

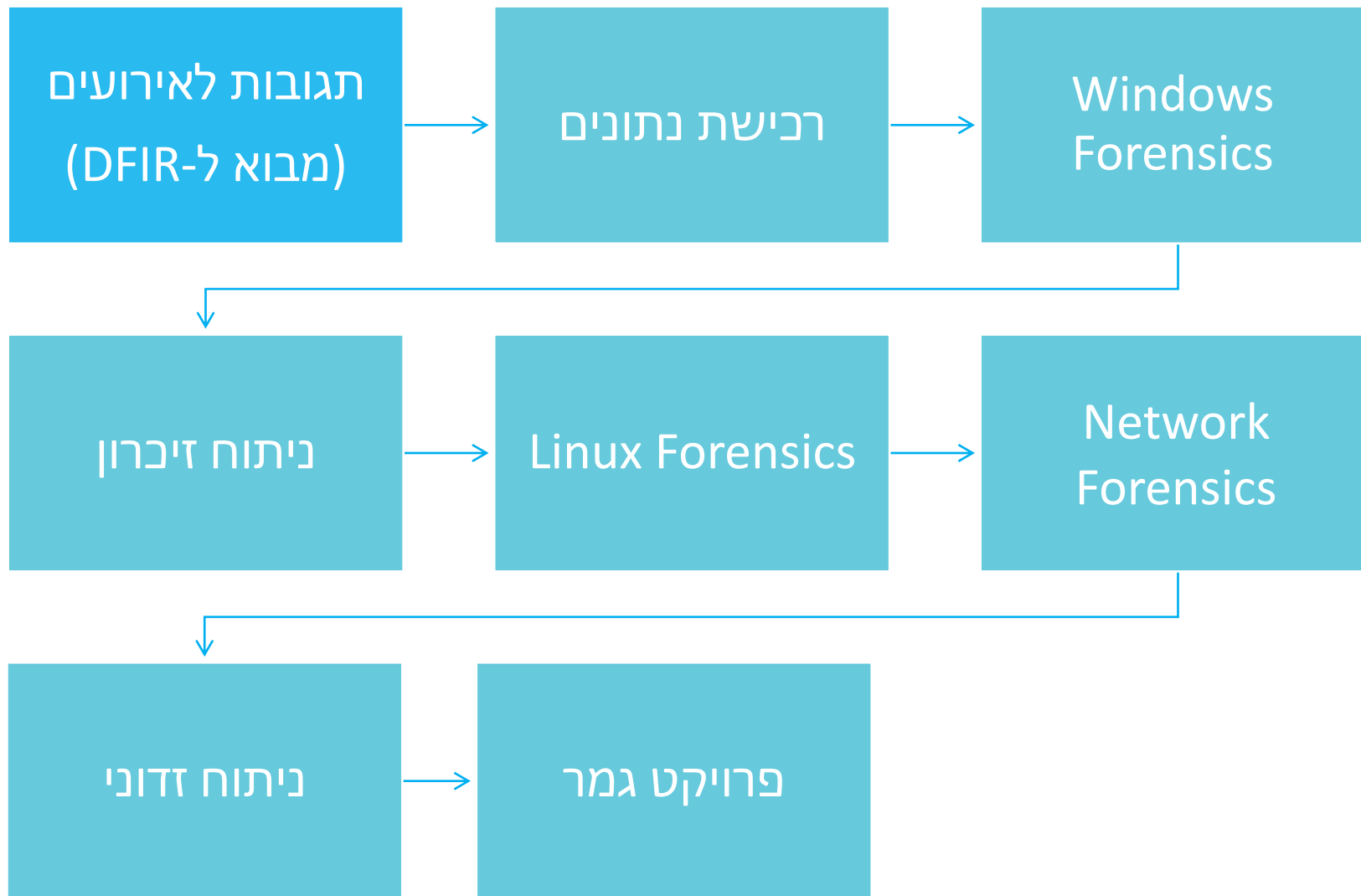
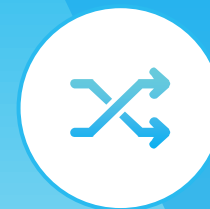
CSRP

תגובות לאירועים



CYBER SCHOOL

מסלול הקורס





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

שיעור 1

תגובה לאירועים

מבוא ל-DFIR

DFIR

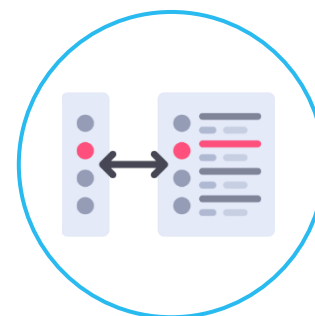


DFIR – חקירת התקפת סייבר אחרי אירוע.

DF – ניתוח artifacts אחרי התקפת סייבר.



IR – ביצוע פעולות כאשר קורית פריצת אבטחה.





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



מה זה תגובה לאירועים (IR)?



ניהול והתמודדות נגד פריצת אבטחה או התקפה.
הפחתת הנזק והעלות של השיקום.

DF Vs IR Vs TH



DF
Digital Forensics
לאחר ההתקפה
מציאת ראיות
מארח ורשת
רמה 3 ב-SOC

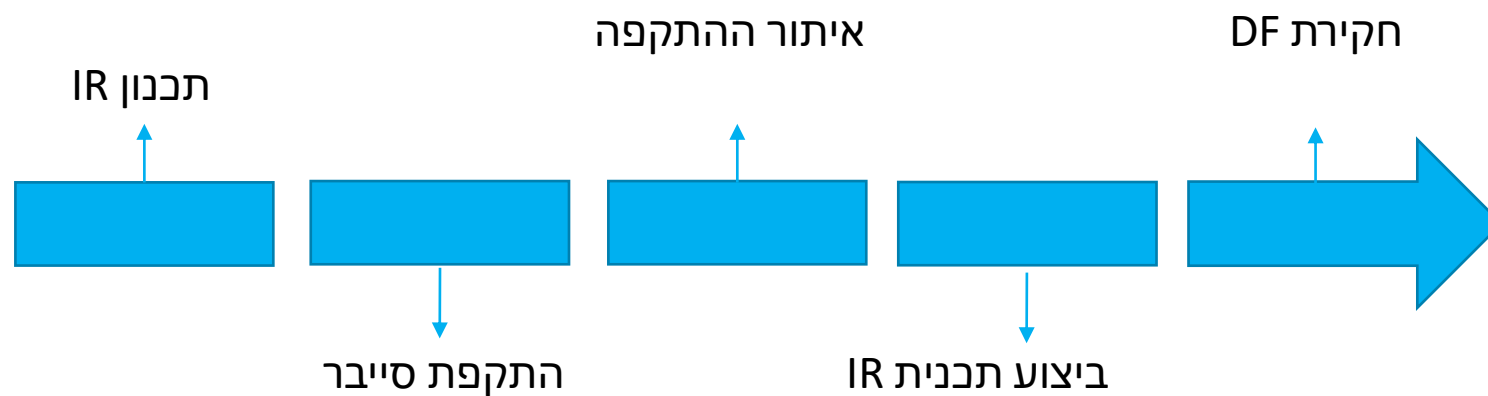
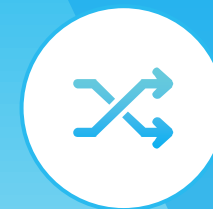
VS

IR
Incident Response תגובה לאירועים
בזמן ההתקפה
מזעור נזקים עתידיים
מארח ורשת
רמה 2 ב-SOC

VS

TH
Threat Hunting מציאת איומים
כל הזמן
מציאת איומים שלא אותרו
מארח ורשת
רמה 3 ב-SOC

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

תגובה לאירועים

תכנון תגובות לאירוע (IR)

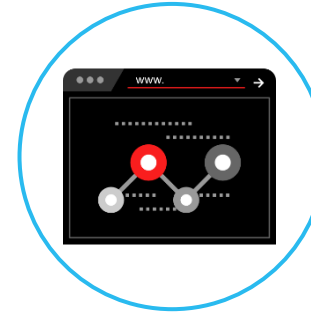
למה אנחנו צריכים IR?



