COMANDĂ, AI ȘI CYBER · SECURITATE CIBERNETICĂ PENTRU OBIECTIVE CRITICE

D-Cyber

C2 Strat · Comandă și securitate cibernetică

Protecție cibernetică pentru obiectivele critice, care funcționează împreună cu sistemele de securitate fizică și de control deja existente.



AVANTAJE PRINCIPALE

01 Tentativele de intruziune, observate din timp
Amenințări și tentative de intruziune monitorizate și detectate în timp real.

02 Serviciile esențiale rămân funcționale
Reacție rapidă pentru a preveni întreruperea serviciului.

03 O imagine unică a securității
Se integrează cu sistemele dumneavoastră existente de control și monitorizare și cu D-Command Control.

CUM FUNCȚIONEAZĂ

01 Protecție
Sistemele critice, protejate împotriva atacurilor digitale.

02 Detecție
Amenințările și tentativele de intruziune, identificate în timp real.

03 Reacție
Acțiune rapidă care menține funcționarea serviciilor esențiale.

SPECIFICAȚII

Domeniu de aplicare	Obiective critice; infrastructură critică națională
Funcții	Protecție împotriva atacurilor digitale · detecția în timp real a amenințărilor și a intruziunilor · reacție rapidă · integrare cu sistemele existente de control și monitorizare
Oferit împreună cu	D-FENCE PIDS și D-Command Control (securitate fizică + securitate cibernetică)
Comunicații wireless ale gateway-ului C2 (D-Command Control)	Wi-Fi / Bluetooth / rețea celulară eliminate din motive de securitate; adăugate la cerere
Protecția la pornire a gateway-ului C2 (D-Command Control)	Protecție hardware împotriva pornirii neautorizate de pe medii de stocare externe
Instalare (D-Command Control)	Permite instalări securizate și izolate
Acces extern (D-Command Control)	API securizat; acces securizat pentru operatori
Se interfațează cu (D-Command Control)	Firewall-uri, antivirus, sisteme de securitate a informației, IoT & SCADA

Specificațiile pot fi modificate fără notificare prealabilă. Ediția 10/2026 · 1/2

04 **Integrare**
Evenimentele sunt partajate cu sistemele de control și monitorizare de pe obiectiv.

TEXT PENTRU CAIETUL DE SARCINI

1. GENERALITĂȚI

Sistemul va fi D-Cyber produs de D-FENCE Electronic Fencing and Security Systems Ltd. (sistem de management al calității certificat ISO 9001:2015) sau un echivalent aprobat care îndeplinește toate cerințele din această secțiune.

2. FUNCȚIONARE

Protecție cibernetică pentru obiectivele critice, care funcționează împreună cu sistemele de securitate fizică și de control deja existente.

3. SISTEMUL TREBUIE SĂ ASIGURE

- **Protecția infrastructurii:** Infrastructura critică națională, protejată împotriva atacurilor digitale.
- **Detecție în timp real:** Amenințările și tentativele de intruziune sunt monitorizate și detectate pe măsură ce au loc.
- **Reacție rapidă:** O reacție rapidă care previne întreruperea serviciilor esențiale.
- **Integrare completă:** Funcționează cu sistemele de control și monitorizare existente deja pe obiectiv.
- **Gateway C2 cu securitate consolidată:** Comunicații wireless eliminate implicit; protecție hardware împotriva pornirii neautorizate.

4. CERINȚE TEHNICE

- **Domeniu de aplicare:** Obiective critice; infrastructură critică națională
- **Funcții:** Protecție împotriva atacurilor digitale · detecția în timp real a amenințărilor și a intruziunilor · reacție rapidă · integrare cu sistemele existente de control și monitorizare
- **Oferit împreună cu:** D-FENCE PIDS și D-Command Control (securitate fizică + securitate cibernetică)
- **Comunicații wireless ale gateway-ului C2 (D-Command Control):** Wi-Fi / Bluetooth / rețea celulară eliminate din motive de securitate; adăugate la cerere
- **Protecția la pornire a gateway-ului C2 (D-Command Control):** Protecție hardware împotriva pornirii neautorizate de pe medii de stocare externe
- **Instalare (D-Command Control):** Permite instalări securizate și izolate
- **Acces extern (D-Command Control):** API securizat; acces securizat pentru operatori
- **Se interfațează cu (D-Command Control):** Firewall-uri, antivirus, sisteme de securitate a informației, IoT & SCADA

5. SECVENȚA DE DETECȚIE

1. **Protecție:** Sistemele critice, protejate împotriva atacurilor digitale.
2. **Detecție:** Amenințările și tentativele de intruziune, identificate în timp real.
3. **Reacție:** Acțiune rapidă care menține funcționarea serviciilor esențiale.
4. **Integrare:** Evenimentele sunt partajate cu sistemele de control și monitorizare de pe obiectiv.

6. DOCUMENTE DE PREZENTAT

Înainte de instalare, contractorul va prezenta spre aprobare fișa tehnică a producătorului, instrucțiunile de instalare și planul zonelor.