שם: _____ תאריך: _____ ציון: _____

# ארכיטקטורת Zero Trust ואבטחה

אימות רציף, חלוקת רשת למקטעים קטנים, ניהול זהויות וגישה, הרשאות מינימליות ובדיקות מצב אבטחה.

## סקירת למידה: אבטחת Zero Trust

### אובטח

**הצפנת נתונים**

תקן AES של 256 סיביות

### תואם

**תקנים עולמיים**

מסגרות GDPR ו-CCPA

### אפס אמון

**מדיניות גישה**

אימות רב-גורמי

**ברוכים הבאים!** חוברת הפעילויות הזו תדריך אתכם דרך ארכיטקטורת Zero Trust ואבטחה. תחקרו אימות מתמשך, מיקרו-פילוח רשת, ניהול זהויות וגישה (IAM), הרשאות מינימליות וביקורת הפעלות.

**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/zero-trust-cyber-security/

# מפת הלמידה שלכם: אסטרטגיית Zero Trust

- הבינו את העיקרון המרכזי של אימות מתמשך.
- יישמו מיקרו-סגמנטציה של הרשת וגישה בהרשאות מינימליות.
- הגדירו בדיקות מצב אבטחה של מכשירים וביקורת על הפעלות פעילות.

### הוראות מדריך אבטחת Zero Trust

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 ארכיטקטורת Zero Trust. ולסיום, פעילות הבונוס "חשבו מהר".

### ארכיטקטורת Zero Trust ואבטחה (מבוא)

אבטחת Zero Trust מחליפה מודלים ישנים של היקף רשת במדיניות קפדנית של 'לעולם אל תסמוך, תמיד אמת'. יישום מיקרו-סגמנטציה, ניהול זהויות והרשאות (IAM), הרשאות מינימום ובדיקות מצב חוסם תנועה רוחבית של איומים.

**קראו כל נקודת ביקורת בעיון ובחרו או כתבו את התגובה הנכונה.**

# נקודת ביקורת 1: אתגר שאלות אמריקאיות

**1** 1. מהו העיקרון המרכזי של אבטחת Zero Trust?

- A. לא לסמוך אף פעם, לאמת תמיד כל בקשת גישה בלי קשר למקור
- B. ההנחה שכל התעבורה בתוך חומת האש הארגונית בטוחה
- C. אחסון קבצי מסד נתונים ללא הצפנה כדי לשפר מהירות
- D. אכיפת אימות דוא"ל באמצעות רשומות SPF בלבד

**2** 2. מהי מיקרו-סגמנטציה של רשת?

- A. פיצול רשתות לאזורים קטנים ומבודדים כדי להכיל תנועה לרוחב
- B. הצפנת כרטיסי רשת בזמן העברת נתונים
- C. חיבור כל השרתים המקומיים לכתובת IP ציבורית אחת
- D. ניטור הקשות מקלדת של משתמשים בהפעלות דפדפן

**3** 3. מהו עיקרון ההרשאה המינימלית?

- A. הגבלת הרשאות הגישה של משתמשים למה שנחוץ לתפקידם בלבד
- B. מתן כל הרשאות המערכת לכל משתמש כברירת מחדל
- C. מתן אפשרות להתחברויות אנונימיות לשרתי מסדי נתונים ארגוניים
- D. הגדרת נתבי Wi-Fi ציבוריים ללא סיסמאות

**4** 4. מהו ניהול זהויות וגישה (IAM)?

- A. מסגרות שמנהלות זהויות דיגיטליות ושולטות בהרשאות מערכת
- B. כלי אנטי-וירוס הסורקים ספריות קבצים מקומיות
- C. מערכת אחסון גיבוי המשתמשת במדיה מנותקת מהרשת (air-gapped)
- D. פרוטוקול שער דוא"ל הדוחה דומיינים מזויפים

**5** 5. מה משמעות אימות רציף?

- A. אימות חוזר ונשנה של זהות המשתמש ומצב המכשיר במהלך הפעלה פעילה
- B. החלפת סיסמת המאסטר כל 10 דקות
- C. גיבוב רשומות של מסד נתונים באמצעות כמה אלגוריתמים
- D. הצפנת חבילות רשת במעבר באמצעות מפתחות TLS

# נקודת ביקורת 2: אתגר נכון או לא נכון

**שאלה 6**

6. Zero Trust מניח שכל התעבורה בתוך חומת האש הארגונית בטוחה.

נכון  לא נכון

**שאלה 7**

7. מיקרו-סגמנטציה מגבילה את יכולת התוקפים לנוע לרוחב השרתים הפנימיים.

