CONTEL
BEYOND TECHNOLOGY

הגנת סייבר ל- OT, תשתיות ו- IT

החטיבה להגנת סייבר ל- OT, תשתיות ו- IT של קבוצת קונטאל משלבת ניסיון של 60 שנות מומחיות ביישום מערכות בקרה ואוטומציה והבנה מעמיקה של צורכי התעשייה הישראלית.

מלווים פרויקטים מורכבים ומאתגרים במגוון תעשיות: תחנות כח, תחנות גז ואנרגיה מתחדשת ומתקנים לייצור אנרגיה ותשתיות, מפעלים פטרוכימיים, מפעלים בתעשיית הפלסטיק, מפעלי מזון ומפעלי תרופות.

בין לקוחותינו: תחנת כח אתגל, מתקן אנרגיה סולארית חלוציות, דוראד, רשות שדות התעופה, עשרות אתרים סולארים בישראל, EDF, שיכון בינוי, TeraLight, מקסימה, רש"ת, אנלייט אנרגיה מתחדשת, logisticare, נגב אשלים ועוד.

החזון שלנו הוא לאפשר את הרציפות התפעולית של לקוחותינו באמצעות שילוב בין ניסיון רב שנים ואינטגרציה של מערכות בקרה, ליישום טכנולוגיות מתקדמות להבטחת זמינות, אמינות וסודיות המידע במרחב הסייבר התפעולי.

הצוות שלנו מורכב ממומחים בעלי ניסיון ייחודי באפיון, אינטגרציה והטמעה של פתרונות אבטחת מידע ל-OT, בהתאמה לצרכי הלקוח והתעשייה, דרישות הרגולציה ולתוצאות סקר הסיכונים ובדיקות חדירות או להמלצות יועץ חיצוני.

אנו פועלים בהתאמה לתקנים המחמירים ביותר, כגון: תו תקן ISO27001 ו- ISO62433 ועובדים בשיתוף מלא עם מערך הסייבר הלאומי, משרד האנרגיה, המשרד להגנת הסביבה ורשות המים.

קונטאל שותפה בפורום הסייבר של התאחדות התעשיינים בישראל (MAI).

שותפים עסקיים:

CISCO · GATESCANNER by Sasa Software · OPSWAT · Terafence IoT Cyber Security · WATERFALL Stronger Than Firewalls

CHECK POINT · SIGA Level Zero OT Resilience · FORTINET · veeam · Rockwell Automation

CONTEL
BEYOND TECHNOLOGY

מערכות איתור חדירות (IDS)

הגנת עומק לרשתות ייצור ותשתיות קריטיות

במפעלים ובמתקני תשתיות, כל חריגה בתנועת הרשת עלולה להשפיע על תהליכים, כדוגמת שינוי פרמטרים בבקרים, עצירת משאבות, הפעלה לא רצויה של ציוד או פגיעה באיכות הייצור. לכן קונטאל משלבת מערכות IDS ייעודיות לסביבות OT, המזהות בזמן אמת ניסיונות חדירה, תעבורה חריגה ופעולות שאינן תואמות את דפוסי העבודה התקינים של רשת הבקרה.

מותאמות לפרוטוקולים תעשייתיים נפוצים ולתצורות רשת מורכבות במתקני מים, אנרגיה, תהליכי ייצור מורכבים, פארמה, מזון ותשתיות לאומיות. מערכות כאמור פועלות ללא הפרעה במסגרת תהליכי הייצור, מתריעות מוקדם על אנומליות, ומאפשרות לצוותי המפעל או האתר להגיב לפני שהאיום מתפתח לאירוע תפעולי.

התוצאה: שכבת זיהוי שמחזקת את ההגנה על רשתות ה־OT ומבטיחה רציפות, יציבות ובטיחות בסביבות הקריטיות ביותר.

