סדרת הוובינרים של נשים משלבות נשים בהייטק

סייבר

עדן כץ

GenAI Security Tech Lead

נעים מאוד – עדן כץ

רקע כללי

במקור ממכבים רעות, היום בגבעתיים

בת 28

בוגרת יחידת מפת״ח חיל הים, קורס מגן סייבר מחזור ט

בשלושה חודשים בין השחרור לקורונה הספקתי (כמעט) את כל יבשת דרום אמריקה - פרו, צ׳ילה, ארגנטינה וברזיל

המסלול האישי שלי

לימודי מחשבים בתיכון -> קורס סייבר בצבא -> שיבוץ בחיל הים כחוקרת תגובה לאירועי סייבר במערכות לחימה -> קצונה - ראש צוות תגובה לאירועים במעל״ח -> חוקרת אירועי סייבר ופורנזיקה באקסנצ׳ר -> מתמחה באבטחת ענן במיקרוסופט -> חוקרת זיהוי מתקפות בזיסקיילר -> יועצת סייבר בתחום הענן באקסנצ׳ר -> הפסקה -> יועצת סייבר עצמאית -> GenAI Security Tech Lead בחברת הייטק בנונית

איך בחרתי את התפקיד הזה? ״התפקיד בחר אותי״

הלכתי למחשבים בתיכון בגלל אמא, הלכתי לסייבר ולא לתכנות בצבא ״בגלל״ אמא, בחרתי לעבוד אחרי הצבא בסייבר כי התאהבתי במקצוע.

זה באמת בצורה הכי טהורה להגן על העולם/רשת מפני אנשים רעים, לשמור שמידע רגיש לא ידלוף, לחסום מתקפות בזמן אמת זה ריגוש. עכשיו בתחום המחקר- כל הזמן להיות ב״קצה של המידע״ לגלות דבר חדש שאף אחד לא הכיר לפניך

התפקיד שלי

GenAI Security Tech Lead -> R&D

- ביום-יום אני מקבלת משימה לכמה ימים, להתחבר למודל, להריץ כמות אדירה של פרומפטים עם שיטות שונות לעקיפת מערכות ההגנה - הרבה מקום ליצירתיות בשביל למצוא דרכים חדשות.
- אני עובדת עם מחברות ג׳וֹפיטר, סקריפטי פייתון, aws s3 buckets
- תקשרות ארגונית פנימית, מיילים, מסמכים וכו׳
- יש לי ראש צוות, שלושה חברי צוות. אנחנו חלק מקבוצה של 27 אנשים שבנויה 4 צוותים
- העבודה שלי בעיקר -פנימית - מול הצוות שעובדים ביחד במקביל על המודל וראש הצוות, ייתכן פעמים שאציג דברים מעניינים שמצאתי ללקוח
- יש איזון בית עבודה. שעות עבודה רגילות. יום עבודה אחד מהמשרד ברמת גן. שמים דגש על תפוקה ולא על שעות מול המחשב..

איך התפקיד נראה בחברות השונות?

🏢 **קופרייפטס -** כמעט ועוד אין צוותים כאלו, אם יש- פנימיים ועובדים כחלק מהמוצר AI עצמו. שעות נוחות, תרבות ארגונית של תאגיד- עובדים על פרויקטים מאוד קטנים לטווח זמן רחוק. יש דגש על הצגת תוצרים בקהילה הטכנולוגית.

🚀 **סטארטאפ בינוני** (כמו זה שאני נמצאת בו) - יש צוות אחד, יושב במחלקת סקיוריטי עם צוותים שעוסקים במחקרי סייבר אחרים. יש כבר פייפליין של לקוחות קבועים שכבר חוזרים עם מוצרים חדשים שלהם לבדיקה. יש תשתית קטנה כבר של אוטומציה.

🌱 **סטארטאפ קטן -** כנראה צוות של בין 1-6 חוקרים, עובדים במקביל לצוות פיתוח מוצר שנותן מענה לכל השירות. עושים הכל מהכל כולל התשתית.

💡 **שלב התחלתי -** הרבה שעות, למצוא את השינוי שיביא את הביזנס. הרבה שעות בשביל להצליח לתפוס לקוחות ראשונים. עושים הכל מהכל כולל התשתית.

אילו סקילס נדרשים?

