



שרות חדש בווי אנקור : מרכז SIEM-SOC מנוהל

זמינות, אמינות, מיקוד

אתגרי אבטחת המידע הולכים ומתעצמים. בכל יום אנו עדים להתראות ולכתבות נוספות על איומים, תקיפות, אובדן וגניבת מידע, התקפות כופר ועוד.

המודעות לנושא אבטחת המידע, הצורך בהקמת תוכנית ארגונית הוליסטית, והקריטיות של תשתיות האבטחה לתהליכים העסקיים בארגון הולכת ומתעצמת.

החוקים והרגולציות מתאימים עצמם לדרישות התקופה, היום, יותר מבעבר מושם דגש לתוכנית אבטחת המידע הארגונית וחובת הארגון לנהל מרכז בקרת אבטחת מידע (SOC) מעוגן במחויבות רגולטיבית (257, 357, PCI, SOX) במגזרים רבים.

חטיבת אבטחת המידע השיקה שירות SIEM SOC AS A SERVICE, מזה 12 שנה ווי אנקור הינה השחקן המוביל בשוק הישראלי בתחום ניהול אירועי אבטחת המידע עם למעלה מ-100 לקוחות בארץ ובעולם והקמה של 12 מרכזי סייבר מבוססי Arcsight, לפני שלוש שנים השקנו שירותי SIEM בענן על מנת לתת שרות נרחב יותר ללקוחות החברה. השירות מבוסס על תשתית WE-CLOUD ומערכות ארכסיט מתקדמות. התקפות הסייבר אשר הולכות ומתעצמות מצריכות מכל ארגון שרכש SIEM או משתמש בשרות ענן להקים SOC (עצמאית או באמצעות שרות חיצוני). אנו שמחים לבשר על השקת שירותי SOC בענן אשר מהווה נדבך נוסף לשירותי SIEM. שירותי SOC בענן מספק פתרון מיידי עם זמן הקמה מינימלי ובעלות על פי שימוש. הידע הרב בשילוב עם הכלים הנכונים אפשרו לנו להקים מרכז סייבר לניהול אירועי אבטחת מידע וצוות תגובה למענה בעת אירוע. המענה מיועד לארגוני Enterprise/SME/SMB אשר יאפשרו להם ליהנות מהטכנולוגיות המובילות בעולם אבטחת המידע, ומהניסיון הרב של צוות יועצי אבטחת המידע שלנו כשירות 24x7.

פתרון ווי-אנקור לשירות המנוהל בענן, פותר את הארגון מהצורך להתמודד עם האתגרים בהקמת SIEM - SOC מקומי:

- יכולת ממשק לכלל המערכות הארגוניות החל בתשתיות ה-IT, שערי יציאת המידע מהארגון וכלה באפליקציות השונות ולתשתיות הפיזיות כגון שערים, דלתות וכו'
- זיהוי אירועי סייבר בזמן אמת תוך כדי ביצוע קורלציות חכמות בין מערכות
- זיהוי אנומאליה ברמה ארגונית על ידי ה-SOC
- צוות CERT לתגובה מהירה בעת אירוע, חקירות מחשב וניתוח אירוע לאחר מעשה.
- הצפת מידע – ברירת המידע הרלוונטי מכמות המידע העצומה המועברת והנאגרת במערכות
- נהלים, ארגון ושיטות (או"ש), תהליכים עסקיים ונהלי עבודה
- עמידה בדרישות התקנים השונים