CONTEL
BEYOND TECHNOLOGY

מתגים וחומות אש
Industrial Switces & Firewalls

רשתות בקרה תעשייתיות נדרשות לפעול ברציפות, לעמוד בעומסים גבוהים ולעבוד בתנאי שטח מאתגרים שכוללים חום, רעידות, לחות ובתנאים סביבתיים נוספים. לכן, כל כשל ברשת עלול להשפיע על תהליך הייצור, לרבות על מערכות האנרגיה, אספקת המים וגם על תשתיות קריטיות. לכן הבחירה במתגים תעשייתיים (Industrial Switches) ובחומות אש ייעודיות ל־ OT היא קריטית ליציבות ולביטחון התפעולי.

קונטאל מספקת פתרון מקיף הכולל תכנון, הטמעה ותחזוקה של מתגי תקשורת וחומות אש תעשייתיים, המותאמים למערכות MES, HMI, PLC, SCADA ולתצורות רשת מורכבות במפעלים ובמתקני תשתיות.

מתגים תעשייתיים, עמוד השדרה של רשת ה־OT:

המתגים התעשייתיים שקונטאל מטמיעה מיועדים לעבודה רציפה מסביב לשעון ובנויים לעמוד בתנאי סביבה קשים.

מתגים תעשייתיים אלו תומכים ב:

- תקשורת יציבה בפרוטוקולים תעשייתיים
- יתירות (Redundancy) מלאה כולל RSTP/DRP/MRP
- ניהול מרכזי וניטור סטטוס בכל רגע נתון
- סגמנטציה של רשתות בקרה למניעת התפשטות תקלות
- התקנה בארונות בקרה, בשטח או בחדרי תקשורת ייעודיים

היתרון: בנית רשת תקשורת יציבה שמבטיחה שהבקרים, יחידות השדה, המחשבים וחדרי השליטה ימשיכו לפעול באופן חלק.

חומות אש תעשייתיות (Industrial Firewalls) הגנה לרשת הבקרה:

בעולמות ה־ OT חומת אש רגילה אינה מספיקה.

קונטאל מטמיעה חומות אש המיועדות לסביבה תעשייתית, יחד עם:

- זיהוי פרוטוקולים תעשייתיים (DPI – Deep Packet Inspection)
- חסימת פקודות מסוכנות לבקרים
- ניהול גישה מרחוק מאובטח לספקים וצד שלישי
- הפרדה בין רשת ה־IT לרשת ה־OT באמצעות DMZ תעשייתי
- סגמנטציה לפי אזורי אבטחה (Zones & Conduits)
- מניעת חדירת קוד זדוני ותעבורה חריגה

אלו מספקות שכבת הגנה משמעותית שמונעת מניפולציות על תהליכי ייצור ומצמצמת את הסיכון לתקיפות סייבר.

הפתרון של קונטאל, שילוב מושלם בין תקשורת לבקרה:

קונטאל מבצעת אינטגרציה מלאה בין מתגי התקשורת, חומות האש ומערכות הבקרה הקיימות, תוך הבנה עמוקה של מבנה המפעל והצרכים התפעוליים.

הפתרון כולל:

1. אפיון והנדסת רשת OT/IT משולבת
יצירת ארכיטקטורה יציבה, מאובטחת ומתאימה לתהליכי הייצור.

2. הטמעה בשטח והקשחת ציוד
התקנה בארונות בקרה, בחדרי תקשורת או בסביבה הפתוחה, הכל בהתאם למבנה האתר.

3. ניהול סגמנטציה ואבטחה
חלוקת הרשת לאזורים, הגדרת תנועת נתונים מאושרת וחסימת תעבורה לא רצויה.

4. ניטור, תחזוקה ושדרוגים שוטפים
תחזוקה מונעת, בדיקות תקופתיות, עדכוני אבטחה ובקרה על ביצועי הרשת.

עם קונטאל, הכל משתלב בצורה מדויקת בתוך מערכות הבקרה והתפעול של האתר, ומאפשר פעילות מאובטחת ויעילה לאורך זמן.

