COMMANDEMENT, IA ET CYBER · CYBERSÉCURITÉ DES SITES CRITIQUES

D-Cyber

C2 Couche · Commandement et cyber

Cyberdéfense avec la rigueur de la sécurité physique : elle protège les sites critiques des attaques numériques, repère les tentatives d'intrusion en temps réel et s'intègre aux systèmes en place.



AVANTAGES CLÉS

01 Repérer tôt les tentatives d'intrusion
Menaces et tentatives d'intrusion détectées et surveillées en temps réel, pour que votre équipe les voie au moment où elles se produisent.

02 Maintenir les services essentiels
Une réponse rapide, conçue pour éviter l'interruption de service.

03 Une vue de sécurité unique
Sécurité physique et cybersécurité réunies dans une seule vue, intégrées à vos systèmes de contrôle et de supervision existants et à D-Command Control.

FONCTIONNEMENT

01 Protéger
Systèmes critiques protégés contre les attaques numériques.

02 Détecter
Menaces et tentatives d'intrusion identifiées en temps réel.

03 Réagir
Une action rapide qui assure la continuité des services essentiels.

CARACTÉRISTIQUES

Champ d'application	Sites critiques ; infrastructures nationales critiques
Fonctions	Protection contre les attaques numériques · détection en temps réel des menaces et des intrusions · réponse rapide · intégration aux systèmes de contrôle et de supervision existants
Proposé avec	PIDS D-FENCE et D-Command Control (sécurité physique + cybersécurité)
Liaisons sans fil de la passerelle C2 (D-Command Control)	Wi-Fi / Bluetooth / cellulaire retirés pour des raisons de sécurité ; ajoutés sur demande
Protection au démarrage de la passerelle C2 (D-Command Control)	Protection matérielle contre le démarrage non autorisé depuis un support de stockage externe
Installation (D-Command Control)	Prise en charge des installations sécurisées et isolées
Accès externe (D-Command Control)	API sécurisée ; accès opérateur sécurisé
S'interface avec (D-Command Control)	Pare-feu, antivirus, systèmes de sécurité de l'information, IoT et SCADA

04 **Intégrer**
Événements partagés avec les systèmes de contrôle et de supervision du site.

TEXTE POUR CCTP

1. GÉNÉRALITÉS

Le système sera D-Cyber de D-FENCE Electronic Fencing and Security Systems Ltd. (management de la qualité certifié ISO 9001:2015), ou un équivalent approuvé satisfaisant à toutes les exigences de la présente section.

2. FONCTION

Cyberdéfense avec la rigueur de la sécurité physique : elle protège les sites critiques des attaques numériques, repère les tentatives d'intrusion en temps réel et s'intègre aux systèmes en place.

3. LE SYSTÈME DOIT ASSURER

- **Protection des infrastructures :** Infrastructures nationales critiques protégées contre les attaques numériques.
- **Détection en temps réel :** Menaces et tentatives d'intrusion surveillées et détectées au moment où elles se produisent.
- **Réponse rapide :** Une réponse rapide pour éviter l'interruption des services essentiels.
- **Intégration complète :** Fonctionne avec les systèmes de contrôle et de supervision déjà présents sur le site.
- **Passerelle C2 durcie :** Liaisons sans fil retirées par défaut ; protection matérielle contre le démarrage non autorisé.

4. EXIGENCES TECHNIQUES

- **Champ d'application :** Sites critiques ; infrastructures nationales critiques
- **Fonctions :** Protection contre les attaques numériques · détection en temps réel des menaces et des intrusions · réponse rapide · intégration aux systèmes de contrôle et de supervision existants
- **Proposé avec :** PIDS D-FENCE et D-Command Control (sécurité physique + cybersécurité)
- **Liaisons sans fil de la passerelle C2 (D-Command Control) :** Wi-Fi / Bluetooth / cellulaire retirés pour des raisons de sécurité ; ajoutés sur demande
- **Protection au démarrage de la passerelle C2 (D-Command Control) :** Protection matérielle contre le démarrage non autorisé depuis un support de stockage externe
- **Installation (D-Command Control) :** Prise en charge des installations sécurisées et isolées
- **Accès externe (D-Command Control) :** API sécurisée ; accès opérateur sécurisé
- **S'interface avec (D-Command Control) :** Pare-feu, antivirus, systèmes de sécurité de l'information, IoT et SCADA

5. SÉQUENCE DE DÉTECTION

1. **Protéger :** Systèmes critiques protégés contre les attaques numériques.
2. **Détecter :** Menaces et tentatives d'intrusion identifiées en temps réel.
3. **Réagir :** Une action rapide qui assure la continuité des services essentiels.
4. **Intégrer :** Événements partagés avec les systèmes de contrôle et de supervision du site.

6. DOCUMENTS À FOURNIR

Avant l'installation, l'entreprise soumettra à approbation la fiche technique du fabricant, les instructions d'installation et le plan de zonage.