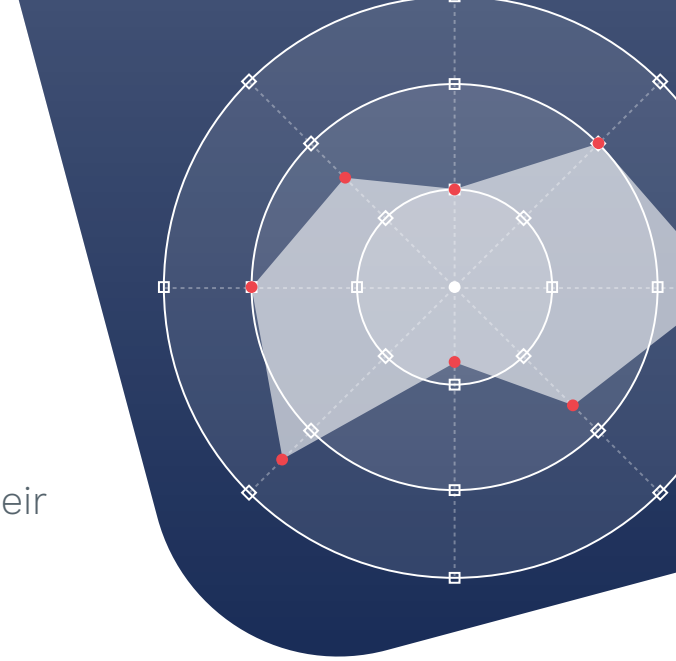
KUDELSKI IOT THINGS



IoT Threat Assessment

Identify the most likely security risks and their potential impact.

CONTEXT

Understand what matters

Connected systems and IoT devices are exposed to a wide range of risks, and companies who are developing IoT solutions need to identify the entry points that matter.

ASSESS
Analyze the threat and constraints landscape

Business Model Analysis
Technology Analysis
Contextual Analysis

UNDERSTAND
Become aware of threat scenarios

DEVELOP
Enable your dev team to reach security targets

PROTECT
Protect exposed assets and processes

Kudelski IoT Labs conducts comprehensive device and system-wide threat assessments that enable your team to secure your business investment and competitive advantage.

OUR APPROACH

Device and system-wide threat assessment service

Our Hardware, Network, Software and Crypto security teams offer a comprehensive combined expertise to support customers in understanding the device and system's potential surface of attack.

The proposed analysis aims at listing possible security threats taking into account the device target market, the presence of customer personal data, the plurality of communication interfaces and the manufacturing processes and partners. The reference threat model is based on an approach similar to the STRIDE methodology used in IT. STRIDE is a methodology developed by Microsoft for describing and categorizing security threats. Threats are classified around 6 security axes:

Spoofing of user or device identity | Tampering | Repudiation | Information Disclosure | Denial of Service | Elevation of Privilege

Each component, process, data flow, external entity, and data store – is exposed to a subset of threat categories, as described in the following table:

Components	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privileges	STRIDE
External entity or interactors	●		●				STRIDE
Process	●	●	●	●	●	●	STRIDE
Data / Keys storage		●		●	●		STRIDE
Data flow		●		●	●		STRIDE
Devices	●	●		●	●	●	STRIDE

Threats on components with STRIDE classification

DELIVERABLES

How we work together

1 Exploration phase

A dedicated technical workshop or conference call with your subject matter experts to review documentation and fully understand your context.

2 Threat model and scenarios

Development of a threat model through analysis of scenarios specific to your technology and context.

3 Threat assessment report

Publishing of a report using the STRIDE methodology with executive summary, a threat matrix, a list of proposed mitigations and recommended security controls.

4 Executive summary presentation

An executive presentation of the results highlighting the issues identified as critical can be provided on request.

OUR PROVEN METHOD

Three steps to IoT success

We have been designing and testing secure devices for our clients for decades. With our help, you can take new products to market with confidence using our proven methodology for IoT security threat identification, mitigation and validation.

IoT THREAT ASSESSMENT

We help you understand potential threats to your business, their likelihood and impact in order to focus security development.

SECURITY ARCHITECTURE REVIEW

We create a security architecture that addresses key threats defined during the Threat Assessment exercise.

LAB SECURITY ASSESSMENT

We test products against defined security requirements and spot any potentially business-impacting vulnerabilities.

ABOUT KUDELSKI GROUP

Kudelski IoT is the Internet of Things division of Kudelski Group and provides end-to-end IoT solutions, IoT product design, and full-lifecycle services to IoT device manufacturers, ecosystem creators and end-user companies.

These solutions and services leverage the group's 30+ years of innovation in digital business model creation; hardware, software and ecosystem design and testing; state-of- the-art security lifecycle management technologies and services and managed operation of complex systems.

$100B
revenues enabled annually

32
offices worldwide

3250
employees

$779M
revenues (2021)

500M
users

70
years of innovation