AHK 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, 06.05.2024

Automated Product Cybersecurity Compliance Management in the light of increased legal regulations and liabilities

Jan C. Wendenburg, ONEKEY

Challenge vs. Demand vs Solution

Challenge

- +40 bn connected devices in 2025*
- Complex technology stacks
- Manual analysis are time consuming & expensive
- Increasing regulations, i.e. EU Cyber Resilience Act, Biden Act

Limited resources, time consuming, expensive!

Demand

- Continuous 24/7 visibility of IoT/IIoT/OT risks
- Auditable software supply chains (SBOM)
- Reduce cost & efforts for product cybersecurity compliance

24/7 full risk visibility & compliance automation!

Solution

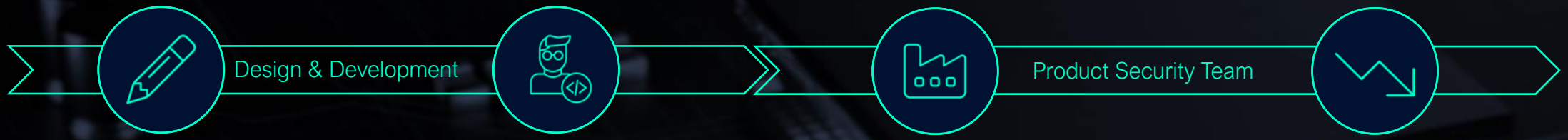
- Automated vulnerability detection** automates SW analysis
- Automated Software Bill Of Materials (SBOM)
- 24/7 risk monitoring
- Compliance automation by patent pending virtual assistant

Automated, highly scalable, 24/7/365 available!

**Artificial Intelligence using Natural Language Processing (NLP)

*Source: Statista 10/2021, ISC2.ORG Cybersecurity Workforce Study

Manufacturer's (cybersecurity & compliance) **view on the entire product lifecycle.**



Design

Security check of third-party components in design phase

Development

Continuous check on security & compliance for pre-release software

Process self-assessment or obtain certification

Production

Transparent, software supply chain (SBOM)

24/7 vulnerability monitoring for PSIRT* over entire lifecycle

End-of-Life

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

*PSIRT = Product Security Incident Response Team

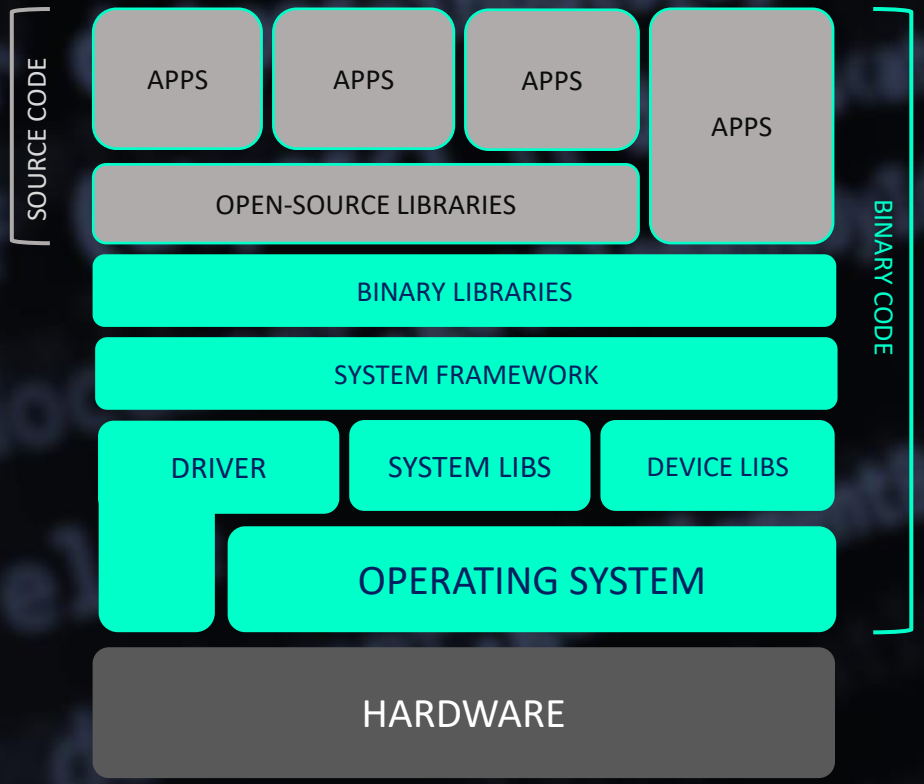
Why do you need full depth components transparency?

