שם: _____ תאריך: _____ ציון: _____

תוכנות אנטי-וירוס ואבטחת נקודות קצה מדריך הגנה

זיהוי חתימות, היוריסטיקה, ניטור התנהגות, ארגז חול, עדכונים

סקירת לימוד תוכנת אנטי-וירוס

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך תוכנות אנטי-וירוס והגנה על נקודות קצה. תחקרו מסדי נתוני חתימות, סורקים היוריסטיים, ניטור התנהגותי, קובצי ארגז חול וירטואליים והפחתת התראות שווא.

אובטח

הצפנת נתונים

תקן AES של 256 סיביות

תואם

תקנים עולמיים

מסגרות GDPR ו-CCPA

אפס אמון

מדיניות גישה

אימות רב-גורמי

נקודות הביקורת בדף העבודה

- [ ] **חלק 1-4: שלטו באבטחת סייבר ובמניעת איומים.**
- [ ] **חלק 5-7: פתרו תשבצים ופאזלי חיפוש מילים.**
- [ ] **חלק 8-9: פתרו מקרי בוחן ואתגר צופן.**
- [ ] **חלק 10: סקרו את דפי השאלות הנפוצות הבסיסיים והמתקדמים.**
- [ ] **חלק 11: חקרו 10 עובדות מעניינות מהעולם האמיתי.**
- [ ] **בונוס: אתגר חשבו מהר**

פתחו את מדריך אבטחת הסייבר של VPN.com

URL: https://www.vpn.com/cybersecurity/antivirus/

מפת הלמידה שלכם: אסטרטגיית אנטי-וירוס

- הבחינו בין זיהוי נוזקות מבוסס חתימות לזיהוי היוריסטי.
- הבינו פרוטוקולים של ניטור התנהגות ובידוד בארגז חול.
- העריכו את השפעת סריקות בזמן אמת על ביצועי המערכת ונקודות הקצה.
- הפחתת סיווגי שווא חיוביים באמצעות אימות תעודות דיגיטליות.
- ניהול הפצה יומית של עדכוני הגדרות בנקודות הקצה הארגוניות.

הוראות מדריך אנטי-וירוס

ענו על שאלות אמריקאיות ועל שאלות נכון/לא נכון, השלימו את המשפטים החסרים בעזרת בנק המילים, התאימו הגדרות ופתרו את התשבץ ואת תפזורת המילים. יישמו את הידע שלכם בנושא אבטחת אנטי-וירוס לנקודות קצה. ולסיום, פעילות הבונוס "חשבו מהר".

הגנת אנטי-וירוס וסריקת חתימות (מבוא)

תוכנת אנטי-וירוס מגנה על נקודות קצה באמצעות זיהוי נוזקות, הצבתן בהסגר והסרתן. מערכות מודרניות משלבות מאגרי חתימות (התאמה להאשים של איומים מוכרים) עם היוריסטיקה (ניתוח מבנה הקובץ) וניטור התנהגות כדי לזהות ניצולי יום אפס.

קראו כל נקודת ביקורת בעיון ובחרו או כתבו את הנכון

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהי מגבלה של זיהוי מבוסס חתימות?

- A. הוא אינו יכול לזהות נוזקות לא מוכרות או ששונו
- B. הוא מייצר שיעור גבוה של התראות שווא
- C. הוא דורש עוצמת עיבוד גבוהה של המעבד
- D. הוא פועל רק כשמחוברים לאינטרנט

2. כיצד סורקים היוריסטיים מזהים גרסאות חדשות של נוזקות?

- A. על ידי זיהוי דפוסים ומבני קוד חשודים
- B. על ידי התאמת האשים של קבצים למסד נתונים של איומים
- C. על ידי מחיקה אוטומטית של כל קובצי ההרצה ללא חתימה
- D. על ידי העלאת כל קובץ לתיקיית ענן ציבורית

3. מהי מטרת הרצת קובץ בארגז חול באנטי-וירוס?

- A. בידוד וניתוח של קבצים בכספת וירטואלית מאובטחת
- B. האצת העברת הגיבוי של מערכת הקבצים המקומית
- C. עדכון תיקוני האבטחה של מערכת ההפעלה המקומית
- D. דחיסת קובצי מסמכים גדולים כדי לחסוך באחסון

4. איזו שיטת זיהוי מסמנת התנהגות מאיימת בזמן אמת?

