

ENISA Good practices for IoT and Smart Infrastructures tool

1 Introduction

This tool intends to provide operators and industries of IoT and Smart Infrastructure with a quick guide to do their own risk assessment (identify threats and prioritise security areas of importance) according to ENISA's recommended security good practices.

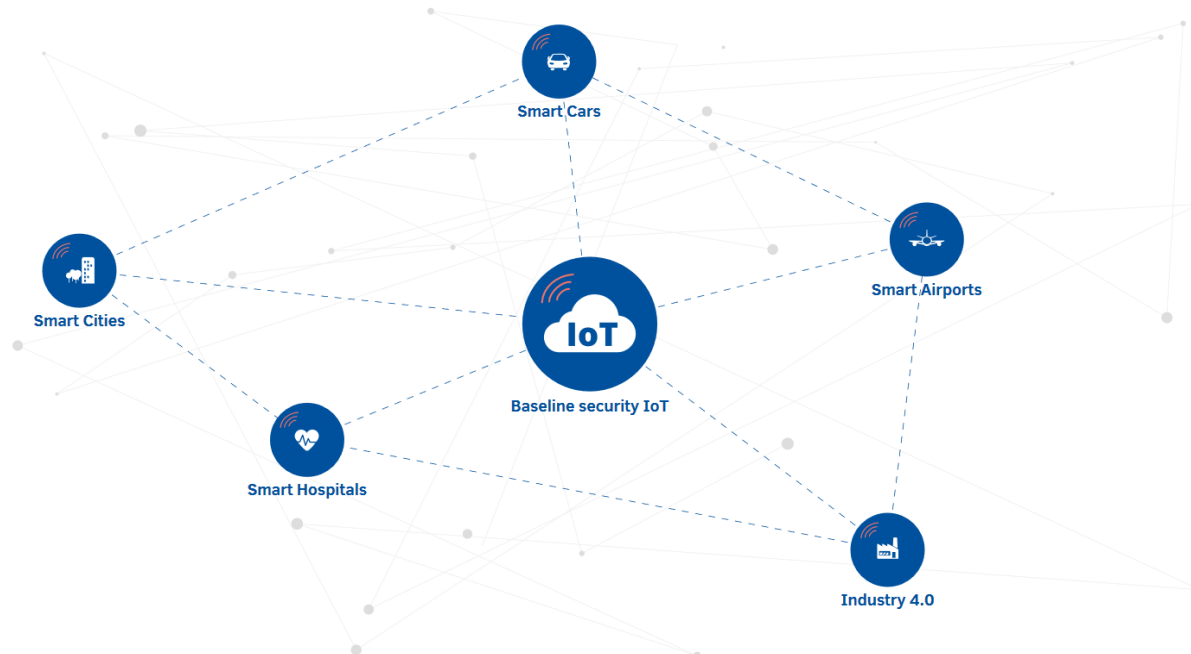
The tool lists security good practices for IoT, Industry 4.0, smart cars, smart airports, smart hospitals, and smart cities. By no means will every security recommendation be relevant to every user.

Each parameter/filter of the tool is addressing the following issues when implementing IoT:

