SCADAfence

Case Study

Taro Pharmaceutical Industries Secures Its Connected OT Environment with SCADAfence Platform

Taro – Global Pharmaceutical Manufacturer

Taro manufactures high-quality, proprietary and off-patent pharmaceuticals in countries such as the US, Canada and Israel. The company manufactures a wide range of prescription and over-the counter products that are distributed globally in dozens of countries. To maintain its global reputation and its competitive edge, Taro has heavily invested in the adoption of advanced technologies that improve operational efficiency and reduce operational costs. These new technologies require increased connectivity between Taro's operational technology (OT) network and their IT systems, as well as increased connectivity to the Internet in order to enable remote maintenance and advanced analytics. In addition, new regulations, such as adoption of Track and Trace systems, as dictated by the FDA, require the establishment of connectivity between machines on the production floor and external, cloud-based systems.

Increased Connectivity Introduces New Security Challenges

Adoption of new technologies within the OT environment has led to a significant increase in the number of devices and the traffic between them. Maintaining the newly-connected OT network using older, manually-generated asset inventory methods proved challenging, as a series of unexplained incidents was difficult to investigate. Moreover, Taro's management was aware of the ever-growing OT attack landscape, in which pharmaceutical manufacturers Merck and Mondelez suffered hundreds of millions of dollars in damages due to attacks on their OT networks.

The fear of a potential attack and the difficulties in controlling OT network activities led Taro to implement a solution that provides the required visibility and security, while taking into consideration the unique characteristics of their OT environment. After evaluating several solutions – including both dedicated OT systems and generic IT security systems – the Taro team decided to deploy SCADAfence Platform, which features continuous monitoring of their OT environment, a deep understanding of OT protocols and equipment, and a user interface that is ideal for use by their OT engineering team.

"SCADAfence's accurate asset inventory and visibility tools allowed me to stop using outdated spreadsheets and to completely digitalize our network management"

Alex Segal, OT Network Administrator, Taro

TARO

Executive Summary

- ***Taro – multinational pharmaceutical company***
  - *Multinational pharmaceutical company with more than $4B in revenue*
  - *Products include over 180 drugs sold in 25 countries*
  - *Manufacturing site produces chemical-based active pharmaceutical ingredients (APIs)*
  - *Complex environment with hundreds of industrial devices on seven production floors*
- ***Taro's Challenges***
  - *Secure OT network, characterized by increasing connectivity and complexity due to regulatory requirements and adoption of advanced technologies*
  - *Overcome lack of visibility into network activities of external contractors and remote maintenance traffic*
  - *Maintain leading position in a competitive market, despite strict FDA regulations that require complete control over production operations*
- ***SCADAfence's Platform***
  - *Accurate asset inventory and visibility that complies with regulation requirements and accelerates adoption of new technologies*
  - *Enforces company information security policies and improves OT network resilience and employee awareness of threats*
  - *Anomaly detection in OT network allows Taro to identify malicious activities and operational errors*

Digitalized Asset Inventory and Risk Reduction

Taro's OT network was built over the years with the help of multiple external contractors and includes equipment vendors such as Rockwell Automation, Siemens and Schneider Electric. Thanks to SCADAfence's ability to non-intrusively monitor these systems and their proprietary protocols, the platform was able to completely digitalize the asset inventory and build an interactive network map, that together, provide unprecedent visibility into day-to-day operations. SCADAfence was able to complete the discovery phase within a matter of hours, and immediately started to provide insights into risks and threats that jeopardize operational continuity. For example, the platform mapped connectivity between Taro's OT network and the Internet and detected new connections – in real time. These new connections were established by employees who needed to update software in the production network. SCADAfence's platform allowed Taro's administrators to immediately enforce the company's policies and to allow only secure and authorized connections.

Benefit Highlights

- Complete visibility of network architecture, assets, connections, and traffic
- Discovery of all devices that communicate with external networks
- Deep knowledge and inspection of OT protocols and warnings upon discovery of anomalies
- Continuous threat detection of malicious and other abnormal activities

Anomaly Detection Goes Beyond Security

Once the SCADAfence Platform completed the discovery process and generation of the network baseline, Taro's OT team started to receive alerts about deviation from normal operational activities. Such abnormalities may be related to malicious threats, but in some cases, they are caused by human error, misconfigurations or malfunctioning equipment. Thanks to SCADAfence's ability to perform deep packet inspection (DPI) on OT protocols, Taro's OT team could track activities, such as firmware updates and configuration changes on their critical-path industrial controllers. In one case, a configuration change was mistakenly performed on the wrong controller. SCADAfence detected the anomalous activity as a deviation from the normal communication pattern between the controller and the management system. The early detection by SCADAfence allowed the Taro OT team to quickly identify the root cause and to minimize its effect on their production activities.

Network Monitoring as an Enabler of Improved Operations

Taro's new digital, continuous view of their OT environment allowed them to reduce operational downtime, enhance network security, and comply with demanding industry regulations. Constant monitoring of all activities within the OT environment allowed Taro to maintain an up-to-date inventory of their production assets, and a complete log of operational configuration changes – data that is crucial for pharmaceutical companies undergoing strict FDA audits, which include inspection of information security and network management capabilities. Taro's new strategy to expand connectivity with external environments was accompanied by the right tools that helped to preserve security as well. By integrating SCADAfence's leading monitoring platform into their Industry 4.0 journey, Taro can ensure the security and operational continuity of its cutting-edge manufacturing facilities.

"Our dynamic and advanced production environment, together with regulator demands such as Track and Trace systems, required a significant improvement in our security capabilities. With SCADAfence, we feel secure while we bring our production environment into the Industrial IoT era"

Itzik Baruch, VP Technical Services, Taro