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



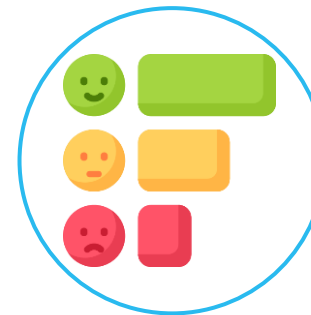
אחריות של מגיב לאירועים



הערכת וסיכום ליקויי אבטחה אפשריים שעלולים להוביל להתקפה.



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

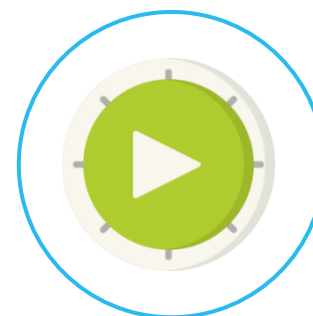


בצע בדיקת חדירות ויצר דו"חות הערכת סיכונים.





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

תגובה לאירועים

תהליך ה-DFIR





ניתוח מת (Dead Analysis)

ניתוח מחשבים כבויים.
יכול לכלול ניתוח של כוננים משובטים.

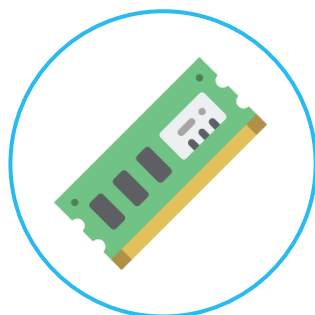


ניתוח חי (Live Analysis)

ניתוח מחשבים פועלים.
טכנית, זה לא שיטת ניתוח פורנזי.



מטרות - Artifacts



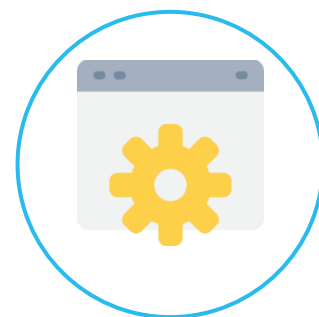
Artifacts
זיכרון



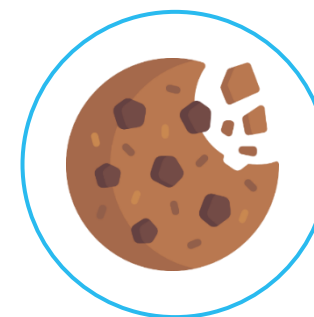
קבצי יומנים



קבצים על
כוננים



תהליכים



נתוני מטמון





Forensics ברשת

מתמקד באסיפת נתונים על תעבורה העוברת דרך ציוד רשת.



Forensics במארח

מתמקד באסיפת נתונים הנוגעים למארחים, כמו קבצים או זיכרון.



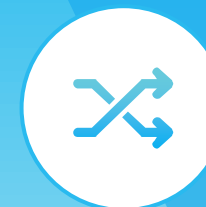


בבית משפט – כל דבר שראית, שמעת או אמרת, שמוכיח שמהו קרה.

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



דוגמה לראיות



Autoruns - Sysinternals: www.sysinternals.com

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run					
Acrobat A...	AcroTray	(Verified) Adob...	c:\program files...	28/03/2017 14:50	
Adobe A...	Adobe Reader ...	(Verified) Adob...	c:\program files...	23/11/2016 9:28	
Adobe Cr...	Adobe Creative...	(Verified) Adob...	c:\program files...	13/09/2018 11:32	
Dropbox	Dropbox	(Verified) Drop...	c:\program files...	17/12/2019 21:28	
KeePass ...	KeePass	(Verified) Open...	c:\program files...	10/09/2019 11:24	
Kraken05...	Razer Kraken 7...	(Verified) Razer...	c:\program files...	08/09/2016 7:59	
QfinderPro	Qfinder Pro	(Verified) QNA...	c:\program files...	19/09/2019 10:29	
Razer Sy...	Razer Synapse	(Verified) Razer...	c:\program files...	28/09/2018 4:57	
SunJavaU...	Java Update Sc...	(Verified) Oracl...	c:\program files...	16/12/2018 7:51	
Truelmag...		(Verified) Acron...	c:\program files...	23/09/2019 9:29	
vmware-tr...	VMware Tray P...	(Verified) VMw...	c:\program files...	17/09/2019 4:03	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run					
com.squir...		(Verified) Slack...	c:\users\lionk\la...	13/12/2016 21:53	
Docker D...			File not found: ...		
Fences	Fences Settings	(Verified) Stard...	c:\program files...	25/05/2018 7:37	
GoogleC...	Google Chrome	(Verified) Goog...	c:\program files...	06/12/2019 23:30	
GoogleDr...		(Verified) Goog...	c:\program files...	01/01/1970 2:00	
JetBrains ...	JetBrains Tool...	(Verified) JetBr...	c:\users\lionk\la...	21/10/2019 17:00	
kpm.exe	Kaspersky Pas...	(Verified) Kasp...	c:\program files...	02/12/2019 14:25	
NordVPN	NordVPN	(Verified) TEFL...	c:\program files...	01/10/2019 15:28	
OneDrive	Microsoft OneD...	(Verified) Micro...	c:\users\lionk\la...	08/11/2019 0:48	
OPENVP...		(Verified) Open...	c:\program files...	01/01/1970 2:00	
Outlook G...			File not found: ...		
uTorrent	µTorrent	(Verified) BitTo...	c:\users\lionk\la...	30/09/2019 21:14	
WindowG...	WindowGrid	(Not Verified) w...	c:\program files...	17/05/2016 13:19	
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup					
AnyDesk.I...		(Verified) phila...	c:\program files...	18/11/2019 20:16	

➤ תוכנות Startup יכולות להיות ראייה לתוכנה זדונית מתמשכת.

➤ תוכנות Startup נמצאות בתיקיות ייעודיות וב-registry keys.

➤ Autoruns הן תוכנות שיודעות כיצד למנוע מקומות פוטנציאליים ל-startup.



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.

קבצים קשורים

מסמך מעבדה

כלים

Autoruns



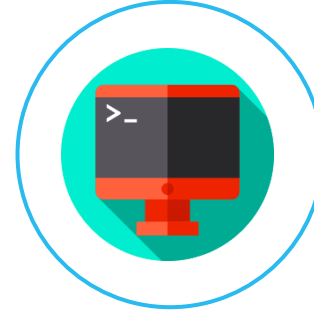
CYBER SCHOOL



CYBER SCHOOL

תגובה לאירועים

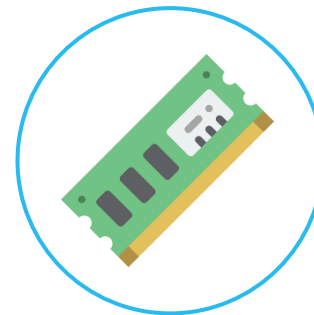
ערכת הכלים של DFIR



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



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



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



Autopsy – קוד פתוח

Autopsy הוא חלק מאוסף ערכות ה-sleuth של כלי פיית'ון המשמשים לחקירות פורנזיות.



