German American Chambers of Commerce
Deutsch-Amerikanische Handelskammern

TeleTrusT
Pioneers in IT security.
IT Security Association Germany

German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC – German American Chamber of Commerce

San Francisco, 28.04.2025

The CRA approved - How to tackle the increasing product regulation challenge?

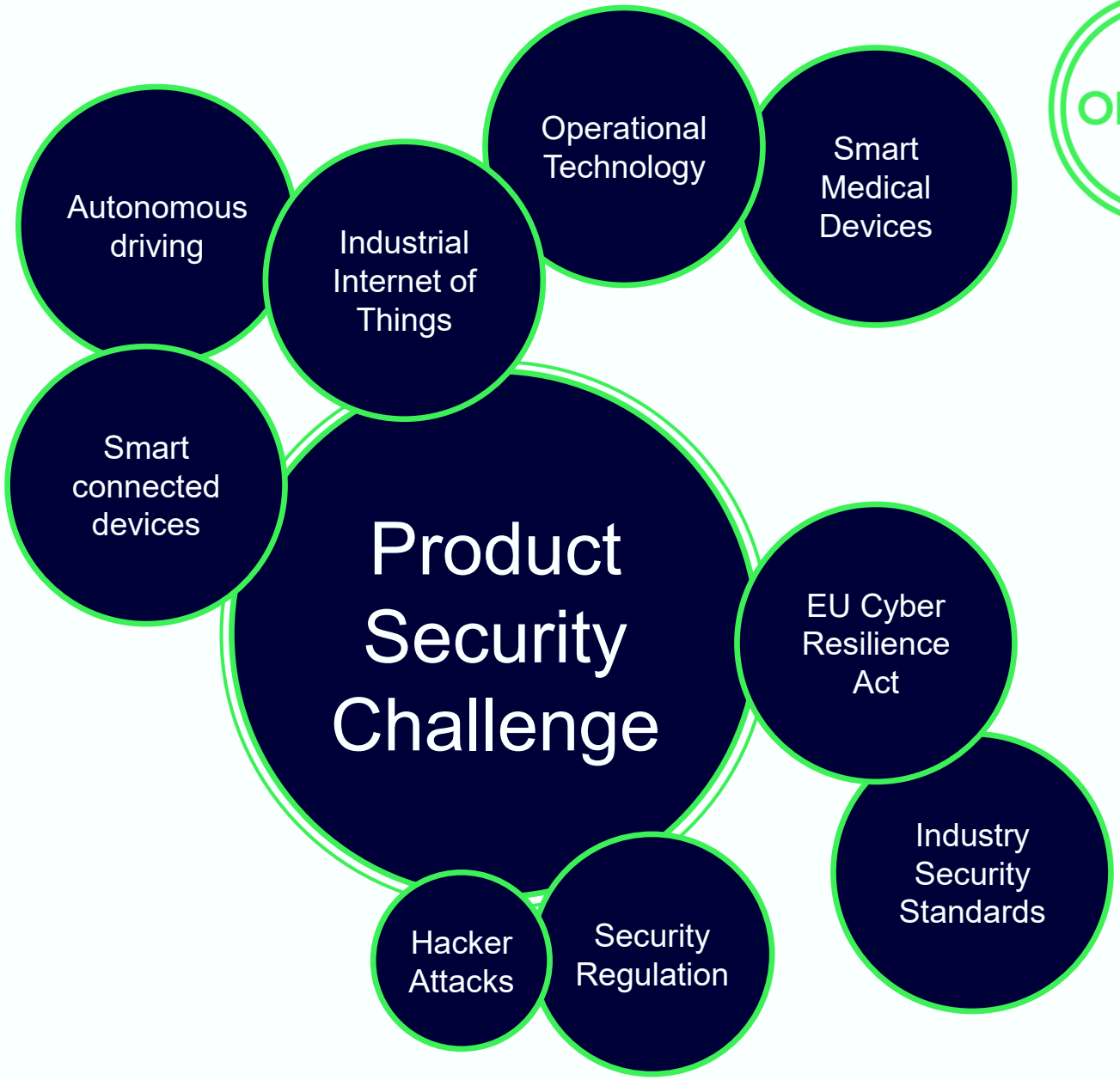
Jan Wendenburg, ONEKEY

EU CYBER RESILIENCE ACT – REAL PROBLEM OR PAPERWORK?

