אוקטובר, 2023

סקירה החברות והשירותים של ספקי שירות אבטחת מידע - אבטחת מערכות למידה

הוכן על ידי צוות מיט"ל

במסמך זה מוצגים פרטי החברות וסקירת השירותים שהחברות מספקות עבור בדיקת פגיעות במערכות למידה, בפרט בדיקות חדירות למערכות למידה (PT - Penetration Test).
בשנים אחרונות מל"ג וות"ת פועלים לקידום הלמידה הדיגיטלית ככלי לשיפור איכות ההוראה וחווית הלמידה, להנגשה רחבה יותר של ההשכלה הגבוהה לכל חלקי האוכלוסייה בישראל ולחיזוק מעמדה של האקדמיה הישראלית בעולם. בהתאם לכך במוסדות רבים מתרחבת מגמה של יצירת קורסים דיגיטליים מסוגים המונגשים הן לסטודנטים והן לקהלים רחבים יותר. המעבר למידה מקוונת טומן בחובו חשיפה גדולה לפרטי המשתמשים והמידע בקורסים השונים לכן כדי למנוע דליפות נתונים והתקפות סייבר שונות יש לבצע בדיקות חדירות סדירות בהתאם לסטנדרטים הגבוהים ביותר.
בבדיקה שנערכה מול המוסדות זיהינו שהמוסדות זקוקים לשירות של חברות עם התמחות בבדיקות חדירות למערכות למידה לניהול הקורסים כגון מוודל (Moodle) בכדי למנוע פגיעות סייבר או זליגת מידע. לכן החלטנו להוסיף לסל הטכנולוגיות של מיט"ל תחום פעילות חדש **"פגיעות במערכות למידה"** בו נציע למוסדות חברות המתמחות בבדיקת חדירות למערכות הלמידה ומכירות את המורכבויות והדרישות של האקדמיה. שלוש חברות בסל, Fensive, Clear Gate, Auren, שכבר עובדות עם האקדמיה ומעוניינות להרחיב את ההתקשות במוסדות.

מידע כללי על כל חברה והמוסדות בהן הן פועלות

ריכוז המידע נאסף מההצעות שהחברות הגישו למחב"א/מיט"ל בהתאם לצורכי המוסדות הדרושים לאבטחת מערכות הלמידה, ולסקר הבוחן את מאפייני המוצר וקריטריונים נדרשים שנשלח לחברות, ובחינה השוואתית של צוות מיט"ל.

חברת Fensive

פנסיב הוקמה על מנת להעלות את רמת אבטחת המידע במוסדות ישראלים בעלי משמעות לאומית גבוהה. הסקטורים בהם אנו מתמקדים הם סקטור הרפואה וסקטור האקדמיה. מטרתנו היא להיות יד ימינם של סקטורים אלו בתחומי בדיקות החדירות וסקרי הסיכונים.
יתרונות החברה -
ניסיון: עוסקים למעלה מעשור באבטחת מידע ובפיתוח מערכות מורכבות. ניסיון החברה מורכב משירות ביחידות מובחרות בצבא והן ממשרות בכירות בחברות אזרחיות. שילוב הניסיון כמפתחי תוכנה וכחוקרי אבטחת מידע מקנה לחברה ראייה הוליסטית של המערכת או התשתית הנבדקת.

שירות פרימיום: כדי להבטיח קבלת שירות מדהים שמשולב עם רמת מקצועיות, מומחיות וניסיון שקיימים בחברה מייסדי החברה מתחייבים לליווי מתמיד לאורך כל הדרך. החברה מתחייבת לביצוע מבדקי החדירה באופן עצמאי עם מידת העומק וכמות הזמן המושקעים בכל בדיקה גבוהה משמעותית מהמקובל בשוק.
מיקוד: החברה מתמקדת במבדקי חדירה עבור סקטור האקדמיה דבר המסייע לפתח מומחיות יוצאת דופן במבדקי חדירה אפליקטיביים ותשתיתיים לסקטור זה. מומחיות זו כוללת פיתוח מתודולוגיות בדיקה ייחודיות לצד ארסנל כלים עוצמתי.
פעילות במוסדות אקדמיים: אונ' העברית בירושלים, אונ' בר אילן, אונ' חיפה, אונ' אריאל בשומרון, סמינר הקיבוצים, ספיר