תכונות רכות

יכולת פתרון בעיות, סבלנות ועיקשות עד שמוצאים פתרון, ראש גדול, לא לקחת כשלונות ללב, יכולות אנליטיות וניתוח נתונים רבים, תקשורת בין אישית ובכתיבה. יכולת לדבר מול ממונה בשביל להציע רעיונות חדשים וגם יכולות הדרכה והעברת חומר לחברי הצוות הנוספים. יכולת לעבוד מאוד מהר בדד ליינים קצרים ולהתמודד עם שינויים דחופים באופן ותעדוף המשימות

תכונות טכניות

כתיבת סקריפטים (פייתון/ג׳אווהסקריפט), פיתוח ושימוש בסביבת ענן, הבנה עמוקה ב״מאחורי הקלעים״ של כלי AI כמו איך ChatGPT עובד, DALL-E, ניסיון בשימוש במודלים מסוגים שונים text2text, text2image, image2text, text2video ועוד, היכרות עם פריימוורקים של אבטחת AI, הגדרות קומפליינס ומדיניות אתיקה. ידע בחולשות AI ודרכי התמודדות.

איזה ניסיון מעשי חשוב שיהיה כדי להגיע לתפקיד הזה?

אין מסלול אחד שרלוונטי אך זה באמת לא מתאים לנשים שלא מגיעות מרקע טכנולוגי עשיר. הייתי אומרת בתחום הסייבר, צריך לצבור 3-4 שנים בתחומים כמו Red Team, PT, Forensics בשביל להיות רלוונטית או שאפשר להגיע אחרי כמה שנים בפיתוח בשפות שונות ושליטה מלאה בעקרונות פיתוח.

איך מגיעים לתפקיד הזה?

אילו הכשרות מומלצות?

הכשרות בעולמות הסייבר, הכשרות בינלאומיות בלבד (**לא קורסי סייבר במכללות ישראליות**)

הכי פשוטות בתחום הן Certified Cybersecurity של ארגון ISC2 אבל זו הסמכה בסיסית מאוד לכלל תחום הסייבר, הסמכות שיותר מתאימות לעולמות של העיסוק הן Certified Ethical Hacker של EC-Council אבל הרלוונטיות ביותר הן של OffSec כמו OSCP, OSWA, OSWE, OSCE3 או של ארגון SANS (GIAC) - הסמכות SEC542 או SEC522

אפשר לצבור ניסיון באתגרי אונליין של חברות סייבר שמתפרסמות מידי פעם, הכי בסיסי שיש פתוח - Gandalf של Lakera AI.

יש גם אתרים כמו TryHackMe או HackTheBox שמציעים מעבדות בסיסיות בתחום הסייבר.

המעבדות של OWASP מורכבות במיוחד לעולמות ה Web Application Security

אילו תפקידים יכולים להוביל לתפקיד הזה?

מסלול סייבר: בודקת חדירות/אנליסיטת סוק/סקיוריטי -> תגובה לאירועים/Malware Analysis/צוות אדום -> Offensive Security <- אבטחת GenAI

מסלול פיתוח: פיתוח אפליקציות ווב, עקרונות פיתוח וחולשות, Reverse Engineering

בשביל להגיע מהר יותר

ללמוד כבר עכשיו כל מה שאפשר על טכנולוגיות AI, להישאר מועדכנות, להתנסות כמה שיותר, לפתח מיינדסט של האקרית, ללכת ישירות לשם ולא הייתי הולכת להיות כמה שנים בIncident Response ובמחקר ענן

איך מחפשים עבודה לתפקיד הזה?

טיפים לחיפוש עבודה בתפקיד הזה

- לצבור ידע וניסיון בצורה עצמאית - לימוד עצמי זה הדבר הכי חשוב בתחום הסייבר, למידה מתמדת.
- ללכת לאירועי סייבר, כנסים, לקרוא בלוגים של חברות
- נטוורקינג במעגלים הנכונים- תחום מאוד קהילתי: המון קבוצות שעוסקות בנושאים ספציפיים.

מילות מפתח חשובות שחשוב שיופיעו בקו״ח

🧠 **תחומים מקצועיים:**
GenAI Security, Adversarial Mindset, Security Research, Prompt Injection, LLM Red-Teaming, Secure Model Deployment

🛠️ **כלים וטכנולוגיות רלוונטיים:**
OpenAI / ChatGPT / GPT-4 / Co-Pilot / Anthropic Claude / Google Gemini / LangChain / Hugging Face / Python
Cloud (AWS / GCP / Azure)

🧪 **מתודולוגיות ויכולות:**
Threat Modeling, Red Team / Blue Team Tactics, Vulnerability Research, Penetration Testing, Incident Response, Ethical Hacking

מה היית עושה בתחילת הדרך אחרת?

