לראות מעבר לגבולות הארגון



מה כבר חשוף על הארגון שלכם?

Cyber Exposure מבית CyberLion מסייע לזהות פרטי גישה, מידע ונכסים נגישים מהאינטרנט הקשורים לארגון שלכם — ולהבין אילו ממצאים דורשים תשומת לב.

מחשיפה חיצונית להחלטות מבוססות מידע

כלי האבטחה שלכם מגנים על הסביבה מבפנים. השירות מוסיף נקודת מבט חיצונית: איזה מידע, חשבונות או פרטי גישה הקשורים לעסק מופיעים במקורות המודיעין שהשירות מכסה?

מה נמצא?	למה זה חשוב?	מה עושים עכשיו?
הבנת החשיפה והקשר שלה לארגון.	בחינת הראיות והסיכון האפשרי.	תעדוף הבדיקה והתגובה.

דומיין אחד. כמה דומיינים. היקף בדיקה מוסכם.

ניתן לרכוש את השירות דרך **ספק שירותים מנוהלים (MSP) או משווק**, עבור דומיין אחד או כמה דומיינים במקביל. אפשר לכלול את הדומיין הראשי, ובכפוף להרשאה ולהסכמה, גם דומיינים של חברות־בת, מותגים או יחידות עסקיות. היקף הכיסוי ואופן הצגת התוצאות יוגדרו לפני הבדיקה.

מתחילים בהערכה. ממשיכים בניטור.

הערכה חד־פעמית מספקת תמונת מצב של הממצאים בהיקף שסוכם. ניטור מתמשך יכול לסייע בזיהוי ממצאים חדשים ושינויים לאורך זמן, בהתאם למסלול השירות שנרכש.

CyberLion Ltd. | טלפון: +972-9-8783333
החרושת 2, כפר סבא, ישראל | ת״ד 2440, כפר סבא 4464002
sales@cyberlion.software | cyberlion.ai

דוח שמסייע להבין — ולפעול

הסבר ברור של הממצאים הרלוונטיים, ההקשר התומך בהם והכוונה מעשית — ולא רק רשימת התראות. התוכן תלוי בראיות הזמינות לגבי הדומיינים שנבדקו.

01 | חשבונות ופרטי גישה שנחשפו

חשבונות ארגוניים או פרטי גישה שנמצאו במאגרי דליפות שנאספו, בראיות הקשורות לנוזקות גניבת מידע או במקורות מנוטרים אחרים, ככל שנמצאו.

הערך עבורכם: זיהוי חשבונות שעשויים לדרוש חקירה, החלפת סיסמה, ביטול חיבורים פעילים או חיזוק האימות. פרטי גישה שנחשפו אינם מוכיחים שבוצעה כניסה למערכות או שהסיסמה עדיין תקפה.

02 | מידע חשוף ואזכורים של הארגון

אזכורי מידע, הצעות למכירת גישה או ראיות אחרות הקשורות לדומיינים, למותגים ולחשבונות שבהיקף הבדיקה.

הערך עבורכם: בסיס לבדיקת חשיפה אפשרית של מידע. פרסום בפורום או טענה למכירת גישה אינם כשלעצמם אירוע פריצה מאומת; יש לבחון את אמינותם ואת הרלוונטיות שלהם.

03 | נכסים נגישים מהאינטרנט

נכסים הנראים מבחוץ ומשויכים לדומיינים שנבדקו.

הערך עבורכם: בדיקה אם הנכסים מוכרים, שייכים לארגון ומנוהלים כראוי. הצוות שלכם או ספק השירות צריכים לאמת שיוכים שאינם ודאיים — שיוך אינו הוכחת בעלות.

04 | ראיות והקשר

מידע תומך המסביר את הממצא. בהתאם למקור, הוא עשוי לכלול מזהים שהושפעו, הקשר המקור ותאריכים רלוונטיים.

הערך עבורכם: הבחנה בין ממצא משמעותי לבין רשומה היסטורית, כפולה או כזו ששויכה לארגון בטעות, והחלטה מה דורש בדיקה נוספת.

05 | סדרי עדיפויות וצעדים מעשיים

הסבר למשמעות הממצאים והכוונה לתעדוף התגובה.

הערך עבורכם: העברת הטיפול לגורם המתאים — בדיקת חשבון, חקירת אזכור מידע, בחינת נכס חשוף או תיאום פעולה עם ספק השירות או המשווק.

להנהלה: ממצאים מרכזיים והחלטות נדרשות. **לצוותי IT ואבטחת מידע:** ראיות להמשך בדיקה. **לספק השירות או למשווק:** בסיס לפירוש הממצאים ולתכנון התגובה.

רוצים להבין את החשיפה של הארגון שלכם?

פנו לספק השירות, למשווק או ל־CyberLion לתיאום בדיקה של דומיין אחד או כמה דומיינים.

חשוב לדעת: אין בדיקה המבטיחה גילוי של כל החשיפות. השירות אינו מחליף מבדק חדירה. תיקון הממצאים הוא פעילות נפרדת, אלא אם נכלל בהסכם. תדירות הניטור, מבנה הדוח והתוצרים נקבעים לפי השירות שהוזמן.

CyberLion Ltd. | טלפון: +972-9-8783333
החרושת 2, כפר סבא, ישראל | ת״ד 2440, כפר סבא 4464002
sales@cyberlion.software | cyberlion.ai