- A. ניתוח התנהגותי שמנטר פעולות תוכנה
- B. בדיקת יומנים היסטוריים הנעשית במהלך הלילה
- C. התערבות ידנית של משתמש בדיווח על אפליקציות איטיות
- D. סקירות ידניות שבועיות של תוכנות מותקנות

5. מדוע עדכוני הגדרות סדירים קריטיים לסורקים?

- A. כדי להזין מנועי חתימות במזהי איומים ממסד נתונים
- B. כדי להגביר את מהירויות השעון של המעבד במהלך פעולות
- C. כדי לשנות את זמני השמירה במטמון של שרתי שמות DNS גלובליים
- D. כדי לאשר את הגדרות העוגיות בדפדפן

נקודת ביקורת 2: אתגר נכון או לא נכון

6 שאלה נכון/לא נכון 6

6. זיהוי חתימות משווה גיבובים קריפטוגרפיים של קבצים לרשימות במסד נתונים.

נכון לא נכון

7 שאלה נכון/לא נכון 7

7. סורקים היוריסטיים עלולים להפעיל התראות שווא על קבצים בטוחים.

נכון לא נכון

8 שאלה נכון/לא נכון 8

8. ארגז חול מאפשר לנוזקות לגשת לקבצי רשת ללא הגבלה.

נכון לא נכון

9 שאלה נכון/לא נכון 9

9. סריקה התנהגותית חוסמת קבצים כאשר הם מפגינים פעולות זדוניות.

נכון לא נכון

10 שאלה נכון/לא נכון 10

10. תוכנת אנטי-וירוס סטנדרטית עוצרת לחלוטין את כל מתקפות היום-אפס.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

קראו כל משפט שלהלן והשלימו את החסר במונח הנכון מבנק המילים.

1. סורק מסורתי מזהה נוזקות מוכרות לפי התאמת _____ .
2. ניתוח דפוסי קוד בקבצים מכונה _____ .
3. כלי אנטי-וירוס מבודדים קבצים חשודים בסביבת _____ .
4. ניטור בזמן אמת עוקב אחר _____ של תוכנות כדי לאתר פעילות חשודה.
5. סורקים מורידים מדי יום _____ של מסד הנתונים כדי לזהות איומים חדשים.
6. תוכנות בטוחות שסומנו בטעות כנוזקות מייצרות _____ .

בנק מילים

אזעקת שווא | אנטיוירוס | ארגז חול | היוריסטיקה | התנהגות | חומת אש | חתימות | עדכונים

כתבו את תשובותיכם כאן:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

נקודת ביקורת 4: התאמת מושגים באבטחה

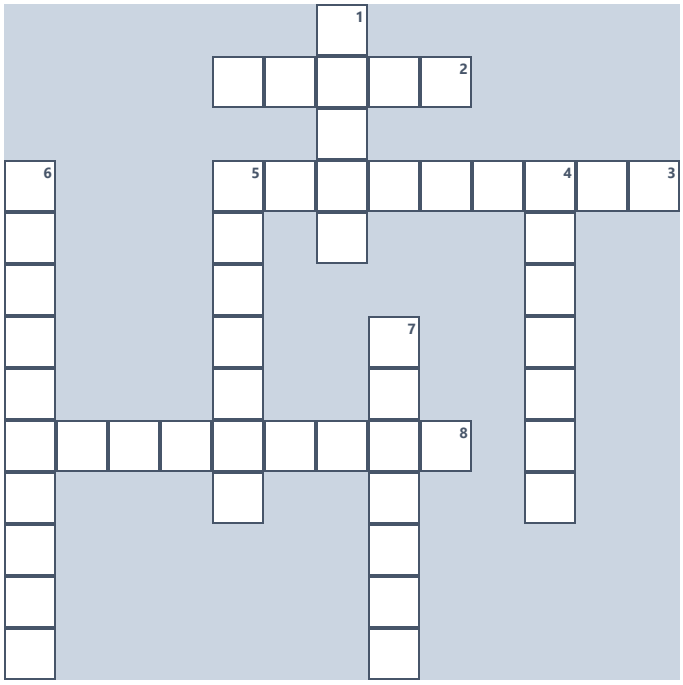
התאמת הגדרות

התאימו כל מונח אוצר מילים בצד ימין להגדרה הנכונה שלו בצד שמאל על ידי כתיבת האות המתאימה (A-H) בתיבת הקלט הניתנת למילוי.

