OTORIO enables integration of OT assets in the automotive industry

A global automotive manufacturer was looking for ways to enable safe OT integrations of lines, machines, and assets into the production floor

Our Findings

The client lacked the security personnel and knowledge to operate complex cyber security solutions to manage their supply chain risk. The process of validating the cybersecurity policies delayed the introduction of new machines into the production shop floor.

Because there was no process to track changes in assets and configurations, critical actions to reduce the risk to the production floor were neglected. We saw that separate systems were handling different security aspects in the OT network and there was only a partial understanding of risk prioritization.

Background

The customer, a manufacturer of commercial vehicles, needed to automate many of their manual security tasks. In addition, they wanted a reliable way to monitor third parties, who might introduce security threats to their production line and possibly increase their attack surface.
OTORIO was tasked with:

- Providing employee training to run complex, cyber security solutions and manage supply chain risks
- Improving and automating the procurement process, to ensure that vendor deliverables are secure and comply with industry standards and company security policies
- Validating the cybersecurity policies in a more efficient way

Moving forward

OTORIO's promoted this organization's business continuity with efficient offline cyber risks monitoring. The client saved time by replacing manual and less comprehensive verification processes with a quick and automated scanning process and gained the tools and strategies to monitor third party security issues.

Recommendations

OTORIO provided the client with spOT so they could scan devices as an integral part of their own security process. They now have unique and sensitive, asset stand-alone discovery, that provides full visibility on each asset within the machine.

spOT also enables smart analytics, threat intelligence, known vulnerabilities discovery and remediation guidelines, and patch impact predictions. The tool automatically generates security and compliance reports and provides vendor/supplier statistics. They are now in a better position to comply with industry standards and enforce policies.

The client has control over the tested policies and the vulnerabilities that are checked, based on OTORIO's threat intelligence research.

We enabled the client to gain tighter control of third-parties that are introduced to the production network. We gave guidelines for the validation and enforcement of configuration baselines. We supervised, verified, and collected vendor-based operational-related statistics. This was done with a simple setup that didn't require any network changes.