6

IT SECURITY STRATEGIES YOU CAN ADAPT FOR OT ENVIRONMENTS

As OT systems connect with IT networks, security gaps are appearing. If you need to help OT leaders adopt a cybersecurity-first approach, change how you talk security.

THE END-USER AWARENESS DISCUSSION

Frame the conversation in terms of the risks OT engineers manage. For them, it's about business, operations, and safety.

01

THE ASSET DISCOVERY FOCUS

Identify assets in the entire OT network - from OS to software - their communications paths, and their criticality to operations.

02

THE NETWORK SEGMENTATION APPROACH

Use the Purdue model to unpack this. Swap air-gapping for system-to- system connectivity. Build hierarchy with firewalls & controls.

03

THE INCIDENT MANAGEMENT PLAN

It's all about planning. The OT teams need to agree with the security teams on "who does what" if a breach occurs.

04

ACCESS CONTROLS

IAM (e.g. access requirements syncs, MFA) should be implemented. But reduce risk by using different remote access solutions for IT and OT.

05

VULNERABILITY & PATCH MANAGEMENT

It's a nonnegotiable: You can't ignore patch management for OT. Complement patches with compensating controls e.g. isolation, privileges.

06

CLICK HERE to watch our webcast on Operational Technology

Get in touch today
info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY