SCADAfence – הגנת סייבר למפעלים תעשייתיים

אודות החברה

חברת סקאדהפנס (SCADAfence) הוקמה בשנת 2014 ע"י יוצאי היחידה הטכנולוגית של חיל מודיעין ע"מ לספק מוצרי הגנת סייבר למגזר התעשייתי. החברה ממוקמת בפארק הסייבר בבאר שבע וממומנת ע"י קרן ההשקעות הגדולה בישראל JVP וע"י המדען הראשי. פתרונות החברה נמכרים ומיושמים כיום ברחבי העולם במגוון תעשיות – החל מתעשיות ייצור בתחומי המזון, התרופות, הבטון ועוד, וכלה תשתיות קריטיות בתחומי החשמל והמים וכדומה. לחברה התקנות בצפון אמריקה, אירופה, אסיה ובישראל כמובן.

תיאור הפתרון

המוצר של חברת SCADAfence, Continuous Network Monitor (CNM) , הינו מוצר תוכנה בלבד המנטר באופן רציף ומתמשך את הרשת התעשייתית (ICS/SCADA/DCS/BMS). הטכנולוגיה הינה פאסיבית, כלומר אינה מסכנת את רציפות התהליך (ייצור, בקרה, וכו'), ובאמצעותה ניתן לנטר את הפעילות היומיומית המתרחשת ברשת המפעל. במהלך הניטור אנו מנתחים את התעבורה ברשת וכאשר אנו מגלים פעילות חריגה (אנומליה), המערכת מתריעה עליה. ניתן להעביר את ההתרעות למערכות יעודיות המאגדות את כלל ההתרעות בארגון כדוגמת מערכת SIEM או למערכות הגנה קיימות של חברות כמו צ'קפוינט, ואף לשלוח הודעות מייל/SMS לבעלי תפקידים רלוונטיים בארגון. ההתקנה פשוטה ואינה מצריכה הפסקת תהליכים. כמו כן, המערכת לומדת באופן אוטומטי את התנהגות הרשת, אינה מצריכה הגדרות ו-configuration מהמשתמש ואינה מעמיסה את הצוות במפעל או בחברה בעבודה מיותרת.

הערך המוסף למפעל המיישם

Asset Inventory

אין אפשרות להגן על מה שאינך יודע מספיק או בכלל אודותיו. המצור מחליף את הרישומים הידניים (Excel ו/או מסמכים) המתעדים את מבנה ורכיבי הרשת ומאפשר דיגיטציה מלאה של מצאי הרכיבים כולל מפת החיבוריות ופרוטוקולי התקשורת.

ניהול סיכוני סייבר

סקאדהפנס מתריעה על סיכונים בצורת הפעולה של הרשת שבמידה ולא יטופלו, יוכלו להפוך לאיום או תקלה המשביתה את פעילות המפעל. לדוגמא, כאשר עובד מחבר את רצפת הייצור ישירות לאינטרנט.

גילוי מתקפות ותקלות

אנו מתריעים במקרה של תקיפה זדונית ואף במקרה של תקלה או טעות תמימה (טעות אנוש) שיכולה להסב נזק. לדוגמא, כאשר מתקפה (כדוגמת מתקפת כופר / ransomware) תוקפת את המפעל.

מקרי בוחן (Case Studies)

מפעל לייצור תרופות – גילינו נוזקה (Malware) על רכיב האחראי על ניהול הציוד התעשייתי שחדרה לרשת כתוצאה מחיבור לא מורשה בין רשת המפעל לרשת ה-IT.

מפעל לייצור מזון ומשקאות – גילינו שחומת האש הארגונית (Firewall) אינה מוגדרת כראוי ומאפשרת גישה בלתי מוגבלת מרשת ה-IT לרשת המפעל.

מפעל המריץ תהליכי ייצור כימיים – גילינו שבניגוד לנהלים, העובדים חיברו את רשת המפעל ישירות לאינטרנט כדי לעדכן תוכנות הרצות בתוך רשת הבקרה.

© Confidential and Proprietary Information of SCADAfence Ltd.