CONTEL
BEYOND TECHNOLOGY

סקרי אבטחת מידע

בעולם שבו מערכות ייצור, אנרגיה, מים ותשתיות קריטיות מתחברות לרשתות IT, לשירותי ענן ולמערכות חכמות, הסיכונים גדלים באופן ישיר, אשר על כן, הצורך בהבנה מדויקת של מצב האבטחה בפועל הופך חיוני יותר. סקר אבטחת מידע מהווה את הצעד הראשון ליצירת שכבת הגנה יציבה המציגה את נקודות התורפה, מנתחת את הסיכונים ומציגה תוכנית פעולה מפורטת לשיפור.
קונטאל מבצעת סקרי אבטחת מידע ייעודיים לסביבות תעשייה ו־OT, הכל תוך דגש על שמירה על זמינות, בטיחות ויציבות תפעולית.

מה כולל סקר אבטחת המידע של קונטאל?

1. מיפוי מלא של הנכסים ורשתות התקשורת:
זיהוי שרתים, תחנות עבודה, בקרים, ציוד תקשורת, מערכות SCADA, רשתות משנה וחיבורי צד ג'.
הינם רק חלק מהנכסים שממופים על ידי קונטאל.
יש לשים דגש על הבנת התמונה האמיתית בשטח.

2. בחינת חולשות וסיכוני אבטחת סייבר:
איתור נקודות מוחלשות כגון:
- גישה מרחוק אשר אינה מבוקרת
- חיבורים בין רשת IT ל־ OT
- פרוטוקולים לא מוצפנים
- עדכונים חסרים
- הגדרות רשת מסוכנות
- הרשאות עודפות

3. בדיקת תהליכי עבודה וניהול:
הערכת נהלים, מתודולוגיות תחזוקה, ניהול משתמשים, תיעוד תצורות ועמידה בסטנדרטים פנימיים ורגולטוריים.

4. בחינת תרחישים וסקרי סיכונים (במידת הצורך, ללא פגיעה בייצור):
בדיקה האם מדובר באירוע סייבר או בתקלה רשתית שעלולים להשפיע על תהליך קיים, על איכות המוצר או על יציבות כלל המערכת.

5. הפקת דוח מקיף עם ממצאים, סדרי עדיפויות ותכנית עבודה:
הצגת תמונה ברורה של:
- מה דחוף?
- מה מסוכן?
- מה ניתן לתיקון מהיר?
- אילו תהליכים דורשים שינוי והתאמות?
- ואילו בקרות יש להוסיף כדי להגיע להגנה מיטבית?

למה לבחור בקונטאל לביצוע סקר אבטחת מידע?

התמחות עמוקה בסביבות OT ו־ICS:
בניגוד לגופי אבטחה כלליים, קונטאל מכירה היטב מערכות שליטה ובקרה, SCADA, PLC ותקשורת תעשייתית, ולכן הסקר מותאם למציאות התפעולית, לא רק להיבטי IT.

ללא פגיעה בתהליך הייצור:
סקר אבטחת המידע מתבצע בשיטות בטוחות המונעות עצירות, עומסים או שינויים המשפיעים על קווי ייצור ובכך אין פגיעה בתהליך הייצור.

הרמוניה של סייבר, הנדסה ובקרה:
הצוותים של קונטאל בעלי ניסיון רב ומגיעים מרקע הנדסי ותפעולי, מה שמבטיח הבנה מעמיקה של השפעת כל סיכון ולא רק סיכונים הקיימים במרחב הדיגיטלי.

התאמה לתקני אבטחה בינלאומיים:
הסקרים מבוצעים בהלימה לסטנדרטים כמו NIST, IEC 62443 ודרישות רגולציה רלוונטיות.

