MANDO, IA Y CIBERSEGURIDAD · CIBERSEGURIDAD PARA EMPLAZAMIENTOS CRÍTICOS

D-Cyber

C2 Capa · Mando y ciberseguridad

Ciberdefensa con la disciplina de la seguridad física: protege emplazamientos críticos frente a ataques digitales, detecta intentos de intrusión en tiempo real y se integra con los sistemas existentes.



VENTAJAS CLAVE

01 **Vea a tiempo los intentos de intrusión**
Amenazas e intentos de intrusión detectados y supervisados en tiempo real, para que su equipo los vea en el momento en que se producen.

02 **Mantenga en marcha los servicios esenciales**
Una respuesta rápida, concebida para evitar la interrupción del servicio.

03 **Una sola imagen de seguridad**
Seguridad física y ciberseguridad en una sola vista, integradas con sus sistemas de control y supervisión existentes y con D-Command Control.

CÓMO FUNCIONA

01 **Proteger**
Sistemas críticos blindados frente a ataques digitales.

02 **Detectar**
Amenazas e intentos de intrusión identificados en tiempo real.

03 **Responder**
Una actuación rápida que mantiene en marcha los servicios esenciales.

ESPECIFICACIONES

Alcance	Emplazamientos críticos; infraestructuras críticas nacionales
Funciones	Protección frente a ataques digitales · detección de amenazas e intrusiones en tiempo real · respuesta rápida · integración con los sistemas de control y supervisión existentes
Se ofrece con	D-FENCE PIDS y D-Command Control (seguridad física + ciberseguridad)
Conectividad inalámbrica del gateway C2 (D-Command Control)	Wi-Fi / Bluetooth / celular retirados por seguridad; se añaden bajo pedido
Protección de arranque del gateway C2 (D-Command Control)	Protección por hardware contra el arranque no autorizado desde almacenamiento externo
Instalación (D-Command Control)	Admite instalaciones seguras y aisladas
Acceso externo (D-Command Control)	API segura; acceso seguro de operadores
Interfaces con (D-Command Control)	Cortafuegos, antivirus, sistemas de seguridad de la información, IoT y SCADA

04 **Integrar**
Eventos compartidos con los sistemas de control y supervisión del emplazamiento.

TEXTO PARA PLIEGO

1. GENERALIDADES

El sistema será D-Cyber de D-FENCE Electronic Fencing and Security Systems Ltd. (gestión de calidad certificada ISO 9001:2015), o un equivalente aprobado que cumpla todos los requisitos de esta sección.

2. FUNCIÓN

Ciberdefensa con la disciplina de la seguridad física: protege emplazamientos críticos frente a ataques digitales, detecta intentos de intrusión en tiempo real y se integra con los sistemas existentes.

3. EL SISTEMA DEBERÁ OFRECER

- **Protección de infraestructuras:** Infraestructuras críticas nacionales protegidas frente a ataques digitales.
- **Detección en tiempo real:** Amenazas e intentos de intrusión supervisados y detectados en el momento en que se producen.
- **Respuesta rápida:** Respuesta rápida para evitar la interrupción de servicios esenciales.
- **Integración completa:** Funciona con los sistemas de control y supervisión ya existentes en el emplazamiento.
- **Gateway C2 reforzado:** Conectividad inalámbrica retirada de serie; protección por hardware contra el arranque no autorizado.

4. REQUISITOS TÉCNICOS

- **Alcance:** Emplazamientos críticos; infraestructuras críticas nacionales
- **Funciones:** Protección frente a ataques digitales · detección de amenazas e intrusiones en tiempo real · respuesta rápida · integración con los sistemas de control y supervisión existentes
- **Se ofrece con:** D-FENCE PIDS y D-Command Control (seguridad física + ciberseguridad)
- **Conectividad inalámbrica del gateway C2 (D-Command Control):** Wi-Fi / Bluetooth / celular retirados por seguridad; se añaden bajo pedido
- **Protección de arranque del gateway C2 (D-Command Control):** Protección por hardware contra el arranque no autorizado desde almacenamiento externo
- **Instalación (D-Command Control):** Admite instalaciones seguras y aisladas
- **Acceso externo (D-Command Control):** API segura; acceso seguro de operadores
- **Interfaces con (D-Command Control):** Cortafuegos, antivirus, sistemas de seguridad de la información, IoT y SCADA

5. SECUENCIA DE DETECCIÓN

1. **Proteger:** Sistemas críticos blindados frente a ataques digitales.
2. **Detectar:** Amenazas e intentos de intrusión identificados en tiempo real.
3. **Responder:** Una actuación rápida que mantiene en marcha los servicios esenciales.
4. **Integrar:** Eventos compartidos con los sistemas de control y supervisión del emplazamiento.

6. DOCUMENTACIÓN A PRESENTAR

Antes de la instalación, el contratista presentará para su aprobación la ficha técnica del fabricante, las instrucciones de instalación y el plano de zonas.