

# **פְּרוֹיִיךְ סִפְיָן**

**למידה ויישום בתחום ה-SOC וה-SIEM**

**מנטורית : שירה כחלון**

**מאת : תמר מנו**

# מי אֲבִי?

- תמר (פרץ) בן  
בת 26, במקור משוהם
- סטודנטית להנדסת תוכנה שנה שלישית
- תקדתי כמנהל רשות בגבול לבנון במהלך שירות הצבאי
- הגעתי למנטריות כדי להעמק את הידע המעשי והתאורטי שלי בעולם הסייבר.

**01**

**02**

**03**

**04**

**05**

# מהו SOC?

SOC (Security Operations Center) הוא מרכז מבצעי המתמקד באבטחת מידע.



תפקיד ה-SOC:

- ניהול ומעקב אחריו מערכות רבות.
- טיפול בכמות גדולה של התרעות אבטחה.
- זיהוי וטיפול בנזקים ובטקיפות.



מטרת ה-SOC:  
להגן על הארגון מפני איומי סייבר ולהבטיח את בטיחות המידע.



# מהי מערךת SIEM?

SIEM היא מערכת שמרכזת ומנתחת נתונים אבטחה מגוון מקורות.

## מטרת ה-SIEM:

- לסייע ל-SOC ליצור סדר.
- להבין את תמונה האבטחה המלאה.

## תפקיד ה-SIEM:

- איסוף וניתוח לוגים מערכות שונות.
- זיהוי והתרעה על אירועים חריגים.
- ניתוח והתמודדות עם איום סייבר בזמן אמת.

# הצורה בידע רחב ועמיק

## חשיבות הידע:

- הבנה עמוקה של נושאי אבטחה שונים חינית לזיהוי והtagוניות מפני איומים.
- ללא הידע, קשה לנוהל ולהבין את האירועים המורכבים המתרכזים בארגון.