1. חתימת גיבוב	A	הגבלת קבצים חשודים כדי למנוע חשיפה של המערכת המקומית.
2. היוריסטיקות קוד	B	חבילת תוכנה הסורקת ומגנה על נקודות קצה מפני ניצול פרצות.
3. ארגז חול לקבצים	C	ניטור פעולות של תוכנה פועלת לאיתור דפוסי פעולה זדוניים.
4. סריקת התנהגות	D	טביעת אצבע קריפטוגרפית ייחודית במסד נתונים המשמשת לזיהוי איומים ידועים.
5. עדכונים יומיים	E	סביבת בדיקה וירטואלית מאובטחת המריצה קוד לא מהימן בבטחה.
6. חיובי שגוי	F	הורדות עדכוני הגדרות סדירות המזינות את מסד נתוני האיומים.
7. בידוד איומים	G	ניתוח מבוסס כללים שמסמן קבצים עם מבני קוד חשודים.
8. כלי אנטי-וירוס	H	התראת אבטחה המסווגת בטעות תוכנה בטוחה כנוזקה.

נקודת ביקורת 5: תשבץ

פתרו את התשבץ על ידי הקלדת אותיות בתיבות הלבנות הפעילות. המספרים מתאימים לרמזים שלהלן.



מאוזן

2. טביעת אצבע קריפטוגרפית ייחודית במסד נתונים, המשמשת לזיהוי איומים מוכרים (5)

3. התראת אבטחה שמסווגת בטעות תוכנה בטוחה כנוזקה (9)

8. חבילת תוכנה הסורקת ומגנה על תחנות קצה מפני ניצול חולשות (9)

מאונך

1. הגבלת קבצים חשודים כדי למנוע חשיפה של המערכת המקומית (5)

4. הורדות סדירות של הגדרות איומים המזינות את מסד נתוני האיומים (7)

5. סביבת בדיקה וירטואלית מאובטחת המריצה קוד לא מהימן בבטחה (7)

6. ניתוח מבוסס כללים המסמן קבצים בעלי מבנה קוד חשוד (10)

7. ניטור פעולות של תוכנות רצות בחיפוש אחר דפוסי פעולה זדוניים (7)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

משתמשי קורא מסך ומקלדת יכולים להקליד את תשובות התשבץ ישירות בשדות הטקסט שלהלן. רמזים אופקיים רמזים אנכיים

מאוזן

2 מאוזן: טביעת אצבע קריפטוגרפית ייחודית במסד נתונים, המשמשת לזיהוי איומים מוכרים (5 אותיות):

3 מאוזן: התראת אבטחה שמסווגת בטעות תוכנה בטוחה כנוזקה (9 אותיות):

8 מאוזן: חבילת תוכנה הסורקת ומגנה על תחנות קצה מפני ניצול חולשות (9 אותיות):

מאונך

1 מאונך: הגבלת קבצים חשודים כדי למנוע חשיפה של המערכת המקומית (5 אותיות):

4 מאונך: הורדות סדירות של הגדרות איומים המזינות את מסד נתוני האיומים (7 אותיות):

5 מאונך: סביבת בדיקה וירטואלית מאובטחת המריצה קוד לא מהימן בבטחה (7 אותיות):

6 מאונך: ניתוח מבוסס כללים המסמן קבצים בעלי מבנה קוד חשוד (10 אותיות):

7 מאונך: ניטור פעולות של תוכנות רצות בחיפוש אחר דפוסי פעולה זדוניים (7 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

מצאו את 8 מונחי המפתח בלוח שלהלן. מילים יכולות להופיע אופקית, אנכית או באלכסון.

ג	ע	ח	ו	מ	ע	ל	ה	ס	ש	ס	מ	ג	צ	פ
פ	ה	ה	י	ט	ב	א	ת	ב	ג	ע	נ	ת	י	ט
ת	י	מ	ש	צ	י	ד	נ	ס	ל	ד	ט	ד	ח	ל
א	ל	י	י	ס	נ	ז	ה	ל	ל	כ	ס	ע	פ	צ
ו	צ	ת	ו	ב	ה	פ	ג	ס	מ	ו	ח	ע	א	ב
ו	ר	ח	ד	פ	י	ם	ו	ק	ג	נ	ם	ר	נ	ו
ש	י	ז	ם	ד	ו	ל	ת	א	ד	י	ע	ש	ט	נ
ת	ב	ק	ב	א	ר	ם	מ	ר	ד	ם	י	א	י	ד
ק	מ	ד	ה	ז	י	ח	ד	ג	ע	ס	ל	ה	ו	ח
ע	ע	ם	פ	ה	ס	ב	ע	ז	ר	ה	א	א	י	ע
ז	נ	ל	נ	צ	ט	י	ש	ח	ס	ט	ע	צ	ר	פ
א	ג	ל	ת	ב	י	ד	ו	ו	ע	ש	ש	ט	ו	א
ע	ם	ת	ת	כ	ק	ו	ו	ל	ח	ל	ע	ט	ס	כ
כ	צ	נ	ז	ס	ה	ד	ס	ז	ם	א	מ	ק	ו	ק
ב	ת	ע	ת	ב	ז	כ	ם	ו	ט	מ	נ	מ	ש	ג

