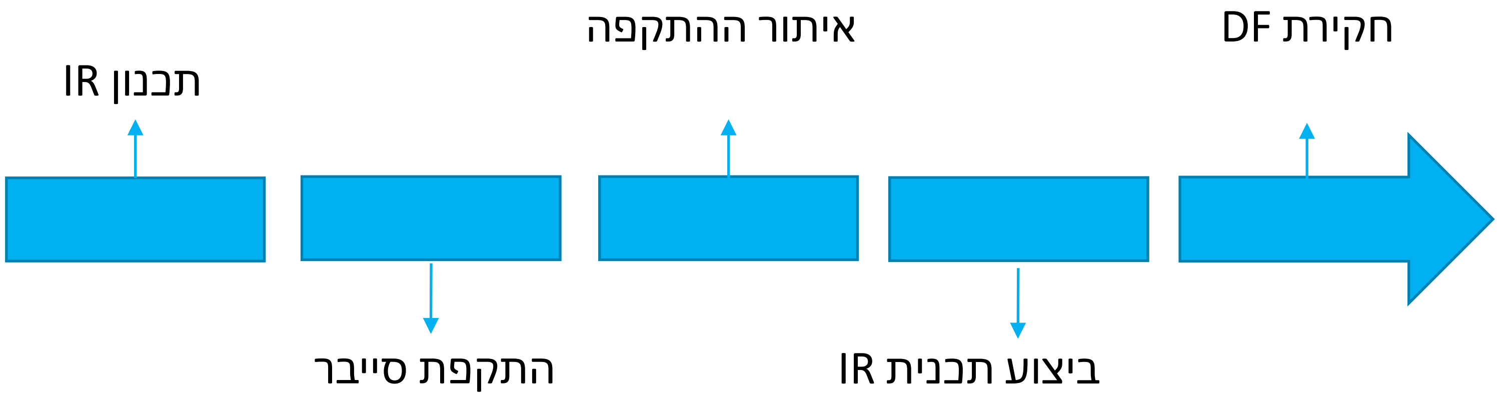
CYBER SCHOOL

DF Vs IR Vs TH

DF	IR	TH
Digital Forensics	Incident Response תגובה לאירועים	Threat Hunting מציאת איומים
לאחר ההתקפה	בזמן ההתקפה	כל הזמן
מציאת ראיות	מזעור נזקים עתידיים	מציאת איומים שלא אותרו
מארח ורשת	מארח ורשת	מארח ורשת
רמה 3 ב-SOC	רמה 2 ב-SOC	רמה 3 ב-SOC

CYBER SCHOOL

ציר הזמן של DFIR



- תכנון IR צריך להיעשות לפני ההתקפה.
- הזמן הממוצע לאיתור התקפה הוא 6 חודשים.
- DF מסתמך על מידע שנאסף במהלך IR.

CYBER SCHOOL

CYBER SCHOOL

תגובה לאירועים

תכנון תגובות לאירוע (IR)

למה אנחנו צריכים IR?

- כדי להכיל איומים ולמנוע מהם להתפשט ולגרום נזק נוסף.
- כדי לעזור לארגון להשתקם אחרי שקורית פריצה.

CYBER SCHOOL

אחריויות של מגיב לאירועים

הערכת וסיכום ליקויי אבטחה אפשריים שעלולים להוביל להתקפה.

זיהוי תוכנות זדוניות פוטנציאליות ואסיפת מידע שינותח על ידי צוות ה-DF.

בצע בדיקת חדירות ויצר דו"חות הערכת סיכונים.

CYBER SCHOOL

ביצוע IR

המפתח ל-IR מוצלח הוא תכנית IR טובה.

תכנית טובה תיתן מענה לכל בעיה רלוונטית.

צוות ה-IR אמור לעקוב אחרי שלבי התכנית.

התכנית צריכה לכלול שלבים מגוונים, כגון הכלה (containment) וחיסול (eradication).

CYBER SCHOOL

CYBER SCHOOL

תגובה לאירועים

תהליך ה-DFIR

תהליך ה-DFIR

CYBER SCHOOL

סוגי הניתוח של DF

ניתוח מת (Dead Analysis)

ניתוח מחשבים כבויים.

יכול לכלול ניתוח של כוננים משובטים.

ניתוח חי (Live Analysis)

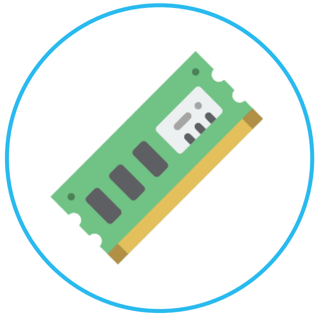
ניתוח מחשבים פועלים.

טכנית, זה לא שיטת ניתוח פורנזי.

CYBER SCHOOL

מטרות - Artifacts

קבצי יומנים



Artifacts זיכרון

נתוני מטמון

תהליכים

קבצים על כוננים

CYBER SCHOOL

Domains של DF

Forensics ברשת
מתמקד באסיפת נתונים על תעבורה העוברת דרך ציוד רשת.

Forensics במארח
מתמקד באסיפת נתונים הנוגעים למארחים, כמו קבצים או זיכרון.