**מתוך הבלאגן  
שב-SOC, הבנו  
שעלינו ללמידה  
ולחקור מגוון  
רחב של נושאים.**

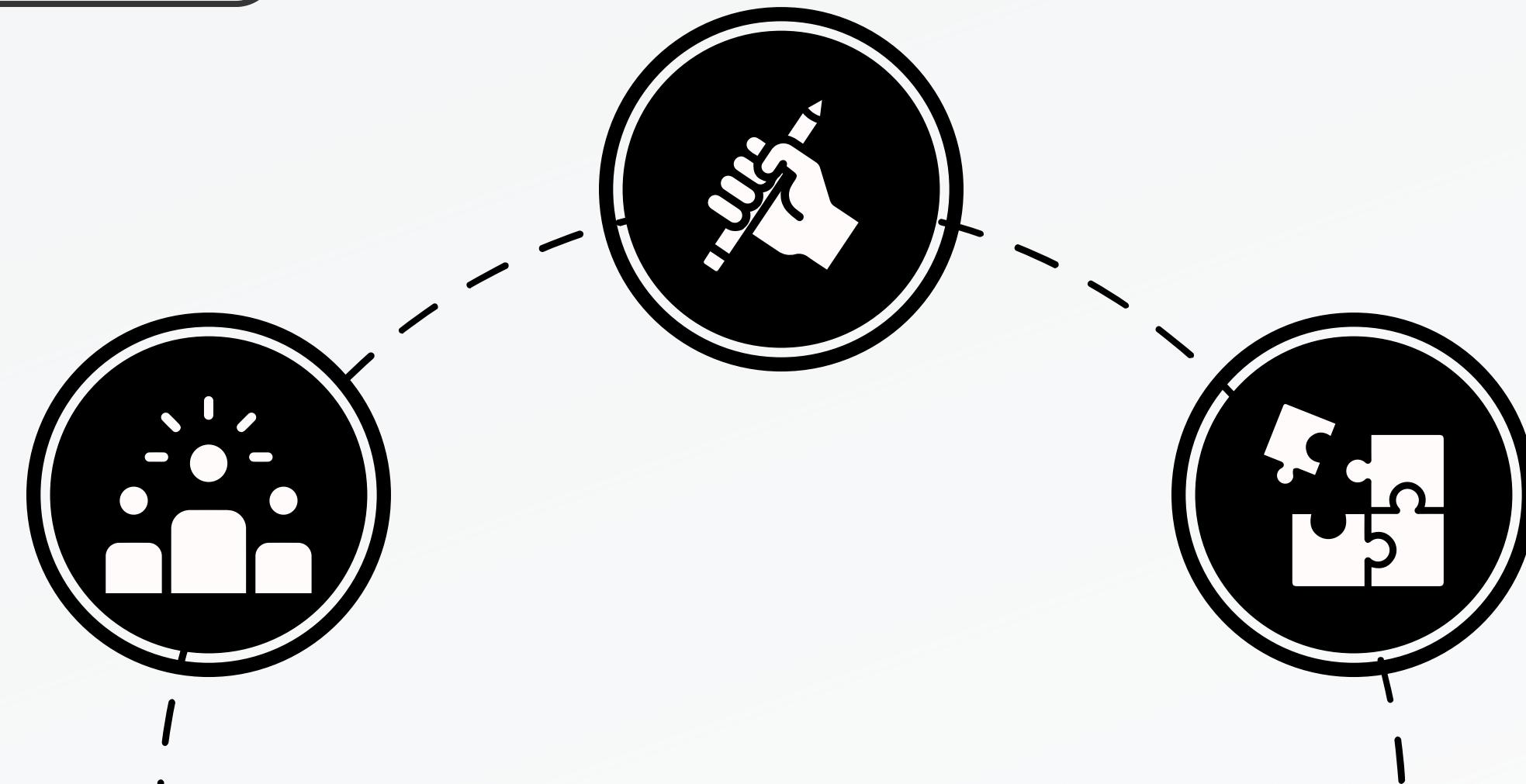


# מה למדנו?

הבנה עמוקה של נושאים אלה חיונית לניהוליעיל של מערכות אבטחה. הידע שצברנו מאפשר לנו להתמודד עם איום סייבר בצורה יעילה ומהירה.

הכרנו חולשות אבטחה שונות, הבנו את עקרונות ה-SIEM וה-SOC, וניתחנו מתקפות סייבר שונות.

במהלך הסמסטר, עברנו תהליכי לימוד עמוק של נושאי אבטחת מידע.



# מהלך הלמידה

- **עקרונות ה AAA**  
Authentication,  
Authorization,  
.Accounting
- **מודל ה-ISO** והשכבות  
השונות שלו.

**מבוא לאבטחת מידע**

- מבנה ותפקיד של  
מערכות הפעלה.
  - **פרוטוקולי תקשורת**  
ב시스ים ויישומים  
ברשות מחשבים.
- מערכות הפעלה  
ותקשורת**

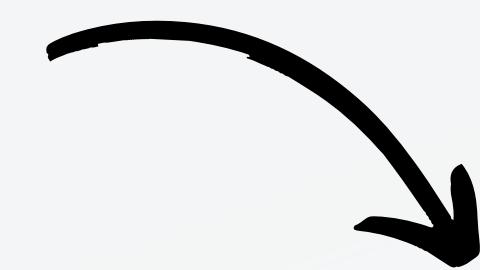
- SQL Injection
- XSS, ARP Spoofing
- דרכי התקיפה והגנה.

**תקיפות סייבר**

# מהלך הלמידה

- למדנו על ניתוח סטטי וдинמי של נזקות.
- רأינו כלים וטכניקות להיווי נזקות.

**חקירת נזקות**



- מערכות SIEM ו-SOAR.
- אנטי וירוס, חוממות אש, מערכות גילוי חדירות.

**מערכות הגנה**



- התנסות בניצול חולשות אבטחה ופתרון.
- **פרויקט סיום:** ניתוח חולשות בשרת פגעה.

**פרויקטים מעשיים**

# פרויקט סופי

- מכל הנושאים בחرتني להתעמק בנושא של-  
התקפות ופגיעות בשרתים.
- הפרויקט עוסק בהקמת שרת פגיע כדי ללמידה ולבחון את  
החולשות השונות במערכת.



**יביצוע התקפות שונות ובחינת ההשפעות שלן על השירות.**

**בדיקות זיהוי של פגיעויות**

**התקנה והגדרה של שרת Flask שהתקנתי והגדרתי מtower פרויקט קיימם בಗיט.**

**יצירת סביבה מוגנת לביצוע הניסויים והבדיקות. עבדתי בסביבת Linux.**

**types:**

Path Traversal

File Upload

etc.