Binary analysis is going beyond source code – it covers full software stack

- Verify & enhance supplier's SBOM information
- Source code component list information does not cover binary blocks & content
- Avoid incomplete SBOMs due to missing or incomplete third-party information

Why do you need to look beyond source code?

VERACODE
Checkmarx
GitLab
Qualys.
SENTINEL Dynamic
Contrast SECURITY
ImmuniWeb® AI for Application Security



The vendor is liable for the compliance & security for the full code stack.

Source code analysis is limited to applications & open source

Full binary BINARY image represents full stack

Secure software supply chains with automated SBOMs

from binary image analyses

Regain & maintain control over your software supply chains

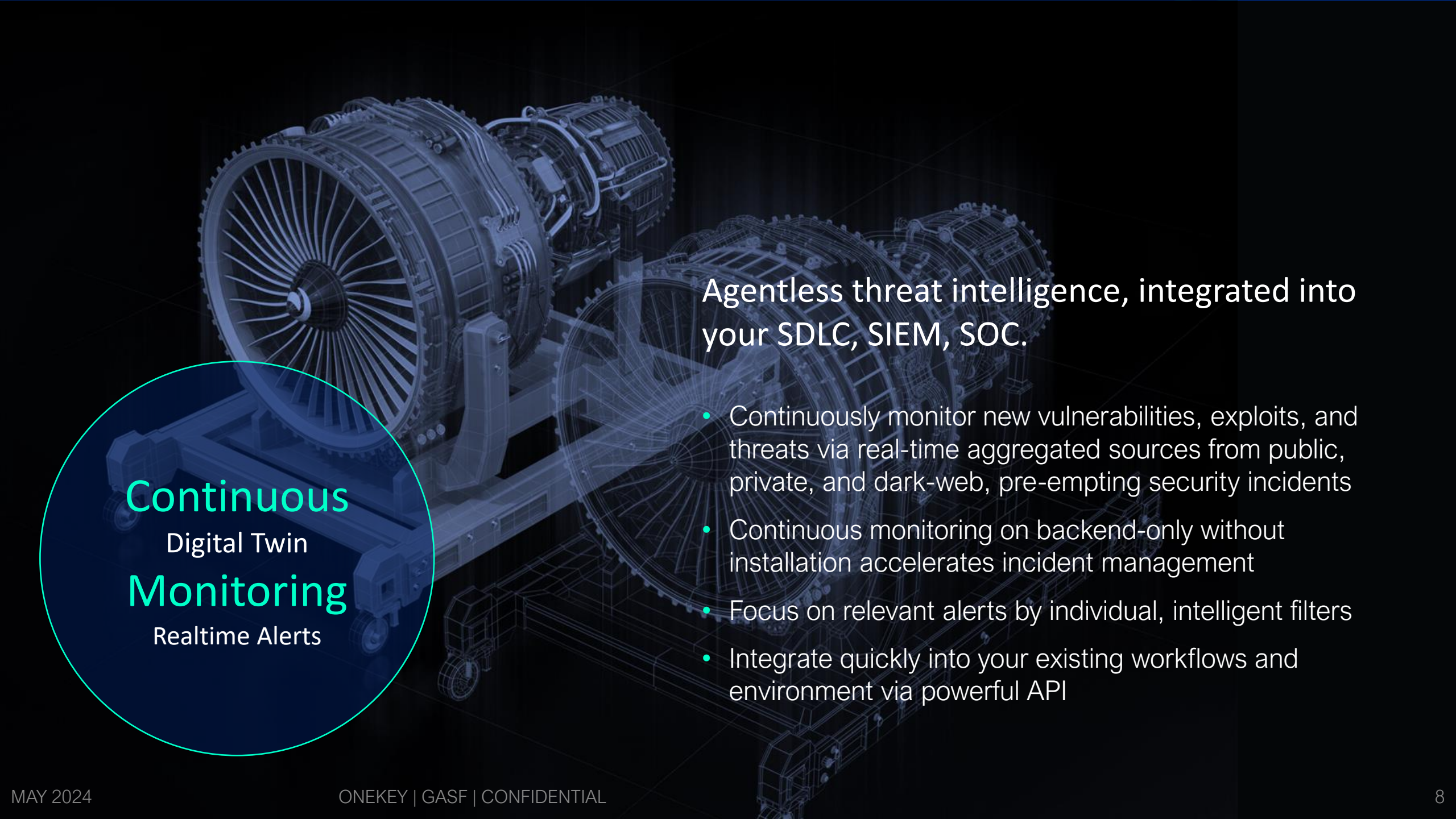
- Generate detailed SBOMs to verify & check your own SDLC and their supplier's software component declaration on binary code level.
- Create deep asset cyber visibility, track and compare components throughout your database
- Make informed, attack-resistant choices about components
- Integrate seamless with PLM, ERP and QMS to show exposed risks wherever needed

