Federal Office
for Information Security

Deutschland
Digital•Sicher•BSI•

Market Surveillance

23.11.2022
ENISA Market Conference

Surveillance of continued compliance with the specified cybersecurity requirements

Market surveillance for certified and labelled products

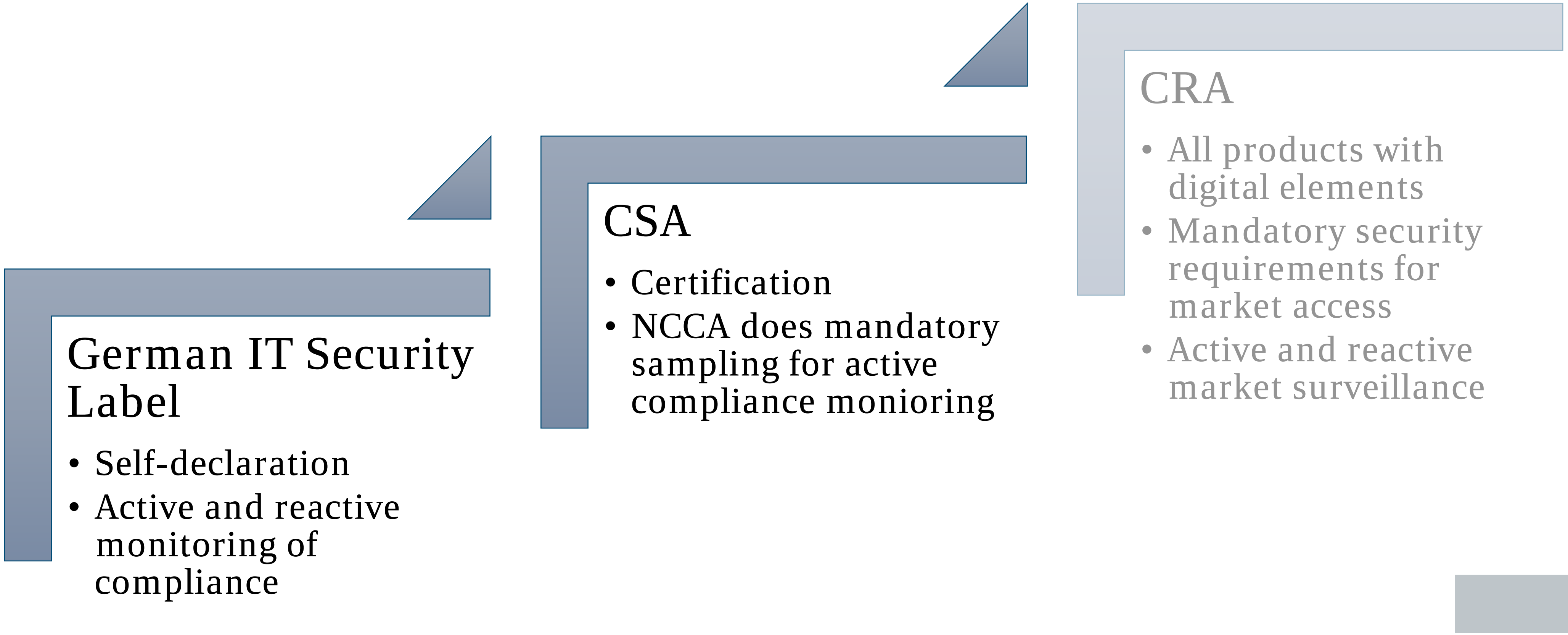
Samples products and tests for conformity

Reacts to reports of vulnerabilities

Can initiate ad-hoc security testing

Provides information about security status to the public for products labelled with the German IT Security Label

Market surveillance in the cybersecurity market



German IT Security Label

- Self-declaration
- Active and reactive monitoring of compliance

CSA

- Certification
- NCCA does mandatory sampling for active compliance moniroing

CRA

- All products with digital elements
- Mandatory security requirements for market access
- Active and reactive market surveillance

Minimal requirements of the CRA increase surveillance

Security requirements relating to the properties of products with digital elements
- Security-by-design, Security-by-default
- protection from unauthorised access; protection of confidentiality and integrety of data
- designed, developed and produced to limit attack surfaces […]