רשימת מילים

חתימה | היוריסטיקה | ארגזחול | התנהגות אנטיוירוס | עדכונים | אזעקתשווא | בידוד

נקודת ביקורת 6 – פעילות חלופית: התאמת אוצר מילים נגישה

התאימו כל אחד מ-8 מונחי המילון מתפזורת המילים להגדרה הנכונה שלו על ידי כתיבת האות (A-H) במקום הריק.

מונחי אוצר מילים
A. חתימה
B. היוריסטיקה
C. ארגזחול
D. התנהגות
E. עדכונים
F. אזעקתשווא
G. בידוד
H. אנטיוירוס

הגדרות ושדות התאמה	
1. ניטור פעולות של תוכנות רצות בחיפוש אחר דפוסי פעולה זדוניים.	
2. חבילת תוכנה הסורקת ומגנה על תחנות קצה מפני ניצול חולשות.	
3. הורדות סדירות של הגדרות איומים המזינות את מסד נתוני האיומים.	
4. ניתוח מבוסס כללים המסמן קבצים בעלי מבנה קוד חשוד.	
5. הגבלת קבצים חשודים כדי למנוע חשיפה של המערכת המקומית.	
6. טביעת אצבע קריפטוגרפית ייחודית במסד נתונים, המשמשת לזיהוי איומים מוכרים.	
7. סביבת בדיקה וירטואלית מאובטחת המריצה קוד לא מהימן בבטחה.	
8. התראת אבטחה שמסווגת בטעות תוכנה בטוחה כנוזקה.	

נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים באבטחת סייבר. כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. מיחהת
2. אגלוחזר
3. וענמכיד
4. דדובי
5. יסהירטיהקו
6. ונגההתת
7. שאואוקזתע
8. סוואינירט

פעילות בונוס: חשבו מהר

כתבו 3 תשובות לכל קטגוריה. מי שמסיים ראשון את הרשימה מנצח.

1	סיבות לעדכן תוכנה			
2	אנשים שאפשר לבקש מהם עזרה ב-IT			
3	דברים שעושים כשהאנטי-וירוס מוצא משהו			
4	סימנים לווירוס במחשב			
5	דברים שמועברים להסגר			
6	מקומות שבהם וירוסים מתחבאים			
7	מידע שלעולם אסור לשתף			
8	סוגי תוכנות זדוניות			
9	כלי אבטחה שאתם מכירים			
10	דברים שאנטי-וירוס סורק			
11	דברים שמגבים			
12	מכשירים שאפשר לפרוץ אליהם			
13	תוכנות אנטי-וירוס שאתם מכירים			
14	סיבות להתראות שווא			
15	הרגלים בטוחים שאפשר להתחיל כבר היום			

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

יישמו את המושגים שלמדתם כדי לפתור את התרחישים מהעולם האמיתי שלהלן.

מקרה בוחן 1: סריקה מבוססת חתימה לעומת סריקה היוריסטית



תרחיש: עובד מוריד כלי עזר מותאם אישית שנבנה בתוך הארגון על ידי צוות אחר. סורק החתימות מאשר אותו, אך הסורק ההיוריסטי מסמן אותו כחשוד.

שאלה לדיון: הסבירו מדוע זה קרה וכיצד אפשר לוודא אם הקובץ בטוח.

מקרה בוחן 2: טיפול בתוצאות חיוביות שגויות



תרחיש: מפתח תוכנה מהדר את האפליקציה שלו. האנטי-וירוס של המערכת מסמן את קובץ ההרצה החדש כנוזקה ומעביר אותו להסגר.

שאלה לדיון: תארו בקצרה את הסיכונים שבהוספה לרשימה הלבנה, ותארו את דרך הפתרון הנכונה.

נקודת ביקורת 9: פענוח הצופן

איש מקצוע באבטחת סייבר מגן על נכסי רשת מפני גורמי איום מקוונים. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה, וכתבו את האותיות המתאימות במקומות הריקים.