And How to tackle it?

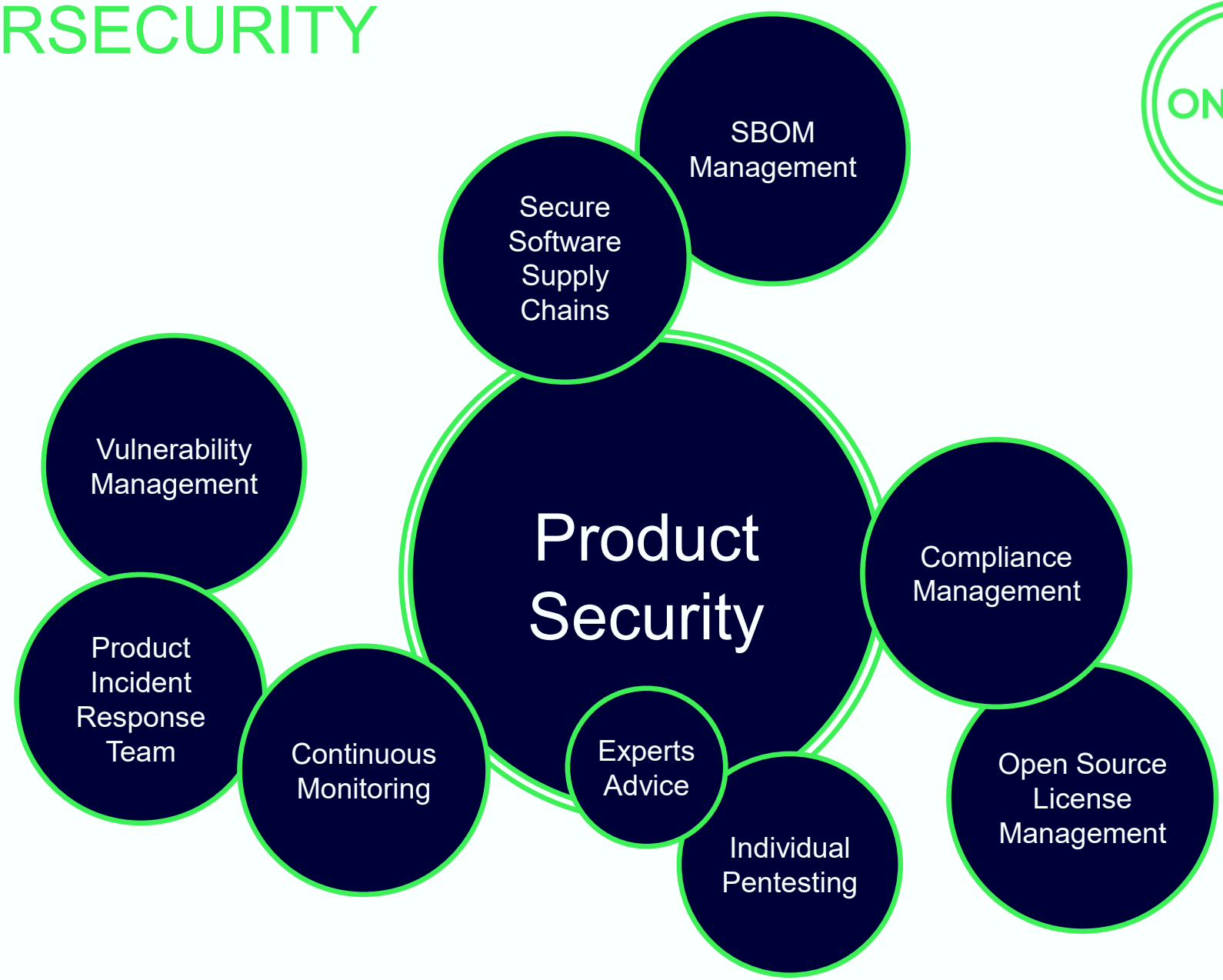
WHY PRODUCT CYBERSECURITY & COMPLIANCE?

- Global digitalization accelerates in every industry
- “Software eats the world”
- +40 billion smart devices in 2027
- Vast amount of different IoT/IIoT/OT technology stacks
- Product software security automation urgently needed



PRODUCT CYBERSECURITY & COMPLIANCE CHALLENGES?