חברת Clear Gate

Clear Gate היא חברה ישראלית הפועלת ברחבי העולם מאז 2016 ומסייעת לחברות להגן על יישומי SaaS שלהם על ידי ביצוע הערכת סיכוני אבטחת מידע. הערכת סיכונים נעשית בעזרת ביצוע מבדקי חדירה על ידי צוות המומחים של החברה.
מבחני חדירה נעשים על ידי אוטומציה לצד בדיקה ידנית ומעמיקה על ידי מומחים.
פעילות במוסדות אקדמיים: אונ' ת"א, הטכניון, אונ' רייכמן, מכון ויצמן למדע

חברת Auren

היא חברת ייעוץ בינלאומית המדורגת ברשימת ה FoF – ובמדד העולמי במקום ה 15
הפירמה מונה בעולם כ 5000 עובדים בכל תחומי הייעוץ.
חטיבת הסייבר היא ח.פ נפרד בתוך הפירמה ובמבנה מיוחד.
חטיבת הסייבר עצמה מונה כמות גדולה מאוד של פרילנסרים ושיתופי פעולה – וכשלושה עובדים על הPayroll.
חטיבת הסייבר הישראלית בפירמה עובדת מסביב לעולם – ובמגוון תצורות – יש מקומות שבהם ישירות מול הלקוח ויש מקומות בהם עובדים כנתוני שירותים כקבלני משנה.
פעילות במוסדות אקדמיים: מכון ויצמן, רשת מכללות עתיד, אוניברסיטת חיפה

<u>פירוט רשימת השירותים ומודל תמחור</u>

חברת Fensive

פירוט השירותים:

1. **מבדק חדירה אפליקטיביים**

- מבדקי חדירה ייעודיים למערכות ה-מודל (Moodle) המשרתות את המוסד האקדמי, איתור חולשה הרצת קוד מרחוק על שרת המודל (RCE), השגת גישה להורדת קבצים רגישים משרת המודול (LFI), הזרקות SQLi בפיתוחים פנימיים של מוסדות אקדמיה ובתוספי צד שלישי המוטמעים במערכת המודל, והשגת Admin במערכת ה- Moodle כתוצאה מחלק מהחולשות שתוארו לעיל.
- מבדקי חדירה אפליקטיביים למערכות ייעודיות (דסקטופ, מובייל ו- Web) שפותחו ע"י המוסד האקדמי או בית תוכנה צד שלישי ייעודי המשרת את הסקטורים הנ"ל.

להלן דוגמאות למוצרי מדף אשר בדקנו בעבר ובהם נעשה שימוש רחב בסקטור האקדמי:

- מערכת Moodle
- מערכת ידיעון.
- מכלול (ראשים).
- Tomax Platform – מוצרי TomaSafe , TomaGrade ו - TomaEtest
- נמלה (Top Solutions) – מוצר נמלה פלוס לניהול משובי עובדים.
- Mobitti Apps – אפליקציות מידע אישי למוסדות אקדמיים.
- WordPress & cPanel & WHM .

2. **מבדקי חדירה לתשתיות פנימיות מקומיות ובענן** - ביצוע מבדקי חדירה מעמיקים לתשתיות פנימיות של מוסדות מסקטורים הרפואה והאקדמיה.

הישגים לדוגמה:

- פעולות RedTeam ברשת הפנימית ממשתמש פשוט ועד ל- Domain Admin , השגת שליטה מלאה על סביבת ה- Active Directory הארגונית במוסד בעל עשרות אלפי עובדים.
- מבדקי חדירה לתשתיות ומערכות ERP , השגת גישה מלאה (Root) למרבית משרתי תשתית ה - ERP וחדירה למאגר הנתונים של מערכת ה- ERP לרבות יכולות כתיבה וקריאה של כלל המידע.
- הסלמת הרשאות מקומית בשרת רגיש ומוגן ע"י EDR (Privilege Escalation)
- התפשטות רוחבית בין עשרות שרתים ברשת הפנימית) Lateral Movement)
- מבדקים לתשתיות ענן כגון Microsoft Azure ו- Amazon AWS המשמשים כתשתיות מחשוב ו\או תשתיות מערכת במוסדות מסקטורים הרפואה והאקדמיה, השגת גישה משתמש פשוט בתשתית (דרך הגדרות תצורה לקויות) ואף מגורם חיצוני לחלוטין (דרך חולשה אפליקטיבית) למשתמש בעל שליטה מלאה בתשתית הענן.

3. **סקרי סיכונים** – ביצוע סקרי סיכונים מקיפים לתשתיות פנימיות וחיצוניות של מוסדות מסקטורים הרפואה והאקדמיה.

