שליטה, AI וסייבר · סייבר לאתרים קריטיים

D-Cyber

C2 שכבה · שליטה וסייבר

הגנת סייבר במשמעת של אבטחה פיזית: מגינה על אתרים קריטיים ממתקפות דיגיטליות, מזהה ניסיונות חדירה ברגע שהם מתרחשים ומתחברת למערכות שכבר פועלות באתר.



יתרונות מרכזיים

01 **רואים ניסיונות חדירה מוקדם**
איומים וניסיונות חדירה מזוהים ומנוטרים בזמן אמת, כך שהצוות שלכם רואה אותם כשהם קורים.

02 **השירותים החיוניים ממשיכים לפעול**
תגובה מהירה, שנבנתה כדי למנוע הפרעה בשירות.

03 **תמונת אבטחה אחת**
אבטחה פיזית ואבטחת סייבר בתמונה אחת, משולבת עם מערכות הבקרה והניטור הקיימות שלכם ועם D-Command Control.

איך זה עובד

01 **הגנה**
מערכות קריטיות מוגנות מפני מתקפות דיגיטליות.

02 **גילוי**
איומים וניסיונות חדירה מזוהים בזמן אמת.

03 **תגובה**
פעולה מהירה ששומרת על רציפות השירותים החיוניים.

04 **שילוב**
האירועים עוברים למערכות הבקרה והניטור באתר.

מפרט

תחום	אתרים קריטיים; תשתיות לאומיות קריטיות
יכולות	הגנה מפני מתקפות דיגיטליות · ניטור וגילוי איומים וניסיונות חדירה בזמן אמת · תגובה מהירה · שילוב עם מערכות הבקרה והניטור הקיימות
מוצע יחד עם	מערכות ה-PIDS של D-FENCE ו-D-Command Control (אבטחה פיזית + סייבר)
תקשורת אלחוטית ביחידת ה-Gateway (D-Command Control)	Wi-Fi / Bluetooth / סלולר הוסרו מטעמי אבטחה; ניתנים להוספה לפי דרישה
הגנת אתחול ביחידת ה-Gateway (D-Command Control)	הגנת חומרה מפני אתחול לא מורשה מהתקן אחסון חיצוני
התקנה (D-Command Control)	תמיכה בהתקנות מאובטחות ומבודדות
גישה חיצונית (D-Command Control)	API מאובטח; גישת מפעיל מאובטחת
ממשקים אל (D-Command Control)	חומות אש, אנטי-וירוס, מערכות אבטחת מידע, IoT ו-SCADA

טקסט מפרט למכרז

1. כללי

המערכת תהיה D-Cyber של D-FENCE Electronic Fencing and Security Systems Ltd. (מערכת ניהול איכות בהסמכת ISO 9001:2015), או שווה ערך מאושר העומד בכל הדרישות שבסעיף זה.

2. ייעוד

הגנת סייבר במשמעת של אבטחה פיזית: מגינה על אתרים קריטיים ממתקפות דיגיטליות, מזהה ניסיונות חדירה ברגע שהם מתרחשים ומתחברת למערכות שכבר פועלות באתר.

3. המערכת תספק

- **הגנה על תשתיות:** תשתיות לאומיות קריטיות מוגנות מפני מתקפות דיגיטליות.
- **גילוי בזמן אמת:** ניטור וגילוי של איומים וניסיונות חדירה ברגע שהם מתרחשים.
- **תגובה מהירה:** תגובה מהירה שנועדה למנוע הפרעה בשירותים חיוניים.
- **שילוב מלא:** עובדת עם מערכות הבקרה והניטור שכבר קיימות באתר.
- **יחידת C2 מוקשחת:** תקשורת אלחוטית מוסרת כברירת מחדל; הגנת חומרה מפני אתחול לא מורשה.

4. דרישות טכניות

- **תחום:** אתרים קריטיים; תשתיות לאומיות קריטיות
- **יכולות:** הגנה מפני מתקפות דיגיטליות · ניטור וגילוי איומים וניסיונות חדירה בזמן אמת · תגובה מהירה · שילוב עם מערכות הבקרה והניטור הקיימות
- **מוצע יחד עם:** מערכות ה-PIDS של D-FENCE ו-D-Command Control (אבטחה פיזית + סייבר)
- **תקשורת אלחוטית ביחידת ה-Gateway (D-Command Control):** Wi-Fi / Bluetooth / סלולר הוסרו מטעמי אבטחה; ניתנים להוספה לפי דרישה
- **הגנת אתחול ביחידת ה-Gateway (D-Command Control):** הגנת חומרה מפני אתחול לא מורשה מהתקן אחסון חיצוני
- **התקנה (D-Command Control):** תמיכה בהתקנות מאובטחות ומבודדות
- **גישה חיצונית (D-Command Control):** API מאובטח; גישת מפעיל מאובטחת
- **ממשקים אל (D-Command Control):** חומות אש, אנטי-וירוס, מערכות אבטחת מידע, IoT ו-SCADA

5. רצף הגילוי

1. **הגנה:** מערכות קריטיות מוגנות מפני מתקפות דיגיטליות.
2. **גילוי:** איומים וניסיונות חדירה מזוהים בזמן אמת.
3. **תגובה:** פעולה מהירה ששומרת על רציפות השירותים החיוניים.
4. **שילוב:** האירועים עוברים למערכות הבקרה והניטור באתר.

6. מסמכים להגשה

לפני ההתקנה יגיש הקבלן לאישור את דף הנתונים של היצרן, את הוראות ההתקנה ואת תוכנית חלוקת האזורים.