מפתח הצפנה של אות למספר

א=1 ב=2 ג=3 ד=4 ה=5 ו=6 ז=7 ח=8 ט=9

י=10 כ=11 ל=12 מ=13 נ=14 ס=15 ע=16 פ=17 צ=18

ק=19 ר=20 ש=21 ת=22 ך=23 ם=24 ן=25 ף=26 ץ=27

22	6	21	4	8		22	6	19	7	6	14		10	6	5	10	7		
10	9	15	10	20	6	10	5		8	6	22	10	14		22	20	7	16	2

ההודעה המפוענחת:

טיפ: כל מספר מייצג אות עברית אחת מהמפתח שלמעלה.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק A)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q1: כיצד תוכנת אנטי-וירוס מזהה נוזקות?

הוא מזהה נוזקות באמצעות התאמת חתימות במסד נתונים, ניתוח היוריסטי של מבנה הקוד וניטור התנהגותי בזמן אמת.

Q2: מהו זיהוי מבוסס חתימות?

זוהי שיטת סריקה שמתאימה גיבובי קבצים קריפטוגרפיים לרשימות במסד נתונים של איומי נוזקות מוכרים.

Q3: מהו סורק היוריסטי?

היוריסטיקות מנתחות את מבנה הקובץ ואת הוראות הקוד שלו ומסמנות דפוסים חשודים הנפוצים בגרסאות של נוזקות.

Q4: מה המשמעות כשקובץ מועבר להסגר?

האנטי-וירוס מעביר את הקובץ לתיקייה מאובטחת ומבודדת וחוסם את הרצתו כדי להגן על מערכת ההפעלה.

Q5: מהו חיובי שגוי באנטי-וירוס?

זוהי שגיאה שבה תוכנה לגיטימית ובטוחה מסומנת בטעות כנוזקה על ידי אלגוריתמי סריקה.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק B)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: כיצד ניטור התנהגותי מגן על מערכות?

הוא מנטר תוכנה פועלת בזמן אמת וחוסם תהליכים שמנסים שינויים חשודים כמו הזרקת קוד.

Q7: מדוע בדיקות בארגז חול חשובות?

Sandboxing מריץ קבצים לא מהימנים במכונה וירטואלית מבודדת וצופה בפעולות בבטחה בלי חשיפת המערכת.

Q8: באיזו תדירות יש לעדכן הגדרות אנטי-וירוס?

סורקים צריכים לעדכן הגדרות מדי יום או מדי שעה כדי לזהות זני נוזקות שהתגלו לאחרונה.

Q9: מה ההבדל בין אנטי-וירוס ל-EDR?

אנטי-וירוס מתמקד בסריקת קבצים, ואילו Endpoint Detection and Response (EDR) מספק מעקב אחר איומים ובלימתם בכל הרשת.

Q10: האם אפשר להריץ שתי תוכנות אנטי-וירוס יחד?

לא. הרצת שני סורקים פעילים גורמת להתנגשויות במערכת, מאטה ביצועים ועלולה לחסום את פעולות זה של זה.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק C)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q1: כיצד כללים היוריסטיים ממזערים עקיפת איומים?

היוריסטיקות מנתחות דפוסי איום כלליים ולא חתימות ספציפיות, ולכן תופסות גרסאות ששונו של משפחות נוזקות מוכרות.

Q2: מהו וירוס פולימורפי?

זוהי נוזקה שמשנה את מבנה הקובץ ואת שגרת הפענוח שלה בכל הרצה, מה שהופך סריקות חתימה ללא יעילות.

Q3: כיצד ארגזי חול (sandboxes) מזהים התחמקות באמצעות מכונה וירטואלית?

ארגזי חול מודרניים מדמים לחיצות עכבר וזמן פעילות של המערכת, ומטעים נוזקות שתוכננו להסתתר כשהן רצות במכונות וירטואליות.

Q4: מהם פורמטי ההורדה של עדכוני חתימות?

עדכונים הם בדרך כלל קובצי הפרשים בינאריים מצטברים קלים, שממזערים את צריכת רוחב הפס של רשת הלקוח.

Q5: כיצד סוכני נקודות קצה מנהלים סריקות מקומיות?

סוכנים מבצעים בדיקות קלות ברקע, ומעבירים חיפושי גיבוב קריפטוגרפיים עמוקים למסדי נתוני איומים בענן.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק D)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q6: מהי סריקת זיהוי rootkit?

הוא סורק טבלאות זיכרון ברמת הגרעין ועוקף ממשקי API של מערכת ההפעלה ש-rootkits תופסים כדי להסתיר את התהליכונים הפעילים שלהם.

