ICS-MONITORING – DIE QUAL DER WAHL

Computacenter, 10.2022

Computacenter

ICS MONITORING

MOTIVATION

Relevante Passagen zum Schwerpunkt: „Systeme zur Angriffserkennung“

„Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten“

(§ 2 Absatz 9b BSIG)

Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen“

(§ 8a Absatz 1a Satz 1, 2 BSIG, Unterstreichungen für diese OH vorgenommen).

Sicherheit durch Prävention

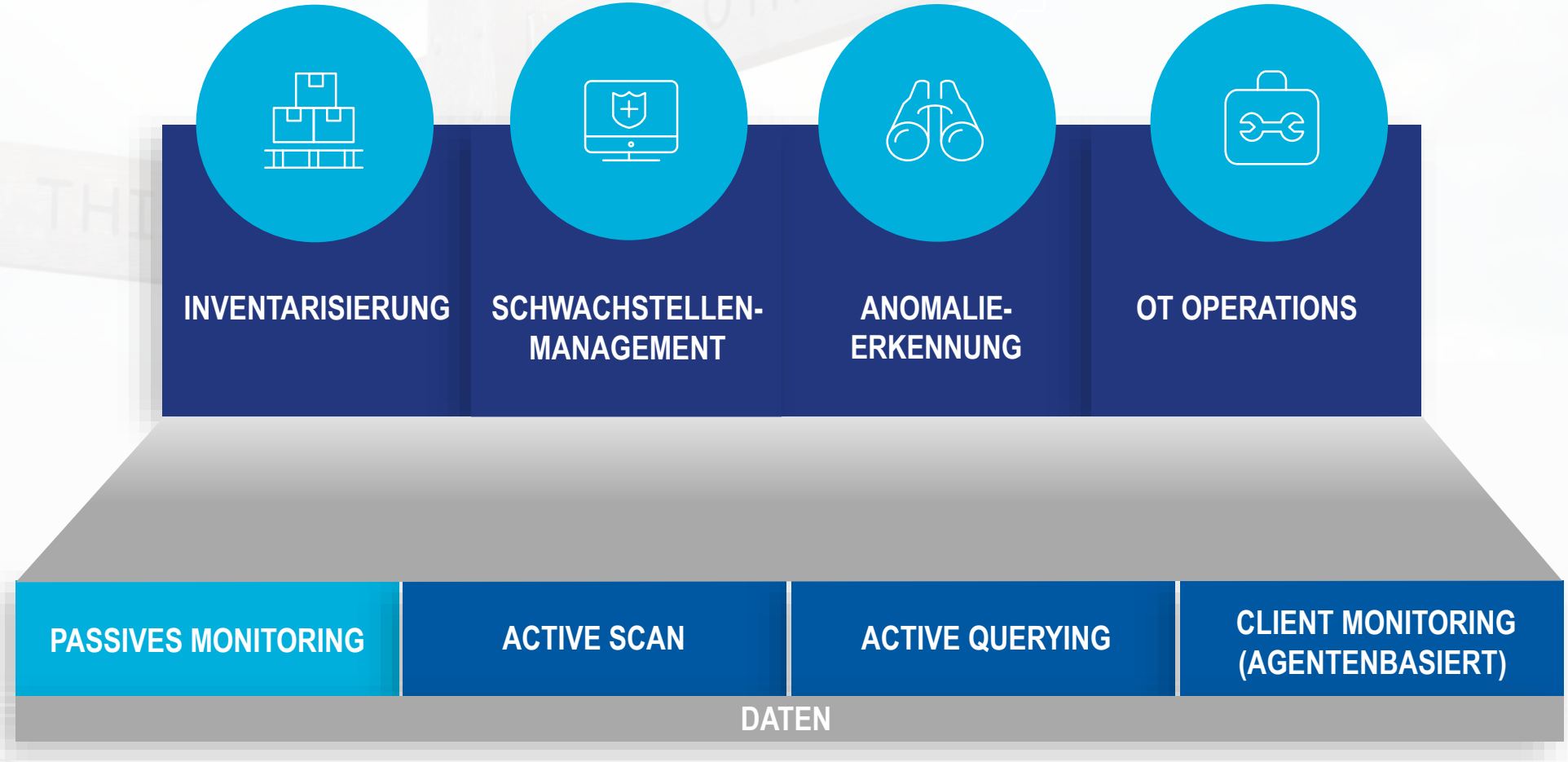
Unzureichend !