FTK - קנייני

כולל כלים לפיקוח על כוננים משובטים.



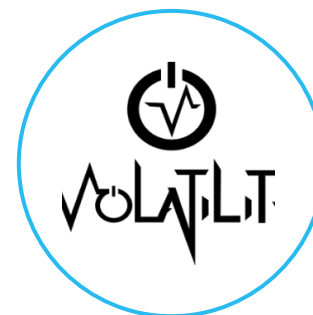
EnCase - קנייני

כולל תכונות מתקדמות רבות של פיקוח על תמונות.



Volatility Framework

אוסף קוד פתוח של כלי פיית'ון, 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.

"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.

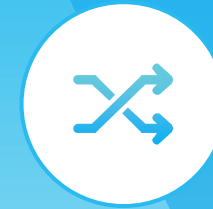


PhotoRec

כלי Carving עוצמתי שמתמקד בעיקר על קבצי מדיה.



"גילוף" נתונים (Data Carving)



HxD - [C:\Users\LionK\Desktop\schem.drawio]

File Edit Search View Analysis Tools Window Help

16 Windows (ANSI) hex

schema.drawio

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	3C	6D	78	66	69	6C	65	20	68	6F	73	74	3D	22	77	77	mxfile host="ww
00000010	77	2E	64	72	61	77	2E	69	6F	22	20	6D	6F	64	69	66	w.draw.io" modif
00000020	69	65	64	3D	22	32	30	31	39	2D	31	32	2D	30	35	54	ied="2019-12-05T
00000030	31	35	3A	34	39	3A	32	31	2E	34	33	37	5A	22	20	61	15:49:21.437Z" a
00000040	67	65	6E	74	3D	22	4D	6F	7A	69	6C	6C	61	2F	35	2E	gent="Mozilla/5.
00000050	30	20	28	57	69	6E	64	6F	77	73	20	4E	54	20	31	30	0 (Windows NT 10
00000060	2E	30	3B	20	57	69	6E	36	34	3B	20	78	36	34	29	20	.; Win64; x64)
00000070	41	70	70	6C	65	57	65	62	4B	69	74	2F	35	33	37	2E	AppleWebKit/537.
00000080	33	36	20	28	4B	48	54	4D	4C	2C	20	6C	69	6B	65	20	36 (KHTML, like
00000090	47	65	63	6B	6F	29	20	43	68	72	6F	6D	65	2F	37	37	Gecko/Chrome/77
000000A0	2E	30	2E	33	38	36	35	2E	39	30	20	53	61	66	61	72	.0.3865.90 Safar
000000B0	69	2F	35	33	37	2E	33	36	22	20	65	74	61	67	3D	22	i/537.36" etag="
000000C0	37	78	4B	5A	64	76	6C	78	5F	65	58	50	7A	39	57	43	7xKZdvlx_eXPz9WC
000000D0	51	49	72	42	22	20	76	65	72	73	69	6F	6E	3D	22	31	QIRB" version="1
000000E0	32	2E	33	2E	37	22	20	74	79	70	65	3D	22	67	6F	6F	2.3.7" type="goo
000000F0	67	6C	65	22	20	70	61	67	65	73	3D	22	31	22	3E	3C	gle" pages="1"><
00000100	64	69	61	67	72	61	6D	20	6E	61	6D	65	3D	22	50	61	diagram name="Pa
00000110	67	65	2D	31	22	20	69	64	3D	22	39	37	39	31	36	30	ge-1" id="979160
00000120	34	37	2D	64	30	64	65	2D	38	39	66	35	2D	30	38	30	47-d0de-89f5-080
00000130	64	2D	34	39	66	34	64	38	33	65	35	32	32	66	22	3E	d-49f4d83e522f">
00000140	37	56	31	62	64	39	71	36	45	76	34	31	50	4D	4B	79	7V1bd9q6Ev41PMKy
00000150	72	4A	76	39	6D	48	76	54	37	44	51	39	54	62	72	33	rJv9mHvT7DQ9Tbr3
00000160	62	6C	2F	4F	55	73	43	41	47	32	50	6E	47	45	4B	54	b1/OUscAG2PnGERT
00000170	2F	50	70	6A	47	78	74	73	61	52	49	4D	53	41	35	51	/PpjGxtsaRIMSASQ
00000180	36	47	6F	57	43	43	50	62	2B	72	36	52	5A	6B	59	7A	6GoWCCPb+r6RZkYz
00000190	34	78	59	2B	47	54	31	66	78	4F	4A	78	65	42	33	31	4xY+GT1fx0JxeB3l
000001A0	76	4B	42	6C	57	37	33	6E	46	6A	35	74	32	54	61	78	vKB1W73nFj5t2Tax
000001B0	47	4F	2F	51	35	45	33	61	39	6A	4A	72	51	35	61	44	GO/Q5E3a9jJrQ5aD
000001C0	5A	79	32	44	32	4F	2F	6C	62	59	75	47	57	2F	2F	56	Zy2D20/1bYuGW//V
000001D0	4B	77	37	4D	57	35	2F	38	6E	6A	65	75	48	44	69	4A	Kw7MW5/8njeuHDiJ
000001E0	6F	6D	44	69	50	31	59	62	75	31	45	59	65	74	31	4A	omDiP1YbulEYet1J
000001F0	70	55	33	45	63	66	53	37	65	6C	67	2F	43	71	70	6E	pU3Ecfs7e1g/Cqpn
00000200	66	52	51	44	54	32	6D	34	37	59	71	67	61	43	33	75	fRQDTm47YqgaC3u
00000210	49	47	33	2F	78	2B	39	4E	68	6E	6B	37	59	75	37	69	IG3/x+9Nhk7Yu7i
00000220	69	30	2B	65	50	78	6A	6D	4A	33	64	73	50	76	76	69	i0+ePxjmJ3dsPvvi
00000230	58	6E	51	66	42	6E	48	30	46	4F	5A	6E	62	4E	6D	34	XnQfBnH0FOZnbNm4

Offset(h): 0

Special editors

Data inspector

Binary (8 bit)	00111100
Int8	60
UInt8	60
Int16	27964
UInt16	27964
Int32	1719168316
UInt32	1719168316
Int64	2334391181808004412
UInt64	2334391181808004412
AnsiChar / char8_t	<
WideChar / char16_t	誣
UTF-8 Codepoint	< (U+003C)
Single (float32)	2.93290476577837E23
Double (float64)	1.27826910364496E-152
OLETIME	30/12/1899
FILETIME	23/05/8998 15:29:40
DOS date	28/09/2034
DOS time	13:41:56
DOS time & date	24/03/2031 13:41:56
time_t (32 bit)	23/06/2024 18:45:16
time_t (64 bit)	Invalid
GUID	{66786D3C-6C69-2065-686F-7374}
Disassembly (x86-16)	cmp al,\$0000006D
Disassembly (x86-32)	cmp al,\$0000006D
Disassembly (x86-64)	cmp al,\$0000006D

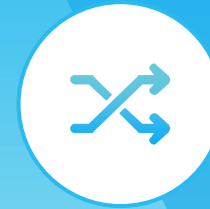
Byte order

Little endian Big endian

Show integers in hexadecimal base

Overwrite

חקירת תהליכים



Windows Sysinternals - Window

https://docs.microsoft.com

Microsoft | Sysinternals Learn Downloads Community

Docs / Sysinternals

Filter by title

Home

> Learn

> Downloads

Downloads

> File and Disk Utilities

> Networking Utilities

> Process Utilities

> Security Utilities

> System Information

> Miscellaneous

Sysinternals Suite

Community

Software License Terms

Licensing FAQ

Windows Sysinternals

12/11/2019 • 5 minutes to read • 🌱 🌱 🌱 🌱 🌱 +1

The Sysinternals web site was created in 1996 by [Mark Russinovich](#) to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.

