SolarWinds זה גם Security

בראיון עם ליאור לוי, מנכ"ל ומייסד פרולוג'יק (Prologic), נציגת SolarWinds בישראל, הוא מציג את פורטפוליו הפתרונות של החברה לעולמות הגנת הסייבר. "גם בתחום הסייבר ואבטחת המידע SolarWinds מביאה פתרונות פשוטים, יעילים ובעלויות נוחות", הוא מציין | **רועי נוימן**

בים מכירים את חברת SolarWinds כאחת מספקיות הטכנולוגיה המובילות בעולמות של ניטור וניהול תשתיות ה-IT הארגוניות. הפלטפורמות של החברה הפכו כבר לסטנדרט בעולמות ניטור הרשת הארגונית, ולמעלה מ-275 אלף ארגונים ברחבי העולם בחרו בפתרונות ניהול ה-IT של SolarWinds. "מה שמקצועני IT פחות מכירים זה את פורטפוליו הפתרונות העשיר של החברה בעולמות ה-Cyber Security", מציין **ליאור לוי**, מנכ"ל ומייסד פרולוג'יק (Prologic), נציגת SolarWinds בישראל, בראיון עימו. "ארגונים שניסו את פתרונות הסייבר של SolarWinds התאהבו בפתרונות הללו, ממש כשם שהם התאהבו בפתרונות ניטור הרשת של החברה. הבסיס הוא אותו בסיס - לה־ביא לשוק פתרונות פשוטים בהפעלה שלהם, יעילים בפונקציונליות שלהם, וביחס עלות-תועלת גבוה".

פתרון ה-SIEM של SolarWinds

קחו לדוגמא את פתרון ה-SIEM של החברה - SolarWinds Security Event Manager, המכונה בראשי התיבות SEM. פתרון זה מצטיין בפשטות, עוצמת הגנת סייבר גבוהה ועלות נוחה. הפתרון מסייע למקצועני אבטחת המידע להדק את חומות הסייבר מסביב לארגון, באמצעות יכולות ניראות גבוהות יותר לתוך פעילות הרשת הארגונית. הפתרון, שהושק במאי השנה ואשר מחליף את הפתרון SolarWinds Log & Event Manager, מאפשר לאסוף ולנתח לוגים המיוצרים ברשת הארגונית במקום מרכזי אחד, לזהות ולהגן מפני איומי סייבר מתקדמים, לספק מענה להתקפות סייבר ולסייע בציות לדרישות רגולטוריות. המערכת אף מאפשרת להעביר לאוטומציה פעילויות רבות שמבצעת מערכת SIEM מסורתית.

ליאור לוי, מנכ"ל ומייסד פרולוג'יק | צילום: נדב כהן יונתן

"המערכת של SolarWinds מזהה פעילות חשודה בזמן אמת ומתריעה מפני איומי סייבר", מפרט לוי. "היא מגיבה בצורה עצמאית כאשר היא מזהה פעילות חשודה ברשת - בין אם זה חסימה אוטומטית של כתובת IP חשודה, ובין אם זה שינוי הרשאות, השבתה של חשבונות חשודים, חסימה של מכשירי USB ועוד", מדגיש לוי, "אך באותה עת היא גם מספקת התאמה לרגולציה עם תאימות מלאה ודו"חות מקיפים המיועדים לספק שקט נפשי בתהליכי ביקורת עבור PCI, HIPPA, DSS, SOX, FISMA, ISO ורגולציות נוספות".

התמודדות עם איומים מבפנים

דוגמא נוספת הינה פתרון SolarWinds Access Rights Manager, המכונה בראשי תיבות ARM - הפתרון המיועד לספק מענה מפני האיום "מבפנים", המוכר בשם Insider Threats. הפתרון מאפשר ניהול אוטומטי של ההרשאות בארגון, כולל אנליטיקה המסייעת בזיהוי חריגים ואכיפה של מדיניות ארגונית. המערכת מציעה פורטל self service למשתמשים, דבר שמוריד מנטל ההתעסקות בנושא של אנשי ה-IT, ובנוסף מספק יכולות ניטור של גישת המשתמשים למערכות הארגוניות, ויכולת לייצר במהירות דו"חות המיועדים לרגולציה של תחום המשתמשים הפנימיים.

