COMANDO, IA E CYBER · CYBERSICUREZZA PER SITI CRITICI

D-Cyber

C2 Livello · Comando e cyber

Difesa cyber con la disciplina della sicurezza fisica: protegge i siti critici dagli attacchi digitali, rileva i tentativi di intrusione mentre avvengono e si integra con i sistemi già presenti.



VANTAGGI PRINCIPALI

01 **Tentativi di intrusione visti per tempo**
Minacce e tentativi di intrusione vengono rilevati e monitorati in tempo reale: il vostro team li vede mentre avvengono.

02 **Servizi essenziali in funzione**
Una risposta rapida, concepita per evitare l'interruzione del servizio.

03 **Un unico quadro di sicurezza**
Sicurezza fisica e cybersicurezza in un unico quadro, integrate con i vostri sistemi di controllo e monitoraggio esistenti e con D-Command Control.

COME FUNZIONA

01 **Proteggere**
Sistemi critici protetti dagli attacchi informatici.

02 **Rilevare**
Minacce e tentativi di intrusione individuati in tempo reale.

03 **Intervenire**
Un intervento rapido che mantiene attivi i servizi essenziali.

SPECIFICHE

Ambito	Siti critici; infrastrutture critiche nazionali
Funzioni	Protezione dagli attacchi digitali · rilevamento di minacce e intrusioni in tempo reale · risposta rapida · integrazione con i sistemi di controllo e monitoraggio esistenti
Offerto con	PIDS D-FENCE e D-Command Control (sicurezza fisica + cybersicurezza)
Wireless del gateway C2 (D-Command Control)	Wi-Fi / Bluetooth / rete cellulare rimossi per sicurezza; aggiunti su richiesta
Protezione dell'avvio del gateway C2 (D-Command Control)	Protezione hardware contro l'avvio non autorizzato da supporti esterni
Installazione (D-Command Control)	Supporta installazioni protette e isolate
Accesso esterno (D-Command Control)	API protetta; accesso protetto per gli operatori
Si interfaccia con (D-Command Control)	Firewall, antivirus, sistemi di sicurezza informatica, IoT e SCADA

04 **Integrare**
Eventi condivisi con i sistemi di controllo e monitoraggio del sito.

TESTO DI CAPITOLATO

1. GENERALITÀ

Il sistema dovrà essere D-Cyber di D-FENCE Electronic Fencing and Security Systems Ltd. (sistema di gestione della qualità certificato ISO 9001:2015), o un equivalente approvato che soddisfi ogni requisito della presente sezione.

2. FUNZIONE

Difesa cyber con la disciplina della sicurezza fisica: protegge i siti critici dagli attacchi digitali, rileva i tentativi di intrusione mentre avvengono e si integra con i sistemi già presenti.

3. IL SISTEMA DOVRÀ GARANTIRE

- **Protezione delle infrastrutture:** Protegge le infrastrutture critiche nazionali dagli attacchi informatici.
- **Rilevamento in tempo reale:** Monitora minacce e tentativi di intrusione e li rileva mentre avvengono.
- **Risposta rapida:** Risposta rapida per evitare l'interruzione dei servizi essenziali.
- **Piena integrazione:** Funziona con i sistemi di controllo e monitoraggio già presenti nel sito.
- **Gateway C2 protetto:** Wireless rimosso di serie, protezione hardware contro l'avvio non autorizzato.

4. REQUISITI TECNICI

- **Ambito:** Siti critici; infrastrutture critiche nazionali
- **Funzioni:** Protezione dagli attacchi digitali · rilevamento di minacce e intrusioni in tempo reale · risposta rapida · integrazione con i sistemi di controllo e monitoraggio esistenti
- **Offerto con:** PIDS D-FENCE e D-Command Control (sicurezza fisica + cybersicurezza)
- **Wireless del gateway C2 (D-Command Control):** Wi-Fi / Bluetooth / rete cellulare rimossi per sicurezza; aggiunti su richiesta
- **Protezione dell'avvio del gateway C2 (D-Command Control):** Protezione hardware contro l'avvio non autorizzato da supporti esterni
- **Installazione (D-Command Control):** Supporta installazioni protette e isolate
- **Accesso esterno (D-Command Control):** API protetta; accesso protetto per gli operatori
- **Si interfaccia con (D-Command Control):** Firewall, antivirus, sistemi di sicurezza informatica, IoT e SCADA

5. SEQUENZA DI RILEVAMENTO

1. **Proteggere:** Sistemi critici protetti dagli attacchi informatici.
2. **Rilevare:** Minacce e tentativi di intrusione individuati in tempo reale.
3. **Intervenire:** Un intervento rapido che mantiene attivi i servizi essenziali.
4. **Integrare:** Eventi condivisi con i sistemi di controllo e monitoraggio del sito.

6. DOCUMENTAZIONE TECNICA DA CONSEGNARE

Prima dell'installazione, l'appaltatore dovrà presentare per approvazione la scheda tecnica del produttore, le istruzioni di installazione e la planimetria delle zone.