Charter of Trust

Partner Use Case

Siemens

Responsibility throughout the digital supply chain

Starting point

Like most Partners of the Charter of Trust, Siemens has a complex and diverse supply chain. Cybersecurity risk in the supply chain is seen as one of the most important risk areas these days (see the latest *Allianz Risk Barometer*) and we need to reduce it to an acceptable level. We faced several challenges:

- Literally every company matters as communication among companies happens electronically.
- The operation of each company today depends to a large extent on up-and-running IT infrastructure.
- IT hardware, software, sensors, and connectivity are very often part of products and services.
- Traditional ways of assessing a company or a supplier are not suitable at this scale.

Objectives

We looked for a proactive approach to increase the cybersecurity posture in our business ecosystem before cybersecurity regulation becomes mandatory. The approach needed to be based on international standards and suitable to be applied globally. That is important in a time of increasing national regulation due to sovereignty politics.

The Charter's Principle 2 Baseline Requirements (described in our Risk-based Approach since 2018) are the common ground all CoT Partners have agreed to. They define the common content and maturity regarding cybersecurity that we expect from every company. This is, from our perspective, the necessary starting point to further develop cybersecurity maturity along the supply chain.

We wanted to test different approaches to verify adherence to our Baseline Requirements. Several approaches were considered to serve the global needs of our organization and Charter Partners in terms of cost, speed, fit for purpose, and local preferences. The idea was to reuse supplier verification results to improve our overall efficiency. The sheer scope of the task required various different solutions and service providers.

Description

As the P2 Baseline Requirements are derived from international standards, we wanted to use existing solutions to verify them. For this, we obtained proposals from:

TÜV SÜD – based on questions selected from ISO 27001 and IEC 62443 verifications

CyberVadis – based on their questionnaire focusing on ISO 27001 and NIST SCF

Panorays – based on the CAIQ 4.0 from the CSA (Cloud Security Alliance)

We also plan to test OneTrust with a selection of the SIG lite

After an internal global announcement in our cybersecurity newsletter, we received several requests from colleagues to join our test phase from November 2021 to April 2022.

Lessons learned/results

Main takeaways:

We achieved our goal to identify suitable external service providers to help us verify our vendors' adherence to the P2 Baseline Requirements. This will enable us to efficiently scale the transparency in our supply chain as needed.

All approaches have different strengths and weaknesses, but all are appropriate so far.

Challenges:

It can be difficult to identify the relevant stakeholders in global organizations (the global CoT newsletter was our breakthrough).

Typically, service providers want to sell their standard solution. To convince them to offer a selection covering only the P2 Baseline Requirements was challenging.

Recommendations:

Start small with some pilot assessments so that your organization has time to learn and gain experience with the P2 approach. Scale will come almost automatically with the right solution.

Communication with all stakeholders is key. This includes business (risk) owners, cybersecurity, procurement, management, and vendors.

Regular progress reporting can help to maintain focus and spread the news.