Vulnerability Management

Product Security Incident Response Teams

Automated results.
Complete coverage, actionable insights.

- Manage vulnerabilities and security gaps in your devices, protecting them from CVEs and Zero-day. All via binary analysis. No source code required.
- Bring context to chaos and eliminate irrelevant vulnerabilities. Prioritize your team's efforts and quickly resolve security gaps, aided by our remediation recommendations.
- Focus only on relevant alerts by intelligent filtering
- Cut response times by acting immediately on mitigation recommendations.



Agentless threat intelligence, integrated into your SDLC, SIEM, SOC.

- Continuously monitor new vulnerabilities, exploits, and threats via real-time aggregated sources from public, private, and dark-web, pre-empting security incidents
- Continuous monitoring on backend-only without installation accelerates incident management
- Focus on relevant alerts by individual, intelligent filters
- Integrate quickly into your existing workflows and environment via powerful API

Compliance Management

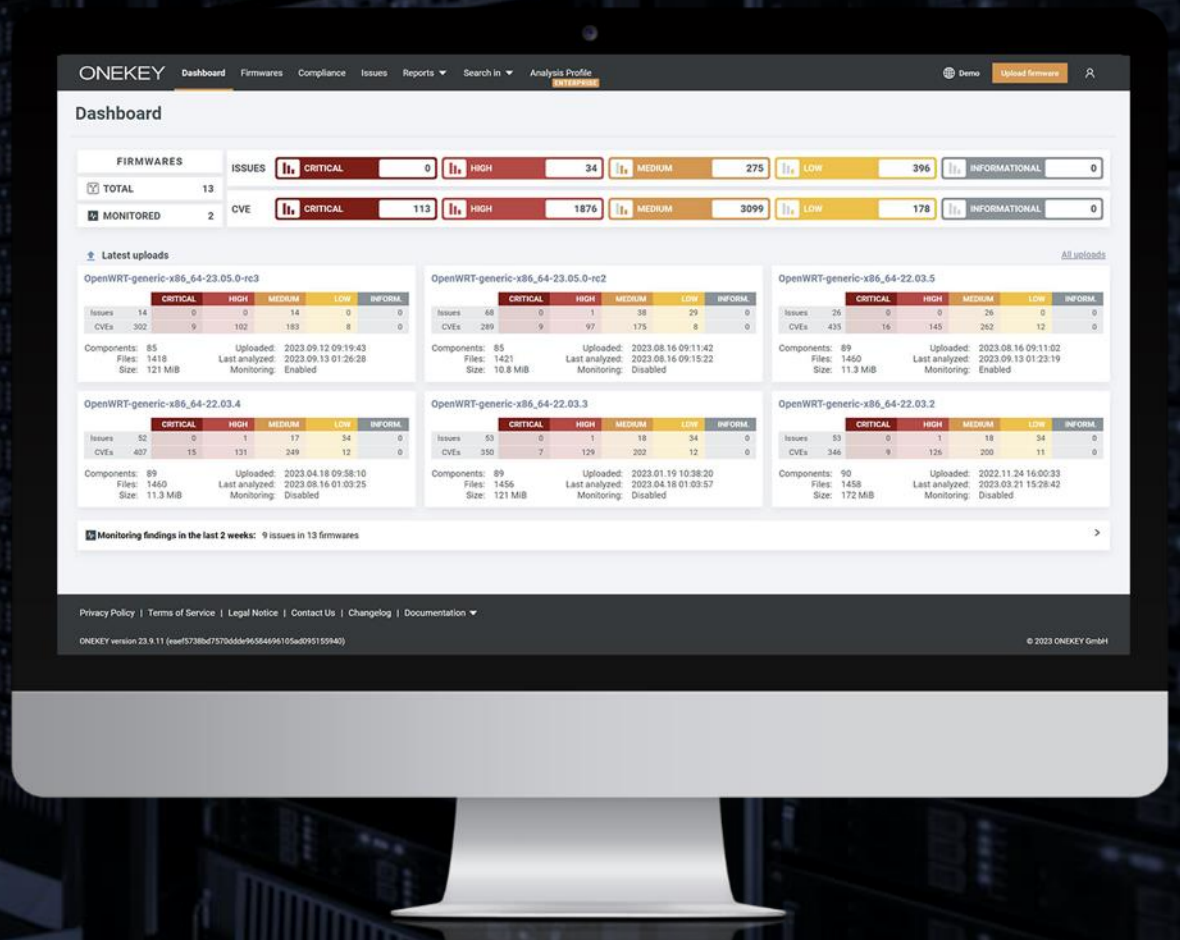
Open Source License Management

Comply on the fly by acting on automated Validation with industry specific standards

- Validate your compliance on the fly, i.e. against IEC62443, EU Cyber Resilience Act, OWASP and others.
- Check and verify cryptographic standards and security such as private keys, key length encryption, hard coded passwords and others.
- Detect open source components and code snippets in binaries.
- Track legal status and reduce manual efforts for compliance validation.

SHOWCASE: Mastering the challenge by automated complex security & compliance analysis in one key SaaS platform.

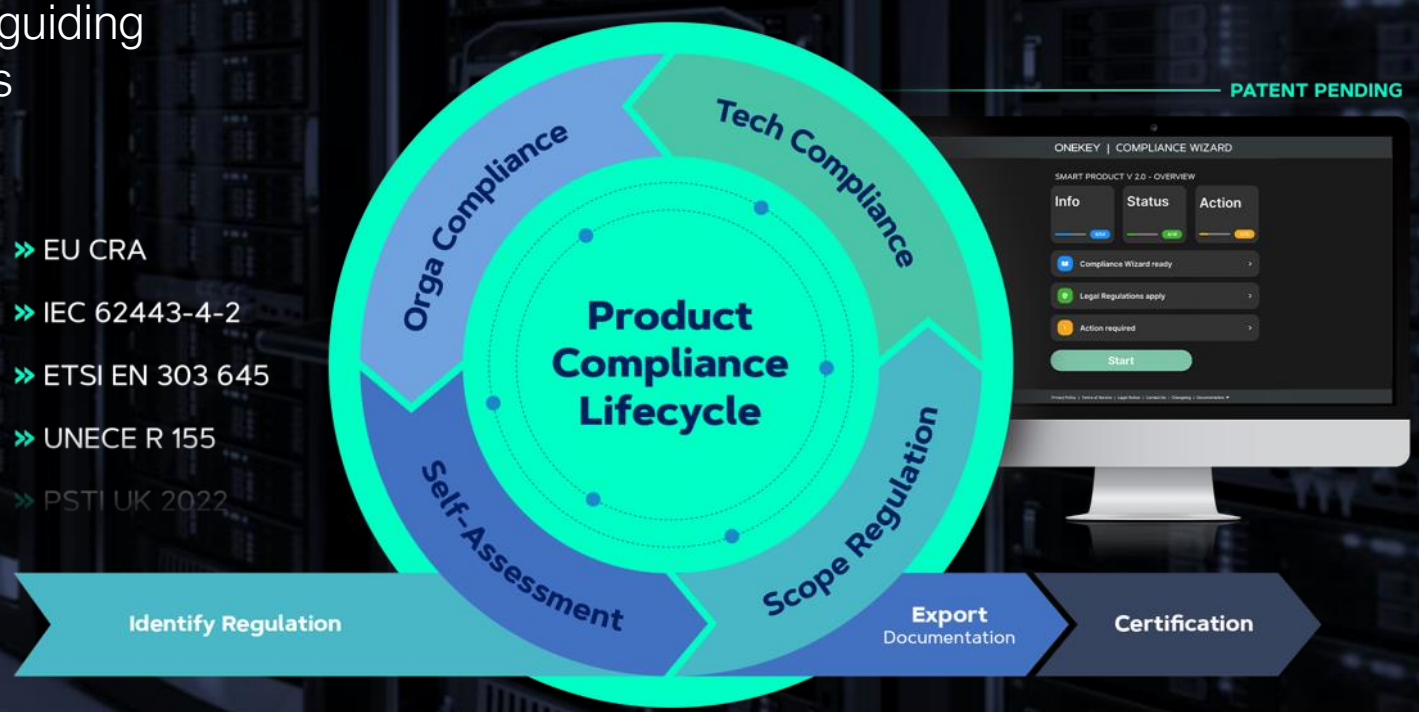
- AI* based security & compliance analyses in minutes vs. days for manual analysis
- Works with binary software images – no source code needed!
- Agentless – no installation/integration
- Powerful API for easy integration
- Flexible SaaS / onPrem subscription plans