CYBER SCHOOL

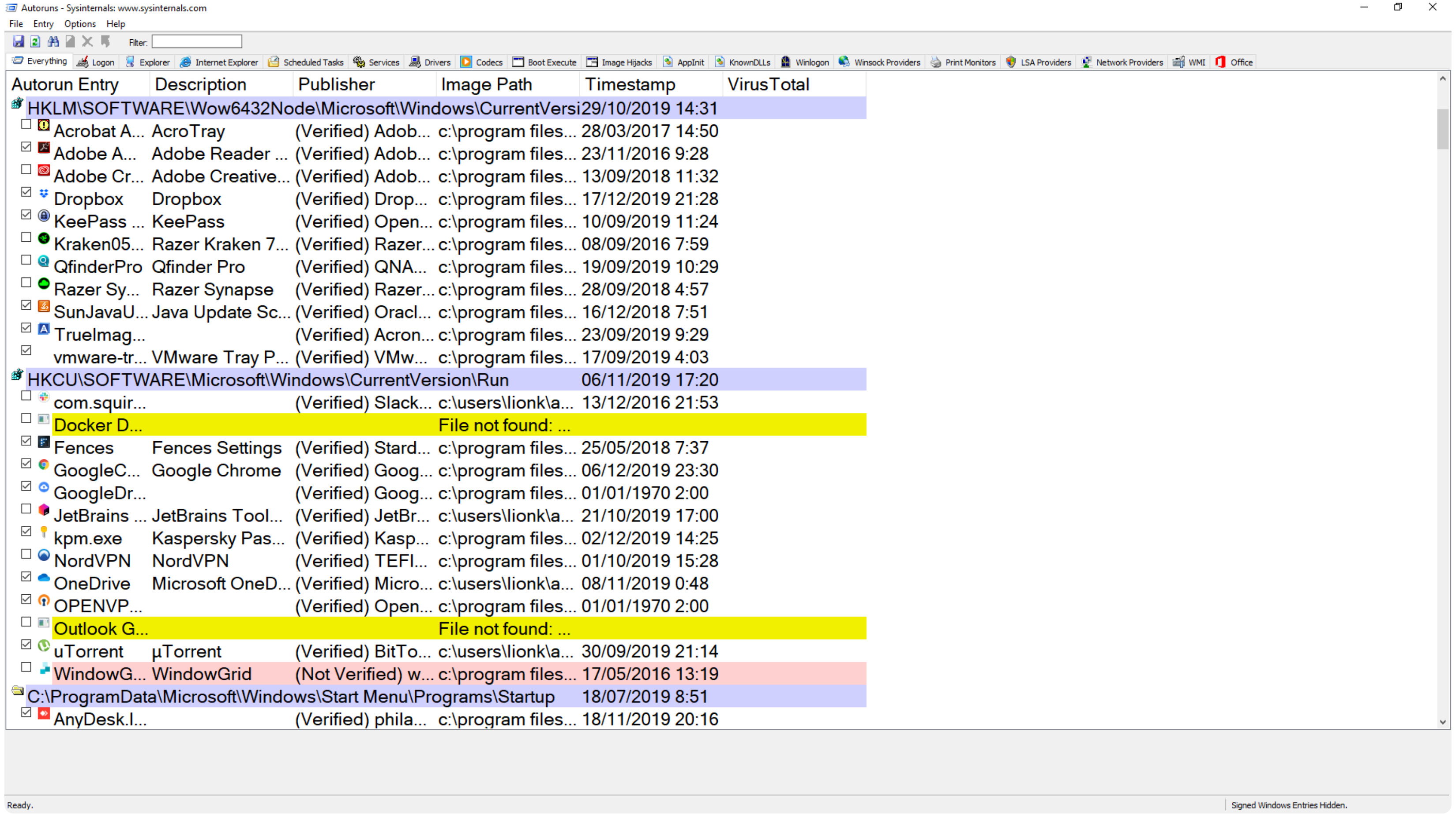
מהן ראיות

בבית משפט – כל דבר שראית, שמעת או אמרת, שמוכיח שמשהו קרה.

ב-DF – רשומות יומן, קבצים, תהליכים וכו'.

CYBER SCHOOL

דוגמה לראייה



- תוכנות Startup יכולות להיות ראייה לתוכנה זדונית מתמשכת.
- תוכנות Startup נמצאות בתיקיות ייעודיות וב-registery keys.
- Autoruns הן תוכנות שיודעות כיצד למנוע מקומות פוטנציאליים ל-startup.

CYBER SCHOOL

מעבדה 1

זיהוי תוכנות
startup

10-15 דקות

המשימה

השג ראיות בנוגע לגבי התוכניות המופעלות בעת הפעלת המחשב שלך.

השלבים

- הורד והתקן Autoruns.
- השלם את המשימות.

כלים

Autoruns

קבצים קשורים

מסמך מעבדה

CYBER SCHOOL

CYBER SCHOOL

תגובה לאירועים

ערכת הכלים של DFIR

כלי השגה

dd – השגת כונן
כלי של CLI המשמש לניהול והמרת כוננים קשיחים.

FTK Imager – השגת כונן וזיכרון
תוכנה מבוססת GUI עם תבונות מתקדמות.

Dumpit – השגת זיכרון
כלי להשגת זיכרון המשומש לרוב במערכת מבוססות Windows

CYBER SCHOOL

כלים לניתוח כוננים

Autopsy – קוד פתוח

Autopsy הוא חלק מאוסף ערכות ה-sleuth של כלי פייתון המשמשים לחקירות פורנזיות.

FTK - קנייני

כולל כלים לפיקוח על כוננים משובטים.

EnCase - קנייני

כולל תכונות מתקדמות רבות של פיקוח על תמונות.

CYBER SCHOOL

ניתוח זיכרון

Volatility Framework
אוסף קוד פתוח של כלי פייתון, תומך גם ב-Windows וגם ב-Linux.

Rekall
מסגרת מתקדמת של תגובות לאירועים פורנזיים, פותחה ע"י גוגל.

- לא קיימים כלים רבים שיכולים לבצע מחקר פלילי (forensics) של זיכרון במחשב.

CYBER SCHOOL

"גילוף" נתונים (Data Carving)

Bulk Extractor

מנסה לשחזר קבצים בלי להשתמש במבנה מערכת הקבצים.

HxD

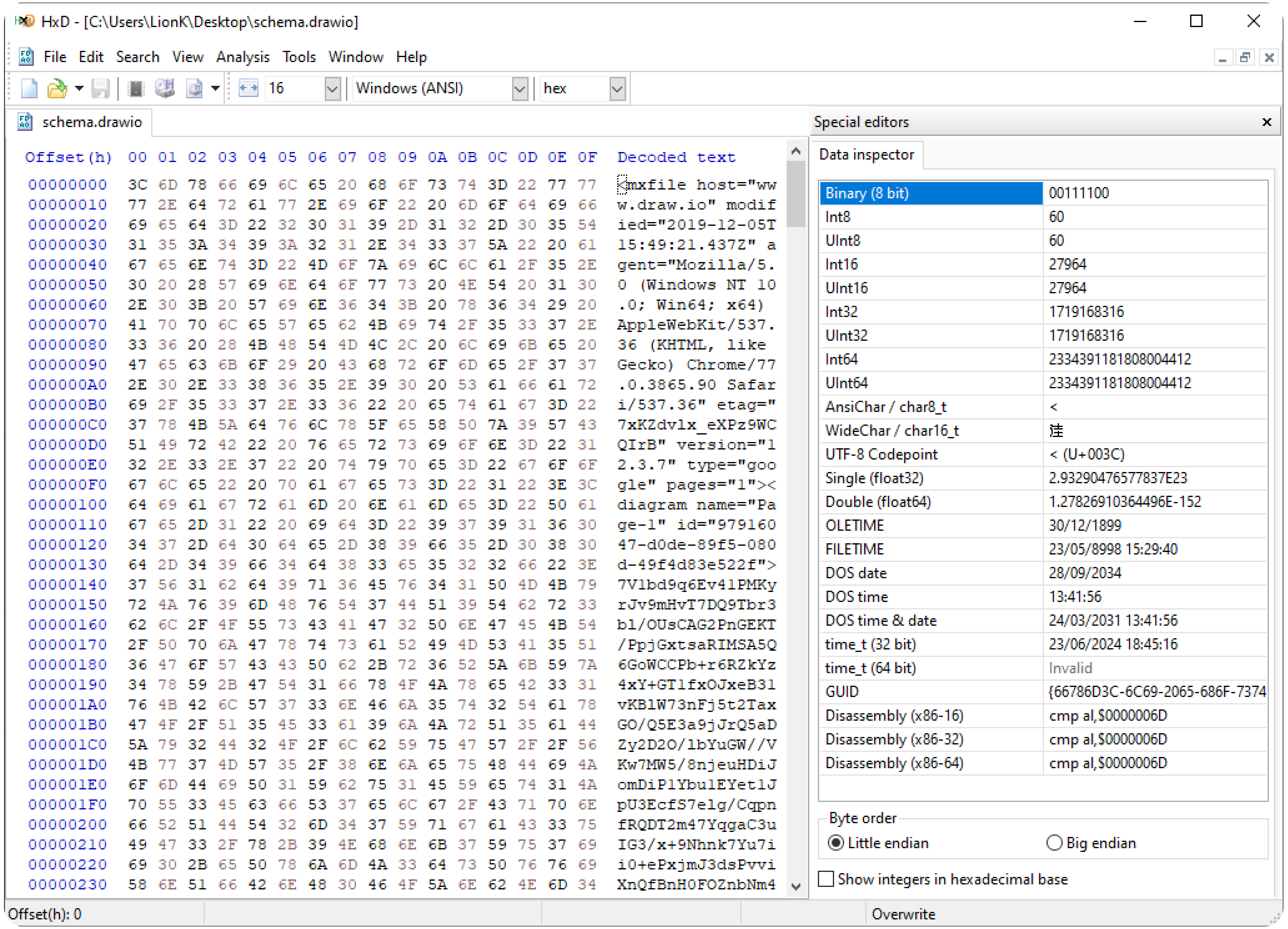
למרות שזו לא תוכנת Carving, היא משמשת לרוב כדי לעיין בנתונים במצב raw.