לוי מדגיש, כי "המציאות והרגולציה מחייבות את הארגונים להיזהר לא רק מפני איומי האקרים המנסים לחדור לתוך הארגון מבחוץ. תרחישי הסיכון כוללים גם עובדים, או גורמי פנים נוספים, שנדרש לוודא שההרשאות שלהם לכניסה למערכות הארגוניות נאכפות, שאין עובד הנחשף למידע שהוא לא רשאי לראותו, ושעובד אינו מוציא מידע מחוץ לארגון. כולנו זוכרים את המקרה של ענת קם, שבמהלך שירותה הצבאי בלשכת מפקד פיקוד מרכז נחשפה ואספה אלפי מסמכים, שבהמשך נמסרו ופורסמו בתקשורת".

SolarWinds ופרולוג'יק - Better Together

SolarWinds פעילה כיום ב-190 מדינות, וכ-275 אלף ארגונים ברחבי העולם הטמיעו את פתרונות החברה. על לקוחותיה נמנים 425 מארגוני US Fortune 500, כולל עשר חברות הטלקום הגדולות בארה"ב, חמש זרועות הצבא האמריקאי וחמש פירמות ראיית החשבון הגדולות, לצד מאות אוניברסיטאות וקולג'ים. במגזר הממשלתי-ציבורי האמריקאי ניתן לציין ארגונים דוגמת: משרד נשיא ארה"ב, הפנטגון, State Department, NASA, NSA, הדואר האמריקאי וגופים אחרים.

בישראל הפכה SolarWinds לסטנדרט בשוק הישראלי, עם מערך מסועף של אינטגרטורים ומיישמים, הפעילים הן בעולמות ביצוע הפרויקטים והן בעולמות השירות והתחזוקה של הסוויטה. "אחד הגורמים להצלחה בישראל", מספר לוי, "הוא התעדוף שאנו מקבלים במטה האזורי של החברה באירלנד, כולל ביקורים סדירים שלהם בארץ ושלנו במשרדי החברה באירלנד. ישראל בהחלט נחשבת שוק צומח ובעל פוטנציאל גידול, ובהתאמה המשאבים שמשקיעה החברה בארץ".

פרולוג'יק, מסכם לוי, מעסיקה כיום למעלה מ-300 עובדים. "החברה פעילה בשלושה תחומים מרכזיים. הראשון, מתן שירותי מיקור-חוץ, שירותים מקצועיים, יועצים והטמעת מערכות במגוון רחב של תחומי תוכנה ו-IT. השני, 'תפירת' חליפה מותאמת לסטארט-אפים ממוקדת בתחום פיתוח תוכנה, AI ו-Machine Learning. השלישי, נוגע בייצוג בישראל של חברות טכנולוגיה גלובליות, דוגמת פתרונות SolarWinds, וספקיות טכנולוגיה גלובליות נוספות בתחומי התשתיות והסייבר".

להבטיח רציפות בפעילות הארגון

"היופי של פלטפורמת SolarWinds הוא ההתאמה שלה גם לארגוני ענק גלובליים וגם לארגונים קטנים", מציין ליאור לוי, מנכ"ל ומייסד פרולוג'יק. "הצורך הבסיסי בשני המקרים הוא אחד - להבטיח רציפות בפעילות הארגון ולהפוך סביבה מורכבת לכזו המנוהלת בפשטות. אף ארגון לא יכול להרשות לעצמו תקלות ברשת הארגונית, זה צורך בסיסי, זה מחזור הדם של הארגון, וזה אחד האתגרים הבסיסיים עימם מתמודד המנמ"ר כיום".