Increased Security and Compliance challenges require Automation!



IEC62443

UNR155

ETSI EN 303645

PURPOSE OF THE CRA

- create conditions for the **development of secure products** with **digital elements** by ensuring that hardware and software products are placed on the market with **fewer vulnerabilities** and ensure that manufacturers **take security seriously** throughout a product's life cycle

- create conditions allowing users to **take cybersecurity into account when selecting and using products** with digital elements

CRA IN A NUTSHELL

- **Cybersecurity rules** for placing hardware and software on the European market
- Obligations for **manufacturers, importers, and distributors**
- Provide **secure products**
- Maintain **vulnerability management**
- **Report** exploited vulnerabilities to ENISA

CRA BASIC REQUIREMENTS (SIMPLIFIED)

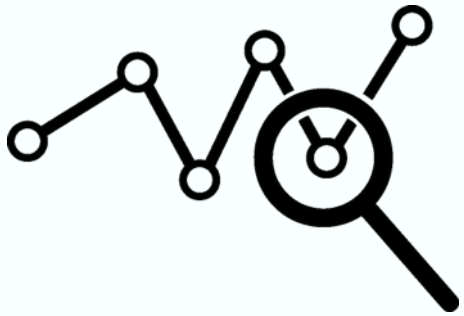
Software supply chain transparency


Emperor Claudius at
the dining table, eating
his mushrooms.


Emperor Claudius at
the dining table, eating
his **poisoned** mushrooms.
...one of the history first supply chain attacks.

CRA BASIC REQUIREMENTS (SIMPLIFIED)

Software supply chain transparency



Vulnerability detection and management

Product lifetime cybersecurity monitoring

HOW TO TACKLE THE CRA?

1. Awareness
2. Assessment
3. Adoption
4. Automation
5. Again

HOW TO TACKLE THE CRA?

1. **Awareness**
2. Assessment
3. Adoption
4. Automation
5. Again

- ✓Read & learn about CRA
- ✓Connect with experts
- ✓Identify the stake holders
- ✓Spread the word
- ✓Get resources to start

HOW TO TACKLE THE CRA?

1. Awareness
2. **Assessment**
3. Adoption
4. Automation
5. Again

- ✓You can’t build a plan when you do not know where you are!
- ✓Get help from experts?
- ✓Check product classifications
- ✓Identify scope
- ✓Verify (w/) the stake holders
- ✓Identify the gaps
- ✓Build a plan & action list
- ✓Request budgets

MANUFACTURER'S (TYPICAL) SCOPE OVER THE ENTIRE PRODUCT LIFECYCLE.

Design

Security & compliance check of third-party (binary) components in design phase.

Development

Continuous check on compiled pre-release software security & compliance for SBOM verification and vulnerability assessment.

Process self-assessment or obtain certification.

Production

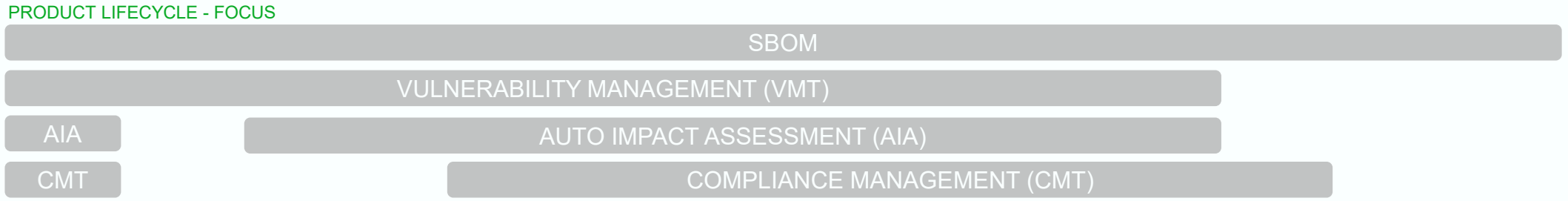
Combining & verify Source-code, build and deployment SBOM to one holistic SBOM.

24/7 vulnerability & compliance monitoring for PSIRT* over entire lifecycle.

End of Life

Risk & vulnerability status information for end-of-life products.

