Industrial security now includes cyber security.

The **Vulnerability Discovery Service** can help you face the increasingly common and costly cybersecurity threats in industrial infrastructure.

ASK YOURSELF

○ Do you understand what assets are connected to your critical applications?

○ Do you know what your most significant cybersecurity threats are and have you addressed them?

○ Are you vulnerable to third-party applications hosted on your network?

○ Does your company have a disaster recovery plan after a cyberattack occurs?

WE HAVE THE EXPERIENCE TO HELP

The first step to securing critical protection and coverage against cyberattacks is a Rockwell Automation Vulnerability Discovery Service. This service can be delivered by your local Rockwell Automation Authorized Service Provider.

A Vulnerability Discovery Service is designed for Customer ease of use. This service will provide visibility into your industrial network assets with no additional hardware, no configuration, and no risk of disruption. The results will provide information to **assess and prioritize** your OT network security risks through asset inventory, vulnerability details, and a risk assessment report.

Rockwell Automation

CHALLENGES YOU FACE

Skills gap

- Lack of qualified personnel
- Achieving productivity goals
- Lack of staffing to expand operations

Vulnerability

- Security is an after thought & standards are evolving
- Aging industrial control systems and protocols
- Lack of proper policies and precedures

Lack of flexibility

- Low adoption of risk management processes
- Shadow/ Stealth IT
- Lack of tools to manage infrastructure
- Too much data, lack of actionable information

IT/OT convergence

- Lack of comprehensive asset inventory
- Integrate: customer demand, supply chain, and industrial processes
- Integration of new technologies

Benefits

Proactively discover your **vulnerabilities, misconfigurations, and unsecured network connections**

Reduce cyber risk in your industrial infrastructure

Identification and classification of assets across your ICS network

Actionable plan for remediation of your hidden threats

WHAT TO EXPECT

1 Vulnerability Discovery Service preparation

The process begins with a pre-site kickoff call with a Rockwell Automation Authorized Service Provider (ASP).

2 On-site data collection process

An ASP Deployment Engineer will run a light weight executable on your plant network to perform the data collection.

3 Remote data review

The captured data is returned to Rockwell Automation for processing and analyzed through the Claroty Threat Detection Software.

4 Study delivery

The Risk Assessment Report is created from analyzed data providing you with an overall health check that you can use to understand all the assets on the plant network along with any Common Vulnerabilities and Exposures (CVEs) that may affect those assets.

The report will provide the following:

- Full Asset Identification of the Environment
- Visibility into IT/OT/IOT assets
- Vulnerability information for Assets (e.g., CVEs)
- Risk identified for assets (e.g., mis-configurations)

Authorized Service Provider
A ROCKWELL AUTOMATION PARTNER

For more information:

Connect with us.

rockwellautomation.com

expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication ASP-SP009A-EN-P March 2024