

TeleTrust-interner Workshop

27.06.2022, Berlin

IoT Security & Compliance automatisieren - Risiken & Kosten minimieren

Jan Wendenburg, ONEKEY

The **Global IoT Challenge** demanding a **New Solution!**

Challenge

- +39 bn connected IoT / IIoT / OT devices in 2025*
- Complex technology stacks
- Manual analysis are time consuming & expensive
- +3.1m cybersecurity professionals missing*

Limited resources,
time consuming,
expensive!

Demand

- Continuous 24/7/365 visibility of IoT/IIoT/OT risks
- Transparent software supply chains
- Realtime alerts for new vulnerabilities on IoT/IIoT/OT devices

Full risk
transparency
& 24/7/365
automated alerts!

Solution

- Scalable platforms automate manual penetration tests (30 minutes vs. 5 days)
- Highly scalable & available 24/7.
- Full software supply chain transparency
- Continuous monitoring & auto risk alerts 24/7/365
- EAI integration

Automated platforms
are highly scalable &
24/7/365 available!

WHY AUTOMATION?

INCREASING PRODUCTIVITY, QUALITY AND COMPLIANCE



Reduction of manual (pen-)testing, analysis & SBOM generation efforts



Reduction of consulting / certification project time

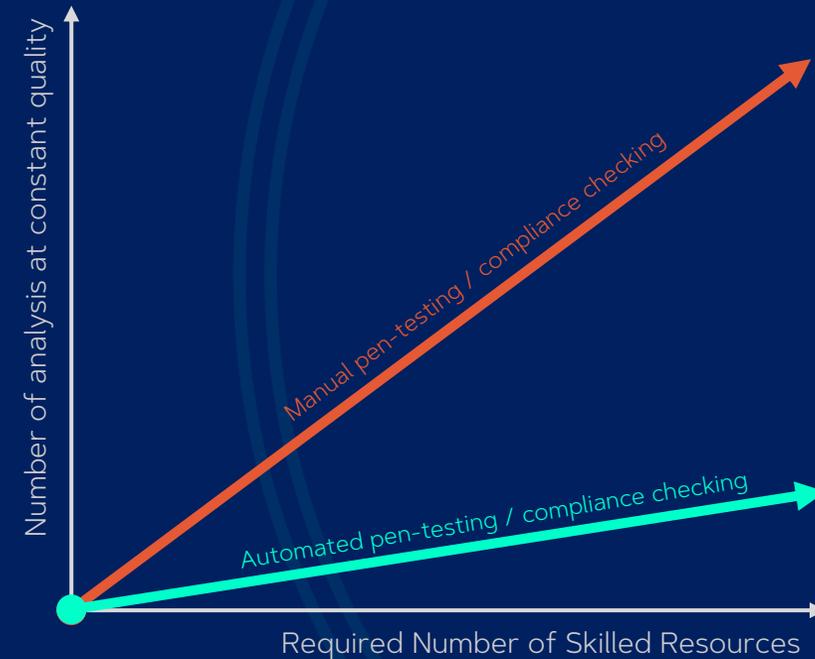


Consistent quality of security & compliance testing



Software Security & compliance monitoring via digital twins

(Automated checking of i.e. OWASP Top 10 IoT, ETSI EN 303 645, DIN SPEC 27072, US or UK legislation, or security recommendations by ENISA or BITAG...)



Automation reduces significantly efforts while maintaining consistent quality.

PROCESS INTEGRATION

CONTINUOUS SECURITY & COMPLIANCE





Device **BUYERS** benefit from a **Security & Compliance Quality Gate** for software and device supply chain.



swisscom

BUYER REFERENCE

- Quality gate for procurement in the IoT supply chain
- Improve transparency of software supply chain
- Comply with legal and regulatory requirements
- Maintain brand reputation
- "Realtime" alerts from automated security & compliance monitoring

ONEKEY saves **SWISSCOM**
more than **400,000 €** per
avoided security incident via
IoT Quality Gate.

Verbund

- Identify vulnerabilities in IoT inventory
- Improve transparency of software supply chain
- Make informed decisions for new IoT purchases
- Comply with regulatory requirements
- “Realtime” alerts from automated security & compliance monitoring

ONEKEY identifies vulnerabilities & non-compliance at Verbund resulting in **reduced operational risk.**



Device **VENDORS** benefit from **Security By Design** through automated feedback to firmware developers.

- Quality gate prior to distribution of new software-firmware releases
- Improve software supply chain transparency
- Comply with legal and regulatory requirements
- Protect brand investments and competitive advantage



ONEKEY enabled ZYXEL to create & maintain a **secure IoT firmware stack** directly within development process.

ONEKEY orchestrates & automates complex security & compliance analysis into one key **service platform**.

- “Digital Twins” from firmware binaries
- Deep security & compliance firmware analysis
- Continuous 24/365 monitoring
- Powerful API integration and auto-alerts



**Experts.
Passion.
Automation.**

ONEKEY GmbH

Jan C. Wendenburg, CEO

Kaiserswerther Straße 45
40477 Düsseldorf / Germany
+49 171 5555312
jan.wendenburg@onekey.com
www.onekey.com

© June 2022



Secur|Ty
made
in
EU

ONEKEY