אולי זה קשה לתיקון - אבל בטוח ללכת למסלול טכנולוגי בצבא, היה יותר קל אפילו לי אם הייתי ב-8200 או הייתי בתפקיד התקפי/הגנה התקפי ולא ״צוות כחול״ בצבא

מה אני אוהבת בתפקיד הזה?

מה ממלא אותי בתפקיד הזה?

תחושת השליחות, ההשפעה של עשיית טוב בעולם, למנוע מהאקרים ואנשים רעים לעשות שימוש לרעה בתוכנות. ספציפית בחברה עכשיו שהלכה למעשה מנקה את האינטרנט מתכנים פוגעניים ומזיקים.

אתגרים שאני נהנית מהם?

אני זוכרת מהתפקיד בצבא של Incident Response היה להצליח לאתר "וירוס" מתוחכם שמחק את כל העקבות שלו במערכת אבל היה אפשר למצוא אותו דרך הרצת כלי שקורא תיקייה שמתעדת תהליכים שרצו על המערכת. הסיבה שהיא שם בשביל לאפשר למערכת לפעול יותר מהר - בשבילנו זה היה חוט הזהב להשלמת החקירה.

בראיון עבודה, הייתי צריכה דרך הזום להעביר פרומפטים שהמראיין יזין למערכת AI המיוחדת שהם בנו ולפי התגובות שראיתי בשיתוף המסך להמשיך עד שהצלחתי לגרום לו להגיד משהו שאסור (כמו במשחק של גנדלף)

שתפי אותנו במשהו אישי ברגש או בחיבור לתפקיד

אני חושבת שהאקריות בסוף זה הדבר שהכי נוגע בי. היום אני נמצאת במחלקה של 27 אנשים, אנחנו שתי נשים שהשנייה עובדת רק מרוחק. זה לא הפריע לי כל המסלול אבל כן אני רואה את ההבדלים בעבודה שהיא גברית ברובה ואת החסרונות בכך. במיוחד שאני יודעת שיש לנשים יכולות מצוינות לתפקיד והרוב נובע מחוסר חשיפה לעולם הזה.

סייבר: לא מה שחשבתן

```
import java.sql.*;
import java.awt.*;

/**
 *
 * @author jeff
 */
public class Main {

    public static String AppName = "SQL Mail";
    public static String AppVersion = " 0.0.1 ";
    public static String AppAuthor = "Jeffrey Cobb";
    public static String AppDate = "August 8th, 2007";
    public static String AppPath = System.getProperty("user.dir");
    public static String AppDriver = "smallsql.database.SSDriver";
    public static String AppDBHeader = "jdbc:smallsql:";
    public static String AppDBPath = AppPath + "/sqlmail";
    public static String AppPreferences = AppPath + "/sqlmail_prefs";
    /** Creates a new instance of Main */
    public Main() {
    }

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws Exception {
        // TODO code application logic here

        boolean bDBConnect = false;
        int result = 0;
        frmMain SQLMailForm = new frmMain();
        System.out.println("\r\n" + AppName + "\r\nVersion" + AppVersion + "\r\nAuthor: " + AppAuthor + "
 -- " + AppDate + "\r\n");

        Toolkit tk = Toolkit.getDefaultToolkit();
        Dimension screen = tk.getScreenSize();
        System.out.println(screen.getWidth() + " ... " + screen.getHeight());
```

חלק מהשקפים הבאים מבוססים על מצגת של חבר קרוב שמעביר גם הרצאות בנושא - אוהד זיידנברג

סייבר - עולם שלם

"נשים משלבות נשים בהייטק" - שם כללי

מה זה הייטק?

מעוניינת להתחיל לעבוד בהייטק
איך מתחילים ?
מאיזה קורס? איך הייתה ההתחלה שלכם?

היי:)
רציתי לדעת ממישהי שמנסה להשתלב בתחום הייטק. מה הייתן ממליצות כדי להתחיל? קורסים, תוכניות, המלצות כלליות?
תודה!!

מסלולי סייבר

יש המון מסלולים שאפשר באמצעותם להגיע לעבודה בסייבר, זה תלוי בכן.