תוכנית פעולה ישימה:
הדוח כולל לא רק את רשימת הבעיות, אלא מספק גם מפת דרכים ברורה וסדורה, שמתורגמת לפרויקטים, נהלים ושיפורים שניתן ליישם בפועל.
לסיכום, סקר אבטחת המידע של קונטאל מעניק לארגון תמונת מצב אמיתית, עדכנית וברורה של רמת האבטחה, ומייצר בסיס איתן להמשך בניית שכבות הגנה, שיפור תהליכים והיערכות לאיומי סייבר, הכל תוך שמירה על היציבות התפעולית של ליבת העשייה התעשייתית.

CONTEL
BEYOND TECHNOLOGY

הגנה על רשתות OT

רשתות OT הפכו יעד מרכזי למתקפות סייבר משום שהן מחברות בין מערכות בקרה קריטיות, כדוגמת PLCs, SCADA, מכשור שדה ומערכות אנרגיה, לבין עולמות ה IT והענן. החיבוריות הזו, שהתרחבה משמעותית בשנים האחרונות לצורך ניתוח נתוני זמן אמת ושיפור תהליכי ייצור, מייצרת נקודות כניסה רבות יותר לתוקפים. בנוסף, מערכות OT נבנו היסטורית עבור יציבות וזמינות ולא עבור אבטחת מידע, ולכן הן פועלות לעיתים ללא הצפנה, ללא מנגנוני הרשאות מתקדמים וללא עדכונים שוטפים. שילוב זה של רשת חשופה, טכנולוגיה תהליכית ישנה ותלות גבוהה בנתונים בזמן אמת הופך כל תקיפה לאירוע אשר משפיע באופן ישיר ושעשוי לכלול: השבתת קו ייצור, שינוי פרמטרים תהליכיים או פגיעה בבטיחות. אשר על כן, רשתות OT נמצאות היום בחזית הזירה של מתקפות כופרה וסייבר תעשייתי.

מדוע צריך הגנה מיוחדת לרשתות OT?

עפ"י ניסיון גדול בשטח, ניתן להסיק שרשתות OT:

- חייבות זמינות גבוהה ולרוב אינן יכולות להיעצר לצורך תחזוקה.
- נשענות על פרוטוקולים תעשייתיים ישנים ולעיתים לא מוצפנים.
- פועלות שנים ארוכות ללא עדכוני תוכנה.
- כל שינוי קטן עלול להשפיע על בטיחות, איכות וייצור.

אשר על כן, הגנת OT דורשת גישה אחרת, זהירה יותר, תהליכית, שכוללת הבנה עמוקה של סביבת הבקרה.

איך ניתן להגן על רשתות OT?

קונטאל משלבת ניסיון של עשרות שנים בעולמות בקרה, אנרגיה ואוטומציה יחד עם יכולות מתקדמות של אבטחת מידע. הגישה שלנו מבוססת על ארבע שכבות מרכזיות:

1. נראות מלאה של רשת הבקרה:

יצירת תמונת מצב מלאה של כל נכסי ה OT שכוללת בין היתר: בקרים, תחנות הנדסה, שרתי SCADA, מתגים, מערכות תקשורת, אפליקציות תפעוליות ועוד.

המטרה: לדעת "מי מדבר עם מי" ולזהות חריגות לפני שהן הופכות לאירוע.

2. תכנון רשת מאובטחת מותאם מפעל

הפרדה בין IT ל-OT, יצירת אזורי אבטחה (Zones) תעשייתיים, ניהול גישה מבוקרת מרחוק, וחיבור בטוח בין PLCs, SCADA, מערכות MES וענן.

הארכיטקטורה נבנית תמיד לפי הצרכים התפעוליים ולא לפי תבנית גנרית.

3. הגנה בזמן אמת על תהליכי הייצור
ניטור תעבורת OT, זיהוי שינויים בפרמטרים תהליכיים, התרעות על הוראות פיקוד חריגות, הגנה על פרוטוקולים תעשייתיים, וגילוי מוקדם של התנהגות לא תקינה בבקרים ובתחנות ההפעלה.

