Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer AISEC

Fraunhofer IEM

Deutschland Digital•Sicher•BSI•

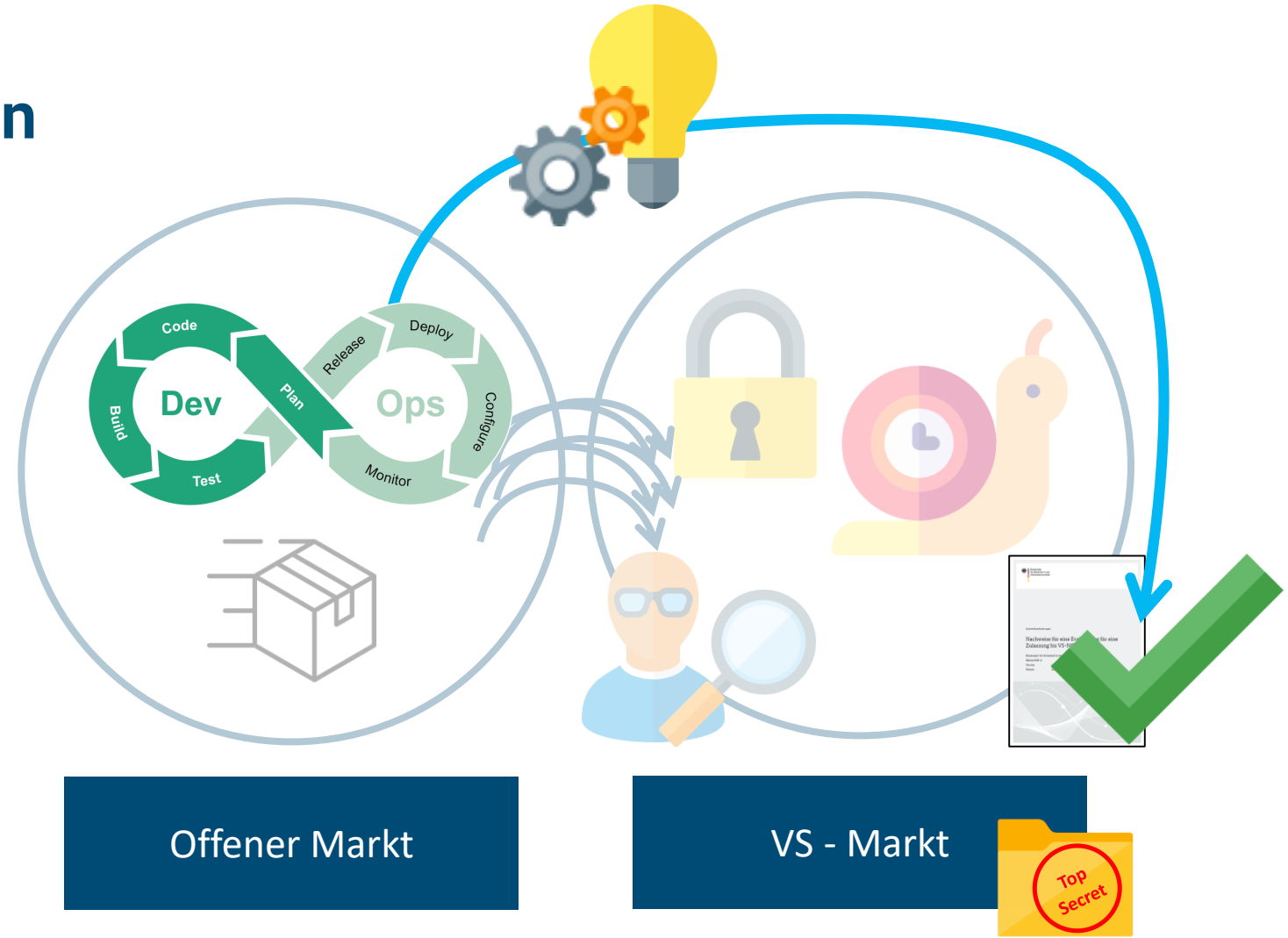
Auf dem Weg zur automatisierten Nachweiserbringung

Ergebnisse aus DUST

Jan Sinkewitz (BSI)
Florian Wendland (Fraunhofer AISEC)