Auszug Stand 27.09.2022
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=4

© Computacenter 2022

ICS MONITORING

FUNKTIONSÜBERSICHT & DATENAKQUISITION



© Computacenter 2022

ICS MONITORING

PARAMETER FÜR DEN ANFORDERUNGSKATALOG

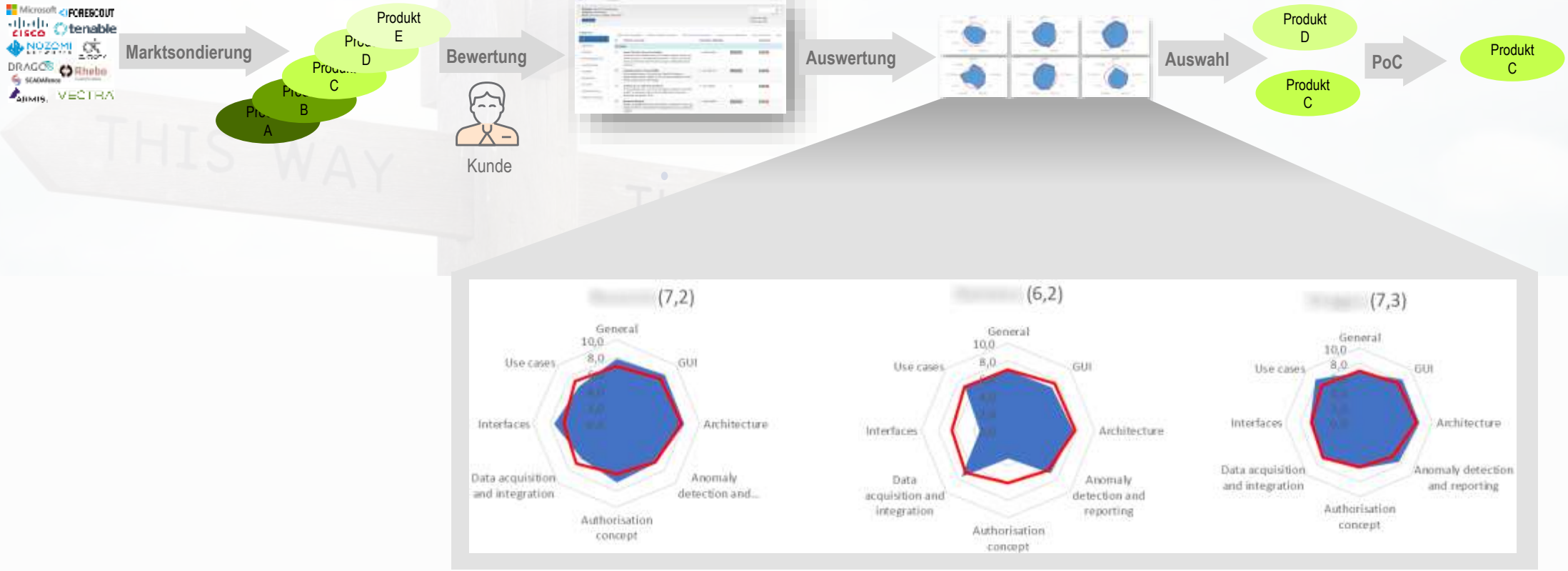
- Welche Funktionen sollen genutzt werden?
  - Wie ist die Priorität?
- Wer betreibt die Lösung?
  - Welche Ressourcen stehen zu Verfügung?
- Mapping zu aktuellen Bedrohungslage
- Definition von funktionalen und nicht funktionalen Anforderungen
- Integration der Lösungen in bestehende Architekturen
  - Wie viele Standorte müssen implementiert werden? (Komplexität und Heterogenität)

© Computacenter 2022

ICS MONITORING

LÖSUNGSVERGLEICH

Hersteller/Produkte (Auszug)



© Computacenter 2022

ICS MONITORING

FAZIT – WAS IST NOTWENDIG?

- Fokussierung bei der Funktionsauswahl
  - Anwendungsbereich: Was sind die primären Ziele?
  - Ressourcen: Wer betreibt die Lösung

- Validierung der Lösung im Anwendungsgebiet
  - Alle Beteiligten frühzeitig mit einbinden
  - Verprobung der Lösungen

- Überführung in den Betrieb
  - Verantwortungen zuweisen
  - Kapazitäten freigeben oder schaffen
  - Prozesse definieren

© Computacenter 2022

DANKE!

Rainer Leisen
Solution Manager – OT Security
Professional Services Enablement

Computacenter

Kokkolastraße 1, 40882 Ratingen, Germany
Computacenter AG & Co. oHG
M: +49 173 42 88 782
E: rainer.leisen@computacenter.com

www.computacenter.com | LinkedIn | Xing | YouTube | Twitter

© Computacenter 2022