**IDOR:**

Insecure Direct Object References

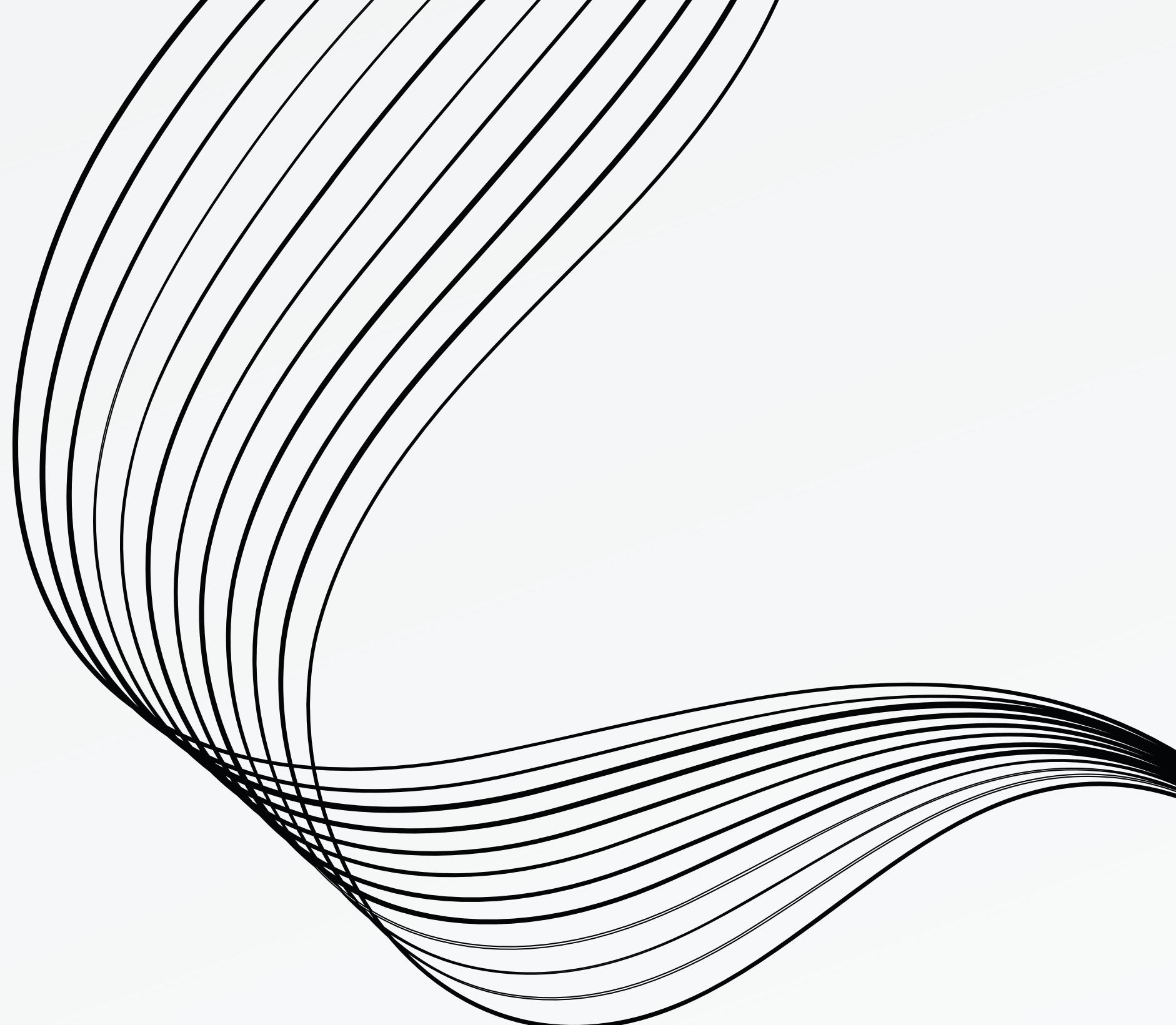
**XSS:**

Cross-Site Scripting

SQL Injection

# סיכון

- למדנו להזות ולהקוף פגיעות בשרתים.
- הבנו את חשיבות מערכות האבטחה וההגנה.
- רכשנו כלים ומומנויות בניתוח וטיפול באירועי סיבר.
- מוכנים להתמודד עם אתגרי האבטחה בשוק העבודה



**תודה  
על הקשבה**