- Read the official guide to the Sysinternals tools, [Troubleshooting with the Windows Sysinternals Tools](#)
- Read the [Sysinternals Blog](#) for a detailed change feed of tool updates
- Watch Mark's top-rated [Case-of-the-Unexplained](#) troubleshooting presentations and other webcasts
- Read [Mark's Blog](#) which highlight use of the tools to solve real problems
- Check out the Sysinternals [Learning Resources](#) page
- Post your questions in the [Sysinternals Forum](#)

Sysinternals Live

Sysinternals Live is a service that enables you to execute Sysinternals tools directly from the Web without hunting for and manually downloading them. Simply enter a tool's Sysinternals Live path into Windows Explorer or a command prompt as `live.sysinternals.com/<toolname>` or `\\live.sysinternals.com\tools\<toolname>`.

You can view the entire Sysinternals Live tools directory in a browser at <https://live.sysinternals.com/>.

Download PDF

➤ 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.





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).



כלים מותאמים אישית



כלים מסוימים יכולים לשמש רק במכשירים
ספציפיים, לדוגמה DVRs.
כלי Forensics מסוימים מיוצרים בהתאמה אישית
לניתוח ייעודי מסוים.



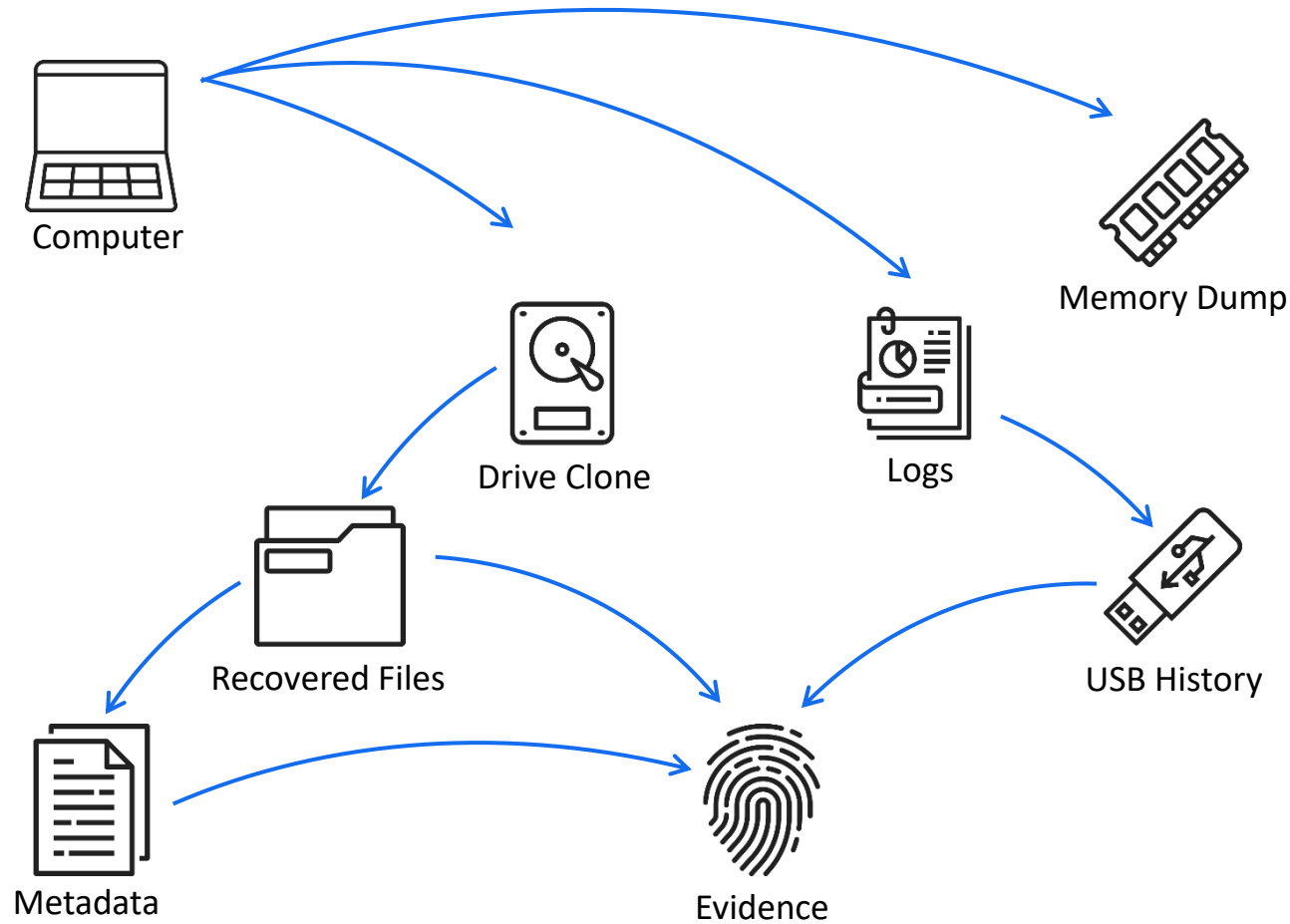
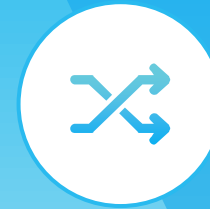


