Greenbone

EU Cyber Resilience Act (CRA): How to handle vulnerabilities

OSADL COOL Session, 2023-11-22

Dr. Jan-Oliver Wagner

CEO

AGENDA

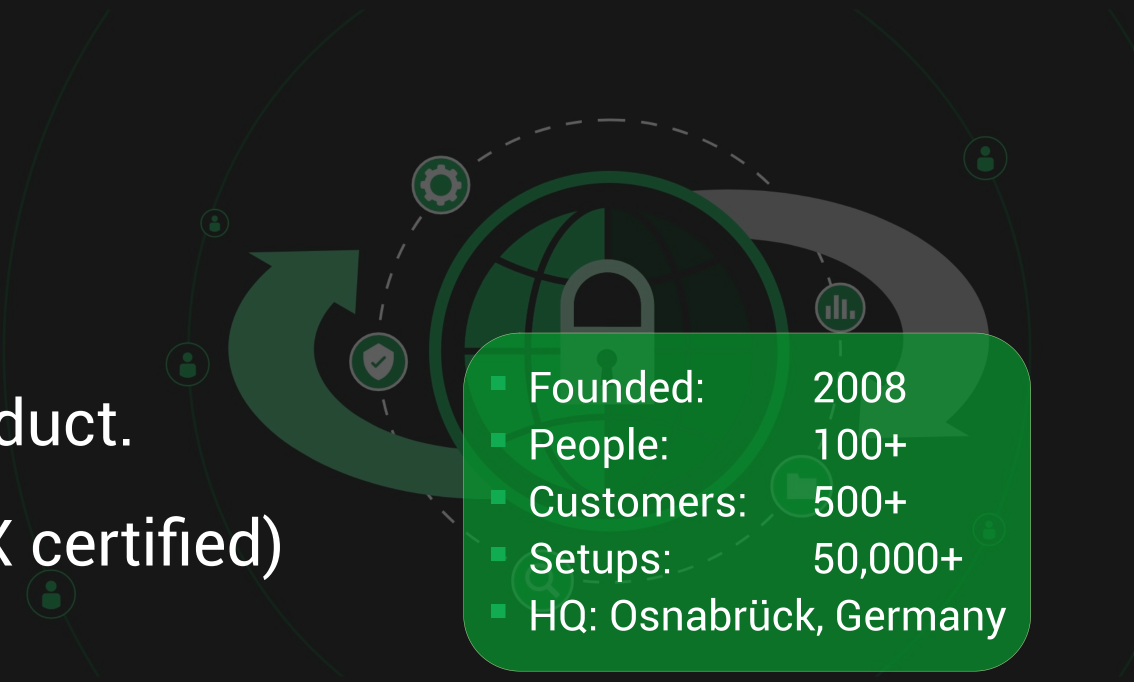
EU Cyber Resilience Act (EU CRA): How to handle vulnerabilities

- About Greenbone AG
- How vulnerability scanning works
- Objectives, impacts and subject of the Cyber Resilience Act
- Vulnerability handling requirements
- How Greenbone addresses the challenge