- ״זה בדם שלי״ – אני פורץ למחשבים מגיל 0, האקר מגיל צעיר
- מסלול המסגרת – למדתי קורס סייבר/תואר טכנולוגי ומשם נכנסתי לעולם הסייבר
- מסלול המרת מקצוע – למדתי מקצוע לא טכנולוגי (עו״ד למשל), באמצעותו הגעתי למרחב הסייבר
- מסלול לימוד עצמאי – למדתי לבד את התחום ונכנסתי לעולם הסייבר
- מסלול הצבא – למדתי בצבא את התחום והמשכתי לחברת סייבר
- מסלול המנטורינג – הלכתי אחרי אדם אחר אשר הוביל אותי לתעשייה
- מסלול ההייטק – התחלתי לעבוד בחברת מוצר העוסקת בסייבר ומשם הגעתי לסייבר

מה המסלול הנכון?

- תלוי בכן! אל תאמינו למי שיש לו את כל התשובות. לכל אחד יש את המסלול שלו.

לימודים

מכללות לתחומי הסייבר מציעים קורסי סייבר שונים, טובים יותר **ופחות**, להסמכות שונות בתחום הסייבר.

- קורסים נפוצים הם מיישמי CCNA (תקשורת מחשבים), בקר SOC, Malware Analysis, OSCP או CEH (פן טסט), CISSP (מוסמך מערכות אבטחת מידע מקצועי)
- קורסים מקצועיים של ארגונים בינ״ל כדוגמת SANS (שווים יותר, יקרים יותר)
- לימודים אקדמיים במסגרת מדעי המחשב – לתחום reverse engineering או malware analysis או רשתות.

האם זה מנדטורי? לא.

האם זה מסייע? כן.

האם הייתי עושה תואר מלא במדעי המחשב רק כי זה מסייע? לא.

ניתן ללמוד את כל התחום בצורה עצמאית ודרך הרשת!

תזכרו - הכל נורא אישי. אין מסלול אחד נכון ויש מגוון דעות

לימוד עצמי

- התכונה הכי קריטית לתפקידי סייבר
- לא מספיק רק ללמוד באופן פורמלי, תחום הסייבר משתנה וחייבים להתפתח איתו

חומרי העשרה

- בלוגים וקורסים שונים בחינם ברחבי הרשת
- סרטוני הדרכה ביוטיוב
- ספרים רבותיי, ספרים!
- הרצאות (אונליין ואופליין, יוטיוב), Meetups
- קריאה יום יומית בגופי חדשות רלוונטיים (Zdent, Bleeping Computer, Dark Reading)
- פודקאסטים
- רשתות חברתיות – נשמע מגוחך, אבל בסייבר זה מהותי ולא רק לקידום עצמי
- טוויטר – כולנו שם, רוב התקיפות והפריצות לא מגיעות לחדשות
- רדיט – אם הגעתם לרמה האולטימטיבית של העמקה, בהצלחה
- הבנה כללית בעולם הסייבר – זה מעולה שאתם רוצים לעבוד בהתקפה, אבל בלי להבין איך מגינים, לא תוכלו להשלים את המשימה בצורה מיטבית. הקפידו ללמוד את המבוא.

איך תדעי שאת יכולה להיות סייבריסטית טובה?