CYBER SCHOOL

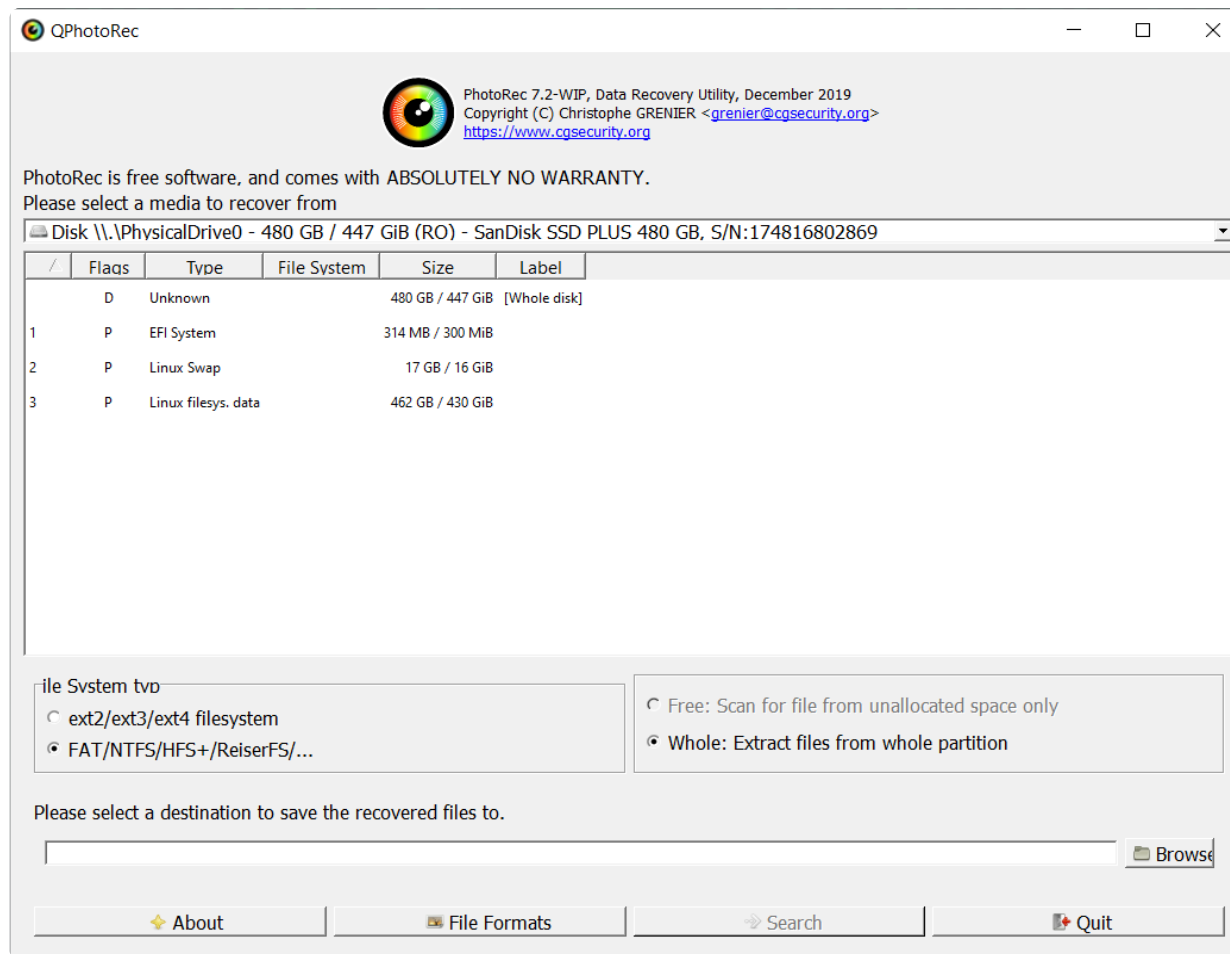
תגובה לאירועים

תרחיש שימוש ב-DFIR

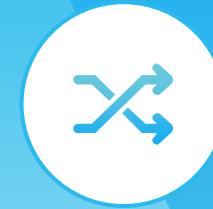
מצבי DF – דליפת נתונים



- 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.



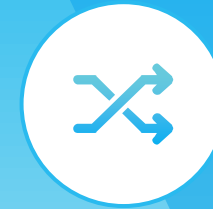
PhotoRec



- קבצים שנמחקים מכונן 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.