נכון  לא נכון

**שאלה 8**

8. עיקרון ההרשאות המינימליות מעניק כברירת מחדל גישה לכל קובצי מסד הנתונים.

נכון  לא נכון

**שאלה 9**

9. אימות רציף בודק את תקינות המכשיר ואת אישורי הגישה לאורך כל הפעלת כניסה.

נכון  לא נכון

**שאלה 10**

10. הטמעת Zero Trust מצמצמת את ההשפעה של פרטי התחברות ארגוניים שנפרצו.

נכון  לא נכון

# נקודת ביקורת 3: השלמת מונחי מפתח

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

1. דרישת אישורים בכל נקודת גישה היא _____ רציף.
2. חלוקת הרשת הארגונית לאזורים זעירים היא מיקרו- _____ .
3. הגדרת זהויות דיגיטליות ובקרת גישה נעשית במערכת _____ .
4. הגבלת הרשאות משתמשים נשענת על העיקרון של _____ מינימלית.
5. הערכת בריאות המכשירים המחוברים סורקת את _____ המכשיר.
6. תיעוד וסקירה של פעילים הם _____ אבטחה.

**בנק מילים**

אימות | ביקורת | הרשאה | חומת אש | נתב | פילוח | תקינות | IAM

**כתבו את תשובותיכם כאן:**

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

# נקודת ביקורת 4: התאמת מושגים באבטחה

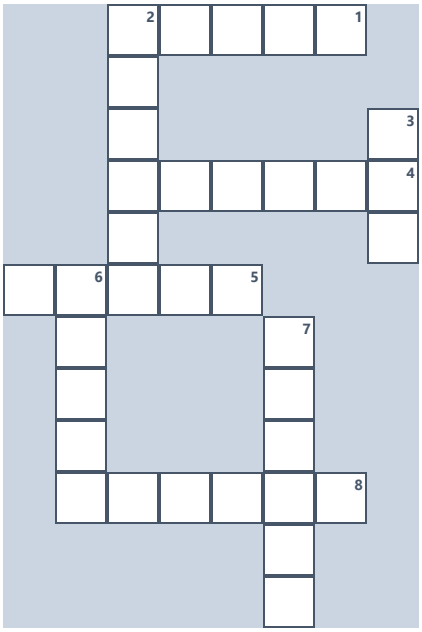
### התאמת הגדרות

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

| | | |
|---|---|---|
| 1. אימות | A | ניהול הגישה לפרטי הזדהות של משתמשים. |
| 2. פילוח | B | עיקרון הרשאות הגישה המינימליות. |
| 3. IAM | C | ניתוב תעבורת חבילות רשת. |
| 4. הרשאה | D | הגנת מחסום רשת חיצוני. |
| 5. מצב אבטחה | E | בדיקת הפעלות גישה שנרשמו ביומן. |
| 6. ביקורת | F | חלוקת אזורי הרשת הפנימית. |
| 7. חומת אש | G | בדיקה תמידית של אישורי משתמשים. |
| 8. נתב | H | הערכת מצב תקינות המכשיר. |