PhotoRec

כלי Carving עוצמתי שמתמקד בעיקר על קבצי מדיה.

CYBER SCHOOL

"גילוף" נתונים (Data Carving)



CYBER SCHOOL

חקירת תהליכים

- שלב חשוב ב-DF הוא חקירת התהליכים של מערכת "נגועה".
- ב-Windows, ניתן לעשות זאת באמצעות כלי Sysinternals.
- כלי Sysinternals כוללים חוקר תהליכים (process explorer) ומוניטור תהליכים.

CYBER SCHOOL

Forensics ברשת

Wireshark – ניתוח סטטי
פועל על נתונים שכבר נלכדו.

NetworkMiner
מתמקד יותר על שחזור artifacts מאשר על ניתוח פרוטוקולים.

- אם פיקוח הרשת לא הוגדר לפני ההתקפה, הוא יהי רלוונטי רק ל- artifacts של זיכרון (MA).

CYBER SCHOOL

כלים מותאמים אישית

כלים מסוימים יכולים לשמש רק במכשירים ספציפיים, לדוגמה DVRs.

כלי Forensics מסוימים מיוצרים בהתאמה אישית לניתוח ייעודי מסוים.

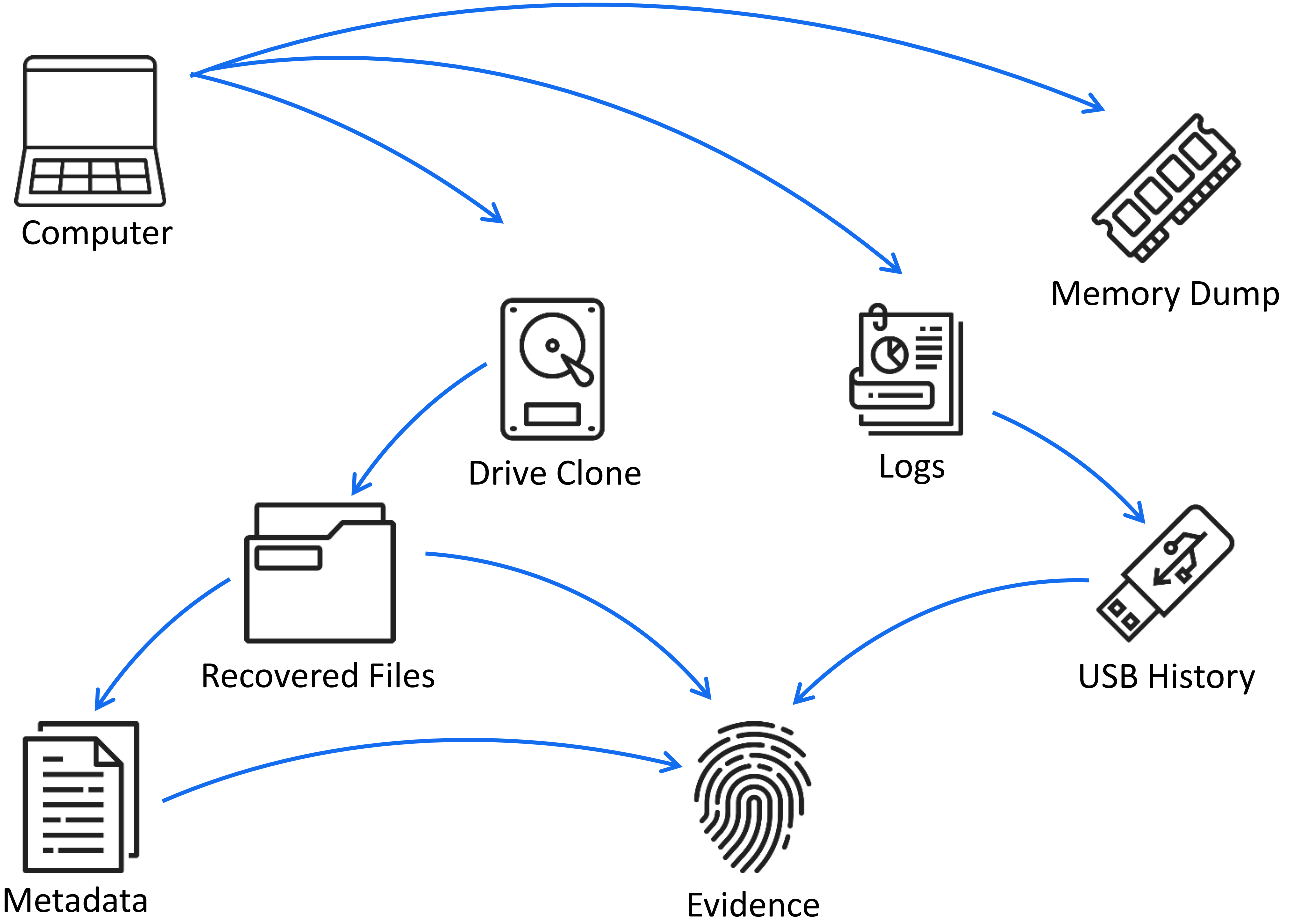
CYBER SCHOOL

CYBER SCHOOL

תגובה לאירועים

תרחיש שימוש ב-DFIR

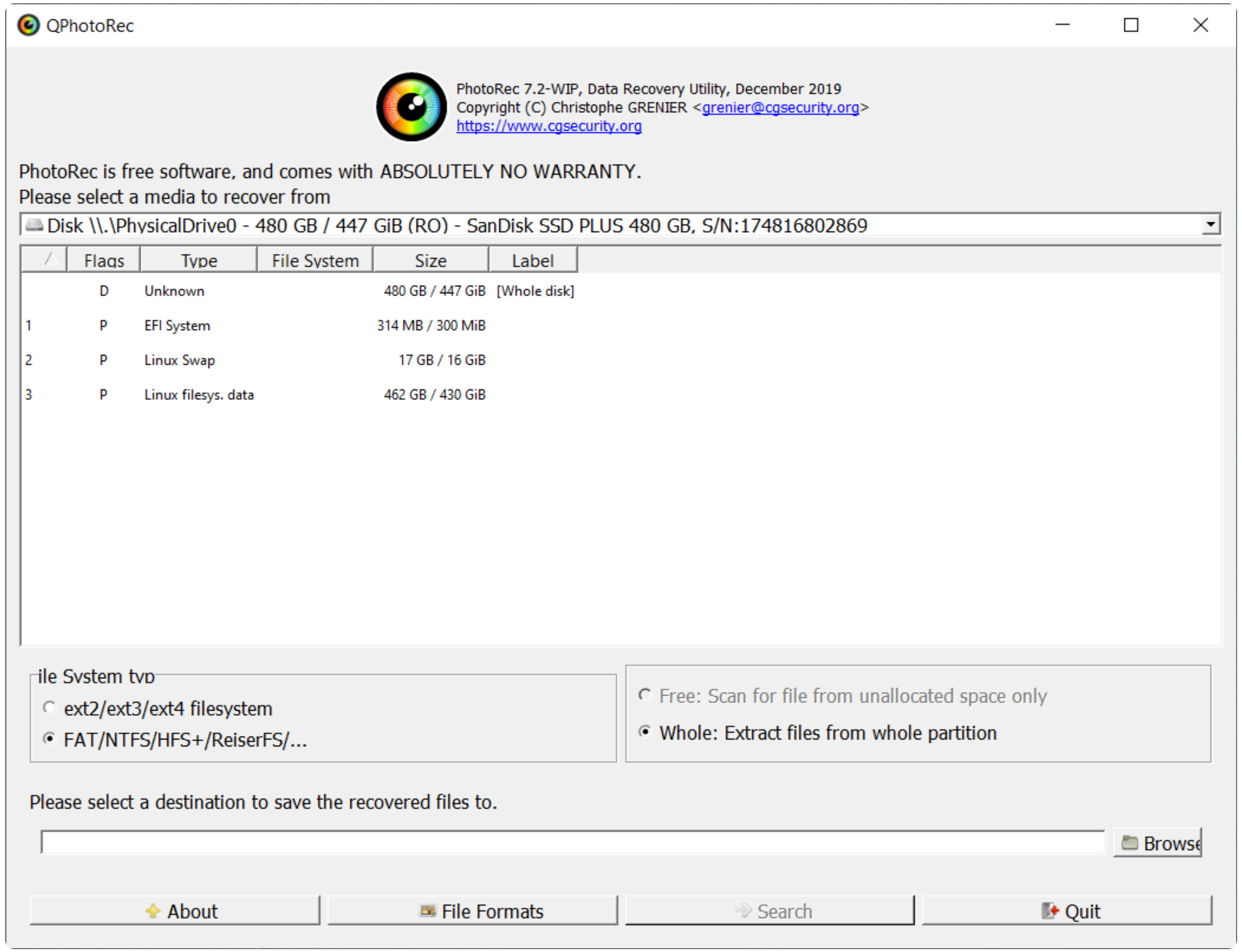
מצבי DF – דליפת נתונים



- ניתן להשתמש ב-DF כדי להוכיח שדליפה קרתה.
- "גילוף" קבצים יכול להוכיח שקבצים היו קיימים על מדיה מסוימת, אפילו אם הם נמחקו.
- ניתן להשתמש ב-Hashing כדי לאמת את זיהוי הקבצים.

CYBER SCHOOL

PhotoRec



- קבצים שנמחקים מכוון לא בהכרח נהרסים.
- לעיתים קרובות ניתן לשחזר אותם באמצעות תוכנות מיוחדות.
- כלים כמו PhotoRec יכולים לנתח תמונות בכוננים מבלי לגשת למערכת הקבצים.
- הם יכולים לזהות קבצים שהמערכת סימנו כמחוקים.

CYBER SCHOOL

Metadata ו-EXIF

```
C:\Users\JohnD\Desktop>exiftool Photo.jpg
ExifTool Version Number         : 11.80
File Name                       : Photo.jpg
Directory                       : .
File Size                       : 78 kB
File Modification Date/Time     : 2019:07:24 09:49:41+03:00
File Access Date/Time           : 2019:12:22 18:39:08+02:00
