CASE STUDY

AUTOMATED VULNERABILITY MANAGEMENT

IN PHARMACEUTICAL AND MEDICAL DEVICE MANUFACTURING

Cyber security in pharmaceutical and medical device manufacturing poses a significant challenge. Legacy equipment, regulatory requirements on validated and/or quality systems, geographically distributed plants often segmented from IT networks, and proprietary embedded devices combine to create barriers to successful vulnerability and security management in these environments.

THE CHALLENGE

A large pharma/medical device manufacturer with dozens of plants worldwide needed to manage vulnerabilities and security posture in manufacturing networks. They tried traditional IT tools such as vulnerability scanning, patch modules, anti-virus, etc. Unfortunately, these tools were inefficient in the segmented networks and created operational and regulatory risks from scanning and changing settings without proper manufacturing team involvement.

VERVE

CASE STUDY

VULNERABILITY MANAGEMENT

PHARMA & MED DEVICE

The client needed an OT-safe vulnerability management approach that provided visibility, assessment, and the ability to remediate efficiently.

The critical customer needs included:

- Visibility into all IT and OT endpoints
- Deployment in multi-site environment with segmented networks
- Endpoint and network vulnerability assessments without running intrusive scans
- Enable analysts to "think global, act local" to scale limited resources with central analysis with safe, plant-level action
- Ongoing solution - not a one-time "event"
- Services resources with deep manufacturing experience to work with operations leaders

THE SOLUTION

The Verve Security Center (VSC) was selected to extend industry-leading BigFix software into OT so leadership could use the same tools as their IT counterparts.

Within one platform, they manage all of the complex proprietary devices that exist in an OT environment using Verve's agentless device interface (ADI).

VSC's "think global, act local" architecture enables multi-site reporting and analysis, with localized actions for patching, configuration, and other protective management.

Assess

- All endpoints
- Network & access

Remediate

- Multiple tools
- Single database

Report

- Multi-site/server
- Easy to use UI

OT-Safe

- Non-intrusive
- Operator controlled
- Proven

FEATURES

- Coverage across all OT vendor platforms
- Integrated IT-OT-IoT management
- Comprehensive solution for NIST CSF, CIS Top 20, and other standards
- Software-based agent and agentless architecture deploys in minutes
- Detailed vulnerability assessments across all hardware, software, & configuration settings
- Closed-loop: Assess and remediate in the same platform
- Think global, act local: Central reporting, analysis and planning with local control over actions
- Rapid, RestAPI integrates with current tools

BENEFITS

- More efficient, integrated IT-OT solution
- Lower cost and faster deployment than alternative OT options
- No impact on network or endpoint architecture
- Faster time to resolution with a single database and console for incident response across all endpoint and network information
- Increased efficiency with central analysis and local action
- Faster time to remediation with closed-loop assess-remediate platform
- Proven safe for all OT environments
- Easy-to-use operations personnel with little additional training required

To learn more, visit www.verveindustrial.com or contact us at info@verveindustrial.com