© European Union

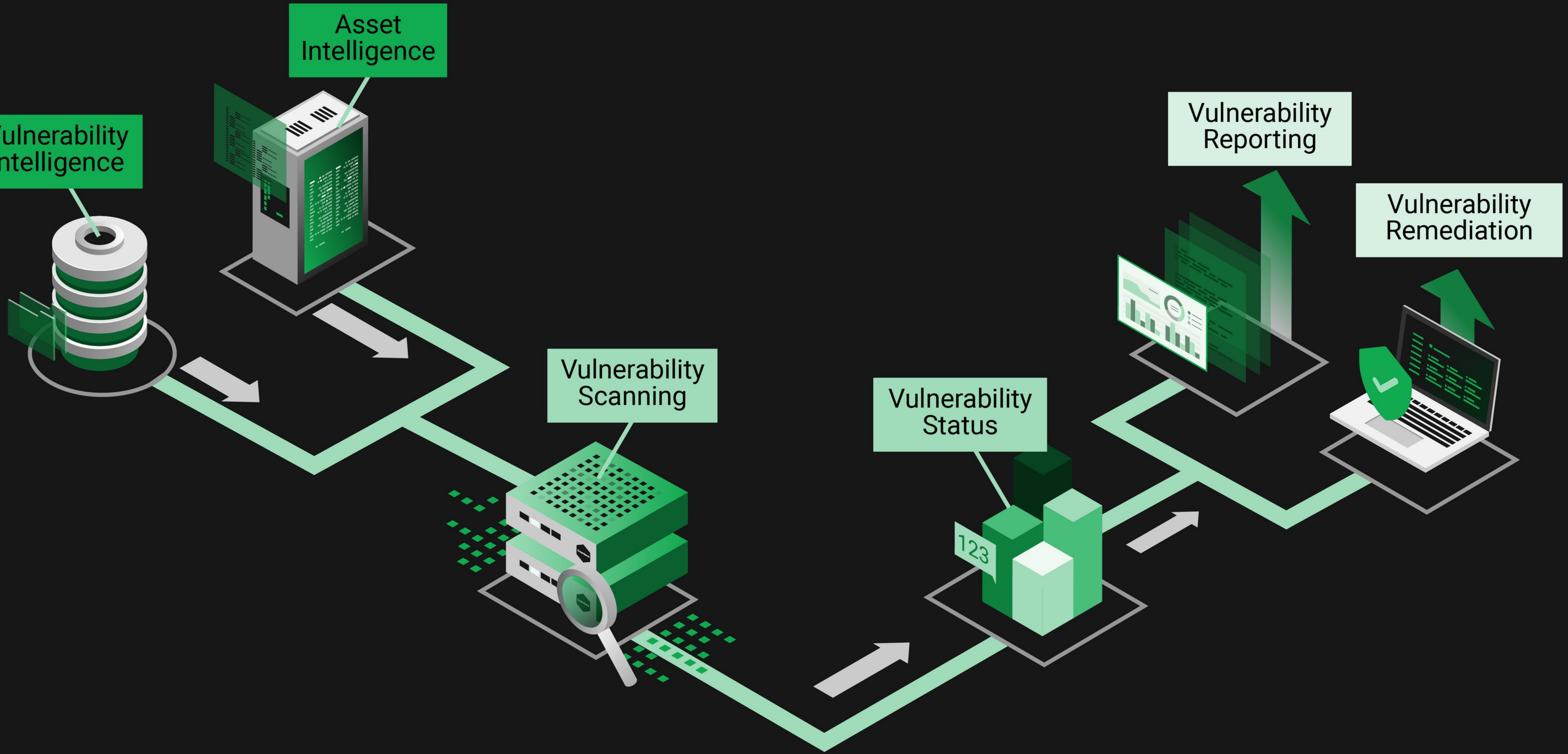
GREENBONE AG

- We are finding cyber weaknesses, and provide instructions for their elimination.
  → On Premise, in the Cloud, everywhere.
- We provide the most popular vulnerability scanning & management - worldwide.
  → Large user base, leading Open Source product.
- Quality oriented (ISO 27001, ISO 9001, TISAX certified) & GDPR compliant.



Founded:	2008
People:	100+
Customers:	500+
Setups:	50,000+
HQ: Osnabrück, Germany	

HOW VULNERABILITY SCANNING WORKS



OBJECTIVES OF THE CYBER RESILIENCE ACT

More Secure hardware and software products

- Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;
- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
- Enhance the transparency of security properties of products with digital elements, and
- Enable businesses and consumers to use products with digital elements securely.

