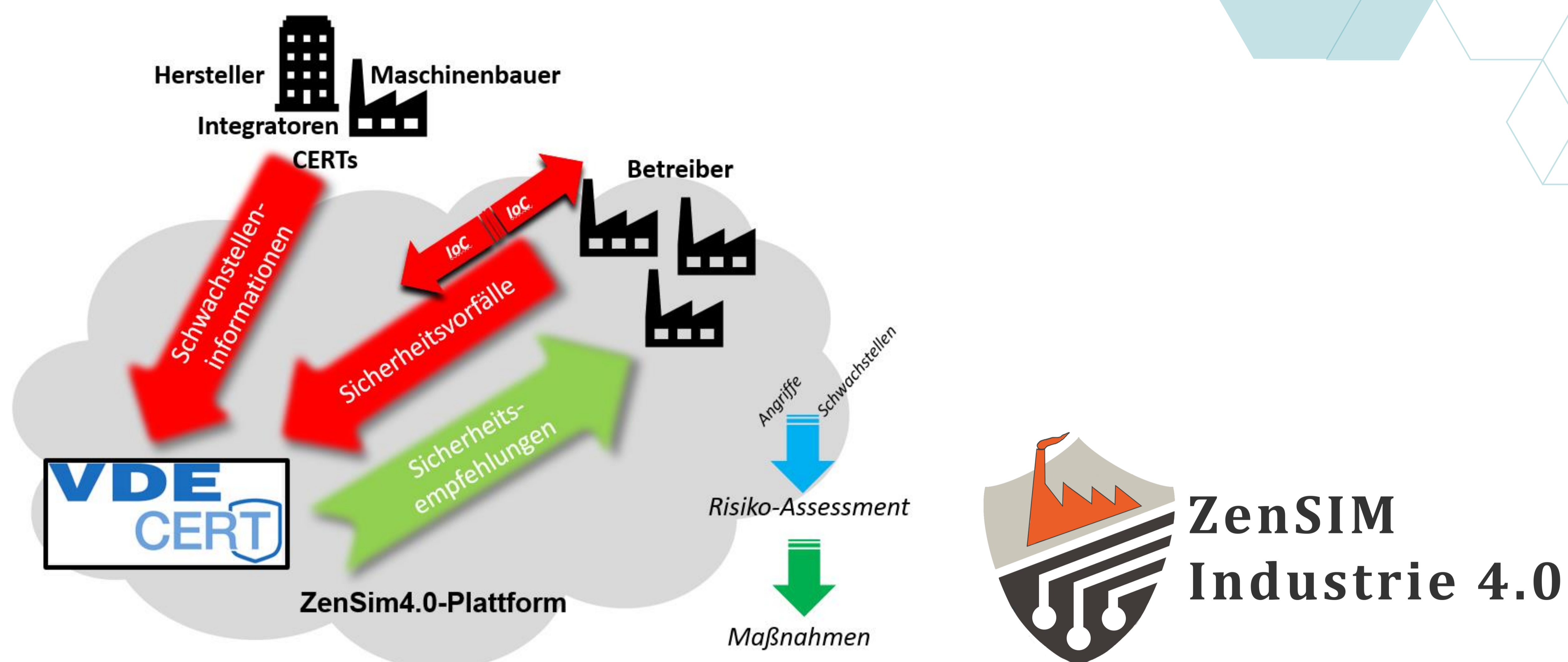


Mittelstandskonferenz 2023

KMU stärken durch digitale Innovationen



ZenSIM 4.0 – Zentrales Security Incident Management für KMU in Industrie 4.0

Problemstellung und Motivation

IT-Sicherheitsmanagement in Industrieumgebungen ist durch die Vernetzung von Komponenten, Cloud-Nutzung und Diversität kein einfaches Unterfangen. Um eine effektive Sicherheit gewährleisten zu können wird daher ein Security Incident Management (SIM) notwendig. Dadurch lassen sich Anomalien und neuste Angriffe kommunizieren, Reaktionszeiten reduzieren sowie ein kontinuierliches, automatisiertes Schwachstellenmanagement durchführen. Dabei werden die gesetzlichen Auflagen und Compliance im Projekt mit berücksichtigt.

Ziele

- Zentrale Plattform für „Security Incident Management“ schaffen, um
 - IT-Schwachstellen im Produkt und OT-Umfeld erkennen zu können.
 - Sicherheitsvorfälle in IT-/OT-Infrastrukturen und schützenswerte Informationen (Assets) bereitzustellen.
- Unterstützung zum selbstständigen Betrieb eines Security Incident Managements, ohne SOC

Ergebnisse

- Nutzung des Common Security Advisory

Framework (CSAF) 2.0 zum Transport von Schwachstelleninformationen, Kritikalität, Herstellerinfos, Gegenmaßnahmen etc.

- Nutzung des SIEM-Systems ScanBox® beim Betreiber, um Schwachstellen erkennen und melden zu können.
- CSAF-Demonstrator zur Kommunikation zwischen SIEM, Asset Collector, CSAF-Consumer und -Aggregator

Projektkoordination

DECOIT® GmbH & Co. KG

Projektlaufzeit

01.10.2021 - 31.09.24

Kontakt

Prof. Dr. Kai-Oliver Detken
Fahrenheitstraße 9, 28359 Bremen
Tel.: +49 (0) 421/596064-01
E-Mail: detken@decoit.de

Förderkennzeichen

16KIS1503K, 16KIS1504 und 16KIS1505

Akronym

ZenSIM 4.0

Projektwebseite

www.zensim-project.de

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung