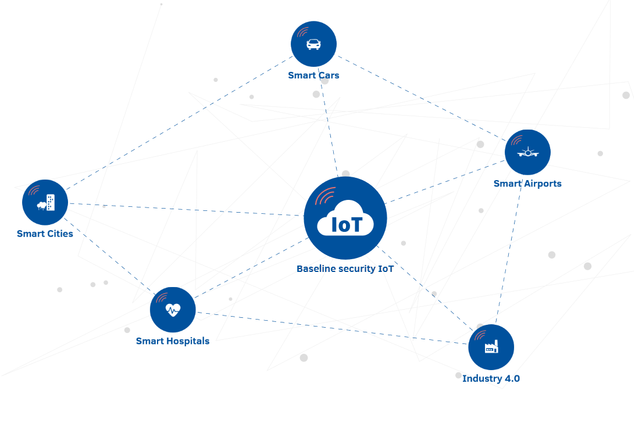
our must-have IoT security checklist: ENISA’s online tool for IoT and Smart Infrastructures Security

ENISA releases today an online tool aimed at guiding IoT operators and industries of IoT and Smart Infrastructure when conducting risk assessments.

Published on January 31, 2019



ENISA Good practices for IoT and Smart Infrastructures Tool

Tagged with

* [Internet of things](https://www.enisa.europa.eu/search?Subject%3Alist=Internet%20of%20things)

The tool, available at <https://www.enisa.europa.eu/iot-tool> , will help users save time when identifying threats and prioritising security areas of importance.

The tool provides a combined view of the security good practices that ENISA has been developing for the last years to secure [IoT](https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot), [Industry 4.0](https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-key-enabler-for-industry-4-0-adoption) and Smart Infrastructures, such as [smart cars](https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars), [smart airports](https://www.enisa.europa.eu/publications/securing-smart-airports), [smart hospitals](https://www.enisa.europa.eu/.../cyber-security-and-resilience-for-smart-hospitals), and [smart cities](https://www.enisa.europa.eu/publications/smart-cities-architecture-model/). The information provided through this tool for each thematic area reflects the information comprised in corresponding ENISA reports that have been released in the past.

The tool allows drawing comparisons between different IoT sectors, since the same ENISA threat taxonomy has been used when defining security measures.

When implementing IoT, each parameter or filter of the tool addresses the following issues:

* What are the threat groups from which you want to protect your organisation?
* What are the security domains you want to cover?
* What security measures categories are you looking for?
* Which security standards and best practices would you like to take into account when securing IoT in your organisation?

On the main webpage, the users of this tool can select the thematic area of interest and then identify the pertinent threats, standards or security measures. The tool accepts one or multiple search criteria to generate results that are most relevant to the users’ needs. Users can navigate through the list to find the Security Measures they seek, according to specific filters, such as Security Measures Category, Security Domains, Threat Groups or even Specific Standards. Additionally, the tool offers the option of either printing or exporting search results for further use.

For example, the CISO of a company wants to make sure the new deployment is secure and covers all the baseline requirements regarding software and firmware updates. The CISO accesses the ENISA IoT Baseline Security Recommendations tool and selects the item referring to ‘Software and Firmware updates’ from the ‘Security measure’ column. The tool returns all baseline recommendations pertinent to this search, as identified in the ENISA report. Now, the CISO is aware of the baseline configurations for this issue (software / firmware updates) on IoT devices of interest.