DOWODZENIE, AI I CYBERBEZPIECZEŃSTWO · CYBERBEZPIECZEŃSTWO OBIEKTÓW KRYTYCZNYCH

D-Cyber

C2 Warstwa · Dowodzenie i cyberbezpieczeństwo

Cyberobrona z dyscypliną ochrony fizycznej: chroni obiekty krytyczne przed atakami cyfrowymi, wykrywa próby włamań na bieżąco i współpracuje z systemami działającymi już w obiekcie.



KLUCZOWE KORZYŚCI

01 **Wczesne wykrywanie prób włamań**
Zagrożenia i próby włamań są wykrywane i monitorowane w czasie rzeczywistym, dzięki czemu Państwa zespół widzi je w chwili, gdy występują.

02 **Ciągłość usług kluczowych**
Szybka reakcja, zaprojektowana tak, aby zapobiegać przerwom w działaniu usług.

03 **Jeden obraz bezpieczeństwa**
Bezpieczeństwo fizyczne i cyberbezpieczeństwo w jednym widoku, zintegrowane z Państwa istniejącymi systemami sterowania i monitoringu oraz z D-Command Control.

JAK TO DZIAŁA

01 **Ochrona**
Systemy krytyczne zabezpieczone przed atakami cyfrowymi.

02 **Wykrywanie**
Zagrożenia i próby włamań identyfikowane w czasie rzeczywistym.

03 **Reakcja**
Szybkie działanie, które utrzymuje ciągłość usług kluczowych.

SPECYFIKACJA

Zakres	Obiekty krytyczne; infrastruktura krytyczna państwa
Funkcje	Ochrona przed atakami cyfrowymi · wykrywanie zagrożeń i prób włamań w czasie rzeczywistym · szybka reakcja · integracja z istniejącymi systemami sterowania i monitoringu
Oferowane wraz z	D-FENCE PIDS i D-Command Control (bezpieczeństwo fizyczne + cyberbezpieczeństwo)
Łączność bezprzewodowa bramki C2 (D-Command Control)	Wi-Fi / Bluetooth / łączność komórkowa usunięte ze względów bezpieczeństwa; dostępne na życzenie
Ochrona rozruchu bramki C2 (D-Command Control)	Sprzętowe zabezpieczenie przed nieautoryzowanym rozruchem z nośników zewnętrznych
Instalacja (D-Command Control)	Obsługa zabezpieczonych, odizolowanych instalacji
Dostęp zewnętrzny (D-Command Control)	Zabezpieczone API; zabezpieczony dostęp operatora
Współpraca z (D-Command Control)	Zapory sieciowe (firewall), oprogramowanie antywirusowe, systemy bezpieczeństwa informacji, IoT i SCADA

04 **Integracja**
Zdarzenia udostępniane systemom sterowania i monitoringu w obiekcie.

ZAPISY DO SPECYFIKACJI PRZETARGOWEJ

1. WYMAGANIA OGÓLNE

Należy zastosować system D-Cyber produkcji D-FENCE Electronic Fencing and Security Systems Ltd. (certyfikowany system zarządzania jakością zgodny z ISO 9001:2015) lub zatwierdzony system równoważny, spełniający wszystkie wymagania niniejszej sekcji.

2. FUNKCJONALNOŚĆ

Cyberobrona z dyscypliną ochrony fizycznej: chroni obiekty krytyczne przed atakami cyfrowymi, wykrywa próby włamań na bieżąco i współpracuje z systemami działającymi już w obiekcie.

3. SYSTEM MUSI ZAPEWNIAĆ

- **Ochrona infrastruktury:** Infrastruktura krytyczna państwa chroniona przed atakami cyfrowymi.
- **Wykrywanie w czasie rzeczywistym:** Zagrożenia i próby włamań monitorowane i wykrywane na bieżąco.
- **Szybka reakcja:** Szybka reakcja zapobiegająca przerwom w świadczeniu usług kluczowych.
- **Pełna integracja:** Współpracuje z systemami sterowania i monitoringu działającymi w obiekcie.
- **Wzmocniona bramka C2:** Łączność bezprzewodowa domyślnie usunięta; sprzętowe zabezpieczenie przed nieautoryzowanym rozruchem.

4. WYMAGANIA TECHNICZNE

- **Zakres:** Obiekty krytyczne; infrastruktura krytyczna państwa
- **Funkcje:** Ochrona przed atakami cyfrowymi · wykrywanie zagrożeń i prób włamań w czasie rzeczywistym · szybka reakcja · integracja z istniejącymi systemami sterowania i monitoringu
- **Oferowane wraz z:** D-FENCE PIDS i D-Command Control (bezpieczeństwo fizyczne + cyberbezpieczeństwo)
- **Łączność bezprzewodowa bramki C2 (D-Command Control):** Wi-Fi / Bluetooth / łączność komórkowa usunięte ze względów bezpieczeństwa; dostępne na życzenie
- **Ochrona rozruchu bramki C2 (D-Command Control):** Sprzętowe zabezpieczenie przed nieautoryzowanym rozruchem z nośników zewnętrznych
- **Instalacja (D-Command Control):** Obsługa zabezpieczonych, odizolowanych instalacji
- **Dostęp zewnętrzny (D-Command Control):** Zabezpieczone API; zabezpieczony dostęp operatora
- **Współpraca z (D-Command Control):** Zapory sieciowe (firewall), oprogramowanie antywirusowe, systemy bezpieczeństwa informacji, IoT i SCADA

5. SEKWENCJA WYKRYWANIA

1. **Ochrona:** Systemy krytyczne zabezpieczone przed atakami cyfrowymi.
2. **Wykrywanie:** Zagrożenia i próby włamań identyfikowane w czasie rzeczywistym.
3. **Reakcja:** Szybkie działanie, które utrzymuje ciągłość usług kluczowych.
4. **Integracja:** Zdarzenia udostępniane systemom sterowania i monitoringu w obiekcie.

6. DOKUMENTY DO PRZEDŁOŻENIA

Przed montażem wykonawca przedłoży do zatwierdzenia kartę katalogową producenta, instrukcję montażu oraz plan podziału na strefy.