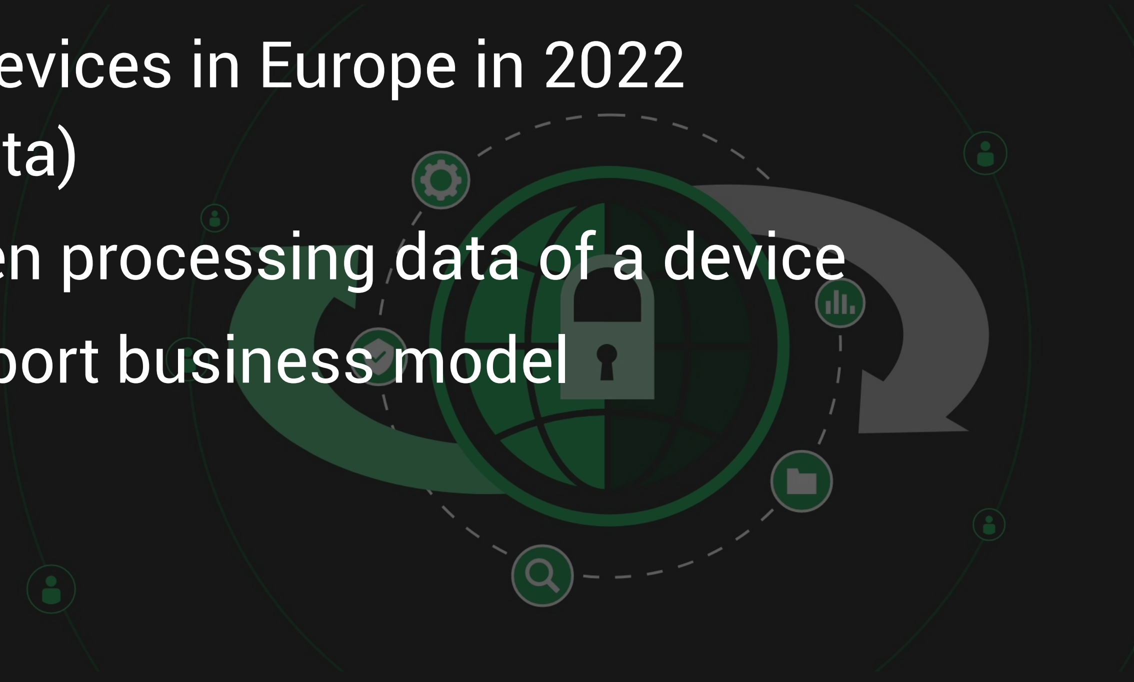
Commission Vice President Margaritis Schinas and Commissioner Thierry Breton at a press conference on the Cyber Resilience Act on September 15, 2022 | Kenzo Tribouillard/AFP via Getty Images

IMPACTS OF THE CYBER RESILIENCE ACT

- For all of us: More secure hardware and software products
- Horizontal: Any device
- Strong: Requirements are mandatory to keep CE marking for products with digital elements
- Concrete: Requirements about vulnerability handling

SUBJECT OF THE CYBER RESILIENCE ACT

- No one really knows the number of different systems and devices in the EU
- We know it is many: IoT alone is 2.7 billion devices in Europe in 2022 Growing to 4.3 billion in 2025 (Source: Statista)
- Even cloud services are in scope of CRA when processing data of a device
- Even free of charge software with just a support business model



- EU assumes:
  - 10% of products in Critical Class I and II
  - 90% in default category

VULNERABILITY HANDLING REQUIREMENTS

EU CRA requirements about supply chain security:

- „ensure that all [...] products are delivered without any known exploitable vulnerabilities“ (Item 32)
- „shall exercise due diligence when integrating components sourced from third parties" (Article 10)
- “apply **effective and regular tests** and reviews of the security of the product with digital elements", Annex, 2 (3)

VULNERABILITY HANDLING REQUIREMENTS

EU CRA requirements about life cycle security (Article 11):

- Report actively exploited vulnerabilities to CSIRTs within 24h
- Report incident to product users, including corrective measures within 72h
- Report identified vulnerabilities in 3rd party elements to respective 3rd parties

VULNERABILITY HANDLING REQUIREMENTS

For EU CRA requirements about supply chain security and life cycle security, product vendors need to have:

- Products' Software Bill of Materials (SBoM)
  - A SBoM is more than a product inventory
- Vulnerability scan showing no weaknesses for passing CE certification
- Continuous vulnerability scanning
  - Daily
  - SBoM updates for product updates
- Process & infrastructure for documenting and reporting product vulnerabilities

VULNERABILITY HANDLING REQUIREMENTS

How Greenbone addresses own and customer requirements

- Supply chain
- Vulnerability scanning
- Vulnerability reporting
- Security updates

VULNERABILITY HANDLING REQUIREMENTS

How Greenbone addresses own and customer requirements

- Supply chain
  - Rules (quality gate, due diligence measures) for adding new third party components
    - Part of our ISO 27001 anyway
  - Automatic creation of SBoMs for all our software modules via github actions and output format SPDX
  - CycloneDX is another popular format