EXIF-ı Metadata



```
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.
- בלים כמו exiftool יכולים לקרוא את נתונים אלו ולעזור לחקירה.



מה זה EXIF?



כולל קואורדינטות של GPS, דגם המצלמה, ואת הזמן המדויק בו תמונה צולמה.
ניתן להשתמש בו כראייה, כאשר חוקר משחזר תמונת.



Hashing



שיטת זיהוי נפוצה מאוד.
יכולה לאמת את הזהות של קבצים ספציפיים.



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.

קבצים קשורים

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

כלים

- PhotoRec
- Exiftool
- תוכנת Hashing



CYBER SCHOOL



CYBER SCHOOL

תגובה לאירועים

סביבת DFIR



CAINE - Computer Aided INvestigative Environment
משמש בעיקר עבור השגת מידע ו-Live Forensics.



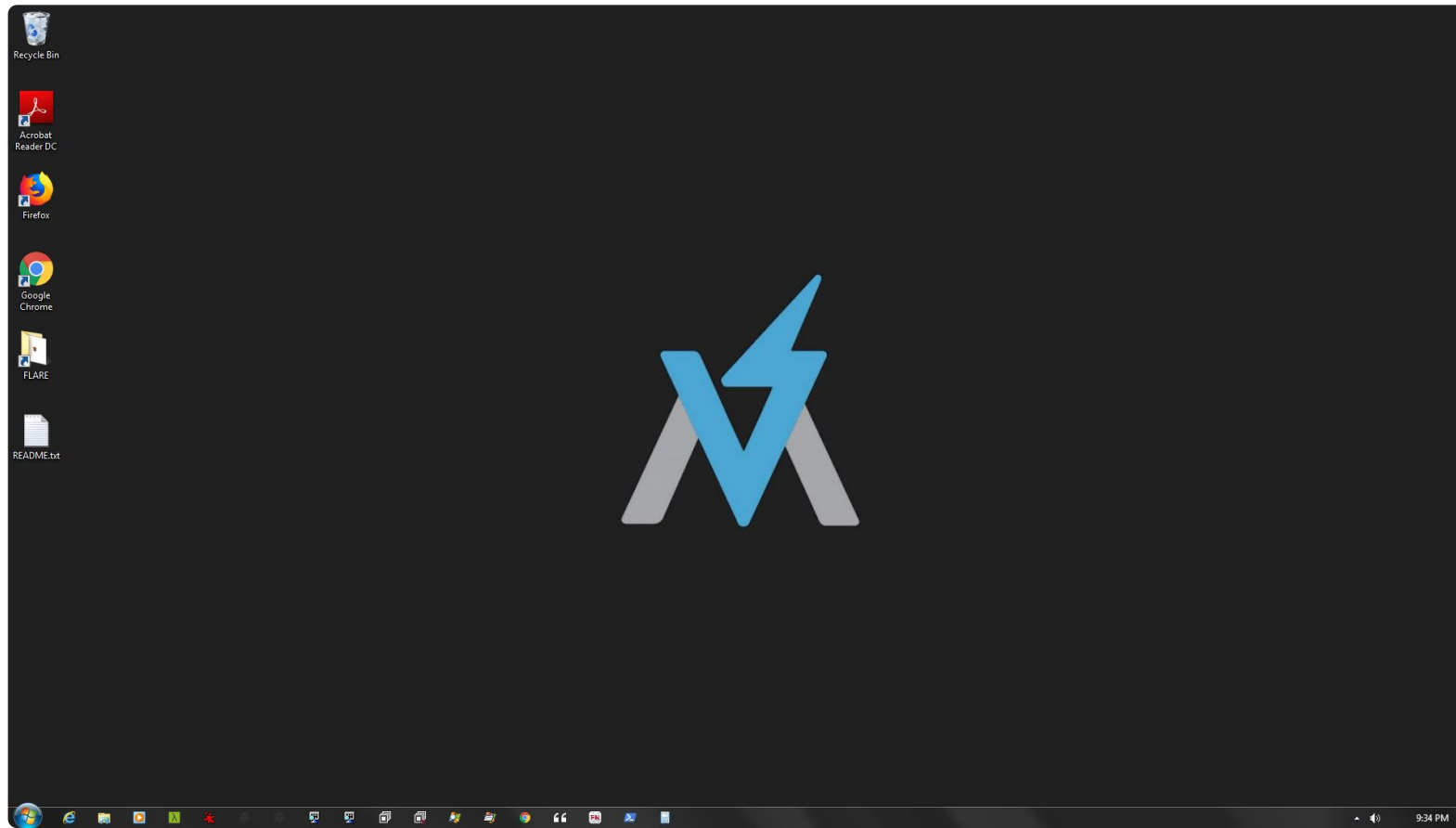
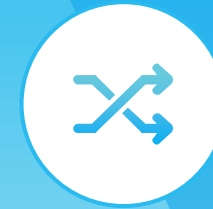
REMnux
משמש בעיקר כמערכת ל-forensics מתמשך עבור artifacts של זיכרון.



➤ רוב כלי ה-forensics מבוססים על Linux וכתובים בפיית'ון.



FlareVM

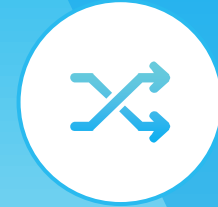


➤ Windows יכול להפוך להיות לסביבת DF באמצעות הסקריפט FlareVM.

➤ הסקריפט מתקין ומגדיר כלי MA ו-RE רבים.

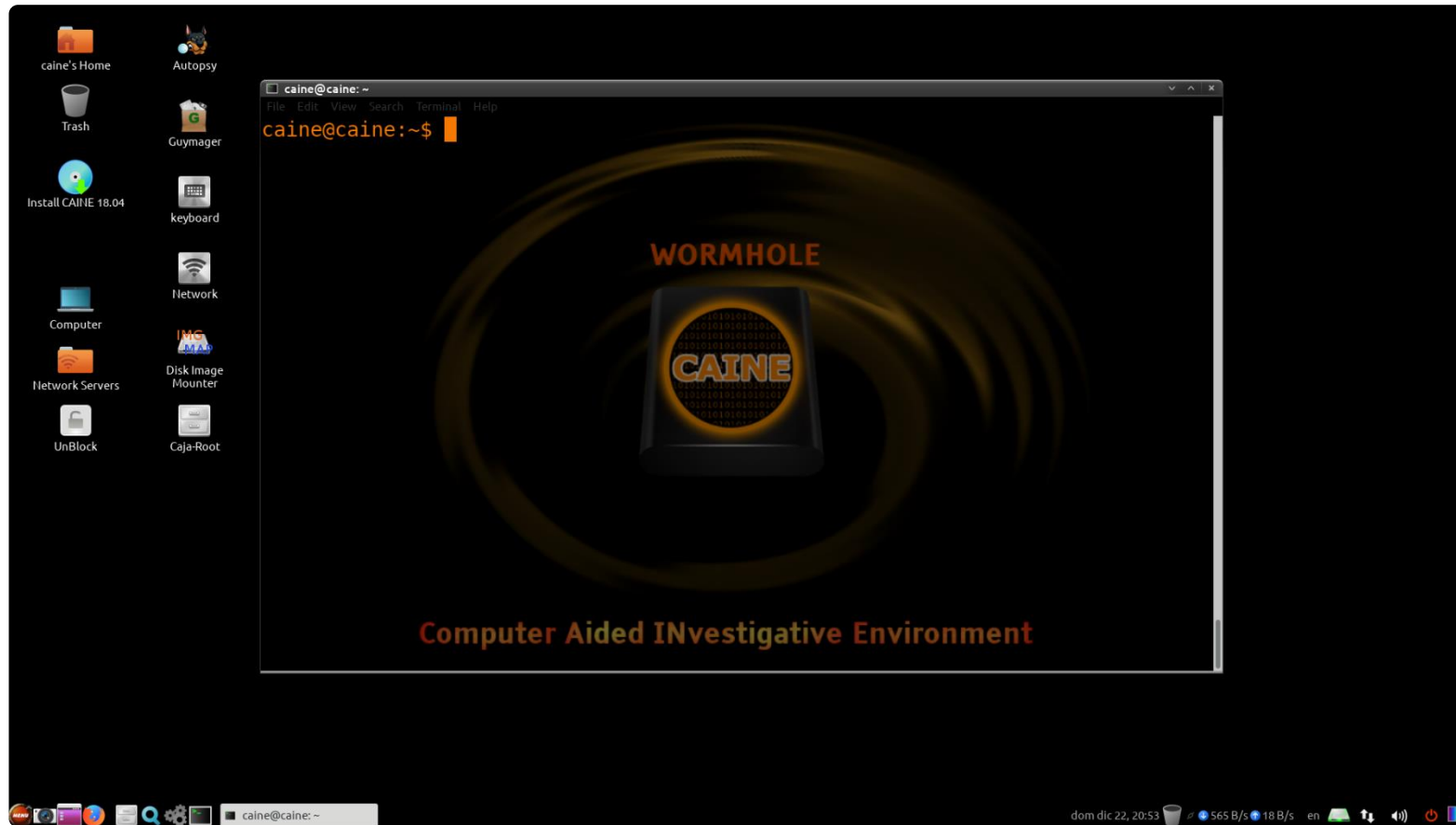
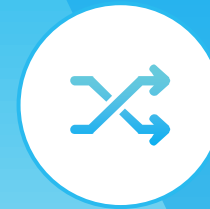


SIFT Workstation



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

CAINE Live



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



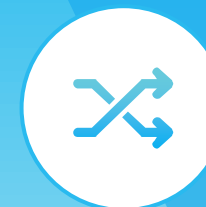
היתרונות של Live USB



חלק חיוני של כל ערכת כלים ל-Forensics.
משמש להשגת מידע ו-Live Forensics.



NirSoft Launcher



NirLauncher - NirSoft Utilities

File Edit View Options Launcher Packages Help

Name	Description	Version	Updated On	Web Page URL
WirelessKeyDump	dumps the list of all wireless keys stored by Wind...		22/12/2019 20:33:00	https://www.nirsoft.net/utis/wireles
Wireless Key View	recovers lost wireless network keys (WEP/WPA) st...	2.10	22/12/2019 20:33:00	https://www.nirsoft.net/utis/wireles
WebBrowserPassView	Recover lost passwords from your Web browser.	1.92	22/12/2019 20:33:00	https://www.nirsoft.net/utis/web_br
VNCPassView	Recover the passwords stored by the VNC tool.	1.05	22/12/2019 20:32:59	https://www.nirsoft.net/utis/vnc_pa
VaultPasswordView	Decrypts passwords stored in Windows Vault	1.08	22/12/2019 20:32:59	https://www.nirsoft.net/utis/vault_p
RunWithoutElevation	RunWithoutElevation	1.00	22/12/2019 20:32:56	https://www.nirsoft.net/utis/run_wit
Remote Desktop PassView	Reveals the password stored by Microsoft Remote...	1.02	22/12/2019 20:32:56	https://www.nirsoft.net/utis/remote
PstPassword	Recover lost password of Outlook PST file.	1.20	22/12/2019 20:32:56	https://www.nirsoft.net/utis/pst_pas
PCAnywhere PassView	Reveals the passwords of pcANYWHERE items.	1.12	22/12/2019 20:32:55	https://www.nirsoft.net/utis/pcanyp
PasswordFox	View passwords stored in Firefox Web browser.	1.60	22/12/2019 20:32:55	https://www.nirsoft.net/utis/passwo
OperaPassView	Password recovery tool for Opera Web browser.	1.10	22/12/2019 20:32:55	https://www.nirsoft.net/utis/opera_p
Network Password Recovery	Recover network passwords on Windows XP/2003...	1.50	22/12/2019 20:32:55	https://www.nirsoft.net/utis/networ
MessenPass	Recovers the passwords of instant messenger pro...	1.43	22/12/2019 20:32:54	https://www.nirsoft.net/utis/mspass
Mail PassView	Recovers email passwords	1.90	22/12/2019 20:32:54	https://www.nirsoft.net/utis/mailpv
LSASecretsDump	Dump the LSA secrets from the Registry.	1.21	22/12/2019 20:32:54	https://www.nirsoft.net/utis/lisa_sec