File Creation Date/Time         : 2019:12:22 18:39:08+02:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
...
Red Tone Reproduction Curve     : (Binary data 2060 bytes, use -b option to extract)
Technology                      : Cathode Ray Tube Display
Viewing Cond Desc               : Reference Viewing Condition in IEC 61966-2-1
Media White Point               : 0.9642 1 0.82491
Profile Copyright               : Copyright International Color Consortium, 2009
Chromatic Adaptation            : 1.04791 0.02293 -0.0502 0.0296 0.99046 -0.01707 -0.00925 0.01506 0.75179
Image Width                     : 628
Image Height                    : 960
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 628x960
```

- קבצים כוללים Metadata שמוסתרת מהמשתמש.
- Metadata יכולה להכיל מידע בנוגע לסוג ומיקום מצלמה.
- כלים כמו exiftool יכולים לקרוא את נתונים אלו ולעזור לחקירה.

CYBER SCHOOL

מה זה EXIF?

כולל קואורדינטות של GPS, דגם המצלמה, ואת הזמן המדויק בו תמונה צולמה.

ניתן להשתמש בו כראייה, כאשר חוקר משחזר תמונה.

CYBER SCHOOL

Hashing

שיטת זיהוי נפוצה מאוד.

יכולה לאמת את הזהות של קבצים ספציפיים.

CYBER SCHOOL

מעבדה 2

חקירת דליפת נתונים

30 – 20 דקות

המשימה

שחזר קבצים מתמונה חשודה של כונן USB והוכח שהם שומשו לגניבת מידע רגיש.

השלבים

- שחזר קבצים מתמונת USB.
- הוכח שהם תואמים את המידע הרגיש.
- חלץ את EXIF ו-metadata.
- מצא את הזהות של המדליף.

כלים

PhotoRec

Exiftool

תוכנת Hashing

קבצים קשורים

- מסמך מעבדה
- Evidence.zip
- testdisk-7.2-WIP.win.zip
- hashmyfiles-x64.zip
- exiftool-11.81.zip

CYBER SCHOOL

CYBER SCHOOL

תגובה לאירועים

סביבת DFIR

מפיצי DF

CAINE - Computer Aided INvestigative Environment

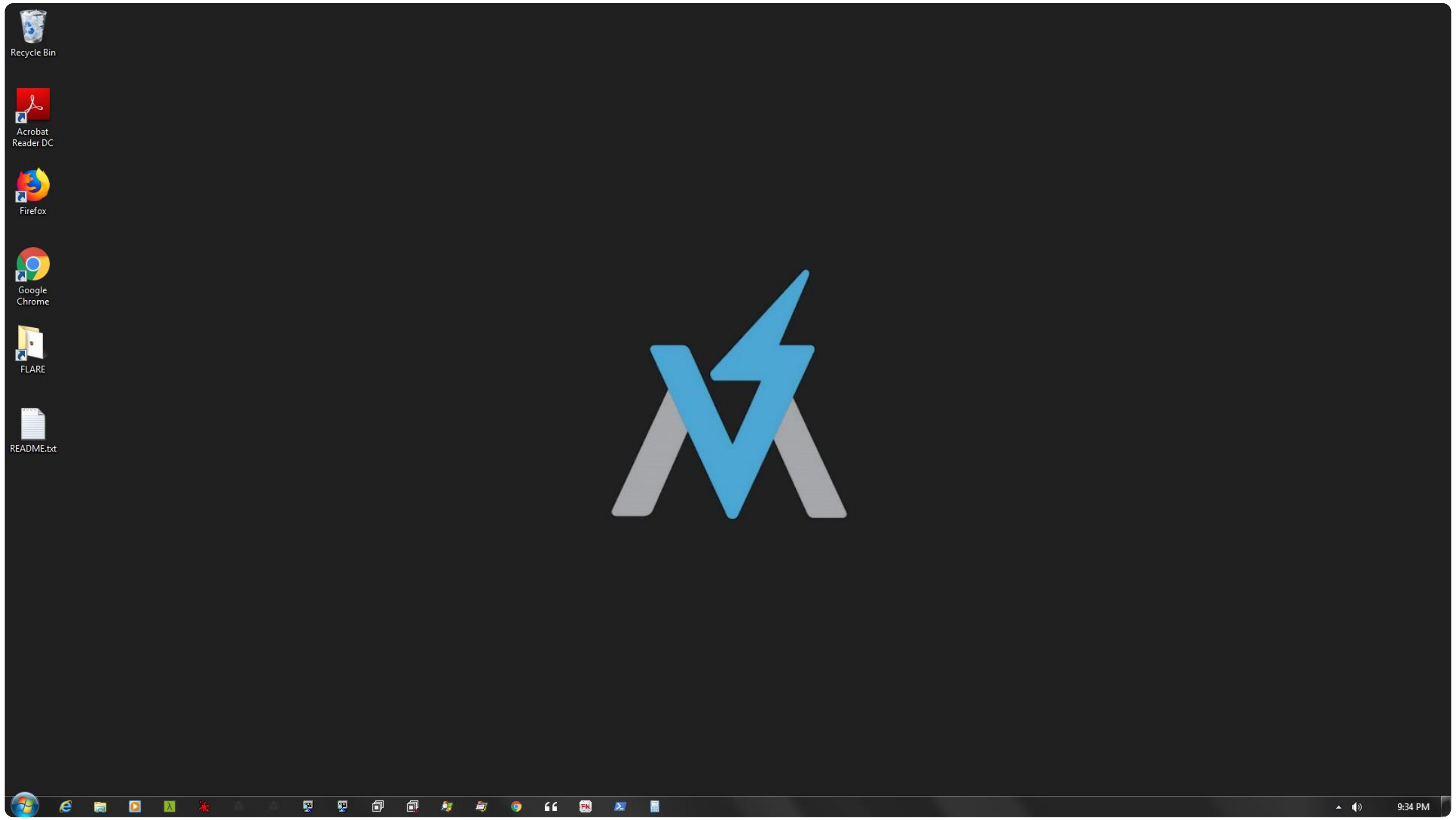
משמש בעיקר עבור השגת מידע ו-Live Forensics.