VULNERABILITY HANDLING REQUIREMENTS

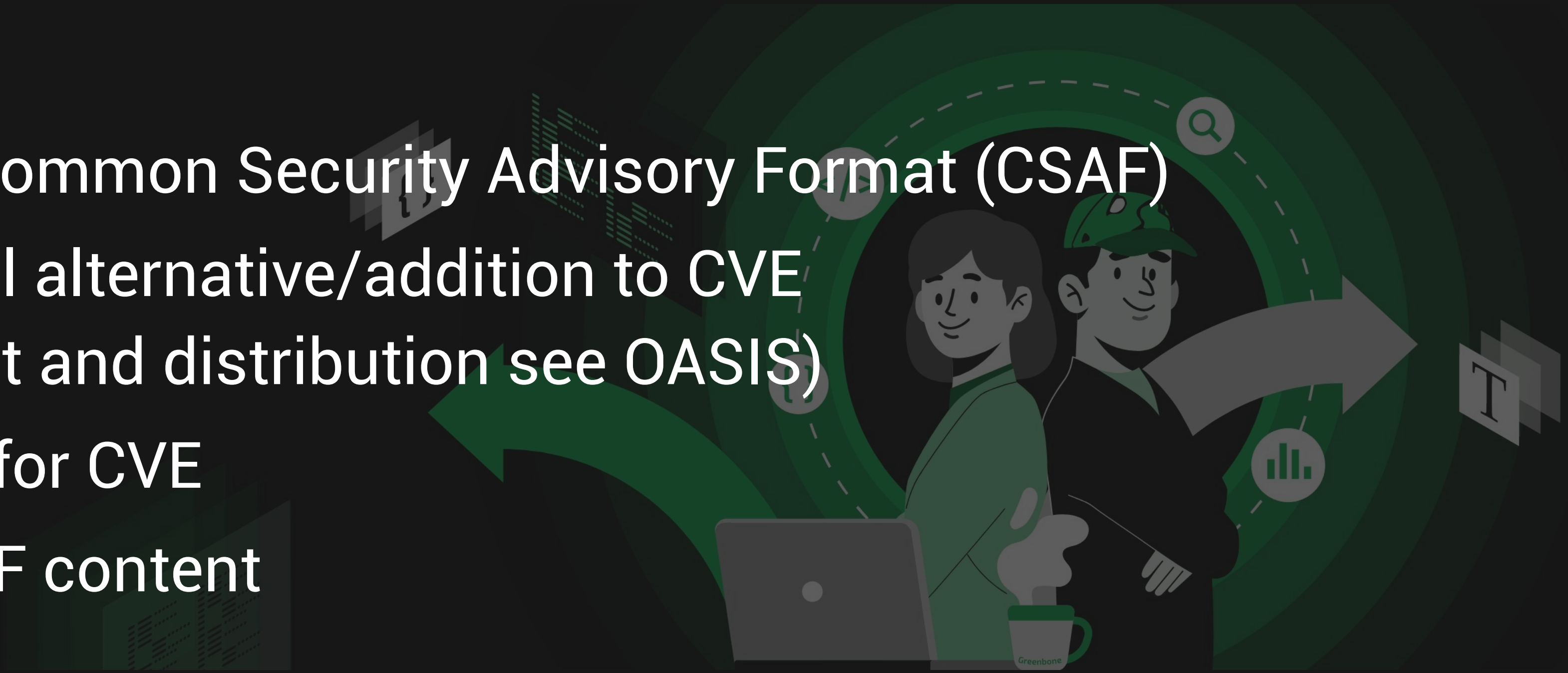
How Greenbone addresses own and customer requirements

- Vulnerability scanning
  - Indirect (=offline) scanning
  - Importing SPDX and CycloneDX
  - Extended testing with analysis of SBoMs
    → Challenge: SBoM is more than just a product inventory
  - Link with security advisories and asset inventories
    → Challenge: Extend product matching
  - Transform findings into Security Advisories and publish them
    → Challenge: Do so timely (CRA requires <24hrs) and in accepted form

