

指挥、AI 与网络安全 · 面向关键站点的网络安全

D-Cyber

C2 防护层 · 指挥与网络安全

为关键站点提供网络防护，与现有的物理安防和控制系统协同工作。



主要优势

- 01 及早发现入侵企图**
实时监测和探测威胁及入侵企图。
- 02 保障关键服务持续运行**
快速响应，防止服务中断。
- 03 统一的安全态势**
与您现有的控制和监控系统以及 D-Command Control 集成。

工作原理

- 01 防护**
保护关键系统免受数字攻击。
- 02 探测**
实时识别威胁和入侵企图。
- 03 响应**
快速行动，保障关键服务持续运行。
- 04 集成**
与现场的控制和监控系统共享事件。

技术规格

范围	关键站点；国家关键基础设施
功能	防御数字攻击 · 实时威胁与入侵探测 · 快速响应 · 与现有控制和监控系统集成
配套方案	D-FENCE PIDS 与 D-Command Control（物理安防 + 网络安全）
C2 网关无线功能（D-Command Control）	出于安全考虑已移除 Wi-Fi / 蓝牙 / 蜂窝网络；可按需添加
C2 网关启动保护（D-Command Control）	防止从外部存储设备进行未经授权启动的硬件保护
安装部署（D-Command Control）	支持安全的隔离部署
外部访问（D-Command Control）	安全 API；安全的操作员访问
对接系统（D-Command Control）	防火墙、防病毒、信息安全系统、IoT 与 SCADA

招标技术规范文本

1. 总则

系统应采用 D-FENCE Electronic Fencing and Security Systems Ltd. (质量管理体系通过 ISO 9001:2015 认证) 的 D-Cyber, 或满足本节全部要求的经批准的同等产品。

2. 功能

为关键站点提供网络防护, 与现有的物理安防和控制系统协同工作。

3. 系统应提供

- **基础设施防护:** 保护国家关键基础设施免受数字攻击。
- **实时探测:** 实时监测和探测威胁及入侵企图。
- **快速响应:** 快速响应, 防止关键服务中断。
- **全面集成:** 与现场已有的控制和监控系统协同工作。
- **加固型 C2 网关:** 默认移除无线功能; 具备防止未经授权启动的硬件保护。

4. 技术要求

- **范围:** 关键站点; 国家关键基础设施
- **功能:** 防御数字攻击 · 实时威胁与入侵探测 · 快速响应 · 与现有控制和监控系统集成
- **配套方案:** D-FENCE PIDS 与 D-Command Control (物理安防 + 网络安全)
- **C2 网关无线功能 (D-Command Control) :** 出于安全考虑已移除 Wi-Fi / 蓝牙 / 蜂窝网络; 可按需添加
- **C2 网关启动保护 (D-Command Control) :** 防止从外部存储设备进行未经授权启动的硬件保护
- **安装部署 (D-Command Control) :** 支持安全的隔离部署
- **外部访问 (D-Command Control) :** 安全 API; 安全的操作员访问
- **对接系统 (D-Command Control) :** 防火墙、防病毒、信息安全系统、IoT 与 SCADA

5. 探测流程

1. **防护:** 保护关键系统免受数字攻击。
2. **探测:** 实时识别威胁和入侵企图。
3. **响应:** 快速行动, 保障关键服务持续运行。
4. **集成:** 与现场的控制和监控系统共享事件。

6. 提交文件

安装前, 承包商应提交制造商的产品规格书、安装说明和防区布局图, 以供审批。