Q7: כיצד סריקת התנהגות חוסמת תוכנות כופר?

הוא מזהה לולאות הצפנה המונית אוטומטית של קבצים ומסיים את תהליך המארח לפני שמסדי נתוני המערכת ננעלים.

Q8: מהו אימות אישור חתימת קוד?

סורקים בודקים חתימות דיגיטליות של קוד מול רשויות אישורים ראשיות מהימנות ומאמתים את זהות מפתח התוכנה.

Q9: כיצד packers משפיעים על מנועי סריקה?

מדחסים (Packers) דוחסים או מצפינים מטעני נוזקה. סורקים חייבים לפרוק את הקובץ בזיכרון לפני שמתבצעות התאמות חתימה.

Q10: כיצד כלי EDR מבצעים בידוד אוטומטי?

סוכני EDR מבודדים בהסגר נקודות קצה שנפרצו ברמת הרשת, וחוסמים תנועה לרוחב תוך מתן גישה לאנליסטים.

חלק 11: 10 עובדות ותובנות מהעולם האמיתי על אבטחת סייבר

עיינו בעובדות מהעולם האמיתי על פריצות אבטחה, מנגנוני הגנה ותקני ציות.

1. תובנות על אבטחה

מסדי נתוני חתימות שומרים גיבובים של נוזקות ידועות, ולכן קבצים חדשים או ששונו אינם מזוהים עד לעדכון ההגדרות.

2. תובנות על אבטחה

מנועים היוריסטיים יכולים לסמן חלק מגרסאות הנוזקה החדשות עוד לפני שקיימות חתימות, במחיר של יותר התראות שווא.

3. תובנות על אבטחה

התראות שווא עולות לצוותי IT בזמן שמושקע באימות ושחזור קבצים שהוסגרו בטעות.

4. תובנות על אבטחה

נוזקה פולימורפית משנה את הקוד שלה בכל עותק, ולכן מגינים משלבים חתימות עם בדיקות היוריסטיות והתנהגותיות.

5. תובנות על אבטחה

מנועי אנטי-וירוס מבוססי ענן בודקים גיבובי קבצים חשודים מול מסדי נתונים גדולים של איומים ברשת כמעט בזמן אמת.

6. תובנות על אבטחה

מפתחי נוזקות כותבים קוד מותאם אישית שבודק סביבות ארגז חול ומעכב את ההרצה כדי לעקוף טיימרים.

7. תובנה על אבטחה

ספקים דוחפים לנקודות הקצה עדכוני הגדרות באופן קבוע כדי שסורקים יוכלו לזהות איומים חדשים שאושרו.

8. תובנה על אבטחה

מנטרי התנהגות של תוכנת כופר מתמקדים בקריאות Win32 API ספציפיות הקשורות להצפנת קבצים ולמחיקת עותקי צל.

9. תובנה על אבטחה

חתימות קוד תקפות יכולות להפחית את הסיכון להתראות שווא, אך קבצים חתומים עדיין נסרקים, שכן גם נוזקה יכולה להיות חתומה.

10. תובנות על אבטחה

רוטקיטים משנים מבני קרנל של המערכת, ולכן נדרשים סורקי זמן-אתחול (boot-time) ייעודיים כדי לזהות ולנקות אותם.

מקורות והפניות טכניים

מדריך הלימוד והפאזלים האינטראקטיביים נערכו על סמך תקנים גלובליים של NIST, OWASP ותאימות לפרטיות נתונים. מקורות אקדמיים ותעשייתיים

מקורות אקדמיים ותעשייתיים

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.

https://csrc.nist.gov/pubs/sp/800/61/r3/final

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 **שאלה 1** חתימות **תשובה נכונה: A**

הערה למורה

סריקת חתימות מסתמכת על גיבובים ידועים במסד נתונים, ולכן אינה מצליחה לזהות נוזקות לא מוכרות או ששונו. מקור: OWASP Secure Configuration.

2 **שאלה 2** היוריסטיקות **תשובה נכונה: A**

הערה למורה

שיטות היוריסטיות מנתחות את מבנה הקוד והפקודות כדי לזהות מאפיינים חשודים של גרסאות חדשות של איומים. מקור: Center for Internet Security (CIS).

3 **שאלה 3** בידוד בארגז חול **תשובה נכונה: A**

הערה למורה

ארגז חול מריץ קבצים חשודים במכונה וירטואלית מבודדת כדי לצפות בבטחה בהתנהגות ההרצה. מקור: NIST Digital Identity.