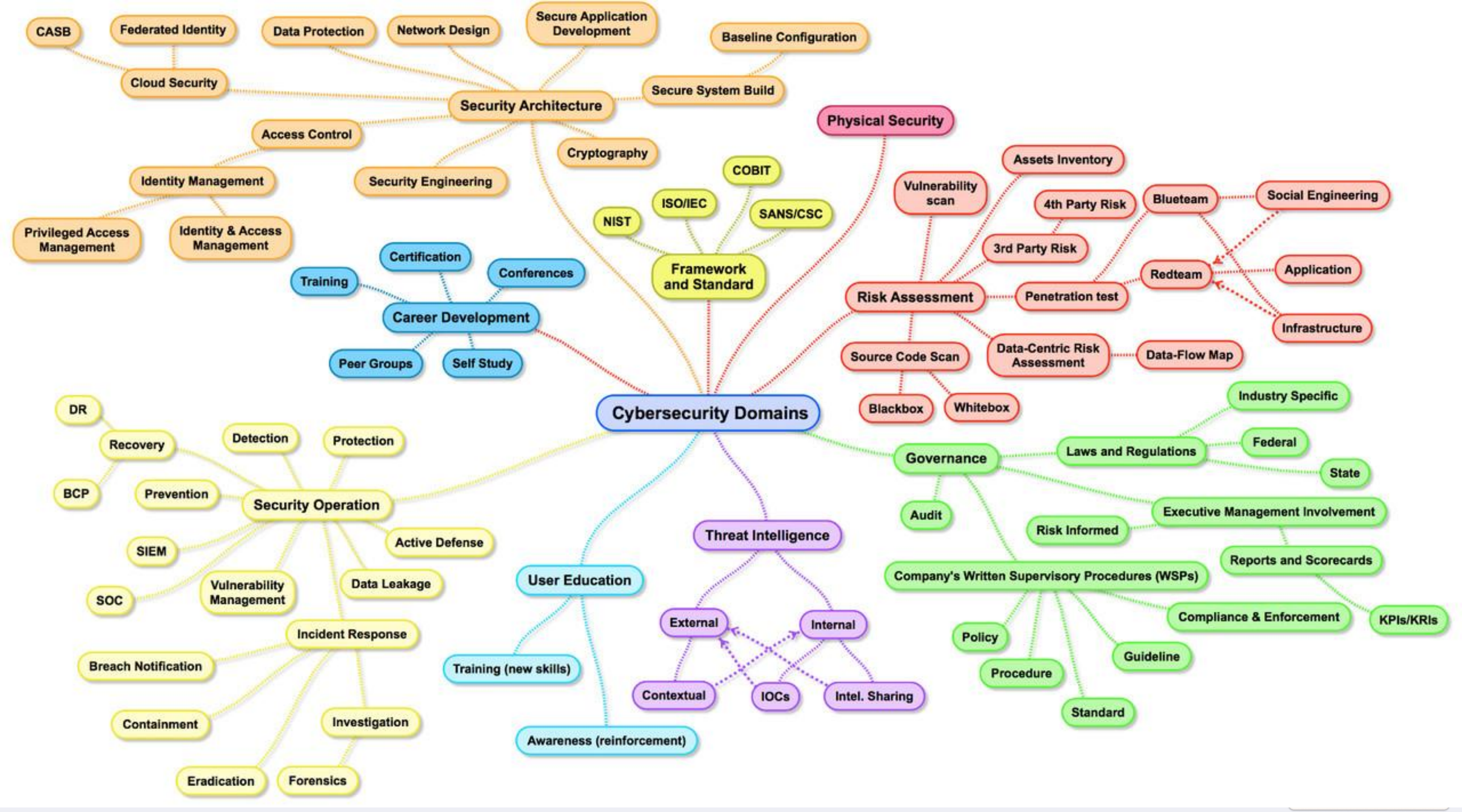
- סקרנות אובססיבית
- נכונות ללמוד ולהתפתח
- יכולת עמידה בלחצים
- חשיבה מחוץ לקופסה
- תקשורת טובה
- סבלנות
- יעזור מאוד גם לחשוב בצורה התקפית (העשרה בעולמות הקרימינולוגיה)
- המיומנויות האלו יתפתחו גם במהלך העבודה, אבל אם תביאו אותם מהבית, זה יהיה בונוס

איך עולם הסייבר נראה?

לפני שניכנס לעולם הסייבר נרצה להבין לאיזה תחום נרצה לכוון, אנחנו לא מתחתנים עם התחום שלנו – נוכל לזוז מבפנים ימינה ושמאלה

בסייבר (באופן מאוד מאוד נרחב) יש 9 דומיינים שונים:

- Security Operations – עולם ההגנה, ניהול פרקטי של סיכונים (עולמות ה-SOC למשל)
- User Education – הדרכות, Awareness
- Threat Intelligence – מודיעין סייבר, התחום שלי. בניית תשתית מודיעינית להגנה והתקפה.
- Governance – מדיניות, רגולציה, משפטים, סקר סיכונים, Audit
- Risk Assessment – עולם התקיפה, מחקר פרקטי של איומים וסיכונים, האקינג
- Physical Security – אבטחה פיזית על מערכות סייבר ובכללי
- Framework and Standard – תקינה של אבטחת מידע, ניהול ידע
- Career Development – כוח אדם, כנסים, סדנאות, הכשרות
- Security Architecture – עולמות התשתית, אבטחת מערכות ארגוניות בצורה תשתיתית


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Cryptography
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Framework and Standard
COBIT
ISO/IEC
SANS/CSC
NIST
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Physical Security
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Penetration test
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Governance
Industry Specific
Laws and Regulations
Federal
State
Executive Management Involvement
Audit
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics

תפקידים שיש בסייבר

בחינה לפי דומיינים (מנוסח בלשון זכר ופונה לשני המינים):

- Security Operations – אנליסט סוק Tier 1 (הנפוץ ביותר), תגובה לאירועים (IR)
- User Education – הדרכה וייעוץ בדגש על מודעות
- Threat Intelligence – אנליסט מודיעין סייבר, חוקר נוזקות
- Governance – ייעוץ אבטחת מידע בדגש על ניהול סיכונים
- Risk Assessment – בדיקת חדירות (PT), Junior Red team, Junior Appsec
- Physical Security – אבטחה פיזית
- Framework and Standard – לא משרות התחלתיות (דורשות מומחיות)
- Career Development – משרות כוח אדם, התנדבות
- Security Architecture – ניהול תשתיות, מערכות ורשתות (קרי, IT), Support, תכנות או QA לאנשי הקוד

תפקידי סייבר ראשוניים

Security Operation Center (SOC) Analysts

Role: monitors alerts, analyzes logs, and escalates incidents.

Skills: SIEM tools, network analysis, basic scripting.

Penetration Testers

Role: Tests systems for vulnerabilities, simulates attacks.

Skills: Knowledge of various attack vectors, network and application security, scripting.

Incident Responders

Role: Investigates incidents, determines impact, mitigates attacks.

Skills: Forensics, malware analysis, investigative mindset.

Cyber Threat Intelligence Analysts

Role: Gathers and analyzes cyber threat, provides intelligence reports

Skills: Data analysis, threat and Intelligence tools, basic scripting.

Threat Hunters

Role: Seeks hidden threats in the network, analyzes attack patterns.

Skills: Advanced knowledge of threat tactics, behavioral analysis, threat intelligence.

GRC Specialists

Role: Ensures compliance, assets risks, establishes security policies.

Skills: Knowledge of industry regulations (GDPR, HIPAA), risk management, documentation.

צעדים ראשונים להפוך למומחית סייבר

1

Gaining Knowledge and Hands-On Experience

- Online Guides
- YouTube Channels
- Cybersecurity Blogs
- Hands-on Workshops
- Online Courses
- Meetups and Conference
- Online Communities and Forums

2

Boosting Your Skills and Master a Specific Field

- Hands-on Practice - personal projects
- Continuous Learning of new attacks and techniques.
- Platforms for Learning:
  - TryHackMe
  - Hack The Box
  - Cloud Academy (now part of QA)

3

Know the Industry and Get Validation

- Networking Community Engagement (Meetups):
  - Mentoring and Guidance
  - Resource Access
  - Job Oppresunies
- Certification
  - CompTIA Security+
  - CEH (Ethical Hacking)
  - CC (ISC2)

איך נסמן למעסיקים שאני מתאימה לתפקיד סייבר?

- בכל שנה יש מאות מסיימים של קורסי סייבר, משתחררים טריים, אנשים שלמדו לבד, איך אפשר להתחרות בכל המועמדים והמועמדות הללו?
- "משרות סייבר ללא ניסיון" הן סוג של אקסיומה, כל אחד רוצה ניסיון כלשהו, בלי ניסיון לחלוטין מדובר בהימור ובמצב השוק הנוכחי, ההימורים מסוכנים.
- כשאנחנו מגישים קו"ח למקום עבודה, נרצה להראות למעסיק כיצד אנחנו מיישמים את הניסיון והידע שרשמנו בקו"ח
- לכל משרה דרישות שונות! לכל דומיין צרכים שונים.
- בשלב סינון קורות החיים, מחפשים את השונה - זה שיש לו יתרון על האחרים
- הבנה בשפות שונות רלוונטיות לתחום המודיעין, אך בלי אנגלית קשה להתקדם בתחום. שפרו את האנגלית שלכם!
- במרחב הסייבר יש סיגנלים שונים שבאמצעותם נוכל לסמן למעסיקים שיש לנו יתרון תחרותי
  - בתחום הקוד – נוכל לתרום לפרויקטים של קוד פתוח שיראו את רמת התכנות שלנו, נוכל לבסס את עצמנו ברשת (בין אם בלינקדין ובין אם במקומות ייעודים כמו Stack Overflow)
  - בכל שאר התחומים – בואו נדבר על סיגנלים שונים