4. חוסן תפעולי והתאוששות מהירה
גיבוי קונפיגורציות, נהלי התאוששות מסודרים, ותרגול צוותי הייצור, התחזוקה והבקרה, הכל כדי לוודא שגם במקרה של אירוע סייבר או תקלה, המפעל יחזור לפעול במהירות.

מה מבדל את קונטאל?

- ניסיון שטח אמיתי במאות מפעלים ותשתיות.
- שילוב מלא בין עולמות בקרה, חשמל, ICS ו- Cyber – והכל בלי ניתוק בין IT ל-OT
- ידע תהליכי המאפשר להבין את ההשפעה המדויקת של כל סיכון על הייצור.
- יכולת אינטגרציה מלאה עם מערכות קיימות: ERP, MES, SCADA, אנרגיה, ענן ועוד.
- ליווי מקצה לקצה – אבחון, תכנון, הטמעה, ניטור והדרכה.

לסיכום,
הגנה על רשתות OT אינה פרויקט, אלא תשתית שמאפשרת לתעשייה להתקדם בבטחה לעולמות של ענן, אוטומציה וטכנולוגיה חכמה.
עם קונטאל, ארגונים מקבלים שכבת הגנה המותאמת בדיוק לסביבה התפעולית שלהם כזו שמבטיחה יציבות, רציפות ייצור ושקט ארגוני אמיתי.

CONTEL
BEYOND TECHNOLOGY

פתרונות למעבר נתונים חד כיווני (דיודות נתונים)

שומרים על רשתות הבקרה מבלי להתפשר על זרימת המידע:

בעידן שבו רשתות בקרה תעשייתיות (OT) נדרשות להתחבר למערכות ארגוניות, לשירותי ענן ולספקי מידע חיצוניים, גוברת מדי יום החשיפה לסיכוני סייבר. בפועל, כל חיבור דו כיווני עלול לשמש כנתיב חדירה חזרה אל מערכות הייצור, דבר שעלול לגרום בין היתר להשבתת קווים, פגיעה באיכות התהליך ואף לסיכון בטיחותי. לכן פתרונות מעבר נתונים באופן חד כיווני (דיודות נתונים) הפכו חיוניים ומאפשרים להעביר נתונים החוצה בצורה בטוחה, מבלי לאפשר בשום דרך תנועה חוזרת פנימה.

איך זה עובד?

דיודת נתונים מבוססת על מנגנון המאפשר זרימת מידע באופן חד־כיווני בלבד.
מהיכן? לדוגמא ממערכות תפעוליות כמו MES, PLC, SCADA ושרתי היסטוריאן אל רשתות IT או מערכות חיצוניות. אין אפשרות טכנית לבצע תקשורת בכיוון ההפוך, ולכן רשת הבקרה נותרת מבודדת ומוגנת.

הפתרון של קונטאל

קונטאל מטמיעה פתרונות חד־כיווניים כחלק ממעטפת אבטחת OT רחבה, המותאמת למפעלים ולמתקני תשתיות:

1. אפיון וארכיטקטורת רשת מותאמים אישית:
הגדרת ואפיון הנתונים שצריך להעביר, ניתוח פרוטוקולים, קביעת נקודות חיבור ובחירת סביבה אופטימלית לשילוב הפתרון.

2. אינטגרציה מלאה עם מערכות הייצור:
שילוב הדיודה עם מערכות כמו MES, SCADA, היסטוריאן, מערכות אנרגיה ופתרונות בקרה נוספים, ללא שינוי תהליכים או פגיעה בתפקוד.

3. התקנה והעלאת הרף ברמת תשתיתית:
התקנה פיזית מבוקרת, הקשחת רשת, הגדרת מסלולי נתונים והבטחת בידוד מוחלט בין הרשתות.

