10-MINUTE SELF-ASSESSMENT

BMS Exposure Quick Check

Print this page. Walk your facility. Check what's true today.

Insane Cyber
insanecyber.com

INTERNET EXPOSURE

- [ ] We've scanned our public IPs for exposed OT services in the last 90 days
- [ ] We know which BMS and OT ports are responding externally
- [ ] MFA is enforced on every remote access path into OT
- [ ] No OT management interface is directly reachable from the internet

VULNERABILITY EXPOSURE

- [ ] OT firmware versions cross-referenced against the CISA KEV catalog in the last 90 days
- [ ] A named person owns OT vulnerability management
- [ ] End-of-life devices identified with documented compensating controls
- [ ] Firmware and software versions documented for every BMS, DCIM, UPS, cooling controller

REMOTE ACCESS

- [ ] We can list every remote access tool in use across OT and who uses each
- [ ] Dormant access (90+ days unused) is terminated on a regular cadence
- [ ] Active vendor access flows through a session-managed jump host with logging
- [ ] We use 4 or fewer remote access tools across the OT environment

SEGMENTATION & MONITORING

- [ ] Current network diagram shows IT, OT, and the boundary
- [ ] Legacy protocols (LonTalk, LonWorks, proprietary) isolated to dedicated segments
- [ ] OT network traffic visible through native logs or passive monitoring
- [ ] A named person reviews OT logs on a defined cadence

14 OR MORE
Strong BMS hygiene
You're in the minority. Focus on continuous improvement.

8 – 13
Typical exposure
The 90-day plan in the full playbook is worth running.

7 OR FEWER
Significant exposure
Consider a formal assessment to compress the timeline and validate findings.

Book a 30-minute Data Center OT Exposure Review

INSANECYBER.COM / CONTACT →