Case Study

Scheer

Creating New Cyber Security Compliance Program at a Major Technology Manufacturer

Summary

A global technology manufacturing organization received new compliance requirements from the Department of Defense (DOD) regarding cyber security at their manufacturing plants. The organization did not have any processes documented relating to the new requirements. The new processes had to be implemented across dozens of plants in the US which brought in another layer of complexity. Each plant had different types of equipment that would need to be evaluated for cyber compliancy based on when the equipment was manufactured and if it could connect to the network. Another hurdle to tackle was to make sure that the unionized plants could still use the processes since they had union rules to navigate as well. The strategy for this project was to break it down in such a way as to not overwhelm the team considering there were many variables involved. One, non-unionized, manufacturing plant was selected to be the test site for the new processes. The team created new processes as a basis for an onsite workshop at the plant. Once onsite, the team was able to test the processes in real time to make sure they could be implemented in a pragmatic way (the real time testing of processes was referred to as GEMBA walks). The new process models finalized after the GEMBA walks were considered to be reference models that the other plants could use to create specific variants, if required, based on different equipment types and union policies.

Organization Background

The organization stands as a prominent global leader in the aerospace industry, specializing in advanced aircraft engines for both commercial and military applications. With over 100 years of experience in this industry, they have a wealth of knowledge and experience in the aerospace industry. The organization has adopted Lean methodology to continuously improve their processes. They are enriching their Lean culture by embracing BPM and the use of process modeling and repository management. Based in the US, they have successfully cultivated partnerships with renowned manufacturers worldwide, expanding their business horizons and amplifying their offerings. With a robust workforce exceeding 50,000 employees, they operate across more than 100 countries, solidifying their international presence and ensuring efficient operations on a global scale.

Business Challenge

The DOD created new cyber security requirements based on the growing threats of cyber breaches happening across the world. The organization didn't have any processes documented that would make them compliant with the new regulations. These processes would have to be created from scratch and they would have to be implemented across many manufacturing plants in the US. This was a daunting task because there were many different types of equipment in each plant, with different entry points where a cyber security breach could happen. The cyber processes had to encompass each type of equipment and bring them all into compliance with the new regulations. The organization had to evaluate the differences in unionized plants vs non-unionized plants because the new compliance requirements also had to follow union rules as well.

The Solution

A smaller, non-unionized, manufacturing plant was selected to be a pilot site where reference process models would be created. We first created drafts of the cyber process models based on tasks that were already being performed at the plant regardless of DOD regulations in order to reduce the risk of a cyber-attack. We then held an onsite workshop at the plant. During the workshop, we used a modified Toyota Kata method to guide the team during the creation of the To-Be process models in their process repository. This method was used by asking the following questions:

- Where do we want to go (To-Be state)?
- Where are we now (As-Is state)?
- How do we get from the As-Is to the To-Be state?
- What obstacles are there and how do we remove them?

We used this method in order to have a more focused discussion. This also helped the team feel less overwhelmed by the prospect of creating brand new processes by having a framework to follow during the modelling sessions. Once the process models were created, team members would go to the shop floor and test out the process in real time (GEMBA walk). The processes were able to be refined based on the observations on the shop floor. For example, the team originally hypothesized that scanning for Malware with a TMPS stick would take hours and it would interfere with manufacturing schedules. When performing the GEMBA walk on the shop floor, the team observed that it took on average15 seconds to perform the scan and did not interfere at all. We were then able to adjust the process models and make it more practical for the plant employees to perform the new compliance tasks. The new reference models were then used as accelerators to bring other similar plants into DOD compliance. The reference models were then used to create variant models at other plants that had union rules and/or other types of equipment not found at the test plant thereby increasing the efficiency of implanting new DOD requirements at all plants in the US.

Results

A successful project achieved the following results:

- Cyber security processes were able to be implemented at the pilot plant, immediately bringing them into compliance with DOD regulations and reducing the risk of a cyber-attack.
- The process models were used to train the shop employees in their new responsibilities for cyber security.
- The reference models were also used as accelerators to bring dozens of plants that did not need process variants into compliance without needing to conduct process workshops.
- Other plants that needed process variants due to other compliance obligations were able to use the reference models as a foundation to their specific process needs. This allowed those plants to quickly implement their variant processes so that they were compliant with the DOD regulations as soon as possible.
- Using a process modeling approach within their repository to model the new processes allows the organization to quickly update the cyber processes if and when the DOD updates their compliance requirements which will reduce implementation time and reduce the risk of a cyber breach.
- Creating the process models in the repository also allows the organization to run reports and immediately see which systems, roles, and processes are affected if a cyber attack does occur which reduces the reaction time of the breach.

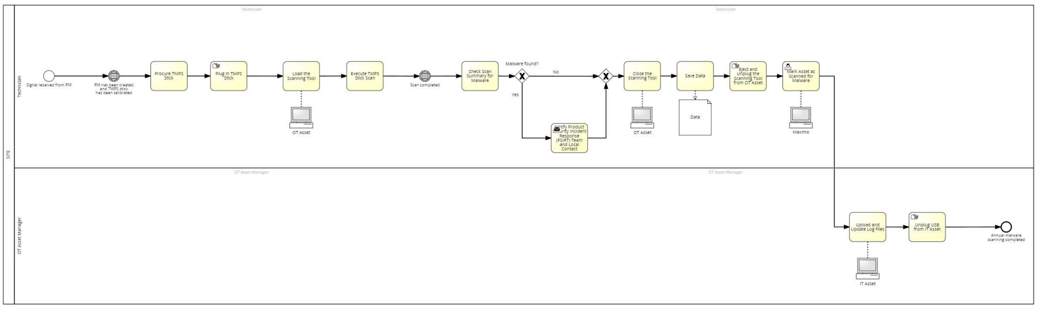
SITE
Technician
Signal received from PM
PM has been created and TMPS stick has been calibrated
Procure TMPS Stick
Plug in TMPS Stick
Load the Scanning Tool
OT Asset
Execute TMPS Stick Scan
Scan completed
Check Scan Summary for Malware
Malware found?
No
Yes
Notify Product Security Incident Response (PSIRT) Team and Local Contact
Close the Scanning Tool
OT Asset
Save Data
Data
Eject and Unplug the Scanning Tool from OT Asset
Mark Asset as Scanned for Malware
Maximo
OT Asset Manager
Upload and Update Log Files
IT Asset
Unplug USB from IT Asset
Annual malware scanning completed

Figure 1: Example process for 'Perform Malware Scanning'

Do you have questions on these subjects, or would you like to talk with us about specific projects?
Simply send us an e-mail or give us a call!

Dr. Mathias Kirchmer | Managing Director | Mathias.Kirchmer@scheer-group.com
Website: https://www.scheer-americas.com