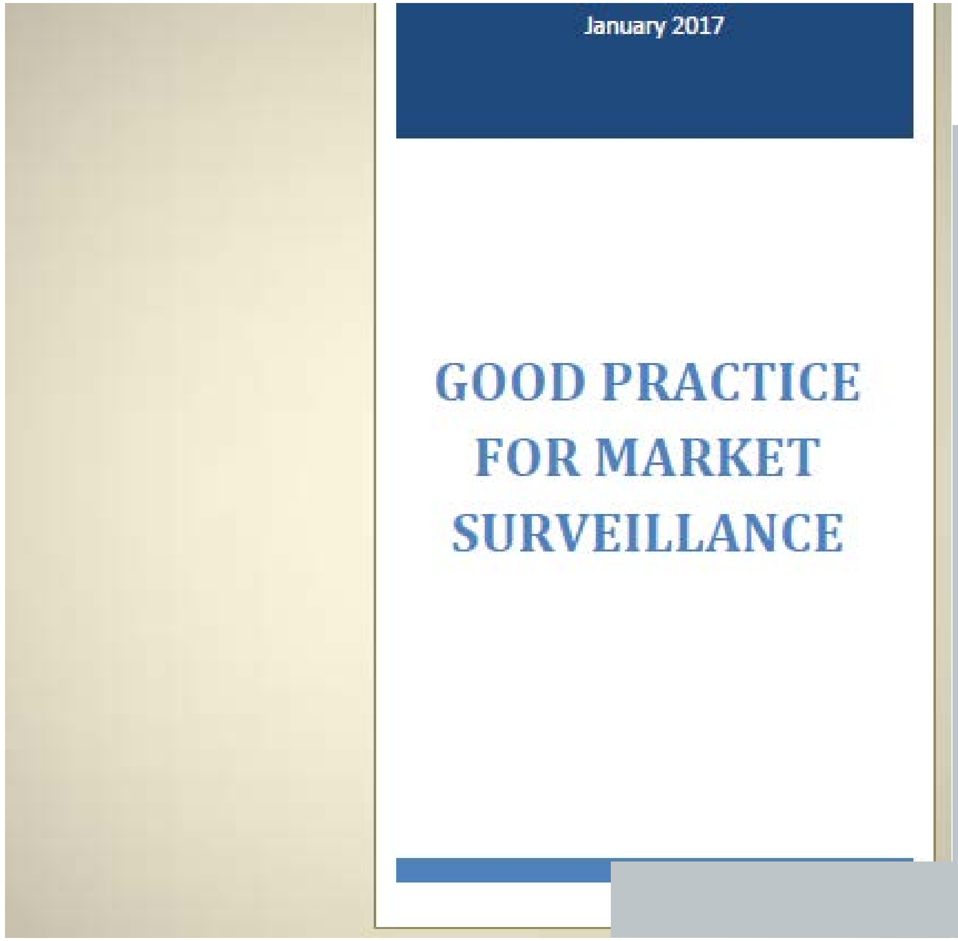
Vulnerability management
- SBOM at the very least the top-level dependencies of the product;
- Address and remediate vulnerabilities without delay, including by providing security updates
- Public disclose of information about fixed vulnerabilities, information allowing users to identify the product […]

Minimal information for the user
- Contact information where cybersecurity vulnerabilities of the product can be reported and received
- Identification of product
- Possibility to asses conformity information and if made available SBOM […]

Good practice for market surveillance

When targeting Economic Operators in a given sector, priority should be given to those that are most likely to break the rules, that do not follow the rules, or that have a history of non-compliance rather than targeting Economic Operators based on random selection

Feedback from industry, consumer organisations, trade unions, labour inspectorates, media, consumer complaints and statistical data can provide a useful source of information when making these decisions.