4. תחזוקה, ניטור ושדרוג מתמשכים:
מעקב תקופתי, בדיקות תקינות, עדכוני תצורה ושילוב הפתרון כחלק מתוכנית הגנת OT כוללת.
יתרונות מרכזיים:

- הגנה מלאה מפני חדירה לרשת ה־OT
- שמירה על רציפות תפעולית ויציבות תהליך
- העברת נתוני זמן אמת ל־IT, BI וענן בלי לסכן את המפעל
- פתרון פיזי שלא תלוי בעדכוני תוכנה
- תואם תקני אבטחת מידע תעשייתית ודרישות רגולציה

לסיכום, פתרונות מעבר נתונים באופן חד כיווני מעניקים למפעלים ולתשתיות את השילוב הנדיר בין גישה לנתונים לבין הגנה מוחלטת על רשת הבקרה, וקונטאל יודעת ליישם אותם בצורה מדויקת, בטוחה ומשתלבת בתוך תהליכי הייצור.

CONTEL
BEYOND TECHNOLOGY

שרתים ועמדות עבודה

התשתית שמחזיקה את המפעל ואת מערכות הבקרה

שרתים ועמדות עבודה הינם המרכיב המרכזי בכל סביבת בקרה, ייצור וניהול תעשייתי. בעולמות שבהם זמינות, אמינות ומהירות תגובה קובעים את היכולת של הארגון לייצר, לפקח ולנהל תהליכים בזמן אמת, האיכות של התשתית המחשובית משפיעה באופן ישיר על הביצועים ועל היציבות התפעולית. בסביבה שבה כל שנייה של עצירה מתורגמת לעלות כספית גבוהה, תשתית מחשוב יציבה, מאובטחת ומתוחזקת היטב היא תנאי מרכזי לרציפות עסקית ולשמירה על יעילות תפעולית.

קונטאל מתמחה בתכנון, אספקה, הטמעה ותחזוקה של שרתים ותחנות עבודה המותאמים במיוחד לצרכים של מערכות MES, PLC, SCADA, דוחות תפעול, מערכות אנרגיה, תקשורת תעשייתית ויישומי OT/IT.

מה כוללת התשתית?

1. שרתים ייעודיים לסביבה תעשייתית:
שרתים חזקים ויציבים אשר מיועדים לפעול מסביב לשעון ולתמוך בעומסים גבוהים.
השרתים מותאמים לעבודה עם מערכות בקרה, ניהול נתונים, היסטוריאן, תקשורת ופתרונות אבטחה.

2 . עמדות עבודה לתפעול, הנדסה ובקרה:
עמדות המותאמות לסביבות ייצור ובקרה:
- תחנות HMI
- תחנות הנדסה לתכנות PLC/RTU
- עמדות בקרה מרכזיות לחדרי שליטה
- תחנות תפעול למערכות SCADA ותהליכי ייצור

מערכות אלו מספקות ממשק יציב ונוח למפעילים, מהנדסים ומנהלי תפעול.

3. תכנון ארכיטקטורה והטמעה מלאה:
הקמת תשתית מחשוב הכוללת שרתים, אחסון, וירטואליזציה, תקשורת, גיבויים וסינכרון בין אתרים.
הכל מתוכנן בהתאם לביצועים הנדרשים, מספר המשתמשים, סוגי המערכות והרגולציה הרלוונטית.

4. חיבור מאובטח ל־ OT ול־IT:
השרתים והעמדות מקושרים בצורה מבוקרת ומאובטחת לרשתות הייצור והבקרה, תוך ניהול ממשקים מול מערכות BI, ERP, MES, וענן.

ומה היתרונות שלנו?

התאמה מלאה למערכות בקרה וייצור:
השרתים והעמדות נבנים בהתאם לדרישות SCADA/PLC לתהליכים תעשייתיים ולסביבת OT קריטית.

אמינות גבוהה ועמידות לאורך זמן:
רכיבים איכותיים, הקשחה, תכנון רשת נכון ופתרונות יתירות מבטיחים זמינות מרבית.