# נקודת ביקורת 5: תשבץ

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




## מאוזן

**1. חלוקת אזורי הרשת הפנימית (5)**

**4. הערכת מצב בריאות המכשיר (6)**

**5. עקרון זכויות הגישה המצומצמות ביותר (5)**

**8. סקירת סשני גישה שתועדו (6)**

## מאונך

**2. הגנת מחסום לרשת חיצונית (6)**

**3. ניתוב תעבורת מנות ברשת (3)**

**6. בדיקה מתמדת של אישורי המשתמש (5)**

**7. ניהול גישה לאישורי משתמשים (6)**

# נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

## מאוזן

**1 מאוזן: חלוקת אזורי הרשת הפנימית (5 אותיות):**

**4 מאוזן: הערכת מצב בריאות המכשיר (6 אותיות):**

**5 מאוזן: עקרון זכויות הגישה המצומצמות ביותר (5 אותיות):**

**8 מאוזן: סקירת סשני גישה שתועדו (6 אותיות):**

## מאונך

**2 מאונך: הגנת מחסום לרשת חיצונית (6 אותיות):**

**3 מאונך: ניתוב תעבורת מנות ברשת (3 אותיות):**

**6 מאונך: בדיקה מתמדת של אישורי המשתמש (5 אותיות):**

**7 מאונך: ניהול גישה לאישורי משתמשים (6 אותיות):**

# נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

**רשימת מילים**

אימות | פילוח | זהויות | הרשאה | תקינות | ביקורת | חומתאש | נתב

# 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 | הגדרות ושדות התאמה |
|---|---|
| **A. אימות** | 1. הגנת מחסום לרשת חיצונית. |
| **B. פילוח** | 2. סקירת ששני גישה שתועדו. |
| **C. זהויות** | 3. עקרון זכויות הגישה המצומצמות ביותר. |
| **D. הרשאה** | 4. חלוקת אזורי הרשת הפנימית. |
| **E. תקינות** | 5. ניתוב תעבורת מנות ברשת. |
| **F. ביקורת** | 6. הערכת מצב בריאות המכשיר. |
| **G. חומתאש** | 7. ניהול גישה לאישורי משתמשים. |
| **H. נתב** | 8. בדיקה מתמדת של אישורי המשתמש. |

## 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. ומאתי
2. תזוויה
3. תינתוק
4. שתמאחו
5. לחפוי
6. אהשהר
7. רבותקי
8. בתנ

# פעילות בונוס: חשבו מהר

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

| | | | |
|---|---|---|---|
| 1 | מידע שלעולם אסור לשתף | | |
| 2 | הרגלים בטוחים שאפשר להתחיל כבר היום | | |
| 3 | דברים שנבדקים במכשיר | | |
| 4 | דברים שנרשמים ביומן | | |
| 5 | מילים הקשורות לאבטחת סייבר | | |
| 6 | דברים ש-Zero Trust בודק | | |
| 7 | מקומות שבהם מציגים תעודה מזהה בחיי היום-יום | | |
| 8 | דרכים להוכיח שזה באמת אתם | | |
| 9 | דברים שעושים אחרי דליפת נתונים | | |
| 10 | סימנים לכך שמחשב נדבק | | |
| 11 | סיבות לעדכן תוכנה | | |
| 12 | רמות גישה בחברה | | |
| 13 | כלי אבטחה שאתם מכירים | | |
| 14 | אזורים שאפשר לפצל אליהם רשת | | |
| 15 | אמרות על אמון | | |

# נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

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

### מקרה בוחן 1: מעבר לארכיטקטורת רשת Zero Trust

👷

**תרחיש:** ארגון גדול משתמש כיום ברשת פנימית שטוחה שבה כל מכשיר ברשת המקומית יכול לגשת לכל השרתים ומסדי הנתונים של החברה.

**שאלה לדיון:** תכננו אסטרטגיית מיקרו-סגמנטציה של הרשת כדי להגביל תנועה רוחבית.

### מקרה בוחן 2: הטמעת בקרות גישה לפי עיקרון ההרשאות המינימליות

👷

**תרחיש:** יומני ביקורת חושפים שמשתמשי מסד נתונים זמניים ועובדים בדרג נמוך מחזיקים בהרשאות קריאה וכתיבה גלובליות למסדי נתונים חשבונאיים קריטיים.