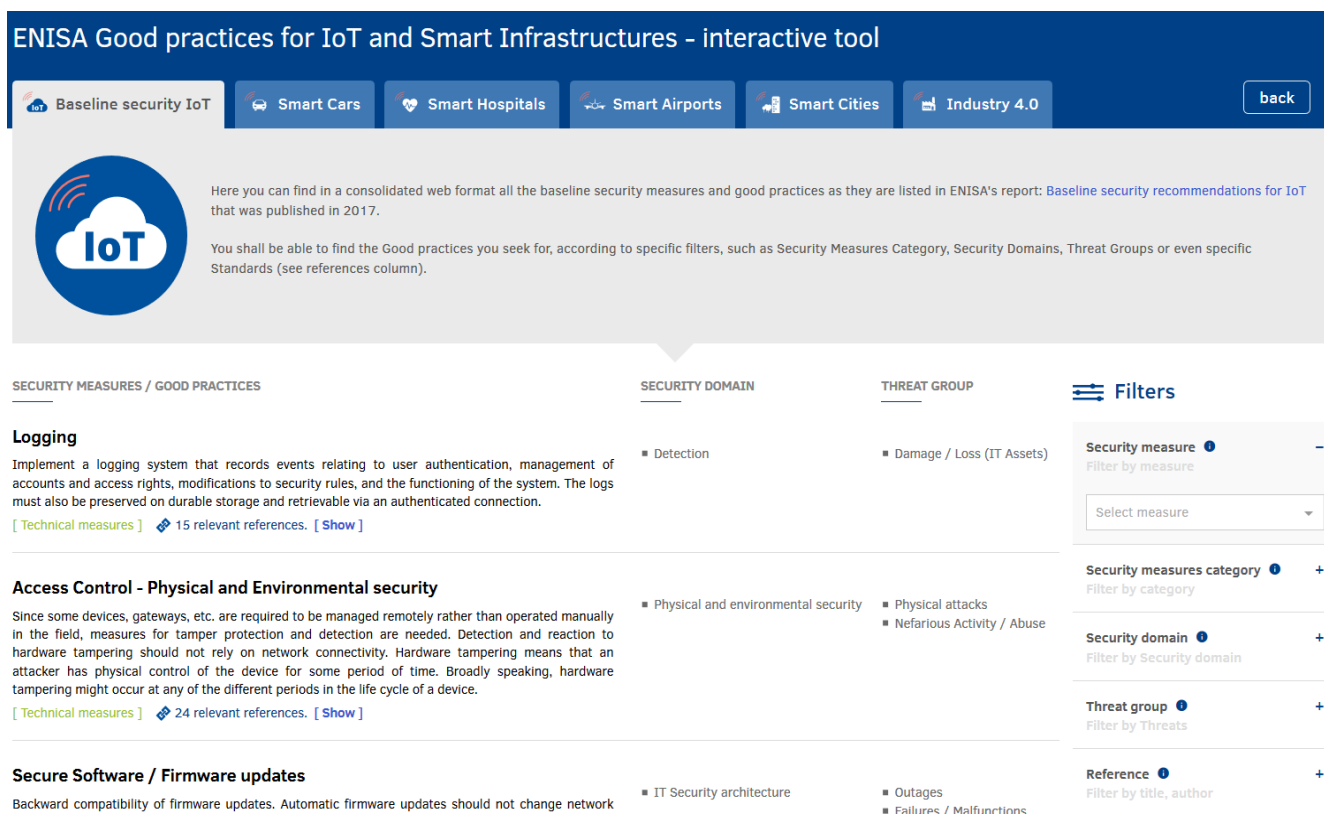
- Which are the threat groups from which you want to protect your organisation?
- What are the security domains you want to cover?
- Which are the categories of security measures you are looking for?
- What are the security Standards/Best practices that you would like to take into account for securing IoT in your organisation?

2 How to use

Step 1: Visit the landing page of the ENISA Good practices for IoT and Smart Infrastructures tool and click on the thematic area that you interested in finding out relevant threats, standards and/or security measures.



Step 2: Select the filters that are relevant for you, and then review the updated table with the Good Practices matching your search criteria. There is also the option (below the table) to print or export in xls format the results of your search.



3 Use Case Scenario

IoT in manufacturing and logistics

In the light of Industry 4.0, a manufacturer implements an IoT solution to track work pieces in real time and automate the flow of materials from the warehouse. RFID tags embedded on the work pieces allow sensors to transmit the position of each component to the relevant software that manages business operations in real time. With this new implementation, human operators refer directly to the business operations system to find out where and when orders are ready for processing. This change on the infrastructure improves a lot the production process but requires also extra attention and an update on the implemented security measures.

The CISO of the company wants to re-assure that this new deployment is secure and that it covers all the baseline requirements regarding Software and Firmware updates. The CISO accesses the ENISA IoT Baseline Security Recommendations tool to consult it. First, she selects from the Security measure column the item referring to Software and Firmware updates. The tool returns all baseline recommendations pertinent to this search (as identified in the ENISA report). The CISO now knows which are the baseline configurations for this issue (software / firmware updates) on IoT devices.