Reduce liability exposure for EOL products.



* Product Security Incident Response Team

HOW TO TACKLE THE CRA?

1. Awareness
2. Assessment
3. **Adoption**
4. Automation
5. Again

- ✓Align stake holders
- ✓Approve plan & action items
- ✓Start step by step
- ✓Transparency = SBOM first
- ✓Vulnerability management second
- ✓Shift left cybersecurity

HOW TO TACKLE THE CRA?

1. Awareness
2. Assessment
3. Adoption
4. **Automation**
5. Again

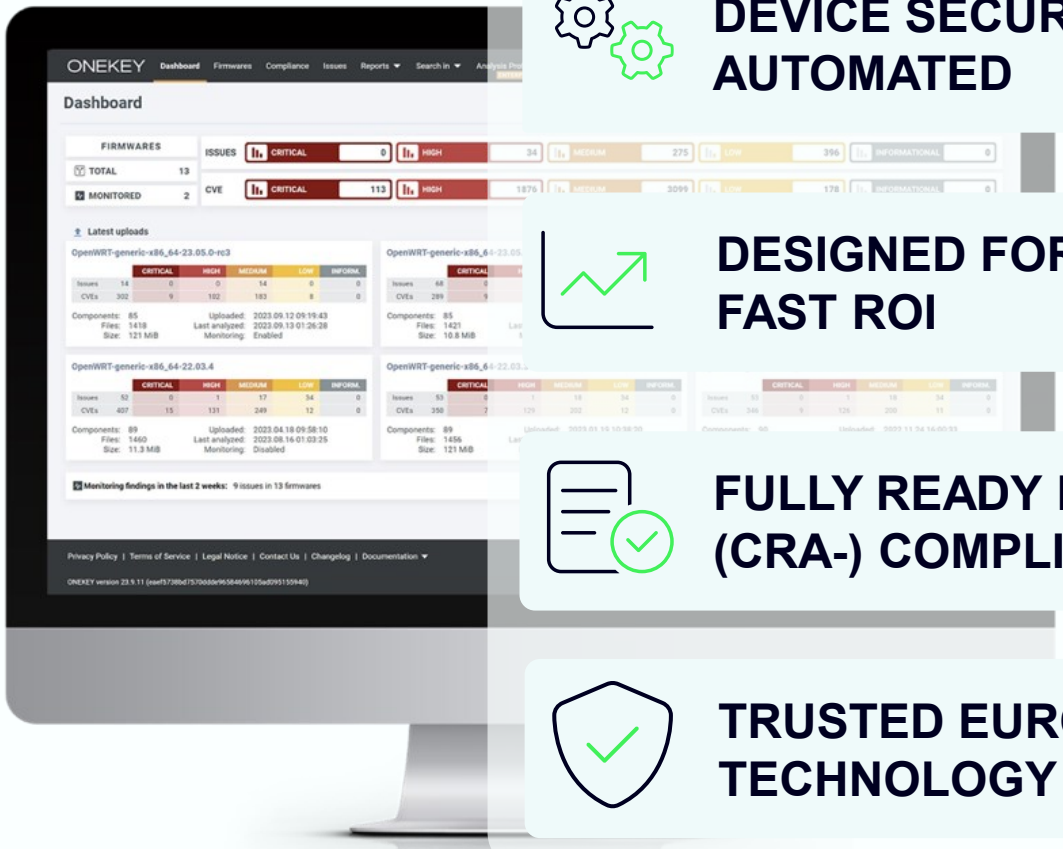
- ✓Automate, automate…
- ✓SBOM verification for third party software
- ✓SBOM generation and management
- ✓Vulnerability detection & priorization saves much time
- ✓Shift-left automated pen-testing into CI/CD pipelines

HOW TO TACKLE THE CRA?

1. Awareness
2. Assessment
3. Adoption
4. Automation
5. **Again**

- ✓Implement automated vulnerability monitoring over the full product lifecycle
- ✓Implement annual (?) controls to ensure matching documentation, process, regulation and reality
- ✓Repeat.

