KOMMANDO, KI OG CYBER · CYBERSIKKERHET FOR KRITISKE ANLEGG

D-Cyber

C2 Lag · Kommando og cyber

Cyberforsvar med disiplinen fra fysisk sikring: det skjermer kritiske anlegg mot dataangrep, oppdager inntrengningsforsøk idet de skjer og kobles til systemene som allerede finnes på anlegget.



FORDELER

01 **Se inntrengningsforsøk tidlig**
Trusler og inntrengningsforsøk oppdages og overvåkes i sanntid, så teamet ditt ser dem idet de skjer.

02 **Hold viktige tjenester i gang**
Rask respons, bygd for å hindre avbrudd i tjenestene.

03 **Ett sikkerhetsbilde**
Fysisk sikring og cybersikkerhet i én visning, integrert med kontroll- og overvåkingssystemene du har og med D-Command Control.

SLIK FUNGERER DET

01 **Beskytt**
Kritiske systemer skjermet mot dataangrep.

02 **Oppdag**
Trusler og inntrengningsforsøk identifisert i sanntid.

03 **Reager**
Rask handling som holder viktige tjenester i gang.

04 **Integrer**
Hendelser deles med kontroll- og overvåkingssystemene på anlegget.

SPESIFIKASJONER

Omfang	Kritiske anlegg; kritisk nasjonal infrastruktur
Funksjoner	Beskyttelse mot dataangrep · deteksjon av trusler og inntrengning i sanntid · rask respons · integrasjon med eksisterende kontroll- og overvåkingssystemer
Leveres med	D-FENCE PIDS og D-Command Control (fysisk sikring + cybersikkerhet)
Trådløst på C2-gateway (D-Command Control)	Wi-Fi / Bluetooth / mobilnett fjernet av sikkerhetshensyn; legges til ved behov
Oppstartsbeskyttelse på C2-gateway (D-Command Control)	Maskinvarebeskyttelse mot uautorisert oppstart fra ekstern lagring
Installasjon (D-Command Control)	Støtter sikrede, isolerte installasjoner
Ekstern tilgang (D-Command Control)	Sikret API; sikret operatørtilgang
Grensesnitt mot (D-Command Control)	Brannmurer, antivirus, informasjonssikkerhetssystemer, IoT og SCADA

TEKST TIL KRAVSPESIFIKASJON

1. GENERELT

Systemet skal være D-Cyber fra D-FENCE Electronic Fencing and Security Systems Ltd. (kvalitetsstyring sertifisert etter ISO 9001:2015), eller et godkjent likeverdig system som oppfyller alle kravene i dette avsnittet.

2. FUNKSJON

Cyberforsvar med disiplinen fra fysisk sikring: det skjermer kritiske anlegg mot dataangrep, oppdager inntrengningsforsøk idet de skjer og kobles til systemene som allerede finnes på anlegget.

3. SYSTEMET SKAL GI

- **Beskyttelse av infrastruktur:** Skjermer kritisk nasjonal infrastruktur mot dataangrep.
- **Deteksjon i sanntid:** Overvåker og oppdager trusler og inntrengningsforsøk idet de skjer.
- **Rask respons:** Handler raskt for å holde viktige tjenester i gang uten avbrudd.
- **Full integrasjon:** Fungerer med kontroll- og overvåkingssystemene som allerede finnes på anlegget.
- **Herdet C2-gateway:** Trådløst fjernet som standard; maskinvarebeskyttelse mot uautorisert oppstart.

4. TEKNISKE KRAV

- **Omfang:** Kritiske anlegg; kritisk nasjonal infrastruktur
- **Funksjoner:** Beskyttelse mot dataangrep · deteksjon av trusler og inntrengning i sanntid · rask respons · integrasjon med eksisterende kontroll- og overvåkingssystemer
- **Leveres med:** D-FENCE PIDS og D-Command Control (fysisk sikring + cybersikkerhet)
- **Trådløst på C2-gateway (D-Command Control):** Wi-Fi / Bluetooth / mobilnett fjernet av sikkerhetshensyn; legges til ved behov
- **Oppstartsbeskyttelse på C2-gateway (D-Command Control):** Maskinvarebeskyttelse mot uautorisert oppstart fra ekstern lagring
- **Installasjon (D-Command Control):** Støtter sikrede, isolerte installasjoner
- **Ekstern tilgang (D-Command Control):** Sikret API; sikret operatørtilgang
- **Grensesnitt mot (D-Command Control):** Brannmurer, antivirus, informasjonssikkerhetssystemer, IoT og SCADA

5. DETEKSJONSFORLØP

1. **Beskytt:** Kritiske systemer skjermet mot dataangrep.
2. **Oppdag:** Trusler og inntrengningsforsøk identifisert i sanntid.
3. **Reager:** Rask handling som holder viktige tjenester i gang.
4. **Integrer:** Hendelser deles med kontroll- og overvåkingssystemene på anlegget.

6. DOKUMENTASJON

Før installasjon skal entreprenøren levere produsentens datablad, monteringsanvisningen og soneplanen til godkjenning.