COMANDO, IA E CIBERSEGURANÇA · SEGURANÇA CIBERNÉTICA PARA INSTALAÇÕES CRÍTICAS

D-Cyber

C2 Camada · Comando e cibersegurança

Defesa cibernética com a disciplina da segurança física: protege instalações críticas contra ataques digitais, identifica tentativas de intrusão no momento em que ocorrem e se integra aos sistemas já existentes no local.



PRINCIPAIS BENEFÍCIOS

01 **Tentativas de intrusão vistas cedo**
Ameaças e tentativas de intrusão são detectadas e monitoradas em tempo real, para que sua equipe as veja no momento em que ocorrem.

02 **Serviços essenciais em funcionamento**
Uma resposta rápida, feita para evitar a interrupção do serviço.

03 **Uma só visão da segurança**
Segurança física e cibernética em uma só visão, integrada aos seus sistemas de controle e monitoramento existentes e ao D-Command Control.

COMO FUNCIONA

01 **Proteger**
Sistemas críticos protegidos contra ataques digitais.

02 **Detectar**
Ameaças e tentativas de intrusão identificadas em tempo real.

ESPECIFICAÇÕES

Escopo	Instalações críticas; infraestruturas críticas nacionais
Funções	Proteção contra ataques digitais · detecção de ameaças e intrusões em tempo real · resposta rápida · integração aos sistemas de controle e monitoramento existentes
Oferecido com	PIDS D-FENCE e D-Command Control (segurança física + segurança cibernética)
Comunicação sem fio do gateway C2 (D-Command Control)	Wi-Fi / Bluetooth / rede celular removidos por segurança; incluídos sob demanda
Proteção de inicialização do gateway C2 (D-Command Control)	Proteção em hardware contra inicialização não autorizada a partir de armazenamento externo
Instalação (D-Command Control)	Admite instalações seguras e isoladas
Acesso externo (D-Command Control)	API segura; acesso seguro do operador
Integra-se a (D-Command Control)	Firewalls, antivírus, sistemas de segurança da informação, IoT e SCADA

03 **Responder**
Ação rápida que mantém os serviços essenciais funcionando.

04 **Integrar**
Eventos compartilhados com os sistemas de controle e monitoramento do local.

TEXTO PARA TERMO DE REFERÊNCIA

1. GERAL

O sistema deverá ser o D-Cyber da D-FENCE Electronic Fencing and Security Systems Ltd. (gestão da qualidade certificada ISO 9001:2015), ou equivalente aprovado que atenda a todos os requisitos desta seção.

2. FUNÇÃO

Defesa cibernética com a disciplina da segurança física: protege instalações críticas contra ataques digitais, identifica tentativas de intrusão no momento em que ocorrem e se integra aos sistemas já existentes no local.

3. O SISTEMA DEVERÁ OFERECER

- **Proteção da infraestrutura:** Protege infraestruturas críticas nacionais contra ataques digitais.
- **Detecção em tempo real:** Monitora e detecta ameaças e tentativas de intrusão no momento em que ocorrem.
- **Resposta rápida:** Age rápido para manter os serviços essenciais funcionando sem interrupção.
- **Integração plena:** Funciona com os sistemas de controle e monitoramento já existentes no local.
- **Gateway C2 reforçado:** Comunicação sem fio removida por padrão; proteção em hardware contra inicialização não autorizada.

4. REQUISITOS TÉCNICOS

- **Escopo:** Instalações críticas; infraestruturas críticas nacionais
- **Funções:** Proteção contra ataques digitais · detecção de ameaças e intrusões em tempo real · resposta rápida · integração aos sistemas de controle e monitoramento existentes
- **Oferecido com:** PIDS D-FENCE e D-Command Control (segurança física + segurança cibernética)
- **Comunicação sem fio do gateway C2 (D-Command Control):** Wi-Fi / Bluetooth / rede celular removidos por segurança; incluídos sob demanda
- **Proteção de inicialização do gateway C2 (D-Command Control):** Proteção em hardware contra inicialização não autorizada a partir de armazenamento externo
- **Instalação (D-Command Control):** Admite instalações seguras e isoladas
- **Acesso externo (D-Command Control):** API segura; acesso seguro do operador
- **Integra-se a (D-Command Control):** Firewalls, antivírus, sistemas de segurança da informação, IoT e SCADA

5. SEQUÊNCIA DE DETECÇÃO

1. **Proteger:** Sistemas críticos protegidos contra ataques digitais.
2. **Detectar:** Ameaças e tentativas de intrusão identificadas em tempo real.
3. **Responder:** Ação rápida que mantém os serviços essenciais funcionando.
4. **Integrar:** Eventos compartilhados com os sistemas de controle e monitoramento do local.

6. DOCUMENTOS PARA APROVAÇÃO

Antes da instalação, a contratada deverá submeter à aprovação a ficha técnica do fabricante, as instruções de instalação e o layout das zonas.