**שאלה לדיון:** בצעו ביקורת והגבילו את הרשאות ה-IAM של מסד הנתונים כדי לאכוף עיקרון של הרשאות מינימליות.

# 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 | 20 | 6 | 9 | 19 | 9 | 10 | 11 | 20 | 1 | 2 | | 4 | 10 | 13 | 22 | | 6 | 22 | 13 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | |
| 22 | 8 | 9 | 2 | 6 | 1 | 13 | | 25 | 6 | 13 | 1 | | 15 | 17 | 1 | | | | | |
| | | | | | | | | | | | | | | | | | | | | |

**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: מהו Zero Trust?**

Zero Trust הוא מסגרת אבטחה המניחה שאיומים קיימים גם מחוץ לגבול הרשת וגם בתוכו, ודורשת אימות לכל בקשה. [1]

**Q2: מהו הכלל המרכזי של Zero Trust?**

לעולם אל תבטחו, תמיד אמתו.

**Q3: מהי מיקרו-סגמנטציה?**

חלוקת רשת למקטעים לוגיים קטנים ומאובטחים כדי לשלוט בתעבורה ולבלום פריצות.

**Q4: מהו עקרון ההרשאה המינימלית (least privilege)?**

מתן הרשאות גישה מינימליות בלבד למשתמשים, כפי שנדרש לביצוע משימות העבודה הספציפיות שלהם. [2]

**Q5: מה פירוש IAM?**

ניהול זהויות והרשאות.

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

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

### Q6: כיצד בדיקת מצב מכשיר עוזרת?

הוא מוודא שהמכשיר מעודכן, מריץ אנטי-וירוס פעיל ומאובטח לפני שהוא מאפשר גישה.

### Q7: מהי תנועה רוחבית (lateral movement)?

התהליך שבו תוקפים נעים ברשת מצומת פרוץ ראשוני אל מערכות בעלות ערך גבוה יותר.

### Q8: האם Zero Trust מחליף חומות אש?

לא, הוא משפר אותם על ידי הוספת בדיקות ממוקדות זהות וחומות אש לפילוח פנימי.

### Q9: מהו אימות מתמשך?

אימות מתמשך של זהות המשתמש לאורך כל הפעלת התחברות פעילה, ולא רק בכניסה הראשונית.

### Q10: מדוע רשת שטוחה מסוכנת?

ברשתות שטוחות, צומת אחד שנפרץ מאפשר לתוקפים לגשת בקלות לכל מסד נתונים ברשת.

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

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

**Q1: כיצד Zero Trust מתמודד עם מודל ההיקף?**

הוא מחליף את מודל ה'טירה והחפיר' המיושן ומעביר את ההגנה מרשתות הגבול לזהויות ולמשאבים ספציפיים.

**Q2: מהי נקודת החלטת מדיניות (PDP)?**

רכיב המערכת שמעריך בקשות הרשאה מול כללי אבטחה כדי להחליט אם להעניק גישה.

**Q3: מהי נקודת אכיפת מדיניות (PEP)?**

צומת המערכת (כמו שער או פרוקסי) שמתיר או חוסם פיזית בקשות חיבור בהתאם להחלטת ה-PDP.

**Q4: כיצד בקרת גישה מבוססת תפקידים (RBAC) תומכת ב-Zero Trust?**

RBAC מקבץ הרשאות לתפקידים מוגדרים, ועוזר למנוע ממשתמשים לרשת הרשאות ניהול מופרזות.

**Q5: מהי בקרת גישה הקשרית?**

הערכת בקשות כניסה באמצעות רמזים משניים כמו מיקום גאוגרפי, מצב המכשיר וזמן הכניסה כדי להעריך סיכון.

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

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

**Q6: במה מיקרו-סגמנטציה שונה מ-VLAN רגילים?**

VLAN מפצלים רשתות למקטעים לוגיים רחבים בשכבה 2, ואילו מיקרו-פילוח משתמש במדיניות תוכנה כדי לבודד עומסי עבודה בודדים.

**Q7: מהי גישה בזמן אמת (JIT)?**

מתן הרשאות ניהול מוגברות באופן זמני וביטולן האוטומטי עם סיום המשימה.

**Q8: כיצד מאבטחים ממשקי API במסגרת Zero Trust?**

על ידי דרישת אסימוני OAuth החתומים קריפטוגרפית וביקורת חתימות הבקשות בכל שער API.