LSASecretsView	displays the list of all LSA secrets stored in the Re...	1.25	22/12/2019 20:32:54	https://www.nirsoft.net/utis/lisa_sec
IE Pass View	Recover passwords stored by Internet Explorer (Ve...	1.41	22/12/2019 20:32:54	https://www.nirsoft.net/utis/interne
HTTPNetworkSniffer	Captures and displays HTTP requests/responses.	1.63	22/12/2019 20:32:53	
EncryptedRegView	Scans the Registry and decrypts the data encrypt...	1.03	22/12/2019 20:32:51	https://www.nirsoft.net/utis/encrypt
Dialupass	Recovers Dial-Up passwords in all versions of Win...	3.61	22/12/2019 20:32:50	https://www.nirsoft.net/utis/dialupa
DataProtectionDecryptor	Decrypt DPAPI-encrypted data of Windows.	1.10	22/12/2019 20:32:50	https://www.nirsoft.net/utis/dpapi_c
CredentialsFileView	Decrypts Credentials files of Windows.	1.07	22/12/2019 20:32:50	https://www.nirsoft.net/utis/credent
ChromePass	Password recovery tool for Google Chrome Web ...	1.46	22/12/2019 20:32:50	https://www.nirsoft.net/utis/chrome
BulletsPassView	Reveals the passwords stored behind the bullets.	1.32	22/12/2019 20:32:50	https://www.nirsoft.net/utis/bullets

Run Advanced Run Web Page Help File Web Search Package Package

24 Utilities, 1 Selected NirSoft Freeware. <http://www.nirsoft.net>

➤ 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.



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.

קבצים קשורים

- מסמך מעבדה
- CAINE.iso
- SIFT.ova

כלים

- VirtualBox
- USB Drive



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 להכין
מלכודות.

DF נגד הנדסה חברתית



העקבות בדרך כלל יהיו דואר אלקטרוני, הודעות
וקישורים חשודים.
הראיות ייאספו בדרך כלל מהעובדים.



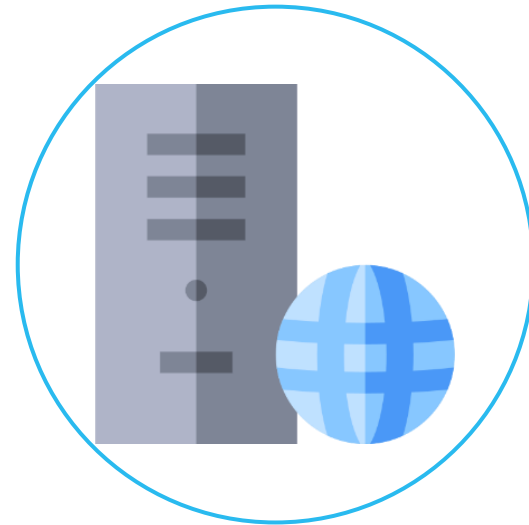
➤ אחרי DF עבור הנדסה חברתית יגיע שלב מציאת האיומים, זאת כדי לברר
אם עובדים אחרים הושפעו גם הם.



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.

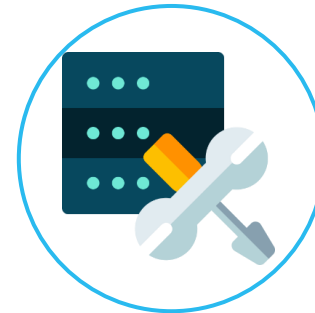
DF נגד השחתת שרת הרשת



איתור חדירה
זיהוי נקודת החדירה.



זיהוי התמדה (persistence)
זהה אם נשארו backdoors.



בקרוב המקרים, פעולות אלו יבוצעו דרך ניתוח היומנים. ➤



IR נגד שתילת סוס טרויאני (Trojan)



התגובה תשתנה בהתאם לאם הסוס הטרויאני כבר בוצע.
אם בוצע – התגובה תתמקד בהכלה ובחיסול.

DF נגד שתילת סוס טרויאני (Trojan)



כולל ניתוח תוכנה זדונית.
חושף את הפעולות שהסוס הטרויאני ביצע
במערכת.



מעבדה 4

בוחר
מתודולוגיית
DFIR



15 – 10 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



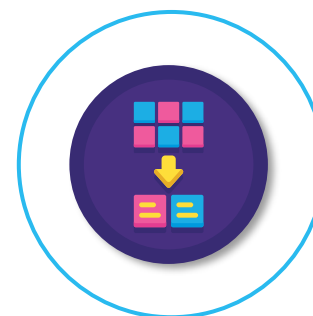
CYBER SCHOOL

שיעור 1

הגדרת נכסים



דבר מה בעל ערך הקשור למטרות הארגון.
יכול להיות מחשב או נתונים.



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



סוגי נכסים



נכסים מוחשיים

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



נכסים לא מוחשיים

קניין רוחני, פטנטים, סימנים מסחריים וכו'.

הנכס החשוב ביותר



העובדים הם הנכס החשוב ביותר בחברה.
כישורי העובדים הם 85% מערכי הנכס בחברה.



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 ככלי או כמדריך עבור אבטחת מערכות מידע.





Confidentiality - סודיות

התחייבות לכך שהגישה לנתונים רגישים היא רק לאנשים מורשים.



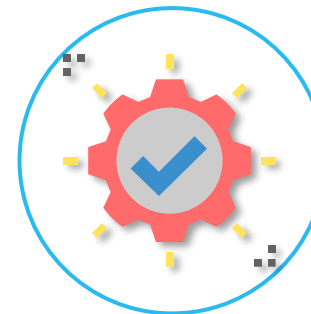
Integrity – שלמות

הוודאות כי הנתונים הם אמינים ומדויקים (לא שונו).



Availability - זמינות

התחייבות לגישה ללא הפסקה לנתונים.



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 ברגיל.



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



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.