REMnux

משמש בעיקר במערכת ל-forensics מתמשך עבור artifacts של זיכרון.

- רוב כלי ה-forensics מבוססים על Linux וכתובים בפייתון.

FlareVM



- Windows יכול להפוך להיות לסביבת DF באמצעות הסקריפט FlareVM.
- הסקריפט מתקין ומגדיר כלי MA ו-RE רבים.

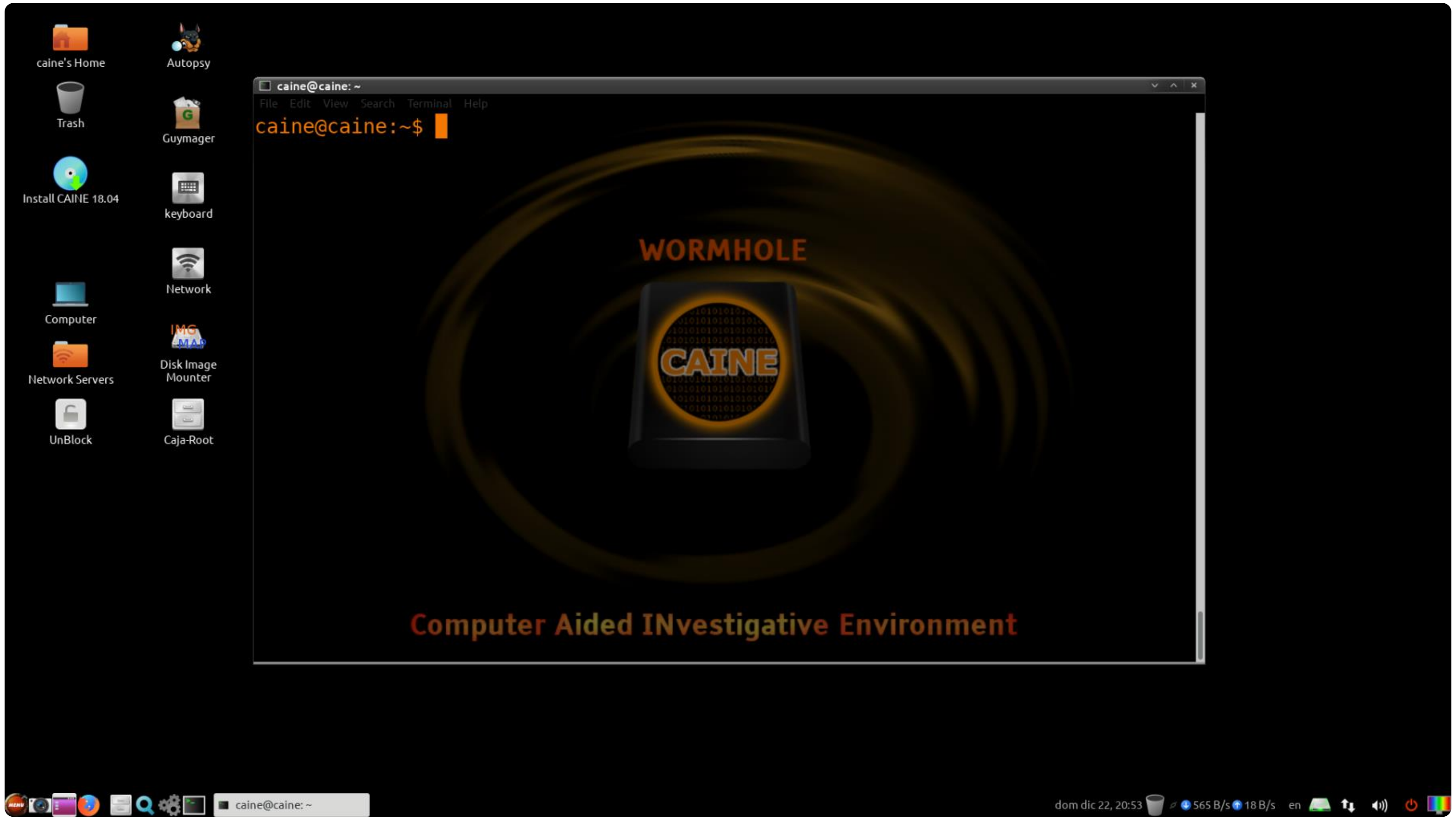
CYBER SCHOOL

SIFT Workstation

- SIFT הוא מכשיר Debian וירטואלי המיועד ל-DF.
- פותח על ידי SANS, מוסד מוביל בתחום ה-DF.
- מגיע ב-OVA ארוז מראש.

CYBER SCHOOL

CAINE Live



- Caine היא הפצה שפועלת מתוך Live USB.
- התבונה העיקרית שלה היא היכולת לרוץ כולה מתוך ה-RAM.
- תכונה זו מאפשרת השגת forensics בזמן אמת.