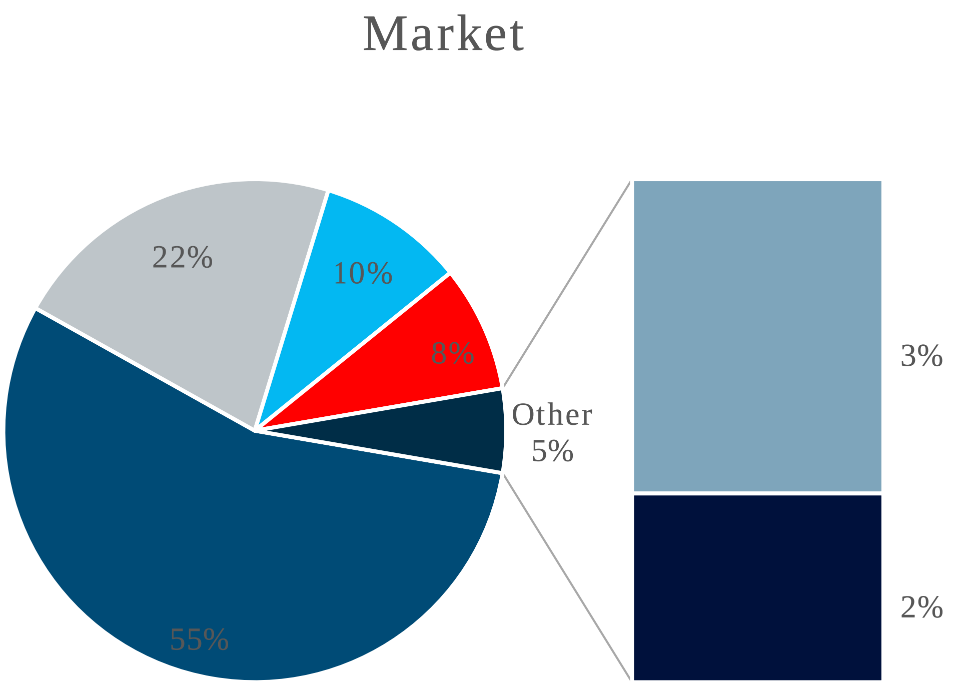
January 2017

GOOD PRACTICE FOR MARKET SURVEILLANCE

https://ec.europa.eu/docsroom/documents/23041
Good practice for market surveillance

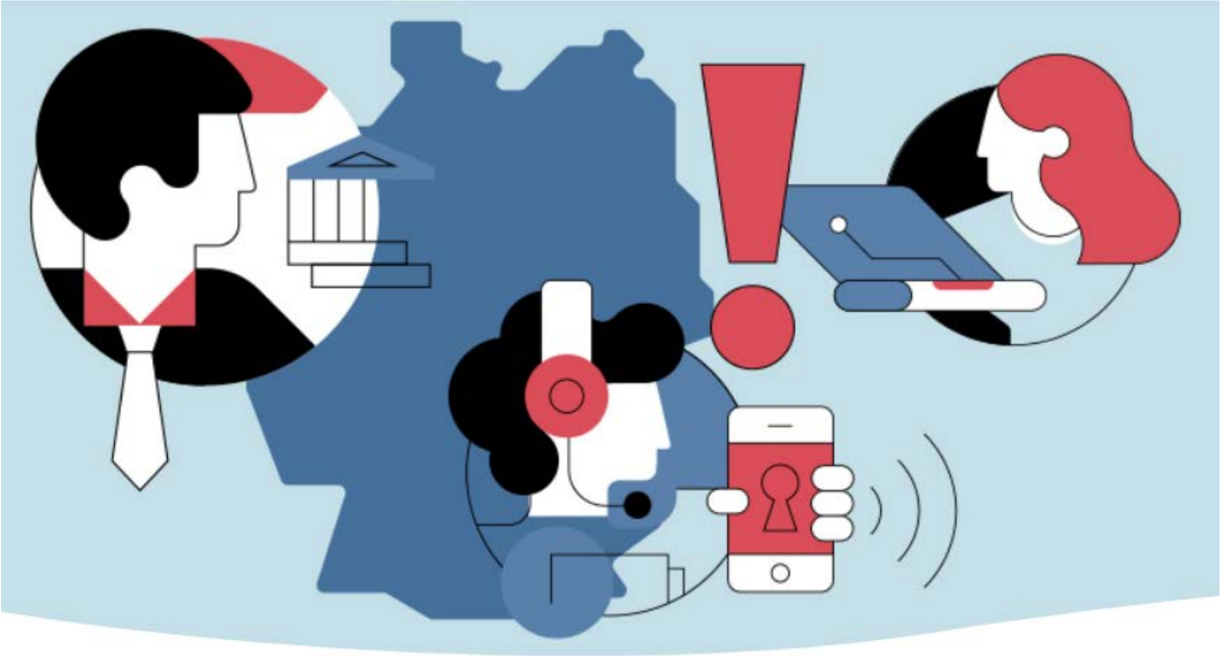
Active surveillance needs information about the market…

- Overall size of the national market, i.e. the amount and type of products supplied on the market
- Names and market share of the Economic Operators supplying given products
- Type of Economic Operator (e.g. manufacturers, importers, distributors) and main channels of sales (e.g. online or retail premises).



Market monitoring identifies security trends…

- Trends in market and consumer preferences
- Threat monitoring
- Statistics on security incidents
- Identification of future fields of action



… tools such as the Table of Eleven can help to assess expected compliance

Spontaneous compliance	Enforcement	
	Sanction dimensions	**Control dimensions**
Knowledge of the rules	Sanction probability	Inspection probability
Cost/Benefit	Sanction severity	Detection probability
Level of acceptance	Quality of the rules	Selectivity
Loyalty of the target group		Risk of being reported
Informal control		
No or minimal influence	*Indirect influence*	*Direct influence*

https://www.prosafe.org/images/Documents/EMARS/The_Book_Annexes.pdf

Thank you for your attention

Deutschland
Digital•Sicher•BSI•

Contact

Anna Schwendicke
Head of Section Market Surveillance of Certified Service Providers and Products
anna.schwendicke@bsi.bund.de

Federal Office for Information Security

Godesberger Allee 185 -189
53175 Bonn

Internet: www.bsi.bund.de