Did you know that Industrial Defender’s Automation Systems Manager (ASM) continuously provides 9 important cybersecurity protections for OT remote access?

Our always-on technology quickly identifies things like suspicious login attempts, unknown devices connecting to the network, and unpatched vulnerabilities that might open your endpoints up to attackers.

9 Threats Related to Remote Access That the ASM Monitors For

- Excessive Login Attempts
- Unknown Devices Connecting to Your Network
- Firewall Configuration Changes to Things Like Rules and User Accounts
- Endpoint Device Configuration Changes, Including Software, System Settings, and Ports & Services
- Policy Non-Conformance of User and Default Account Credentials, Such as Age or Complexity of Passwords
- Unpatched Vulnerabilities in OT Devices
- Deep Packet Inspection to Watch for TCP/IP and Industrial Protocol Abuse
- Critical Security Events Like Malware or Man-in-the-Middle (MITM) Attacks
- Central Log Database for Forensic Investigation That Captures Every Login