הישגים לדוגמא :

- אותרו ממשקים מסוכנים וזליגת מידע בין רשתות ציבוריות (כגון רשת ה- Wi-Fi הציבורית) של המוסד לבין רשתות פנימיות רגישות ביותר (כגון רשת המנהלה המכילה את כלל שרתי הארגון כגון שרת ה- Domain Controller).
- נחשפו בין היתר חולשות אבטחה קריטיות המובילות להרצת קוד מרחוק (RCE) על שרתי מפתח בארגון ואף על רכיבי הגנה קריטיים .

מתודולוגיית מבדק החדירה:

1. איסוף המידע

a. מיפוי הנכסים, השרתים והשירותים בתשתית הנבדקת. וכן המסכים, הקלטים ו ה API ים הרלוונטיים במערכת האפליקטיבית הנבדקת.
b. עיון בקוד מקור המערכת החשוף ציבורית לזיהוי מהיר של בעיות פוטנציאליות.
c. שימוש בכלי OSINT שונים)לרבות כלים פנימיים שפותחו על ידנו, כלים מסחריים, ומגוון מנועי חיפוש(על מנת לעבות את המידע על המטרה הנתקפת לצרכי גילוי וקטורי תקיפה נוספים.
d. שימוש בכלי תשאול ידניים ואוטומטים)כגון nmap, dnsenum, sslscan, netcat ועוד(ובכלי סריקת חולשות)לרבות כלים פנימיים שפותחו על ידנו, וכלים מסחריים כגון Burp Suite Scanner, Nessus (במטרה לדלות עוד מידע באופן אקטיבי ולזהות נקודות תורפה באמצעות סורקים אוטומטים שמחפשים ליקויי אבטחה נפוצים יותר ונפוצים פחות .

2. הערכת סיכונים וניתוח נתונים בשלב זה תבוצע הערכת סיכונים וניתוח הנתונים שנאספו בשלב איסוף המידע על מנת למפות את מרכיבי התכולה הנבדק ת ולשים את האצבע על האזורים הרגישים והמשמעותיים ביותר הן במערכת והן בתשתית.
בשלב זה נלקח בחשבון גם ה Business Logic של הארגון כדי להבין –
1. מאילו שרתים, שירותים ומסכים ו API ים המערכת בנויה, ומה הם הרכיבים במערכת ובתשתית שסביר יותר שיהיו פגיעים להתקפות השונות.
2. אילו סוגי כשלים לוגים או כשלי קונפיגורציה יכולים להימצא במערכת או בתשתיתי שעשויים לגרום לליקוי אבטחתי חמור.
3. האם יש חשד להימצאות חולשה מוכרת או לא מוכרת באחד ממרכיבי המערכת או התשתית, אם כן מה מידת הנזק שהיא עשויה לגרום והאם ניתן לנצלה.

3. בדיקת חדירות מעמיקה בשלב זה אנו חוקרים בפועל את כל המסקנות שהגענו אליהן מניתוח הנתונים שאספנו ומוכיחים את הימצאותם של ליקויי אבטחה וחולשות אבטחה במערכת ובתשתית. בשלב זה יבוצעו טכניקות תקיפה מתקדמות בהתאם לממצאים שעלו משלבי איסוף המידע, ניתוחו וביצוע הערכת סיכונים.
*שיטות החקירה והתקיפה הייחודיות שפיתחנו כוללות למעלה מ- 52 וקטורי תקיפה שונים בהם אנו מתכננים להשתמש על מכלולי הבדיקה.

4. כתיבת דו"ח מפורט. בשלב הזה אנו מייצרים דו"ח מפורט עם כל הממצאים שמצאנו בסעיפים הקודמים, הדו"ח כמובן יכלול גם המלצות מפורטות לטיפול בליקויים האבטחתיים שיתגלו. לאחר הגשת הדו"ח יינתן מענה שוטף לשאלות מקצועיות אודות לדו"ח ולהמלצותיו.

5. בדיקה חוזרת. לאחר יישום המלצות הדו"ח וביצוע התיקונים ע"י הלקוח, תסופק בדיקה חוזרת שנועדה לוודא כי עבור כל ממצא בדו"ח הוטמע תיקון ראוי. הבדיקה תסופק ללא עלות וזאת בתנאי שלא חלפו 90 ימים ממועד שליחת הדו"ח הסופי ללקוח.

תמחור:

- עלות מבדק החדירה נקבעת לאחר שיחת תיחום ייעודית אודות התכולה הנבדקת. על בסיס שיחה זו ניתן לאפיין את הבדיקה ולהחליט מהו מספר ימי הבדיקה הנדרש על מנת לבחון באופן יסודי את התכולה הנבדקת.