ניהול וגיבוי מרכזיים:
כלל הגדרות, קונפיגורציות, מסכי HMI וקבצי פרויקטים מגובים ומנוהלים בצורה בטוחה ויעילה.

תמיכה ושירות של מומחי בקרה ומחשוב:
צוותי קונטאל משלבים ידע ב־ IT תקשורת, OT ובקרה, אלו מהווים יתרון משמעותי בסביבה שבה כל חלק חייב לעבוד יחד בהרמוניה.

שרתים, עמדות עבודה ושירות תחזוקה מקצועי מהווים את הבסיס לתפעול יציב, מאובטח ויעיל.
קונטאל מספקת פתרון כולל, מהגדרה וארכיטקטורה ועד תחזוקה שוטפת, הכל כדי לוודא שהמערכות הקריטיות ימשיכו לעבוד בדיוק כמו שצריך.

CONTEL
BEYOND TECHNOLOGY

שירותי תחזוקה שוטפים למערכי מחשוב וסייבר

היציבות התפעולית מתחילה בתחזוקה נכונה

בכל מפעל ומתקן תשתיות, מערכי המחשוב והסייבר מהווים שכבת תפעול קריטית: שרתים, מערכות שליטה ובקרה, תחנות הנדסה, מערכות תקשורת, מסדי נתונים, ציוד רשת, מערכות אבטחה ואינטגרציה בין OT ל־ IT ועוד. כל איום סייבר, תקלה תשתיתית או עדכון שבוצע בזמן לא מתאים, עשוי להשפיע באופן ישיר על קווי ייצור, מערכות אנרגיה, מפעלי מים, מתקני אחסון, חדרי בקרה מרכזי שליטה ועוד.
קונטאל מספקת שירותי תחזוקה שוטפים המבטיחים רציפות תפעולית, אבטחה גבוהה ושקט ניהולי והכל תוך התאמה מותאמת אישית לאופי הייחודי של הסביבה התעשייתית.

מה כולל השירות?

1. ניהול עדכונים ופאצ'ים בצורה מבוקרת:
יישום עדכוני אבטחה ותוכנה נעשה בזהירות יתרה, לאחר בדיקות התאמה מקדמיות וללא השבתה מיותרת שעשויה להוביל לאובדן הכנסות.
שיטת העבודה שלנו מותאמת לסביבה תעשייתית, שבה כל שינוי חייב להיות מתואם עם המפעל ורצפת הייצור.

2. תגובה לאירועים ושיקום מהיר:
לקונטאל יש פרוטוקול מסודר שכולל מודל תגובה מסודר לאירועי סייבר ותקלות תפעוליות, אשר כולל בין היתר:
- איתור של מקור התקלה
- בידוד מהיר של הרכיב הפגוע
- שיקום ויישום בקרות מנע
- דרכים להפקת לקחים ושיפור מתמשך

3. גיבוי, שחזור והבטחת חוסן תפעולי:
גיבוי סדיר של קונפיגורציות בקרה, מסכים, תצורות, PLC/RTU בסיסי נתונים ועוד.
בדיקות התאוששות מתבצעות באופן תקופתי כדי לוודא שהמערכות יוכלו לחזור לפעילות מלאה תוך זמן קצר.

4. אבטחת מידע כחלק מהשגרה:
הטמעת מדיניות גישה, ניהול הרשאות, בקרה על חיבורי צד ג', הקשחת ציוד תקשורת והדרכת עובדים. הכל תוך כדי שימת דגש על יצירת הרגלי עבודה נכונים בסביבה שבה טעויות יכולות להשפיע על בטיחות ותפוקה.

למה לבחור בקונטאל?

מומחיות עמוקה בעולמות OT, בקרה ותשתיות:
קונטאל מבצעת פרויקטים מורכבים של PLC, SCADA, אנרגיה ותשתיות מזה עשרות שנים, ולכן מכירה לעומק את ההבדל בין "תקלת IT" לבין "תקלת תפעול" שעלולה לעצור תהליך פיזי.