**Q9: מהו לקוח גישת רשת Zero Trust (ZTNA)?**

סוכן תוכנה שמקים חיבורים יוצאים מאובטחים ומוצפנים ליישומים ספציפיים ולא לתת-רשתות גולמיות.

**Q10: כיצד ביקורת לוגים מסייעת ל-Zero Trust?**

רישום רציף מאפשר לכלי ניתוח אבטחה אוטומטיים לזהות חריגות ולהשהות מיד כניסות זדוניות.

# 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

ארכיטקטורות Zero Trust מחליפות את מודל המצודה והחפיר הישן בכללי אימות מבוססי זהות.

### 2. תובנות על אבטחה

מיקרו-פילוח רשת מצמצם את האזור שנוזקה יכולה להגיע אליו על ידי בידוד עומסי עבודה לאזורים קטנים מוגנים.

### 3. תובנות על אבטחה

Zero Trust מתמקד בהגנה על משאבים כמו נכסים, שירותים וחשבונות ולא על מקטעי רשת. [1]

### 4. תובנות על אבטחה

מדיניות גישה במינימום הרשאות מפחיתה את הסיכון להברחת נתונים ממסדי הנתונים המרכזיים בידי גורם פנימי.

### 5. תובנות על אבטחה

אימות מצב מכשיר בודק בזמן אמת את רמות העדכון של מערכת ההפעלה ואת מצב האנטי-וירוס הפעיל.

### 6. תובנות על אבטחה

מתווכי Zero Trust Network Access (ZTNA) יכולים להחליף או להשלים VPN ארגוניים כדי להגביל את היקף גישת המשתמשים.

### 7. תובנה על אבטחה

האצלת הרשאות ניהול Just-in-Time (JIT) מצמצמת את הסיכון לגניבת פרטי התחברות בבקרי דומיין.

### 8. תובנה על אבטחה

יומני אימות רציף וביקורת התנהגות הפעלות משהים משתמשים שמציגים דפוסי הרצת סקריפטים חריגים.

### 9. תובנה על אבטחה

הגנות היקפיות מסורתיות אינן מצליחות לחסום התקפות רוחביות לאחר שפרטי כניסה ניהוליים דלפו.

### 10. תובנות על אבטחה

הפרסום המיוחד NIST 800-207 (2020) נותן הגדרה מופשטת לארכיטקטורת Zero Trust, עם מודלי פריסה. [1]

# מקורות והפניות טכניים

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

## מקורות אקדמיים ותעשייתיים

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

# מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

**1 שאלה 1** — תשובה נכונה: A

### הערה למורה

מהו העיקרון המרכזי של אבטחת Zero Trust? → לא לסמוך אף פעם, לאמת תמיד כל בקשת גישה בלי קשר למקור

**2 שאלה 2** — תשובה נכונה: A

### הערה למורה

מהי מיקרו-סגמנטציה של רשת? → פיצול רשתות לאזורים קטנים ומבודדים כדי להכיל תנועה לרוחב

**3 שאלה 3** — תשובה נכונה: A

### הערה למורה

מהו עיקרון ההרשאה המינימלית? → הגבלת הרשאות הגישה של משתמשים למה שנחוץ לתפקידם בלבד

**4 שאלה 4** — תשובה נכונה: A

### הערה למורה

מהו ניהול זהויות וגישה (IAM)? → מסגרות שמנהלות זהויות דיגיטליות ושולטות בהרשאות מערכת

**5 שאלה 5** — תשובה נכונה: A

### הערה למורה

מה משמעות אימות רציף? → אימות חוזר ונשנה של זהות המשתמש ומצב המכשיר במהלך הפעלה פעילה

## מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

**6 שאלה 6**

תשובה נכונה: לא נכון

### הערה למורה

לא נכון: Zero Trust אינו מעניק אמון מובלע על סמך מיקום ברשת, בתוך או מחוץ.

**7 שאלה 7**

תשובה נכונה: נכון

### הערה למורה

נכון: אזורים קטנים ומבודדים מגבילים עד כמה מרחוק פורץ יכול לנוע בין שרתים.

**8 שאלה 8**

תשובה נכונה: לא נכון

### הערה למורה

לא נכון: עיקרון ההרשאות המינימליות מעניק רק את הגישה המינימלית שכל תפקיד צריך.