INTRODUCING: ONEKEY'S SAAS PLATFORM TO AUTOMATE COMPLEX SECURITY & COMPLIANCE ANALYSIS FOR CONNECTED DEVICES



DEVICE SECURITY, AUTOMATED

- Most efficient, automated vulnerability analysis of software (operator or producer) in the market
- Lowest level of false positive vulnerabilities in testing

DESIGNED FOR FAST ROI

- Cost attractive tool and services for developers (APIs), management (dashboards) and IoT security (compliance)
- Easy check any software of 3rd party connected devices

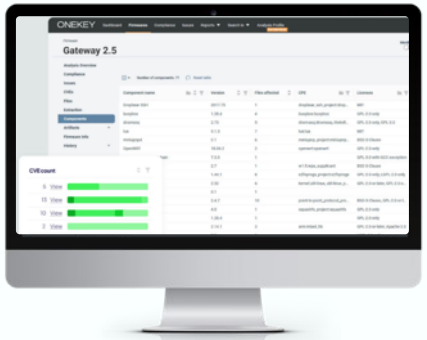
FULLY READY FOR (CRA-) COMPLIANCE

- Guiding customers from analysis of device software to compliance readiness for CRA and other intl. regulations
- EU-funded CRA Compliance Wizard™

TRUSTED EUROPEAN TECHNOLOGY

- Analysis in EU cloud and/or local (onPremises) tenant
- Senior cyber professionals serving large to small cap
- Trusted brand with front runner advantages

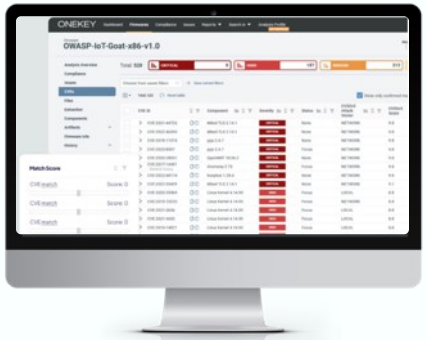
ONEKEY ENABLES MANUFACTURERS AND OPERATORS OF CONNECTED DEVICES TO FOCUS ON THEIR PRODUCT NEEDS



SBOM

Automated software composition analysis

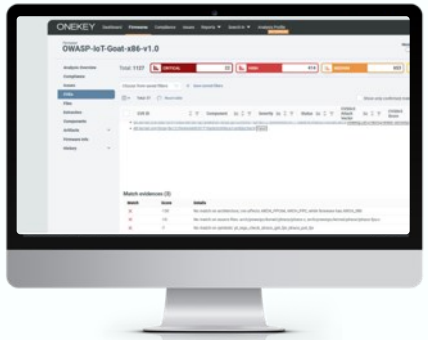
- Detailed overview of software bill of materials (SBOM) with one click.
- Ensure connected products are secure and compliant.
- No source code or network access required.



VULNERABILITY ANALYSIS

Find known & unknown weaknesses faster

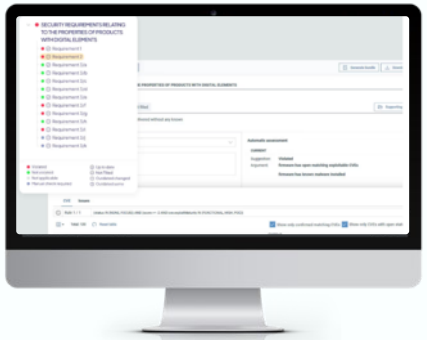
- Detect and prioritize firmware vulnerabilities.
- Maintain an overview with CVE* and Zero-Day impact assessments.
- Mitigate risks and avoid incidents quickly.



IMPACT ASSESSMENT

Faster, cost efficient risk assessments

- Automated scans cover certificates, cloud storage, attack vectors, exploitability, and dependencies.
- Severity reports with mitigation strategies.



