Honeywell

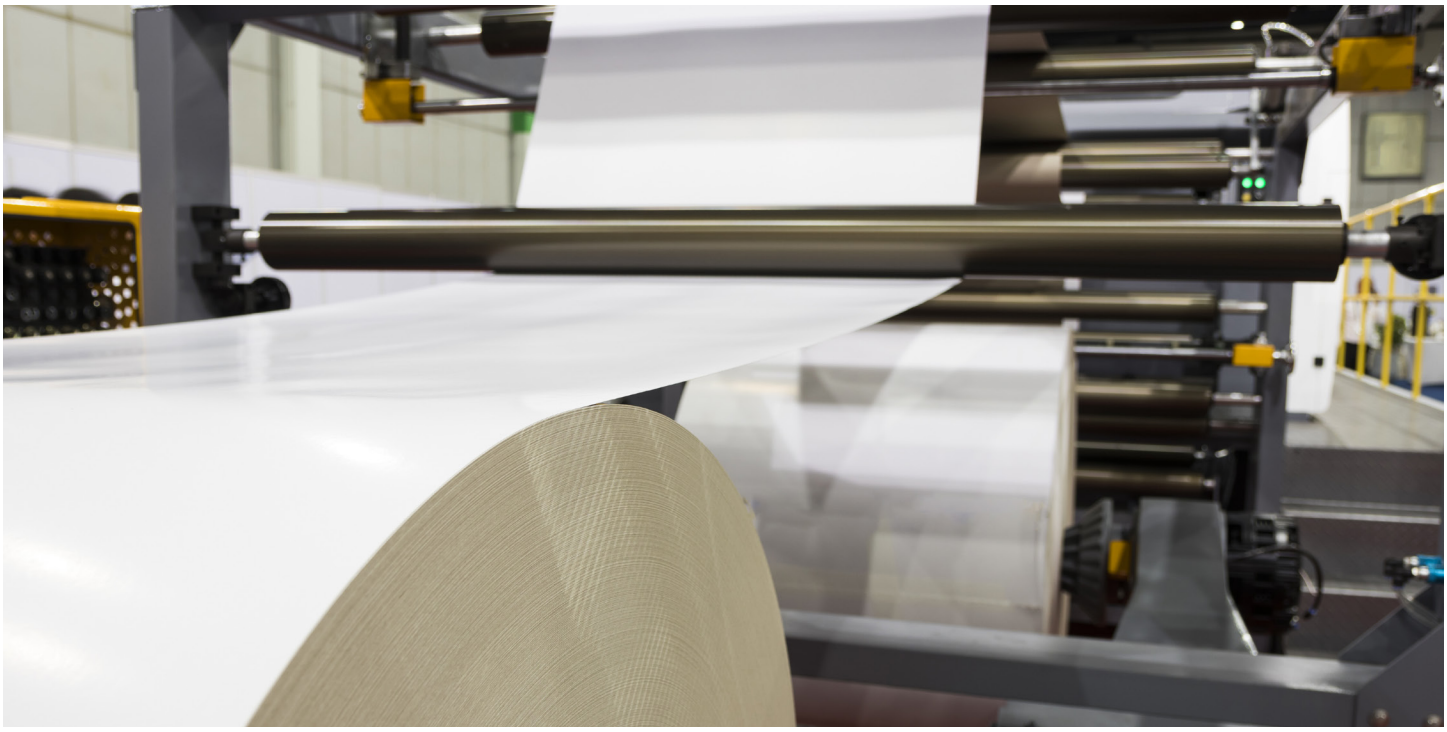
PULP AND PAPER PRODUCER MINIMIZES CYBERSECURITY GAPS

Major North American Company Trusted Honeywell to Assess Cyber Risks

Getting Ahead of the Problem

The number of malicious attacks on the modern industrial control system (ICS) is constantly growing. In today's challenging industrial cybersecurity environment, it's imperative to find weak spots in the control system architecture and take corrective action before threats can cause critical damage or disrupt operations. These malicious cyber threats may come in the form of accidents by staff, uninformed contractors, malicious software, hackers, and others.

Our customer, a major pulp and paper producer, realized that threats in its industry could lead to system shutdowns. So it was time to get proactive. Protection only works if you get ahead of the problem. Far ahead. So the customer reached out to the Honeywell team to assess its infrastructure.



AN EXPERT ASSESSMENT

Honeywell operational technology (OT) cybersecurity experts performed the Cybersecurity Vulnerability Assessment . This type of assessment is a general technical review of the ICS/OT infrastructure from the Process Control Network (PCN) through Level 3.5 Demilitarized Zone (DMZ) network and firewall performance.

The customer then received a detailed analysis of its OT cybersecurity processes, procedures, and safeguards used to protect its ICS from internal and external threats.

To perform such an analysis, our experts:

- Performed a basic walkthrough and inspection of critical areas of the ICS components
- Interviewed key personnel
- Assessed existing wired and wireless networks
- Identified possible problem areas with current networks
- Analyzed collected documentation

The Honeywell team also leveraged some of the highest industry standards and governmental guidelines, such as IEC-62443 and NIST 800-82.

After careful analysis, our experts created an ICS Cybersecurity Assessment Report. To help the customer better understand, prioritize and mitigate their cybersecurity gaps and vulnerabilities, we provided:

- Observations and recommendations report
- An Analysis of ICS survey results relative to cybersecurity
- A logical diagram of existing ICS infrastructure

OUTCOMES AND ACTIONS

Honeywell's Cybersecurity Vulnerability Assessment enabled this pulp and paper producer to better identify people, processes, and systems including vulnerable systems, networks, and applications. The assessment also provided step-by-step recommended actions to help address the identified vulnerabilities and help the customer adopt industrial cybersecurity standards.

The Honeywell cybersecurity consultants:

- Analyzed the collected documentation
- Reviewed the customer's security policies and procedures
- Discovered crucial access control weaknesses effecting OT assets
- Detected critical vulnerabilities in the ICS environment
- Identified problem areas within the network architecture

After completing the assessment process, the customer better understood the gaps that existed in its OT cybersecurity posture at each site. It can now actively work on remediation of those findings, with Honeywell providing support as required. If remediation support is needed, Honeywell consultants will visit each site and provide an executive summary of the progress made in addressing gaps.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.becybersecure.com

Case Study | Rev | 08/2021

THE FUTURE IS WHAT WE MAKE IT

Honeywell