CYBER SCHOOL

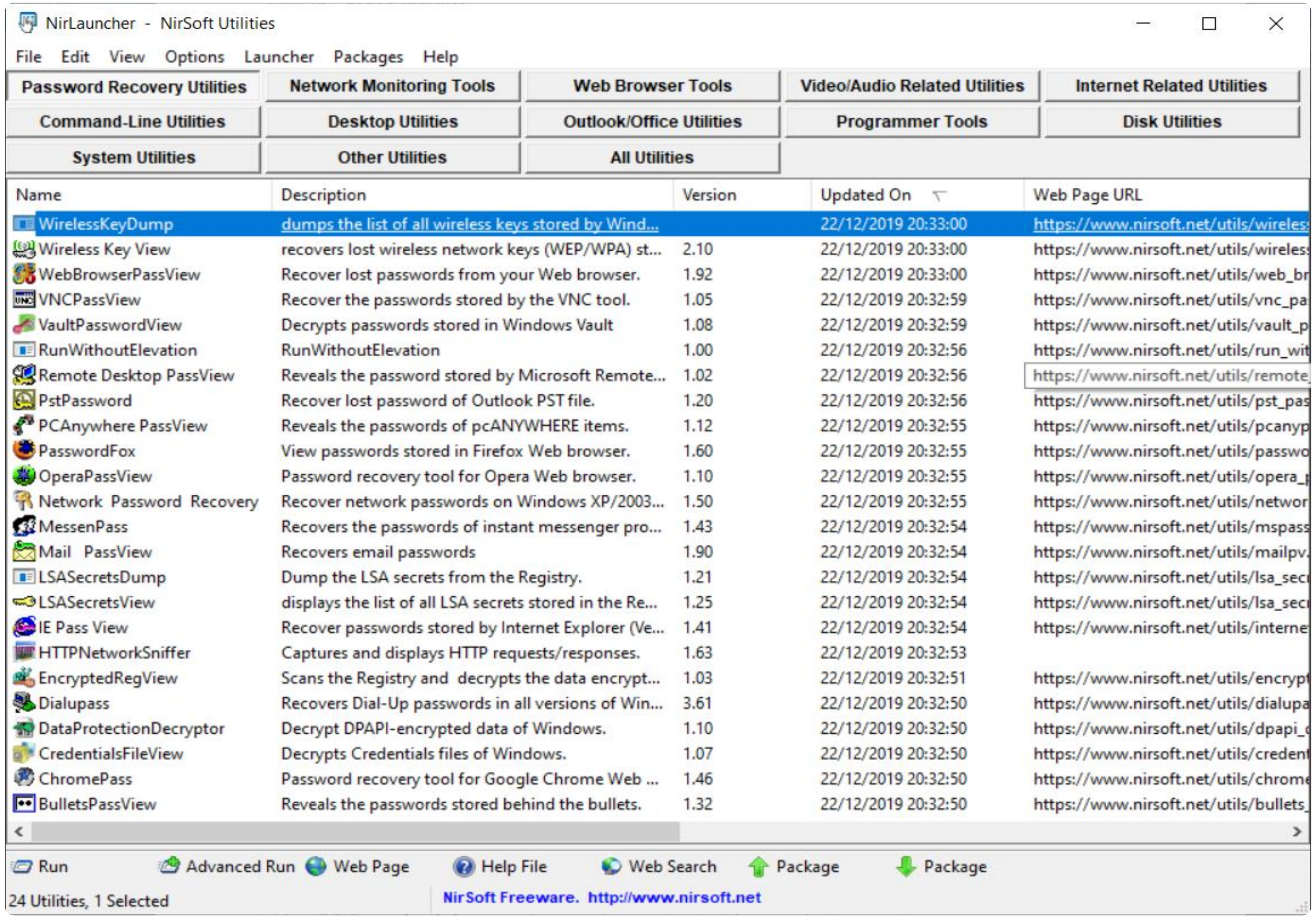
היתרונות של Live USB

חלק חיוני של כל ערכת כלים ל-Forensics.

משמש להשגת מידע ו-Live Forensics.

CYBER SCHOOL

NirSoft Launcher



- כמו ב-Live USB, מרבית הפצות ה-Forensics כוללות כלים נוספים.
- ניתן לבצע את הכלים מבלי לאתחל את ההפצה.
- NirSoft Launcher הוא דוגמה של ממשק אחיד לכלים כאלו.

CYBER SCHOOL

מעבדה 3

התקנת סביבה

30 -40 דקות

המשימה

צור ערכת וסביבת Forensics לשימוש עתידי בשיעורים.

השלבים

- התקן את SIFT workstation.
- צור Live USB עבור CAINE.
- בדוק את הכלים ב- USB Live.

כלים

VirtualBox

USB Drive

קבצים קשורים

- מסמך מעבדה
- CAINE.iso
- SIFT.ova

CYBER SCHOOL

CYBER SCHOOL

שיעור 1

מתודולוגיית DFIR

IR נגד הנדסה חברתית

ב-phishing – חקירת ההודעה והקישורים המצורפים לה.

בהנדסה חברתית בתעשייה, צוות ה-IR יכול להבין מלכודות.

CYBER SCHOOL

DF נגד הנדסה חברתית

העקבות בדרך כלל יהיו דואר אלקטרוני, הודעות וקישורים חשודים.

הראיות ייאספו בדרך כלל מהעובדים.

- אחרי DF עבור הנדסה חברתית יגיע שלב מציאת האיומים, זאת כדי לברר אם עובדים אחרים הושפעו גם הם.

CYBER SCHOOL

IR נגד השחתת שרת הרשת

מזהים אם ואיך ההשחתה קרתה.

משחזרים את התוכן של האתר המקורי בשביל גיבוי.

במקרים מסוימים, הבעלים יכול לבחור ולשחזר את האתר מיידית בלי ה-DF.

CYBER SCHOOL

DF נגד השחתת שרת הרשת

איתור חדירה

זיהוי נקודת החדירה.

זיהוי התמדה (persistence)

זהה אם נשארו backdoors.

- בקרוב המקרים, פעולות אלו יבוצעו דרך ניתוח היומנים.

CYBER SCHOOL

IR נגד שתילת סוס טרויאני (Trojan)

התגובה תשתנה בהתאם לאם הסוס הטרויאני כבר בוצע.

אם בוצע – התגובה תתמקד בהכלה ובחיסול.

CYBER SCHOOL

DF נגד שתילת סוס טרויאני (Trojan)

כולל ניתוח תוכנה זדונית.

חושף את הפעולות שהסוס הטרויאני ביצע במערכת.

CYBER SCHOOL

מעבדה 4

בוחן מתודולוגיית DFIR

10 – 15 דקות

המשימה

נתח מספר תרחישי התקפה על ארגון, ובחר במתודולוגיית ה-DFIR הטובה ביותר לכל תרחיש.

השלבים

- עיין בתרחיש.
- ענה על השאלות.

כלים

כתבן

קבצים קשורים

- מסמך מעבדה

CYBER SCHOOL

CYBER SCHOOL

שיעור 1

הגדרת נכסים

נכס - הגדרה

דבר מה בעל ערך הקשור למטרות הארגון.

יכול להיות מחשב או נתונים.

לנכסים מאפיינים הקשורים זה לזה, כגון ערך, חשיבות ומעורבותם ביעדים העסקיים.

CYBER SCHOOL

סוגי נכסים

נכסים מוחשיים

חפצים פיזיים, כגון רכבי חברה, בניינים, חומרה, תוכנה וכו'.

נכסים לא מוחשיים

קניין רוחני, פטנטים, סימנים מסחריים וכו'.

CYBER SCHOOL

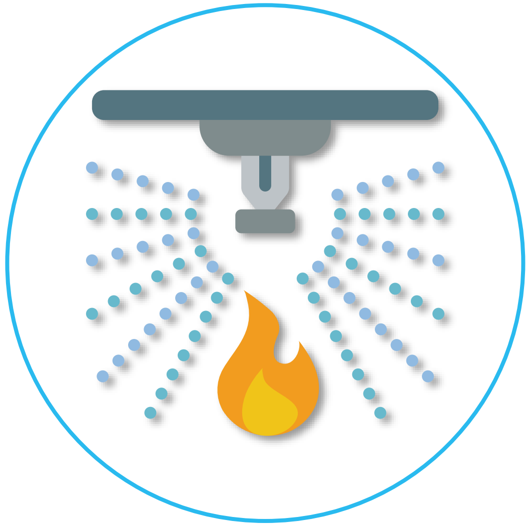
הנכס החשוב ביותר

העובדים הם הנכס החשוב ביותר בחברה.

כישורי העובדים הם 85% מערכי הנכס בחברה.

CYBER SCHOOL

הגנה על נכסים



מה המשמעות של "מאובטח" בעולם הסייבר?

האם אבטחת סייבר מספקת הגנה מלאה?

האם ישנו פתרון יחיד לכל האירועים והתקריות?

האם יש רשימת הגנה אחת לכל הנכסים?

CYBER SCHOOL

שיעור 1

שלישיית ה-CIA
(CIA Triad)

מה זה CIA?

אבן פינה לתשתית האבטחה של ארגון.

עוזר למתלמדי אבטחה עם הערכת סיכונים וניהול נכסים.

משמש כבלי או כמדריך עבור אבטחת מערכות מידע.

CIA - הגדרה

Confidentiality - סודיות

התחייבות לכך שהגישה לנתונים רגישים היא רק לאנשים מורשים.

Integrity – שלמות

הוודאות כי הנתונים הם אמינים ומדויקים (לא שונו).

Availability - זמינות

התחייבות לגישה ללא הפסקה לנתונים.

CYBER SCHOOL

תרחיש של הפרת סודיות

אתר פופולרי נפרץ. התוקף מוריד את כל בסיס הנתונים, הכולל שמות משתמשים וסיסמאות, ומוכר אותו ב-darknet.

הערה: אסור שהנתונים ישתנו, ועל האתר להמשיך לרוץ כרגיל.

זוהי הפרה של הסודיות, מכיוון שנתוני לקוחות רגישים נחשפו לאדם לא מורשה.

CYBER SCHOOL

תרחיש של הפרת שלמות

תוקף מבצע התקפת SQL injection מוצלחת על אתר פיננסי, התקפה שמשנה את ערכי המניות בבסיס הנתונים, למען רווח פרטי.

זוהי הפרת שלמות שמבוססות על חבלה ומניפולציה של נתונים.

CYBER SCHOOL

תרחיש של הפרת זמינות

Mirai Botnet מבצע התקפות DDOS נגד ספקי DNS גדולים וכתוצאה מכך לא ניתן לגשת למספר אתרים בעלי פרופיל גבוה.

זוהי הפרת זמינות כיוון שהאתרים לא היו נגישים ללקוחות לגיטימיים.

CYBER SCHOOL

קונספטים נוספים

אי-דחייה

מספק הוכחה של המקור ואת שלמות הנתונים.

ניתן להשיג זאת עם חתימות דיגיטליות או חותמות זמן.

אחריות

עוקב אחרי פעולות המשתמשים במהלך אירוע.

נאכף באמצעות ביקורות.

CYBER SCHOOL

מעבדה 5

נכסי רשת

30 – 20 דקות

המשימה

התקן והגדר תוכנת ניהול נכס רשת בסיסית.

השלבים

- התקן והגדר LanSweeper.
- סרוק והוסף נכסי רשת.
- הוסף תיעוד של הנכסים שהתגלו.

כלים

Windows VM

קבצים קשורים

- מסמך מעבדה

CYBER SCHOOL

CYBER SCHOOL

תגובה לאירועים

מרכז מבצע אבטחה (SOC)

אסטרטגיות ניהול

גישת Top-Down
הערכה, ניהול וביצוע החלטות עסקיות שהתקבלו על ידי מנהלים בכירים.

גישת Bottom-Up
עובדים חולקים את רעיונותיהם ותצפיותיהם על השוק.

CYBER SCHOOL

אחריויות של SOC

אחראי על מערכות ה-IT הקריטיות ביותר בחברה.

איתור, ניתוח ונתינת מענה לאירועי אבטחת סייבר.

מעסיק אנשים עם כישורים טובים ב-IT ואבטחת מידע.

תפקידים ב-SOC

מנהל SOC

רמה 2

CISO

רמה 3

רמה 1

CYBER SCHOOL

תפקידים נוספים במקרה של פריצה

מנכ"ל	צוות רשת
יחסי ציבור	NOC
ועד הדירקטוריון	Help Desk
צוות מערכת	יועצים חיצוניים

CYBER SCHOOL

טבלת RACI

Responsible, **A**ccountable, **C**onsulted, **I**nformed

התכלית העיקרית של הטבלה היא ניהול פרויקטים.

משמשת להקצאת תפקידים ואחריויות לכל התראת אירוע.

CYBER SCHOOL

דוגמה ל-RACI

כל אות בראשי התיבות מסמנת רמת אחריות למשימות.

אירוע	ניתוח אירועים	מנהל אירועים	עזרת רמה 2/3	צוות IT
שלב הזיהוי	R	R	R	R
סיווג אירוע	-	-	-	I
בקשת שירות	-	-	-	I
סדר עדיפויות	C	R,C	-	C,I
מקרה רציני (Major)	-	A,R,C,I	-	I
הסלמה פונקציונאלית	C	-	C,I	I
שיקום	-	-	R,C,I	R,C,I

CYBER SCHOOL

מעבדה 6

תרחישי
שלישיית CIA

10 – 15 דקות

המשימה

הבן את שלישיית CIA דרך תרגול סיטואציות.

השלבים

- זהה את סוג הפריצה שקורית בכל סיטואציה, מנקודת מבט של CIA.

כלים

כתבן

קבצים קשורים

- מסמך מעבדה

CYBER SCHOOL

CYBER SCHOOL

תגובה לאירועים

תכנית תגובה לאירועים

SANS & NIST

- ארגון פרטי שהוקם ב-1989.
- מציע מחקר וחינוך בתחום אבטחת המידע.