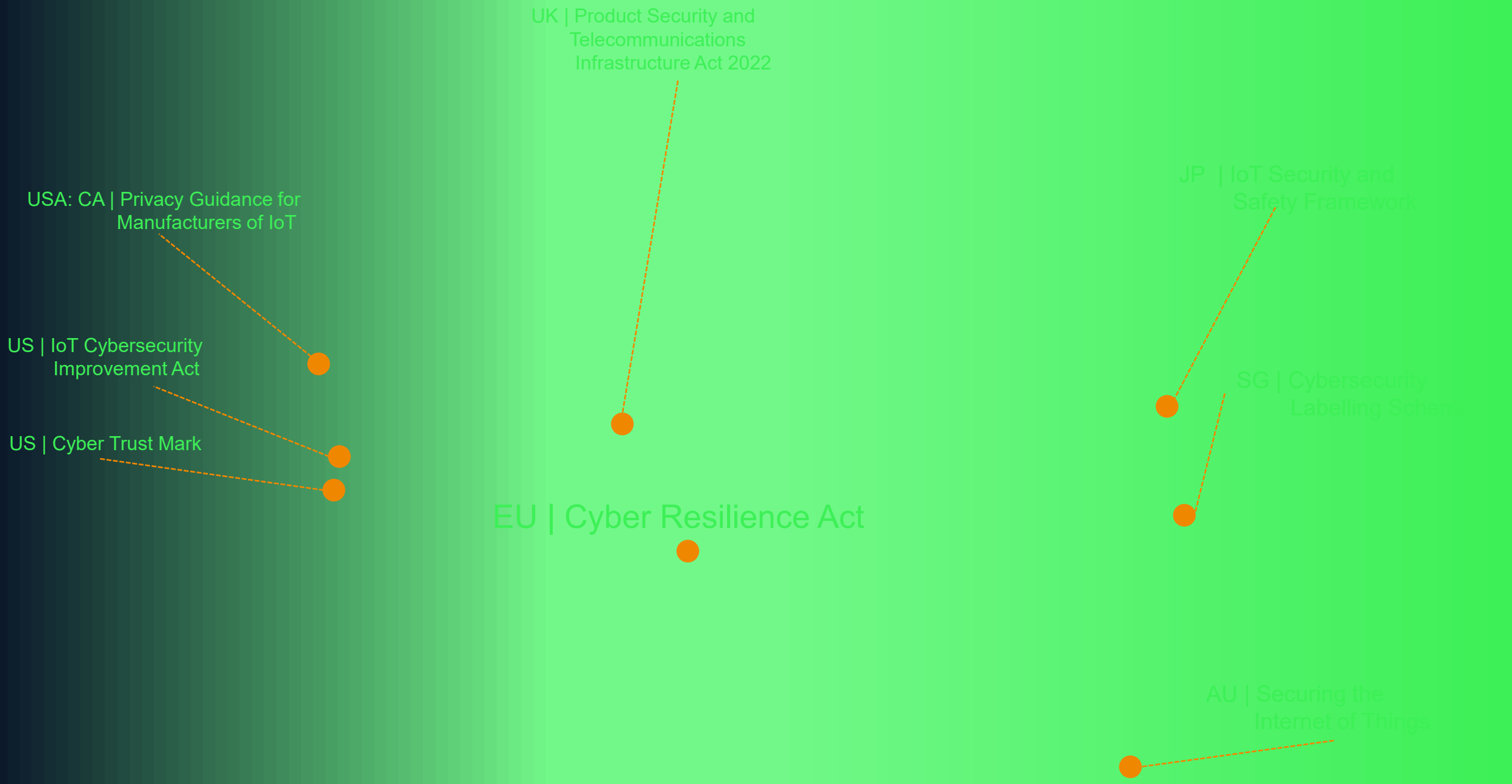
CYBERSECURITY COMPLIANCE

Simplify compliance assessments

- Manage regulatory requirements, prioritized and automated.
- Includes a virtual assistant for regulations.
- Navigate standards: EU Cyber Resilience Act, IEC 62443, ETSI 303 645.

* CVE: Common Vulnerabilities and Exposures

GOING GLOBAL?


UK | Product Security and Telecommunications Infrastructure Act 2022
USA: CA | Privacy Guidance for Manufacturers of IoT
US | IoT Cybersecurity Improvement Act
US | Cyber Trust Mark
EU | Cyber Resilience Act
JP | IoT Security and Safety Framework
SG | Cybersecurity Labelling Scheme
AU | Securing the Internet of Things

BUILD. COMPLY.
RESIST. REPEAT.

ONEKEY GmbH
Jan C. Wendenburg, CEO
+49 171 5555312
jan.wendenburg@onekey.com
Kaiserswerther Straße 45
40477 Düsseldorf / Germany
www.onekey.com

CYBERSECURITY™
MADE IN EUROPE