A Large Petrochemical Company Utilizes AutoSave in its Goal to Achieve Cyber Immunity

THE CHALLENGE
A large multi-national petrochemical company seeking to harden its cyber-defenses (or said another way, seeking cyber immunity) realized the need to protect their controls environment against the inevitability of cyber-attacks. To accomplish this, they needed a way to track and control all of their programmable automation devices to protect them from unauthorized access. History has shown not managing these devices well results in downtime, product errors and safety issues.

Specifically, the customer needed to protect the data in thousands of automation devices in their upstream operations in the Permian Basin in the U.S. They are aware that one of the most dangerous ways to attack their operation is to gain access to control systems that operate and/or automate industrial processes, such as programmable logic controllers (PLC.) It was vital to find a solution for identifying and eliminating hazardous situations while controlling risks to production that can result from cyber-attacks targeting OT systems.

THE SOLUTION
The customer selected the market-leading solution that captures all automation device programmatic changes in support of the goal of cyber immunity = AutoSave. AutoSave provides the ability to:

- Back up data (configurations, logic, code, etc.) from industrial controls to a central repository with appropriate access protection/management, for both networked and non-networked devices.
- Authenticate users’ access to workstations
- Manage workstation backup/images
- Identify firmware and software versions for risk mitigation

These features enabled the company to prepare for an attack by securing program intellectual property, detecting unauthorized program changes, and rapidly restoring and recovering the correct program after an attack.
RECOVER:
With an archive of all program revisions, using AutoSave, users can quickly restore the latest approved program after an unauthorized change.

PREPARE:
AutoSave saves a copy of each program revision in a central repository. Access to program folders and programs is managed via a flexible privileging system.

DETECT:
AutoSave compares the latest program copy on file in AutoSave with the program running in each device to identify any differences. If differences are found, the appropriate people are notified with an email highlighting the differences.
THE RESULTS

This customer is now using AutoSave to manage all program configurations. AutoSave is authenticating users that have permission to make a change to the program. However, if a change is made outside of the AutoSave, they have greatly increased their resiliency against a breach to the controls system simply by knowing right away that a breach has occurred and being able to quickly revert systems back to the state they were in prior to the breach. To restore operations, the latest approved program can now be downloaded to the device very quickly. For operations to maintain uptime when faced with normal hazards, such as power outages, human error and equipment failure, AutoSave enables users to quickly retrieve the most current copy of the program and resume operations. When the change is malicious and unauthorized, AutoSave becomes even more vital in reaching cyber immunity.

MORE INFORMATION


Petrochemical Industry Article: “A cyberattack on a U.S. gas pipeline has us asking: Are utilities prepared for a rise in cybersecurity attacks and what can be done about it?”