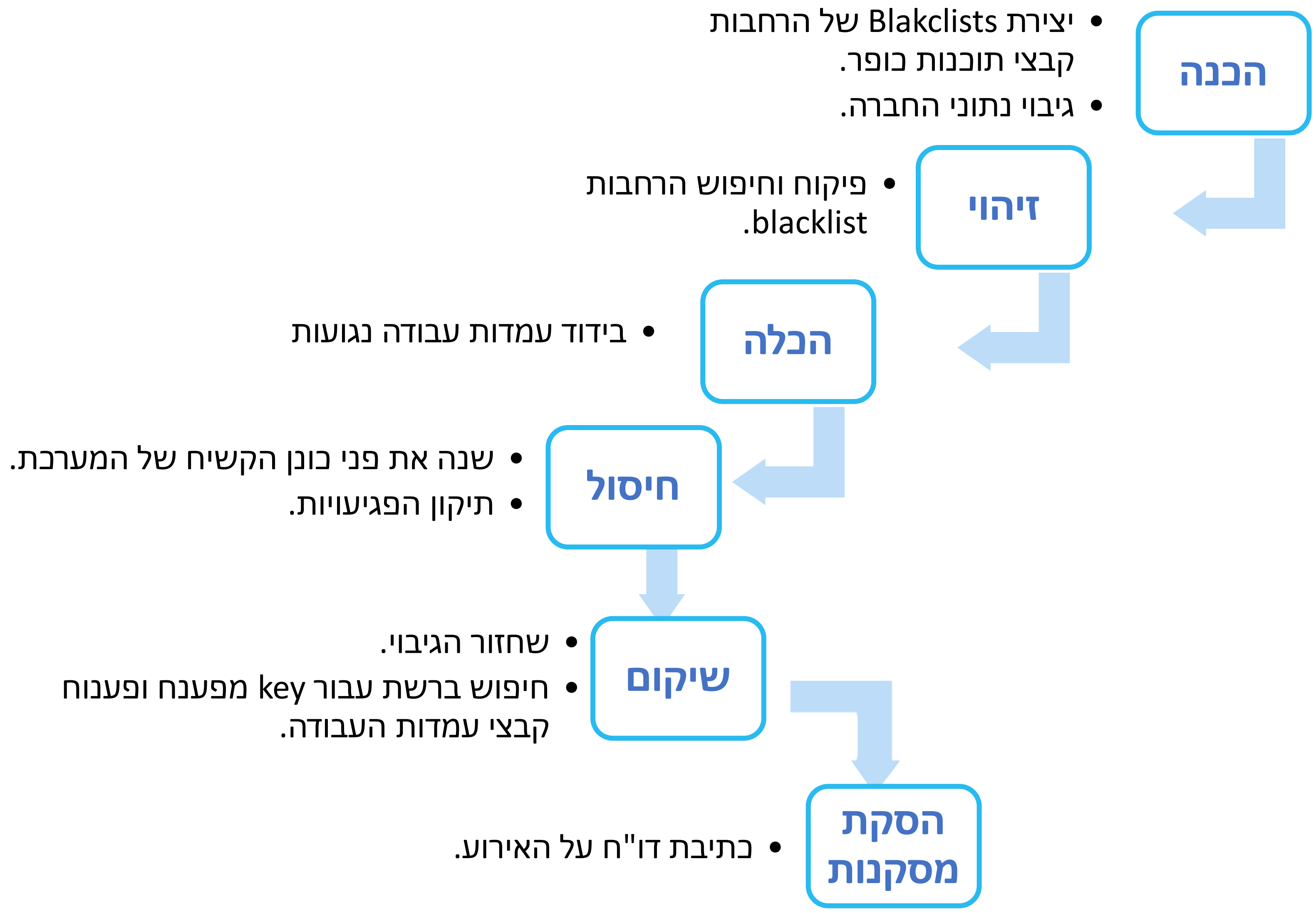
- National Institute of Standards and Technology
- סוכנות ממשלתית לא רגולטורית המפתחת טכנולוגיה, מדדים וסטנדרטים.
- חלק ממחלקת המסחר האמריקאית.

שלבים לתגובה לאירועים של SANS	
הכנה	• הגדרת אירועי ביטחון קריטיים • ביצוע הערכת סיכונים • זיהוי והגדרת נכסים רגישים.
זיהוי	• פיקוח על מערכות IT ואיתור סטיות מהפעילות הרגילה.
הכלה	• הכלה לטווח קצר. • בידוד חלק ברשת. • כיבוי שרתים שנפרצו
חיסול	• הסרת תוכנה זדונית מהמערכת הנגועה. • זיהוי ותיקון שורש הבעיה.
שיקום	• החזרת מערכות הייצור הנגועות לפעולה.
הסקת מסקנות	• הכנת תיעוד מלא של האירוע.

CYBER SCHOOL

Incident Response Plan

Ransomware Incident



CYBER SCHOOL

מעבדה 7

תכנית תגובה לאירועים

20 – 30 דקות

המשימה

תרגל כיצד ליצור תכנית תגובה לאירוע עבור התרעות שונות.

השלבים

- צור תכנית תגובה לאירוע של מייל זדוני.
- צור תכנית תגובה לאירוע של השחתת פני אתר.

כלים

כתבן

קבצים קשורים

- מסמך מעבדה

CYBER SCHOOL

CYBER SCHOOL

שיעור 1

הכנה טכנית

הכנה לאירוע

יצירת "jump kit" עם כלים להתמודדות.

שימוש ב-CD-ROMs או כונן ניידים עם מתגי RO.

בניית VM לצורך מחקר וניתוח תוכנות זדוניות.

עבודה עם snapshots אחרי אתחול המערכת.

צעדים אלו הם בגדר חובה לניהול מתמשך של אירועים.

CYBER SCHOOL

חפצים
ב-Jump Kit

1

לפטופ חזק

2

"מסניפי"
פקטות

3

מברגים, פנסים,
פינצטות וכו'

4

דיסק און קי עם יישומים
נחוצים (קריאה בלבד –
(read-only

CYBER SCHOOL

חפצים
ב-Jump Kit

5
כונן דיסק מדיה ריק

6
כבלי רשת

7
Network hub or tap

8
מכשירים חוסמים כתיבה וכוננים קשיחים

CYBER SCHOOL

CYBER SCHOOL
שיעור 1
תכנית שיקום לאחר אסון

הגדרה – DRP (Disaster Recovery plan)

מגדירה קווים כללים לאסטרטגיות התגובות לאירועים בלתי צפויים.

עוזרת למזער את הנזקים של אסון.

רעידות אדמה, שריפות, הצפות, התקפות סייבר וכו'.

קובעת אילו יישומים חייבים להישאר תמיד פעילים.

תכנית שיקום לאחר אסון של EC-Council

1
הגדרת יעדי שיקום ברורים

2
זיהוי אנשי מקצוע מעורבים

3
הכנת טיוטת תיעוד מפורט של הרשת

4
בחירת טכניקת שחזור נתונים

CYBER SCHOOL

תכנית שיקום לאחר אסון של EC-Council

5

הגדרת רשימת קריטריונים לאירוע

6

תיעוד כל תהליך השיקום מהאסון.

7

בדיקה באופן קבוע של ה-DRP

8

עדכון מתמשך של תכנית השיקום

CYBER SCHOOL

אתרי גיבוי

Hot Site הוא אתר גיבוי שפועל כל הזמן ומוכן למעבר נתונים מיידי.

Warm Site מכיל שרתים ומשאבים נוספים למטרות גיבוי, אך הוא אינו מוכן למעבר נתונים מיידי כמו Hot site.

Cold Site, האופציה הזולה ביותר, לא תמיד כולל את כל הציוד הנדרש בכדי לאפשר את חידוש הפעילות הרגילה.

CYBER SCHOOL

CYBER SCHOOL

שיעור 1

תאימות ל-GRC

נקודת מבט ממשלתית

הנחיות

המלצות או הצעות שאינן בהכרח בגדר חובה.

הליכים

תיאור כל שלב הנדרש לביצוע משימה מסוימת.

תקנים

רמת איכות מקובלת

מדיניות

הצהרות רשמיות שמציגות את העמדה והכיוון של הניהול הבכיר.

CYBER SCHOOL

תקנים ורגולציות

ISO

HIPAA

GDPR

SOX

PCI DSS

CYBER SCHOOL

מעבדה 8

יצירת סביבת מעבדת Windows

10 דקות

המשימה

הבן מכונת Windows 7 שתשמש לאורך הקורס.

השלבים

- צור מכונה וירטואלית עם Windows 7 מותקן בתוכה.
- התקן Flare-VM על המכונה הוירטואלית.

כלים

מכונה וירטואלית

Windows 7 Image

קבצים קשורים

מסמך מעבדה

CYBER SCHOOL

CSRP

DFIR

תגובה לאירועים

שאלות?