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.

1 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.

2 The asset discovery focus

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

3 The network segmentation approach

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

4 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.

5 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

6 Vulnerability and patch management

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

CLICK HERE to watch our webcast on Operational Technology

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona with operations in countries around the world.

info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY