कमांड, AI और साइबर · महत्वपूर्ण प्रतिष्ठानों की साइबर सुरक्षा

D-Cyber

C2 परत · कमांड और साइबर

भौतिक सुरक्षा के अनुशासन के साथ साइबर रक्षा: यह महत्वपूर्ण प्रतिष्ठानों को डिजिटल हमलों से बचाती है, घुसपैठ के प्रयासों को होते ही पकड़ती है और साइट पर पहले से मौजूद प्रणालियों से सीधे जुड़ती है।



मुख्य लाभ

01 **घुसपैठ के प्रयास पहले देखें**
खतरों और घुसपैठ के प्रयासों की पहचान और निगरानी वास्तविक समय में होती है, ताकि आपकी टीम उन्हें होते ही देखे।

02 **आवश्यक सेवाएँ चलती रहें**
त्वरित प्रतिक्रिया, जो सेवा में रुकावट रोकने के लिए बनी है।

03 **सुरक्षा की एक तस्वीर**
भौतिक और साइबर सुरक्षा एक ही दृश्य में, आपकी मौजूदा नियंत्रण और निगरानी प्रणालियों और D-Command Control के साथ जुड़ी हुई।

यह कैसे काम करता है

01 **बचाव**
महत्वपूर्ण प्रणालियाँ डिजिटल हमलों से सुरक्षित।

02 **पहचान**
खतरे और घुसपैठ के प्रयास वास्तविक समय में पहचाने जाते हैं।

03 **प्रतिक्रिया**
त्वरित कार्रवाई, जो आवश्यक सेवाओं को चालू रखती है।

04 **इंटीग्रेशन**
घटनाएँ साइट की नियंत्रण और निगरानी प्रणालियों के साथ साझा होती हैं।

विनिर्देश

दायरा	महत्वपूर्ण प्रतिष्ठान; महत्वपूर्ण राष्ट्रीय अवसंरचना
कार्य	डिजिटल हमलों से सुरक्षा · खतरों और घुसपैठ की रीयल-टाइम पहचान · त्वरित प्रतिक्रिया · मौजूदा नियंत्रण और निगरानी प्रणालियों के साथ इंटीग्रेशन
किसके साथ उपलब्ध	D-FENCE PIDS और D-Command Control (भौतिक सुरक्षा + साइबर सुरक्षा)
C2 गेटवे वायरलेस (D-Command Control)	सुरक्षा के लिए Wi-Fi / Bluetooth / सेल्युलर हटाए गए; माँग पर जोड़े जाते हैं
C2 गेटवे बूट सुरक्षा (D-Command Control)	बाहरी स्टोरेज से अनधिकृत बूट के विरुद्ध हार्डवेयर सुरक्षा
इंस्टॉलेशन (D-Command Control)	सुरक्षित, पृथक इंस्टॉलेशन का समर्थन
बाहरी पहुँच (D-Command Control)	सुरक्षित API; सुरक्षित ऑपरेटर पहुँच
किनसे जुड़ता है (D-Command Control)	फ़ायरवॉल, एंटीवायरस, सूचना-सुरक्षा प्रणालियाँ, IoT & SCADA

टेंडर विनिर्देश टेक्स्ट

1. सामान्य

प्रणाली D-FENCE Electronic Fencing and Security Systems Ltd. (ISO 9001:2015 प्रमाणित गुणवत्ता प्रबंधन) की D-Cyber होगी, या कोई स्वीकृत समकक्ष प्रणाली जो इस खंड की हर आवश्यकता पूरी करे।

2. कार्य

भौतिक सुरक्षा के अनुशासन के साथ साइबर रक्षा: यह महत्वपूर्ण प्रतिष्ठानों को डिजिटल हमलों से बचाती है, घुसपैठ के प्रयासों को होते ही पकड़ती है और साइट पर पहले से मौजूद प्रणालियों से सीधे जुड़ती है।

3. प्रणाली प्रदान करेगी

- **अवसंरचना की सुरक्षा:** महत्वपूर्ण राष्ट्रीय अवसंरचना को डिजिटल हमलों से बचाता है।
- **रीयल-टाइम पहचान:** खतरों और घुसपैठ के प्रयासों की होते ही निगरानी करता है और उन्हें पकड़ता है।
- **त्वरित प्रतिक्रिया:** तेज़ी से कार्रवाई करता है, ताकि आवश्यक सेवाएँ बिना रुकावट चलती रहें।
- **पूर्ण इंटीग्रेशन:** साइट पर पहले से मौजूद नियंत्रण और निगरानी प्रणालियों के साथ काम करता है।
- **सुदृढ़ C2 गेटवे:** वायरलेस डिफ़ॉल्ट रूप से हटाया गया; अनधिकृत बूट के विरुद्ध हार्डवेयर सुरक्षा।

4. तकनीकी आवश्यकताएँ

- **दायरा:** महत्वपूर्ण प्रतिष्ठान; महत्वपूर्ण राष्ट्रीय अवसंरचना
- **कार्य:** डिजिटल हमलों से सुरक्षा · खतरों और घुसपैठ की रीयल-टाइम पहचान · त्वरित प्रतिक्रिया · मौजूदा नियंत्रण और निगरानी प्रणालियों के साथ इंटीग्रेशन
- **किसके साथ उपलब्ध:** D-FENCE PIDS और D-Command Control (भौतिक सुरक्षा + साइबर सुरक्षा)
- **C2 गेटवे वायरलेस (D-Command Control):** सुरक्षा के लिए Wi-Fi / Bluetooth / सेल्युलर हटाए गए; माँग पर जोड़े जाते हैं
- **C2 गेटवे बूट सुरक्षा (D-Command Control):** बाहरी स्टोरेज से अनधिकृत बूट के विरुद्ध हार्डवेयर सुरक्षा
- **इंस्टॉलेशन (D-Command Control):** सुरक्षित, पृथक इंस्टॉलेशन का समर्थन
- **बाहरी पहुँच (D-Command Control):** सुरक्षित API; सुरक्षित ऑपरेटर पहुँच
- **किनसे जुड़ता है (D-Command Control):** फ़ायरवॉल, एंटीवायरस, सूचना-सुरक्षा प्रणालियाँ, IoT & SCADA

5. पहचान का क्रम

1. **बचाव:** महत्वपूर्ण प्रणालियाँ डिजिटल हमलों से सुरक्षित।
2. **पहचान:** खतरे और घुसपैठ के प्रयास वास्तविक समय में पहचाने जाते हैं।
3. **प्रतिक्रिया:** त्वरित कार्रवाई, जो आवश्यक सेवाओं को चालू रखती है।
4. **इंटीग्रेशन:** घटनाएँ साइट की नियंत्रण और निगरानी प्रणालियों के साथ साझा होती हैं।

6. प्रस्तुत किए जाने वाले दस्तावेज़

इंस्टॉलेशन से पहले ठेकेदार निर्माता की डेटाशीट, इंस्टॉलेशन निर्देश और ज़ोन लेआउट अनुमोदन के लिए प्रस्तुत करेगा।