שילוב בין IT ל־OT תחת מקשה אחת:
כשה־ IT וה־ OT מנוהלים על ידי גורם אחד שמבין את שני העולמות, קל יותר למנוע תקלות, לזהות סיכונים ולהבטיח שהמערכות עובדות יחד בצורה מאובטחת ורציפה.

זמינות גבוהה ותגובה מהירה:
צוותי קונטאל זמינים לטיפול בתקלות בזמן אמת, במיוחד בסביבות שאינן יכולות להרשות לעצמן השבתה.

פתרון מקצה לקצה:
מניטור ועד גיבוי, מהקשחת רשת ועד בדיקות התאוששות, כל שכבות המחשוב והסייבר מנוהלות תחת מעטפת שירות אחת.

למי השירות מתאים?

- מפעלי תעשייה תהליכית
- מפעלי מזון ופארמה
- ייצור ואוטומציה
- אנרגיה וחשמל
- מים, ביוב והתפלה
- תשתיות תחבורה, אספקה ואגירה
- קמפוסים תעשייתיים ומתקנים רגישים

שירותי התחזוקה של קונטאל מבטיחים שגם מערכות IT וגם מערכות OT יישארו יציבות, מאובטחות ומתואמות לתהליכי העבודה, הכל כדי שהמפעל או האתר ימשיכו לפעול בבטחה, יעילות ובאופן רציף.

CONTEL
BEYOND TECHNOLOGY

קבוצת קונטאל

אודות קבוצת קונטאל

קונטאל מבצעת פרויקטים ומספקת מערכות וציוד באוטומציה תעשייתית, מערכות חשמל, בקרת תהליכים, בקרת מבנים, ניהול אנרגיה ובקרת מיזוג אוויר. החברה ממוקמת בפארק דניב, קרית אריה, פתח תקווה, סניף נוסף בפארק התעשיה עומר אשר מספק תמיכה טכנית ומעטפת הנדסית לתעשייה ולחברות הנדסה בדרום, סניף נוסף בפארק תעשיות מבוא כרמל שמספק אף הוא שירותי הנדסה וכן משכנו של מפעל לוחות החשמל והבקרה החדיש של החברה.
סניף נוסף בעפולה, מספק פתרונות סוף קו (אריזה) ופתרונות רובוטיקה וסניף חדש בשער הנגב - משמש את מהנדסי החברה בעוטף עזה ומאפשר לשפר את יכולות השירות שלנו באזור עוטף עזה ותורם לשיקום ותמיכה.
פעילויות קונטאל מכסות כמעט את כל דרישות השוק לאוטומציה ובקרה, ובקרת תהליכים. כאינטגרטור מערכות, קונטאל מציעה ללקוחות פתרונות הכוללים ציוד וחומרה שהמערכות דורשות, יחד עם ניתוח המערכת, תוכנה וביצוע, לוחות חשמל ובקרה, הנדסה והתקנה, ובאופן טבעי, הדרכה ושירותים, הכל מותאם לדרישות הספציפיות של הלקוח. חלק גדול מהציוד מגיע בעיקר מהשותפים העסקיים של קונטאל יצרנים עולמיים המובילים בתחומם.

קורסים מקצועיים:

סייבר הלכה למעשה – יסודות הסייבר לרשתות OT, מפעלי תעשייה ומתקני תשתיות לאומיות.
https://contel.co.il/course/cyber-security-course-online/

בין לקוחותינו:

LogistiCare Beyond logistics
רשות שדות התעופה בישראל ISRAEL AIRPORTS AUTHORITY
דוראד אנרגיה
שיכון ובינוי מקבוצת אריסון סולל בונה – תשתיות
TERALIGHT Innovative Energy
משק אנרגיה
EDF power solutions
NEGEV ENERGY
MAXIMA
enlight
BELECTRIC
powergen
DORAL
PRIME ENERGY