4 **שאלה 4** התנהגותי **תשובה נכונה: A**

הערה למורה

סריקת התנהגות מנטרת תוכנות פועלות בזמן אמת כדי לחסום שינויי מערכת לא מורשים. מקור: Center for Internet Security (CIS).

5 **שאלה 5** עדכונים **תשובה נכונה: A**

הערה למורה

סורקים מורידים מדי יום עדכוני הגדרות מצטברים כדי להישאר מסונכרנים עם נוף האיומים. מקור: OWASP Secure Configuration.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **שאלה 6** — חתימות — **תשובה נכונה: נכון**

הערה למורה

תשובה נכונה: נכון כלי חתימות מחשבים גיבובים קריפטוגרפיים ומתאימים אותם למסד נתונים של גיבובי איומים ידועים. מקור: OWASP Secure Configuration.

7 **שאלה 7** — היוריסטיקות — **תשובה נכונה: נכון**

הערה למורה

תשובה נכונה: נכון מנועים היוריסטיים מריצים פריסות מבוססות כללים שעלולות לסמן קבצים לגיטימיים ובטוחים כחשודים. מקור: Center for Internet Security (CIS).

8 **שאלה 8** — בידוד בארגז חול — **תשובה נכונה: לא נכון**

הערה למורה

תשובה נכונה: לא נכון ארגז חול מריץ קוד במכולה וירטואלית וחוסם בהחלט גישה לשיתופי רשת. מקור: NIST Digital Identity.

9 **שאלה 9** — התנהגותי — **תשובה נכונה: נכון**

הערה למורה

תשובה נכונה: נכון ניטור בזמן אמת מסמן תהליכים פועלים שמנסים כתיבות אסורות או נעילת קבצים. מקור: Center for Internet Security (CIS).

10 **שאלה 10** — **תשובה נכונה: לא נכון**

הערה למורה

תשובה נכונה: לא נכון. אף אנטי-וירוס אינו עוצר כל התקפת zero-day; איומים לא מוכרים יכולים להתחמק מחתימות ומהיוריסטיקה.

מפתחות אוצר מילים ומחוון הערכה

מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 6 נקודות).

נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

D 1. חתימת גיבוב	G 2. היוריסטיקות קוד	E 3. ארגז חול לקבצים	C 4. סריקת התנהגות
F 5. עדכונים יומיים	H 6. חיובי שגוי	A 7. בידוד איומים	B 8. כלי אנטי-וירוס

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 חתימות	2 היוריסטיקה	3 ארגז חול	4 התנהגות
5 עדכונים	6 אזעקת שווא		

נקודת ביקורת 6 – פעילות חלופית: מפתח תשובות – התאמת אוצר מילים

1 D – התנהגות	2 H – אנטיוירוס	3 E – עדכונים	4 B – היוריסטיקה
5 G – בידוד	6 A – חתימה	7 C – ארגזחול	8 F – אזעקתשווא

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את חתימת גיבוב, היוריסטיקות קוד ו-ארגז חול לקבצים ונותנים דוגמה לכל אחד מהם.

מקרי בוחן:
בקשו מהתלמידים לבסס את ההמלצות שלהם על עובדות מדף העבודה ולא על דעות.

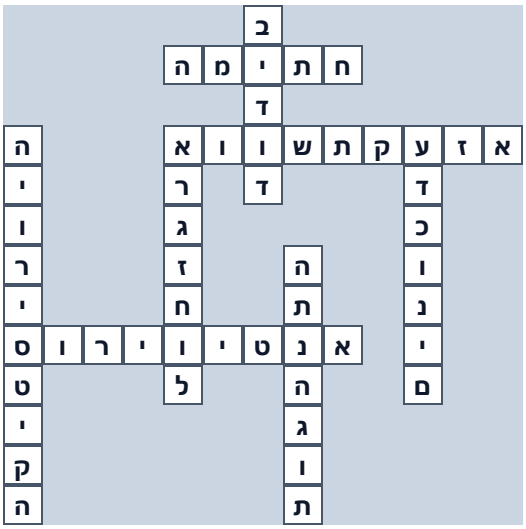
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