צעדים מעשיים "סיגנלים"

- בלוגים – בלוג אבטחת מידע עצמאי שמראה יכולות מחקר בתחומים שונים הוא אקוטי
- מדיה חברתית – טוויטר היא רשת הבית של חוקרי אבטחת המידע, רצוי להתעדכן שם
- פרויקטים – פיתחתם טכנולוגיה מסויימת? בניתם מתודלוגיה? יצרתם כלי? תפרסמו אותו!*
- השתתפות באתגרי CTF – נפתור אתגרים שכאלה, נלמד יותר על התחום שלנו וגם נמצב את עצמנו כמביני עניין. נוכל להעלות את הנושא בראיונות עבודה.
- הכשרות, הסמכות, תעודות – לא חובה, אבל גם יכול לעזור לחלק מהמקצועות.
- Bug Bounty – סיגנל סופר משמעותי, אם תצליחו למצוא חולשה באתר או שירות**
- חברים, מפגשים, meetup, כנסים – בואו לפגוש אותי במציאות!
- אתגרי מוסד, שב"כ וכו' בימי עצמאות
- התנדבות – בואו לקחת חלק בפעילות למען הקהילה. גם בהאקריות (כבר נגיע לזה)

*קחו בחשבון שאם תפתחו כלי התקפי הוא בהכרח יגיע לידיים של תוקפים ולכן תדגישו שמדובר בכלי מחקרי.

**שימו לב שהדיווח על bug bounty דורש הבנה בתהליך. הוא צריך להיעשות בצורה חוקית לחלוטין ולדווח לפי כללי אתיקה.

מפגשים ואירועים שונים בסייבר

- BsidesTLV – כחלק משבוע הסייבר של אוניברסיטת תל אביב (כנס עולמי ענק), השנה יהיה ב26.6, ההרשמה פתוחה (בתשלום)
- הכנס השנתי של האקריות 9-10.9 באוניברסיטת תל אביב - הרשמה תיפתח בקרוב (בינתיים בחודש הקרוב יש עוד אירועים מקומיים בב״ש, ת״א, ירושלים וחיפה)
- DC9723 – פורום Defcon (כנס סייבר בלאס וגאס) ישראלי שקורה אחת למספר חודשים (הוקפא בזמן המלחמה)
- Meetups – תעקבו אחרי meetup.com ותתעדכנו בקבוצות השונים
- BlueHatIl – כנס אבטחה של מיקרוסופט, מתרחש כל השנה (היה לפני פסח השנה)
- Intend - כנס סייבר של חברת צ׳קמארקס. קורה בנובמבר.
- AppSec IL – הכנס השנתי של OWASP - קורה ב 5.6 - הרשמה פתוחה ובתשלום
- ועוד מיטאפים של עוד קהילות וחברות סייבר

קבוצות סייבר

- DC9723 – בהמשך לשקופית הקודמת, הקבוצה הרשמית של המפגשים
- "סייבר ואבטחת מידע: צעדים ראשונים וכניסה לתעשייה" בפייסבוק
- Think Cyber Safe של מיי ברוקס קמפלר בפייסבוק
- Cloud Security Alliance Israel - וואטסאפ
- לנשים בלבד:
- Leading Cyber Ladies - נשים שכבר בתחום
- Hackeriot - נשים שרוצות להתחיל
- ועוד

האקריות

- ארגון התנדבותי שמחבר נשים לסייבר ע"י יצירת רשת קשרים נשית, ומהווה קרש קפיצה להשגת משרה ראשונה. הוקם ב-2022. מופעל 100 אחוז על ידי מתנדבים, יוזמה ללא מטרת רווח.
- הפעילות של האקריות:
  - כנס ארצי שנתי
  - 4 סניפים: חיפה,תל אביב,ירושלים,באר שבע
  - תוכניות ארוכות טווח: MentoRiot,SecureAcademy,תוכנית 'פרויקט גמר'

האתר: www.hackeriot.org

חפשי אותנו בפייסבוק, באינסטגרם ובלינקדאין

הצטרפות לקהילת הוואטסאפ:

להתנדב בקהילה (לא חייבים לדעת סייבר):

שאלות?