

D-Cyber

C2 الطبقة • القيادة والأمن السيبراني

حماية سيبرانية للمواقع الحيوية، بالتكامل مع أنظمة الأمن المادي والتحكم القائمة بالفعل.



المواصفات

المواقع الحيوية؛ البنية التحتية الوطنية الحيوية	النطاق
الحماية من الهجمات الرقمية • كشف التهديدات والاختراقات في الوقت الفعلي • الاستجابة السريعة • التكامل مع أنظمة التحكم والمراقبة القائمة	الوظائف
D-Command Control و D-FENCE PIDS (الأمن المادي + الأمن السيبراني)	يُقدَّم مع
أُزيلت Wi-Fi / Bluetooth / الشبكة الخلوية لدواعٍ أمنية؛ وتُضاف عند الطلب	الاتصال اللاسلكي لبوابة C2 (D-Command Control)
حماية على مستوى العتاد من الإقلاع غير المصرح به من وحدات تخزين خارجية	حماية الإقلاع لبوابة C2 (D-Command Control)
يدعم التركيبات الآمنة والمعزولة	التركيب (D-Command Control)
واجهة API آمنة؛ وصول آمن للمشغل	الوصول الخارجي (D-Command Control)
جدران الحماية، مكافحة الفيروسات، أنظمة أمن المعلومات، IoT و SCADA	يتكامل مع (D-Command Control)

المزايا الرئيسية

- رصد مبكر لمحاولات الاختراق**
رصد التهديدات ومحاولات الاختراق وكشفها في الوقت الفعلي.
- استمرارية الخدمات الأساسية**
استجابة سريعة لمنع انقطاع الخدمة.
- صورة أمنية واحدة**
يتكامل مع أنظمة التحكم والمراقبة القائمة لديكم ومع D-Command Control.

آلية العمل

- الحماية**
تحسين الأنظمة الحيوية من الهجمات الرقمية.
- الكشف**
تحديد التهديدات ومحاولات الاختراق في الوقت الفعلي.
- الاستجابة**
إجراء سريع يحافظ على استمرارية الخدمات الأساسية.
- التكامل**
مشاركة الأحداث مع أنظمة التحكم والمراقبة في الموقع.

1. عام

يكون النظام D-Cyber من إنتاج D-FENCE Electronic Fencing and Security Systems Ltd. (إدارة جودة معتمدة وفق ISO 9001:2015)، أو بديلاً معتمداً مكافئاً يستوفي جميع متطلبات هذا القسم.

2. الوظيفة

حماية سيبرانية للمواقع الحيوية، بالتكامل مع أنظمة الأمن المادي والتحكم القائمة بالفعل.

3. يجب أن يوفر النظام

- حماية البنية التحتية: حماية البنية التحتية الوطنية الحيوية من الهجمات الرقمية.
- كشف في الوقت الفعلي: رصد التهديدات ومحاولات الاختراق وكشفها لحظة حدوثها.
- استجابة سريعة: استجابة سريعة تمنع انقطاع الخدمات الأساسية.
- تكامل كامل: يعمل مع أنظمة التحكم والمراقبة القائمة في الموقع.
- بوابة C2 مُحَصَّنة: الاتصال اللاسلكي مُزال افتراضياً؛ حماية على مستوى العتاد من الإقلاع غير المصرَّح به.

4. المتطلبات الفنية

- النطاق: المواقع الحيوية؛ البنية التحتية الوطنية الحيوية
- الوظائف: الحماية من الهجمات الرقمية · كشف التهديدات والاختراقات في الوقت الفعلي · الاستجابة السريعة · التكامل مع أنظمة التحكم والمراقبة القائمة
- يُقدَّم مع: D-FENCE PIDS و D-Command Control (الأمن المادي + الأمن السيبراني)
- الاتصال اللاسلكي لبوابة (C2 (D-Command Control): أزيلت Wi-Fi / Bluetooth / الشبكة الخلوية لدواعٍ أمنية؛ وتُضاف عند الطلب
- حماية الإقلاع لبوابة (C2 (D-Command Control): حماية على مستوى العتاد من الإقلاع غير المصرَّح به من وحدات تخزين خارجية
- التركيب (D-Command Control): يدعم التركيبات الآمنة والمعزولة
- الوصول الخارجي (D-Command Control): واجهة API آمنة؛ وصول آمن للمشغل
- يتكامل مع (D-Command Control): جدران الحماية، مكافحة الفيروسات، أنظمة أمن المعلومات، IoT و SCADA

5. تسلسل الكشف

1. الحماية: تحصين الأنظمة الحيوية من الهجمات الرقمية.
2. الكشف: تحديد التهديدات ومحاولات الاختراق في الوقت الفعلي.
3. الاستجابة: إجراء سريع يحافظ على استمرارية الخدمات الأساسية.
4. التكامل: مشاركة الأحداث مع أنظمة التحكم والمراقبة في الموقع.

6. المستندات المطلوبة

قبل التركيب، يُقدَّم المفاضل للاعتماد ورقة بيانات الشركة المصنّعة وتعليمات التركيب ومخطط تقسيم المناطق.