VULNERABILITY HANDLING REQUIREMENTS

How Greenbone addresses own and customer requirements

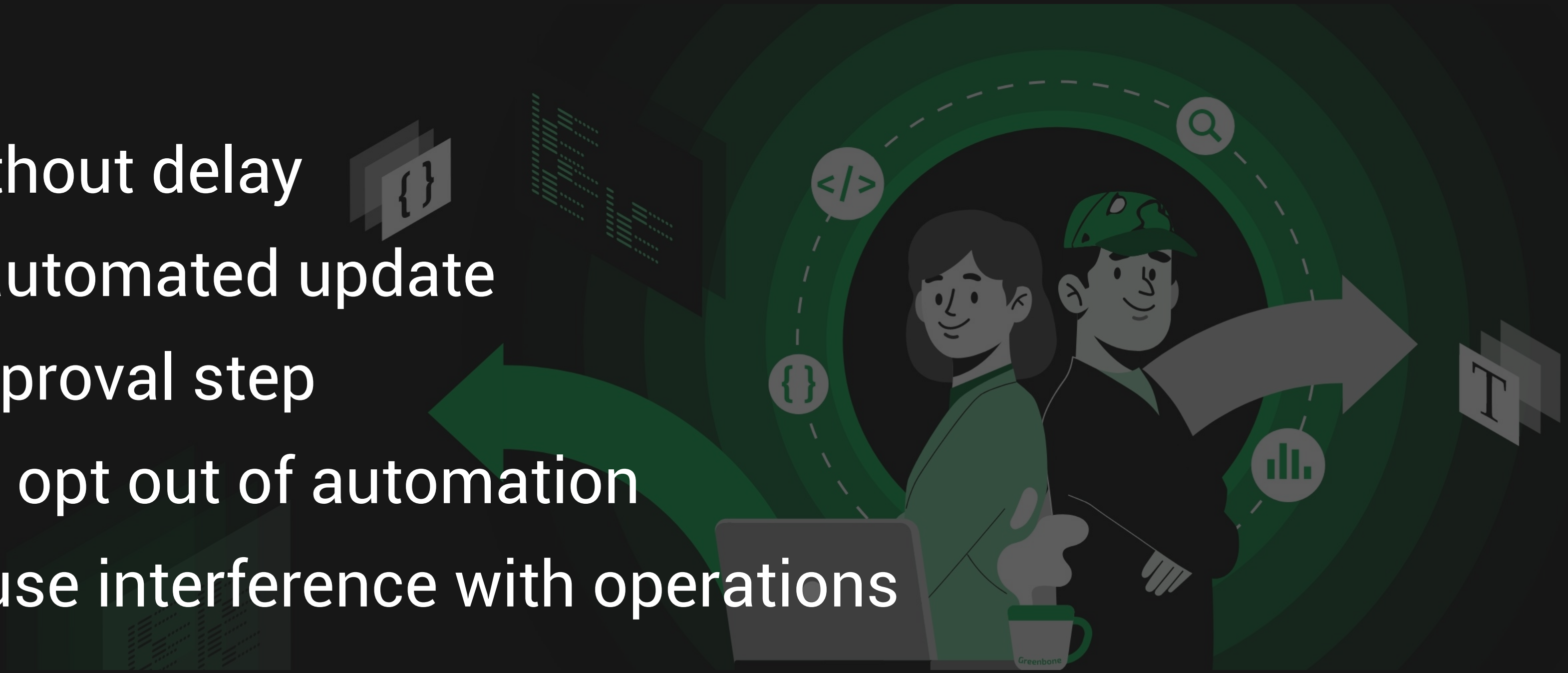
- Vulnerability reporting
  - Set up infrastructure for Common Security Advisory Format (CSAF)
  - CSAF is a non-hierarchical alternative/addition to CVE (for specification of format and distribution see OASIS)
  - Publication is faster than for CVE
  - Create and distribute CSAF content



VULNERABILITY HANDLING REQUIREMENTS

How Greenbone addresses own and customer requirements

- Security updates
  - Making them available without delay
  - Design products to have automated update
    - With optional manual approval step
    - With clean instruction to opt out of automation
    - Not where this could cause interference with operations



Thank You!
Questions?

Greenbone