- בהצעה זו מתומחר יום בדיקה בודד וכן יינתנו דוגמאות לעלויות של בדיקות בסדרי גודל שונים על בסיס מחיר יום הבדיקה הבודד הנ"ל.
- המחיר הנקוב בהצעה הינו מחיר מיוחד ומותאם עבור סל הטכנולוגיות של מיט"ל.

חברת Clear Gate

פירוט השירותים:

1. מבדקי חדירה (Penetration test) לפי תקן OWASP:
   - עבור אפליקציות אינטרנט
   - עבור אפליקציות מובייל

מתודולוגיית עבודה:

1. פתיחת רישום במערכת על ידי מיט"ל (עד 7 ימי עבודה)
2. הקצאת משאבים ומסגרת זמן (עד 21 ימי עבודה)
3. ביצוע מבדקי חדירה בצורה ידנית ומעמיקה על פי תקן OWASP (עד 21 ימי עבודה)
4. ביצוע הערכת סיכונים ומסירת דוח הממצאים (עד 2 ימי עבודה)
5. יישום התוכנית על ידי מיט"ל/מוסד אקדמי (עד 90 ימי עבודה)
6. ביצוע בדיקה חוזרת כדי לוודא שהמערכת מאובטחת (עד 5 ימי עבודה)
7. מסירת הדוח הסופי ואישור הפעילות (עד 2 ימי עבודה)

תמחור:

מודל התשלום שעתי - העלות הכוללת נקבעת לאחר שיחת תיחום ייעודית אודות התכולה הנבדקת והגדרת מסגרת זמן העבודה הנדרש.

חברת Auren

פירוט השירותים:

להלן רשימת השירותים העיקריים עבור לקוחות מיט"ל:

1. **מבדקי חדירות** –
   - אפליקטיביים – אתרים, מערכות, תוכנות, מובייל ועוד
   - תשתיתיים – פנימיים וחיצוניים
   - חומרה
   - גלי רדיו
   - ועוד מגוון רחב של טכנולוגיות
2. **סקרי סיכונים** –
   - סקרי סיכונים מתודולוגיים
   - סקרי סיכונים טכנולוגיים
3. **הדרכות** –
   - הדרכות מודעות
   - הדרכות פיתוח מאובטח

- הדרכות הנהלה

במקרה של הדרכה ההדרכות שלנו יכולות להיות מאוד תיאורתיות ומאוד טכנולוגיות.

קהל הידע משתנה בין עובדים, סטודנטים, מפתחים, הנהלה.

מתאימים את ההדרכות בהתאם לביקוש.

תדירות נקבעת בהתאם לצורך של הלקוח, וזמינות אנחנו צריכים כשבועיים התראה מראש.

תמחור:

תמחור מרבית הפרוייקטים נעשה בהתאם לצורך ונקבע במהלך פגישה, תוצר הפגישה יוגש במסמך מפורט בעברית (אלא אם מתבקש אחרת). המסמך יכלול:

1. פרטי הבודק
2. תיאור המערכות הנבדקות מתוך כלל מערכות הארגון.
3. סיכום מנהלים - פירוט כללי והסבר באשר לרמת הסיכון של המערכת, כנגזרת מהממצאים.
4. פירוט הממצאים: תאור ופירוט הממצא (לדוגמה: ניתן לפרוץ ומהיכן ניתן), צילומי מסך והמלצות לתיקון ליקויים.
5. מתודולוגיה.

סיכום:

שלוש החברות מספקות שירותי אבטחת מידע ובדיקת פגיעות במערכות למידה, בעיקר מבדקי חדירה למערכות למידה ומספקים סקרי סיכונים מקיפים עם הסבר על רמת הסיכון ודרכי פעולה מומלצות. ההתמחות במערכות למידה מאפשר התמקצעות יחודית הרלוונטית למוסדות החברים במיט"ל.

השוואת רשימת השירותים של החברות	Auren	Fensive	Clear gate
סקרי סיכונים מקיפים	V	V	V
מבחני חוסן אפליקטיביים מתקדמים	V	V	V
מבדקי חדירה תשתיתיים לתשתיות חיצוניות ופנימיות	V	V	V
אופרציות RedTeam מלאות		V	
חבילות מודעות – לומדות, תרגולי דיוג והרצאות	V		

לשלוש החברות ניסיון רחב בעבודה עם מוסדות אקדמיים, עם זאת חברת Fensive מעידה על עצמה כחברה שמתמקדת במבדקי חדירה עבור סקטור האקדמיה, ובכך פיתחה מומחיות יוצאת דופן במבדקי חדירה אפליקטיביים ותשתיתיים למוסדות האקדמיה, בנוסף החברה מציעה צוות תמיכה במצבי חירום בהם נדרשת התערבות חיצונית.