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.





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.



מעבדה 5

נכסי רשת



20 – 30 דקות

המשימה

התקן והגדר תוכנת ניהול נכס רשת בסיסית.

השלבים

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

קבצים קשורים

- מסמך מעבדה

כלים

Windows VM



CYBER SCHOOL



CYBER SCHOOL

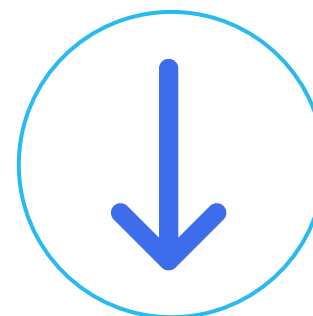
תגובה לאורועים

מרכז מבצע אבטחה (SOC)

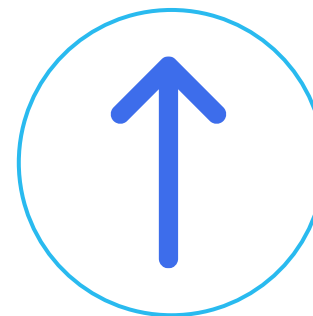
אסטרטגיות ניהול



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



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



אחריות 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



רמה 2



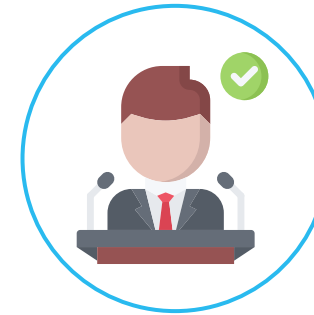
מנהל SOC



רמה 1



רמה 3



CISO



תפקידים נוספים במקרה של פריצה



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



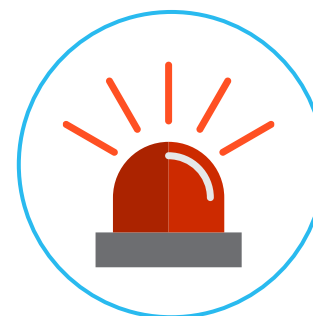
טבלת RACI



Responsible, Accountable, Consulted, Informed
התכלית העיקרית של הטבלה היא ניהול פרויקטים.



משמשת להקצאת תפקידים ואחריות לכל התראת אירוע.



דוגמה ל-RACI



כל אות בראשי התיבות מסמנת רמת אחריות למשימות.

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



מעבדה 6

תרחישי
שלישיית CIA

10 – 15 דקות 



כלים

כתבן

המשימה

הבן את שלישיית CIA דרך תרגול סיטואציות.

השלבים

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

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.

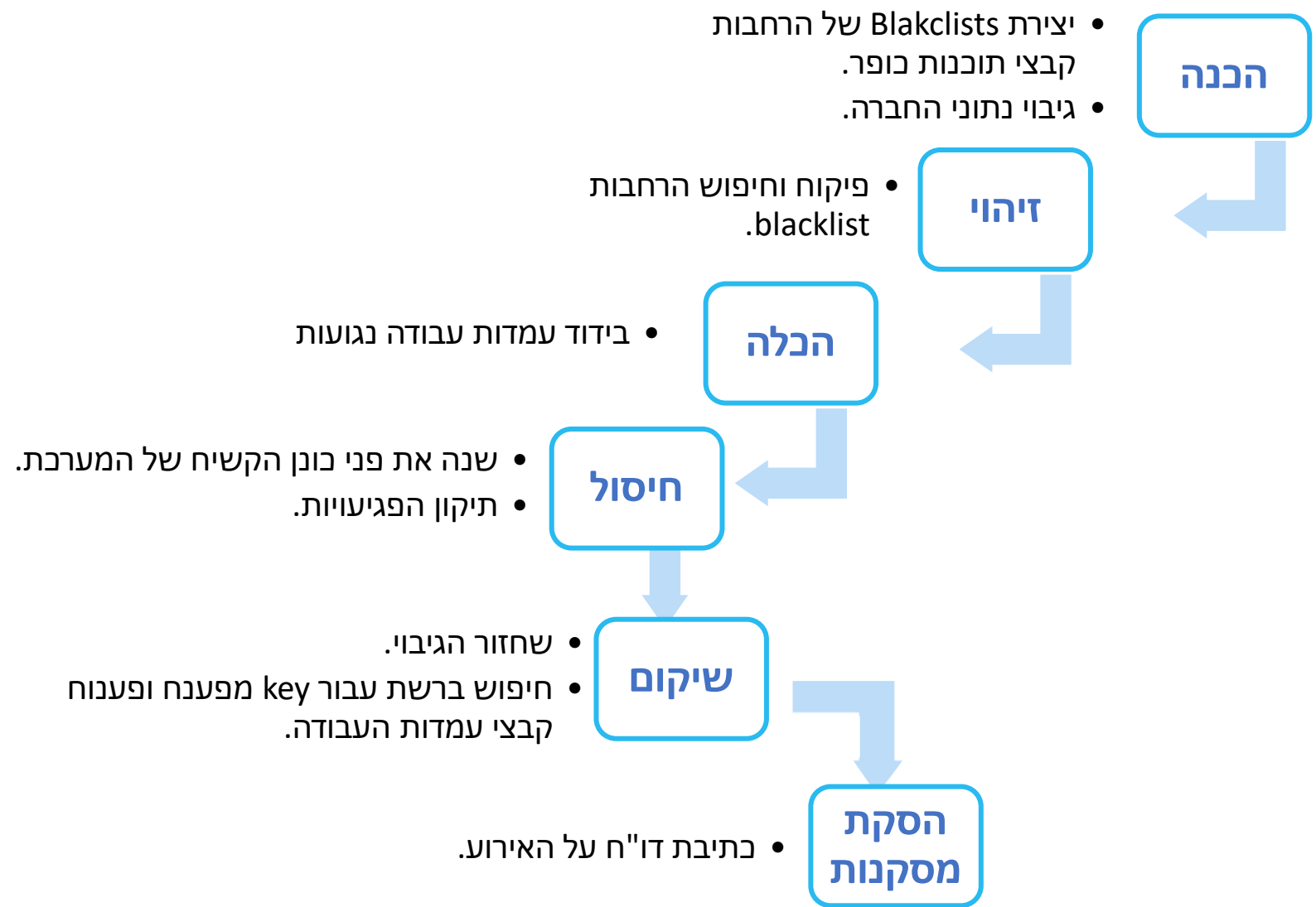
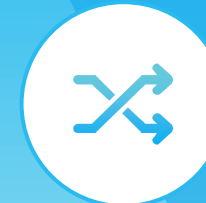


שלבים לתגובה לאירועים של SANS

<ul style="list-style-type: none">• הגדרת אירועי ביטחון קריטיים• ביצוע הערכת סיכונים• זיהוי והגדרת נכסים רגישים.	הכנה
<ul style="list-style-type: none">• פיקוח על מערכות IT ואיתור סטיות מהפעילות הרגילה.	זיהוי
<ul style="list-style-type: none">• הכלה לטווח קצר.• בידוד חלק ברשת.• כיבוי שרתים שנפרצו	הכלה
<ul style="list-style-type: none">• הסרת תוכנה זדונית מהמערכת הנגועה.• זיהוי ותיקון שורש הבעיה.	חיסול
<ul style="list-style-type: none">• החזרת מערכות הייצור הנגועות לפעולה.	שיקום
<ul style="list-style-type: none">• הכנת תיעוד מלא של האירוע.	הסקת מסקנות



Incident Response Plan Ransomware Incident



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.

קבצים קשורים

- מסמך מעבדה

כלים

כתבן



CYBER SCHOOL



CYBER SCHOOL

שיעור 1

הכנה טכנית



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.



חפצים

ב-Jump Kit

1

לפטופ חזק

2

"מסניפוי"
פקטות

3

מברגים, פנסים,
פינצטות וכו'

4

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



חפצים ב-Jump Kit

5

כונן דיסק מדיה ריק

6

כבלי רשת

7

Network hub
or tap

8

מכשירים חוסמים כתיבה
ובוננים קשיחים



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



8

עדכון מתמשך של תכנית
השיקום

7

בדיקה באופן קבוע
של ה-DRP

6

תיעוד כל תהליך השיקום
מהאסון.

5

הגדרת רשימת קריטריונים
לאירוע

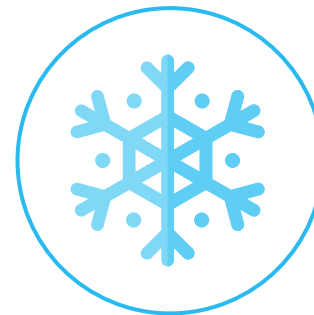




Hot Site הוא אתר גיבוי שפועל כל הזמן ומוכן למעבר נתונים מיידי.



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

שיעור 1

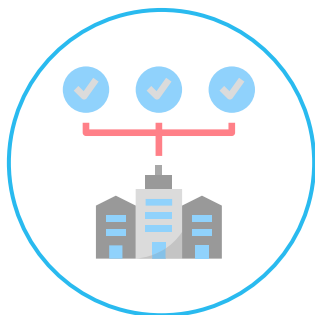
תאימות ל-GRC

נקודת מבט ממשלתית



מדיניות

הצהרות רשמיות שמציגות את העמדה והכיוון של הניהול הבכיר.



תקנים

רמת איכות מקובלת



הליכים

תיאור כל שלב הנדרש לביצוע משימה מסוימת.



הנחיות

המלצות או הצעות שאינן בהכרח בגדר חובה.



תקנים ורגולציות



ISO



HIPAA



GDPR



SOX



PCI DSS



מעבדה 8

יצירת סביבת
מעבדת
Windows

10 דקות 



המשימה

הכן 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?