ג	ע	ח	ו	מ	ע	ל	ה	ס	ש	ס	מ	ג	צ	פ					
פ	ה	ה	י	ט	ב	א	ת	ב	ג	ע	נ	ת	י	ט					
ת	י	מ	ש	צ	י	ד	נ	ס	ל	ד	ט	ד	ח	ל					
א	ל	י	י	ס	נ	ז	ה	ל	ל	כ	ס	ע	פ	צ					
ו	צ	ת	ו	ב	ה	פ	ג	ס	מ	ו	ח	ע	א	ב					
ו	ר	ח	ד	פ	י	ם	ו	ק	ג	נ	ם	ר	נ	ו					
ש	י	ז	ם	ד	ו	ל	ת	א	ד	י	ע	ש	ט	נ					
ת	ב	ק	ב	א	ר	ם	מ	ר	ד	ם	י	א	י	ד					
ק	מ	ד	ה	ז	י	ח	ד	ג	ע	ס	ל	ה	ו	ח					
ע	ע	ם	פ	ה	ס	ב	ע	ז	ר	ה	א	א	י	ע					
ד	נ	ל	נ	צ	ט	י	ש	ח	ס	ט	ע	צ	ר	פ					
א	ג	ל	ת	ב	י	ד	ו	ו	ע	ש	ש	ט	ו	א					
ע	ם	ת	ת	כ	ק	ו	ל	ו	ח	ל	ע	ט	ס	כ					
כ	צ	נ	ז	ס	ה	ד	ז	ס	ם	א	מ	ק	ו	ק					
ב	ת	ע	ת	ב	ז	כ	ם	ו	ט	מ	נ	מ	ש	ג					

פתרון תשבץ



מאוזן

2 מאוזן: חתימה טביעת אצבע קריפטוגרפית ייחודית במסד נתונים, המשמשת לזיהוי איומים מוכרים (5 אותיות)

3 מאוזן: אזעקתשווא התראת אבטחה שמסווגת בטעות תוכנה בטוחה כנוזקה (9 אותיות)

8 מאוזן: אנטיוירוס חבילת תוכנה הסורקת ומגנה על תחנות קצה מפני ניצול חולשות (9 אותיות)

מאונך

1 מאונך: בידוד הגבלת קבצים חשודים כדי למנוע חשיפה של המערכת המקומית (5 אותיות)

4 מאונך: עדכונים הורדות סדירות של הגדרות איומים המזינות את מסד נתוני האיומים (7 אותיות)

5 מאונך: ארגזחול סביבת בדיקה וירטואלית מאובטחת המריצה קוד לא מהימן בבטחה (7 אותיות)

6 מאונך: היוריסטיקה ניתוח מבוסס כללים המסמן קבצים בעלי מבנה קוד חשוד (10 אותיות)

7 מאונך: התנהגות ניטור פעולות של תוכנות רצות בחיפוש אחר דפוסי פעולה זדוניים (7 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. מיחהת — חתימה
2. אגלוחזר — ארגזחול
3. וענסכיד — עדכונים
4. דדובי — בידוד
5. יסהירטיהקו — היוריסטיקה
6. ונגההתת — התנהגות
7. שאואוקזתע — אזעקתשווא
8. סוואינירט — אנטיוירוס

מפתח אתגר הצופן הסודי

"זיהוי נוזקות חדשות בעזרת ניתוח היוריסטי"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: סריקה מבוססת חתימה לעומת סריקה היוריסטית

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: עובד מוריד כלי מותאם שנבנה פנימית על ידי צוות אחר. סורק החתימות מאשר אותו, אך הסורק ההיוריסטי מסמן אותו כחשוד.
- אסטרטגיה ופתרון מומלצים: למה זה קרה: סריקת חתימות בודקת גיבובי קבצים; מאחר שהוא מותאם אישית, הוא אינו נמצא במסד נתוני האיומים. היוריסטיקות מנתחות מבנה וסימנו פעולות חשודות (למשל כתיבות ל-Registry). אימות: הריצו את הקובץ ב-sandbox כדי לצפות בפעולות, בדקו חתימות דיגיטליות ושלחו את הגיבוב לפורטלי מודיעין איומים.

B מקרה בוחן 2: טיפול בתוצאות חיוביות שגויות

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: מפתח תוכנה מקמפל את היישום שלו. האנטי-וירוס של המערכת מסמן את קובץ ההפעלה החדש כנוזקה ומעביר אותו להסגר.
- אסטרטגיה ופתרון מומלצים: סיכוני רשימה לבנה: עקיפת סורקים עלולה לאפשר הרצה של קוד נגוע אמיתי. נתיב פתרון: שלחו את הקובץ לספק האנטי-וירוס לניתוח, חתמו דיגיטלית על הקוד באמצעות רשויות אישורים, והגדירו זמנית חריגים לתיקיות ספציפיות במקום לכבות את האנטי-וירוס.