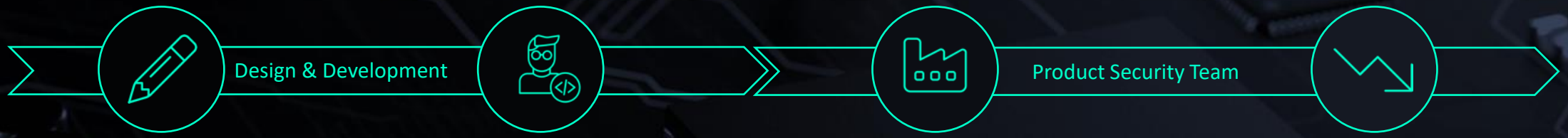
*Artificial Intelligence using Natural Language Processing

SHOWCASE: Compliance automation for cybersecurity standard self-assessment & certifications

- New, disruptive, patent-pending approach to simplify self-assessments and certifications
- Simple, **dialog-based virtual assistant** guiding through complex cybersecurity regulations
- Partnering with certification bodies to enable smooth, simplified workflow from data-collection to successful certification
- Integrated in ONEKEY SaaS platform



Automation enables simplified (cybersecurity & compliance) product lifecycle management.



	Design	Development	Production	End-of-Life
CUSTOMER NEED	Analyze third-party components on security in design phase	Instant & continuous feedback on security & compliance for pre-release software builds	Transparent auditable software supply chain Software security monitoring over entire lifecycle	Vulnerability status & security trend information for products near end of / after production
AUTOMATION VALUE	Automated security analysis before purchase / integration	Scalable, automated and continuous security and compliance analysis and assistant for pre-release software	Automated, exportable software-bill-of-materials (SBOM) 24/7 monitoring cuts response & fix times	24/7 monitoring including vulnerability impact analysis reduces risks and efforts by focusing on fixing high impact vulnerabilities

Experts.
Passion.
Automation.

ONEKEY GmbH

Jan C. Wendenburg, CEO

+49 171 5555312
jan.wendenburg@onekey.com

Kaiserswerther Straße 45
40477 Düsseldorf / Germany
www.onekey.com

ONEKEY

FIC STARTUP AWARD WINNER 2023

ECS STARTUP AWARD WINNER 2024

TOP INDUSTRIAL IOT SOLUTIONS PROVIDER IN EUROPE 2022 ONEKEY

DEUTSCHER STARTUP-POKAL UNITED INNOVATIONS AWARDS WINNER 2023