LOGIIC™

Linking the Oil and Gas (O&G) Industry to Improve Cybersecurity

In 2022, LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) surveyed asset owners and vendors to understand how they approach Multi-Factor Authentication (MFA) and Allowlisting in their operational technology environments. LOGIIC members developed the following positions on MFA and Allowlisting based on the analysis of the survey results and member best practices.

MFA Position:

On the topic of multi-factor authentication, the best practice access approach is to implement MFA at logical boundaries and provide physical badge access to the control rooms. This ensures that all ingress points, logical and physical, are protected. Anything beyond this would be additional layers of security and would be aspirational.

Allowlisting Position:

For allowlisting functionality, the best practice recommendation is to block unauthorized applications, services and code in the operational technology (OT) environment. Allowlisting will not be implemented in the information technology (IT) environments that are not directly connected to the OT environment and not required for OT operations because there is sufficient risk mitigation at the OT/IT boundary with protections such as firewalls.

LOGIIC Survey Results

These are key findings from the MFA and Allow-List survey:

Multi-Factor Authentication:

1) Two of the MFA vendors said they helped their customers to implement MFA for non-service accounts accessing information in Operational Technology Systems and the other one was planning to address this.
2) Two MFA vendors said their product was not certified by any Automation Vendors; One other said they were certified by two vendors and to NERC CIP.
3) Half the Automation vendors said they don't have certified MFA solutions, and another said they provide the MFA solution as part of their product.
4) Pipeline Operators had greatly different approaches to MFA in the operational technology environment. Some focused MFA on remote access only while others implemented it on different components of IACS.

Allowlisting:

1) Allow-List vendors were able to apply their technology to both information technology and operational technology systems.
2) Automation vendors described their solutions as being Allow-List capable. Allow-List requirements were driven by budget and/or staffing limitations.
3) Automation vendors who responded to this survey had not certified any Allow-List solutions to work with their automation products.
4) Pipeline Operators said they had already implemented or were in the process of implementing Allowlisting solutions. Only one Pipeline Operator believed they had fully implemented Allowlisting both in its information technology and operational technology environments. Only one Pipeline Operator said they would be implementing allowlisting.
5) 40% of the Pipeline Operators had found an Allow-List solution certified by their Automation Vendors; the other 60% did not find a certified solution; of these 2 of 3 Operators planned to use a non-certified Allow-List product.

About LOGIIC

The Linking the Oil and Gas (O&G) Industry to Improve Cybersecurity (LOGIIC) consortium was established in partnership with the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate to review and study cybersecurity issues in industrial control systems (ICS) that impact safety and business performance as they pertain to the O&G sector.