**9 שאלה 9**

תשובה נכונה: נכון

### הערה למורה

אימות רציף בודק את תקינות המכשיר ואת אישורי הגישה לאורך כל הפעלת כניסה.

**10 שאלה 10**

תשובה נכונה: נכון

### הערה למורה

הטמעת Zero Trust מצמצמת את ההשפעה של פרטי התחברות ארגוניים שנפרצו.

# 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

| | | | |
|---|---|---|---|
| G 1. אימות | F 2. פילוח | A 3. IAM | B 4. הרשאה |
| H 5. מצב אבטחה | E 6. ביקורת | D 7. חומת אש | C 8. נתב |

## נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

| | | | |
|---|---|---|---|
| 1 אימות | 2 פילוח | 3 IAM | 4 הרשאה |
| 5 תקינות | 6 ביקורת | | |

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

| | | | |
|---|---|---|---|
| 1 G – חומתאש | 2 F – ביקורת | 3 D – הרשאה | 4 B – פילוח |
| 5 H – נתב | 6 E – תקינות | 7 C – זהויות | 8 A – אימות |

### הערות לדיון עבור מורים

**מונחי מפתח:**
ודאו שהתלמידים מסבירים במילים שלהם את אימות, פילוח ו-IAM 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

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

## פתרון תשבץ




## מדריך למורה לפתרונות התשבץ

### מאוזן

**1 מאוזן: פילוח** חלוקת אזורי הרשת הפנימית (5 אותיות)

**4 מאוזן: תקינות** הערכת מצב בריאות המכשיר (6 אותיות)

**5 מאוזן: הרשאה** עקרון זכויות הגישה המצומצמות ביותר (5 אותיות)

**8 מאוזן: ביקורת** סקירת סשני גישה שתועדו (6 אותיות)

### מאונך

**2 מאונך: חומתאש** הגנת מחסום לרשת חיצונית (6 אותיות)

**3 מאונך: נתב** ניתוב תעבורת מנות ברשת (3 אותיות)

**6 מאונך: אימות** בדיקה מתמדת של אישורי המשתמש (5 אותיות)

**7 מאונך: זהויות** ניהול גישה לאישורי משתמשים (6 אותיות)

# מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

### מפתח פענוח מילים מבולבלות

1. ומאתי — אימות
2. תזוויה — זהויות
3. תינתוק — תקינות
4. שתמאחו — חומתאש
5. לחפוי — פילוח
6. אהשהר — הרשאה
7. רבותקי — ביקורת
8. בתנ — נתב

### מפתח אתגר הצופן הסודי

**"אמתו תמיד בארכיטקטורת אפס אמון מאובטחת"**

# מפתח תשובות למקרי הבוחן

## A מקרה בוחן 1: מעבר לארכיטקטורת רשת Zero Trust

פתרון למורה

### הנחיות הערכה

### תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: ארגון גדול משתמש כעת ברשת פנימית שטוחה שבה כל מכשיר ברשת המקומית יכול לגשת לכל השרתים ומסדי הנתונים הארגוניים.
- אסטרטגיה ופתרון מומלצים: חלקו את הרשת השטוחה לאזורי מחלקות מבודדים. התקינו חומות אש פנימיות לשליטה בתעבורה בין האזורים, וחייבו אימות אסימון חיבור לכל גישה.

## B מקרה בוחן 2: הטמעת בקרות גישה לפי עיקרון ההרשאות המינימליות

פתרון למורה

### הנחיות הערכה

### תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: יומני ביקורת מגלים שלמשתמשי מסד נתונים זמניים ולעובדים בדרגה נמוכה יש הרשאות קריאה וכתיבה גלובליות למסדי נתוני הנהלת חשבונות קריטיים.
- אסטרטגיה ופתרון מומלצים: בטלו את כל ההרשאות הניהוליות הגלובליות. יישמו בקרת גישה מבוססת תפקידים (RBAC) שתתאים בדיוק לתפקידים, והגדירו בדיקות הרשאות אוטומטיות שבועיות.