LEITSYSTEM, KI & CYBER · CYBERSICHERHEIT FÜR KRITISCHE STANDORTE

D-Cyber

C2 Schicht · Leitstelle& Cyber

Cyberabwehr mit der Disziplin physischer Sicherheit: Sie schützt kritische Standorte vor digitalen Angriffen, erkennt Eindringversuche in Echtzeit und fügt sich in vorhandene Systeme vor Ort ein.



KERNVORTEILE

01 **Eindringversuche früh erkennen**
Bedrohungen und Eindringversuche werden in Echtzeit erkannt und überwacht, damit Ihr Team sie sieht, während sie geschehen.

02 **Wesentliche Dienste aufrechterhalten**
Schnelle Reaktion, ausgelegt darauf, Dienstunterbrechungen zu verhindern.

03 **Ein gemeinsames Sicherheitslagebild**
Physische Sicherheit und Cybersicherheit in einer Ansicht, integriert in Ihre vorhandenen Leit- und Überwachungssysteme und in D-Command Control.

SO FUNKTIONIERT ES

01 **Schützen**
Kritische Systeme werden gegen digitale Angriffe abgeschirmt.

02 **Erkennen**
Bedrohungen und Eindringversuche werden in Echtzeit identifiziert.

03 **Reagieren**
Schnelles Handeln, das den Betrieb wesentlicher Dienste aufrechterhält.

SPEZIFIKATIONEN

Anwendungsbereich	Kritische Standorte; kritische nationale Infrastrukturen
Funktionen	Schutz vor digitalen Angriffen · Echtzeiterkennung von Bedrohungen und Eindringversuchen · schnelle Reaktion · Integration in vorhandene Leit- und Überwachungssysteme
Angeboten mit	D-FENCE PIDS und D-Command Control (physische Sicherheit + Cybersicherheit)
Drahtlose Schnittstellen des C2-Gateways (D-Command Control)	WLAN / Bluetooth / Mobilfunk aus Sicherheitsgründen entfernt; auf Wunsch nachrüstbar
Boot-Schutz des C2-Gateways (D-Command Control)	Hardwareschutz gegen unbefugtes Booten von externen Speichermedien
Installation (D-Command Control)	Unterstützt gesicherte, isolierte Installationen
Externer Zugriff (D-Command Control)	Gesicherte API; gesicherter Bedienerzugang
Schnittstellen zu (D-Command Control)	Firewalls, Virenschutz, Informationssicherheitssysteme, IoT & SCADA

04 **Integrieren**
Ereignisse werden mit den Leit- und Überwachungssystemen vor Ort geteilt.

AUSSCHREIBUNGSTEXT

1. ALLGEMEINES

Vorzusehen ist D-Cyber von D-FENCE Electronic Fencing and Security Systems Ltd. (zertifiziertes Qualitätsmanagement nach ISO 9001:2015) oder ein freigegebenes gleichwertiges System, das alle Anforderungen dieses Abschnitts erfüllt.

2. FUNKTION

Cyberabwehr mit der Disziplin physischer Sicherheit: Sie schützt kritische Standorte vor digitalen Angriffen, erkennt Eindringversuche in Echtzeit und fügt sich in vorhandene Systeme vor Ort ein.

3. DAS SYSTEM MUSS BIETEN

- **Infrastrukturschutz:** Kritische nationale Infrastrukturen, geschützt vor digitalen Angriffen.
- **Echtzeiterkennung:** Bedrohungen und Eindringversuche werden überwacht und erkannt, während sie geschehen.
- **Schnelle Reaktion:** Schnelle Reaktion, um Unterbrechungen wesentlicher Dienste zu verhindern.
- **Vollständige Integration:** Arbeitet mit den vorhandenen Leit- und Überwachungssystemen vor Ort.
- **Gehärtetes C2-Gateway:** Drahtlose Schnittstellen standardmäßig entfernt; Hardwareschutz gegen unbefugtes Booten.

4. TECHNISCHE ANFORDERUNGEN

- **Anwendungsbereich:** Kritische Standorte; kritische nationale Infrastrukturen
- **Funktionen:** Schutz vor digitalen Angriffen · Echtzeiterkennung von Bedrohungen und Eindringversuchen · schnelle Reaktion · Integration in vorhandene Leit- und Überwachungssysteme
- **Angeboten mit:** D-FENCE PIDS und D-Command Control (physische Sicherheit + Cybersicherheit)
- **Drahtlose Schnittstellen des C2-Gateways (D-Command Control):** WLAN / Bluetooth / Mobilfunk aus Sicherheitsgründen entfernt; auf Wunsch nachrüstbar
- **Boot-Schutz des C2-Gateways (D-Command Control):** Hardwareschutz gegen unbefugtes Booten von externen Speichermedien
- **Installation (D-Command Control):** Unterstützt gesicherte, isolierte Installationen
- **Externer Zugriff (D-Command Control):** Gesicherte API; gesicherter Bedienerzugang
- **Schnittstellen zu (D-Command Control):** Firewalls, Virenschutz, Informationssicherheitssysteme, IoT & SCADA

5. DETEKTIONSABLAUF

1. **Schützen:** Kritische Systeme werden gegen digitale Angriffe abgeschirmt.
2. **Erkennen:** Bedrohungen und Eindringversuche werden in Echtzeit identifiziert.
3. **Reagieren:** Schnelles Handeln, das den Betrieb wesentlicher Dienste aufrechterhält.
4. **Integrieren:** Ereignisse werden mit den Leit- und Überwachungssystemen vor Ort geteilt.

6. EINZUREICHENDE UNTERLAGEN

Vor der Installation legt der Auftragnehmer das Datenblatt des Herstellers, die Montageanleitung und den Zonenplan zur Freigabe vor.