Charter of Trust

Partner Use Case

TotalEnergies

Principle 2 "Responsibility throughout the digital supply chain"

Starting point

As a multinational enterprise, TotalEnergies has thousands of suppliers from many different countries all around the globe. The key challenge was to ensure that all of our suppliers meet CoT's Principle 2 baseline requirements so that there are no critical cybersecurity gaps in the company's supply chain. We had to achieve this no matter where in our complex organizational network these many suppliers are integrated.

Objectives

TotalEnergies wanted to ensure that all its suppliers have a sufficient level of cybersecurity maturity to:

- protect information and assets of the company
- ensure the continuity of the services provided to the company. The solution to be found should also cover all supplier stages: sourcing, contracting and delivery.

Description

TotalEnergies tackled the problem by making four structuring choices:

The first one was to ensure that the company had access to all types of suppliers in order to identify and focus on sensitive goods and services. Also, the process was started with centralized purchasing, local purchasing to be added later on.

Secondly, TotalEnergies deployed an industrial solution: The company assessed the cyber maturity of suppliers via a collaborative platform and provided reports about their maturity to suppliers, including recommendations for improvement.

Thirdly, the company decided to set up a dedicated support to assist buyers in making autonomous decisions in their supplier selection process. Moreover, TotalEnergies developed a communications kit, FAQ, and reporting mechanism to support this effort.

Lastly, TotalEnergies sought to tailor cyber requirements to the type of purchase. This meant the company had to formalize cyber contract requirements in order to make them applicable to all types of contracts.

This formalization of requirements resulted in three categories for purchases of IT and non-IT good and services: non-sensitive, sensitive, and very sensitive. Depending on the category of a purchase, supplier contracts would then include either 21, 54 or 64 cybersecurity requirements.

In addition to these varying requirements, TotalEnergies decided that for all sensitive and very sensitive purchases, a cyber assessment via an independent third-party provider is mandatory. Once an assessment is complete, the third-party expert issues a cybersecurity scorecard to suppliers, which clearly indicates the supplier's cyber maturity and provides recommendations for improvement.

Partner Use Case

TotalEnergies

Principle 2 "Responsibility throughout the digital supply chain"

Lessons learned/results

Overall, this process enabled TotalEnergies to define a cyber-governance covering the entire organisation, including controls and key security indicators.

To conduct such a major project, it is essential to support buyers and managers in your company with information and guidance. Moreover, it is key to explain the company's approach and rationale not only to buyers but also to suppliers to ensure an efficient and transparent process.

TotalEnergies is convinced that evaluating the cybersecurity maturity of sensitive and very sensitive purchases strengthens supplier relationships through greater trust and transparency.