

COMMAND, AI & CYBER · CYBER SECURITY FOR CRITICAL SITES

D-Cyber

C2 Layer · Command & cyber

Cyber protection for critical sites, working with the physical security and control systems already in place.



KEY BENEFITS

- 01 See intrusion attempts early**
Threats and intrusion attempts monitored and detected in real time.
- 02 Keep essential services running**
Rapid response to prevent interruption of service.
- 03 One security picture**
Integrates with your existing control and monitoring systems and with D-Command Control.

HOW IT WORKS

- 01 Protect**
Critical systems shielded against digital attacks.
- 02 Detect**
Threats and intrusion attempts identified in real time.
- 03 Respond**
Rapid action that keeps essential services running.
- 04 Integrate**
Events shared with the control and monitoring systems on site.

SPECIFICATIONS

Scope	Critical sites; critical national infrastructure
Functions	Protection against digital attacks · real-time threat and intrusion detection · rapid response · integration with existing control and monitoring systems
Offered with	D-FENCE PIDS and D-Command Control (physical security + cyber security)
C2 gateway wireless (D-Command Control)	Wi-Fi / Bluetooth / cellular removed for security; added on demand
C2 gateway boot protection (D-Command Control)	Hardware protection against unauthorised boot from external storage
Installation (D-Command Control)	Supports secured, isolated installations
External access (D-Command Control)	Secured API; secured operator access
Interfaces with (D-Command Control)	Firewalls, antivirus, information-security systems, IoT & SCADA

TENDER SPECIFICATION TEXT

1. GENERAL

The system shall be D-Cyber by D-FENCE Electronic Fencing and Security Systems Ltd. (ISO 9001:2015 certified quality management), or an approved equivalent that meets every requirement in this section.

2. FUNCTION

Cyber protection for critical sites, working with the physical security and control systems already in place.

3. THE SYSTEM SHALL PROVIDE

- **Infrastructure protection:** Critical national infrastructure protected against digital attacks.
- **Real-time detection:** Threats and intrusion attempts monitored and detected as they happen.
- **Rapid response:** Fast response that prevents interruption of essential services.
- **Full integration:** Works with the control and monitoring systems already on site.
- **Hardened C2 gateway:** Wireless removed by default; hardware protection against unauthorised boot.

4. TECHNICAL REQUIREMENTS

- **Scope:** Critical sites; critical national infrastructure
- **Functions:** Protection against digital attacks · real-time threat and intrusion detection · rapid response · integration with existing control and monitoring systems
- **Offered with:** D-FENCE PIDS and D-Command Control (physical security + cyber security)
- **C2 gateway wireless (D-Command Control):** Wi-Fi / Bluetooth / cellular removed for security; added on demand
- **C2 gateway boot protection (D-Command Control):** Hardware protection against unauthorised boot from external storage
- **Installation (D-Command Control):** Supports secured, isolated installations
- **External access (D-Command Control):** Secured API; secured operator access
- **Interfaces with (D-Command Control):** Firewalls, antivirus, information-security systems, IoT & SCADA

5. DETECTION SEQUENCE

1. **Protect:** Critical systems shielded against digital attacks.
2. **Detect:** Threats and intrusion attempts identified in real time.
3. **Respond:** Rapid action that keeps essential services running.
4. **Integrate:** Events shared with the control and monitoring systems on site.

6. SUBMITTALS

Before installation, the contractor shall submit the manufacturer's datasheet, the installation instructions and the zone layout for approval.