DYNICS' INDUSTRIAL AUTOMATION SOLUTIONS, SECURING THE OT NETWORKS FOR THE AUTOMOTIVE MARKET

Overview

DYNICS, a leader in industrial automation solutions, plays a pivotal role in transforming the automotive industry with innovative technologies. This application case explores how DYNICS' Industrial Computers, OT Cybersecurity solutions ICS360.DCC, ICS360.Defender and Veracity OT SDN (software-defined networking) solutions have significantly enhanced operational efficiency, sustainability, and security in automotive manufacturing and highlight the benefits and outcomes of these strategies.

Challenges

Operational Efficiency

Unauthorized Access & Insider Threats

Scalability & Regulatory Compliance

Solutions

Product Lifecycle/Sustainability

Security for Industrial Computers and Networks

Simplified Network Management and Enhanced Scalability

Implementation

1. The first step involved a thorough assessment of the existing OT network infrastructure. This included identifying key areas for improvement and planning the integration of Dynic's ICS360.Defender and OT SDN to address specific challenges.
2. The deployment phase involved OS management, configuring ICS36.Defender Rule Sets, Creating policy within the OT SDN Controller to operate under the Zero Trust and Deny by Default models. This can be accomplished with minimal disruption to ongoing production activities.
3. The DYNICS total solution is configured to meet the specific needs of the individual automotive manufacturer or facility. Extensive testing ensures that the system effectively detects and mitigates potential threats.
4. Comprehensive training sessions is available for network administrators and OT support staff to ensure they are equipped to manage and maintain the new system. Ongoing support is also available to address any issues and optimize performance.

Results

Increased Efficiency and Resilience

Automotive manufacturers using DYNICS' solutions have reported significant reductions in downtime and maintenance costs, leading to higher productivity.

Improved OS Security

With Unified Write Filter (UWF) technology and whitelisting, manufacturers have experienced fewer security breaches and blocked installation of unauthorized software on industrial pcs and servers.

Simplified Network Management, Scalability and Compliance

The centralized management capabilities of ICS360.DCC and the SDN OT Controller have significantly reduced the time and effort required for network configuration and maintenance.

Conclusion

DYNICS' industrial automation solutions, along with the implementation of hardened and secure industrial computers, comprehensive OT Cybersecurity products such as ICS360.DCC, ICS360.Defender and SDN in OT networks have revolutionized the critical components of automotive manufacturing. The adoption of Zero Trust Networks and a Deny by Default approach has been highly effective in securing the automotive manufacturer's OT network. By eliminating implicit trust and enforcing strict access controls, these security strategies have enabled the company to protect critical assets and maintain a robust security posture in an increasingly complex threat landscape.