Berlin, 22.01.2024

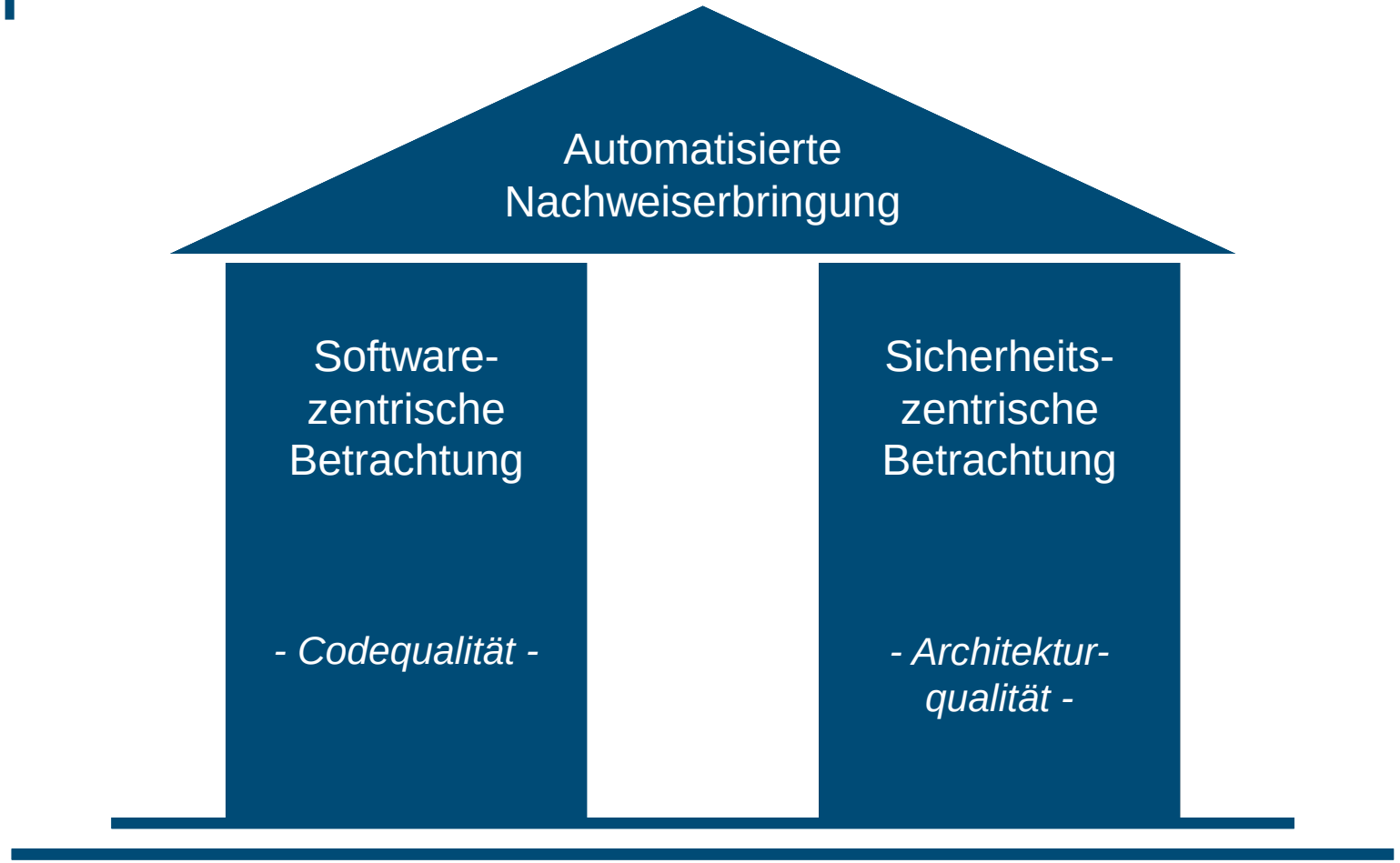
Motivation



Offener Markt

VS - Markt

Vision


Automatisierte
Nachweiserbringung
Software-
zentrische
Betrachtung
- Codequalität -
Sicherheits-
zentrische
Betrachtung
- Architektur-
qualität -

Projekt 552 - DUST

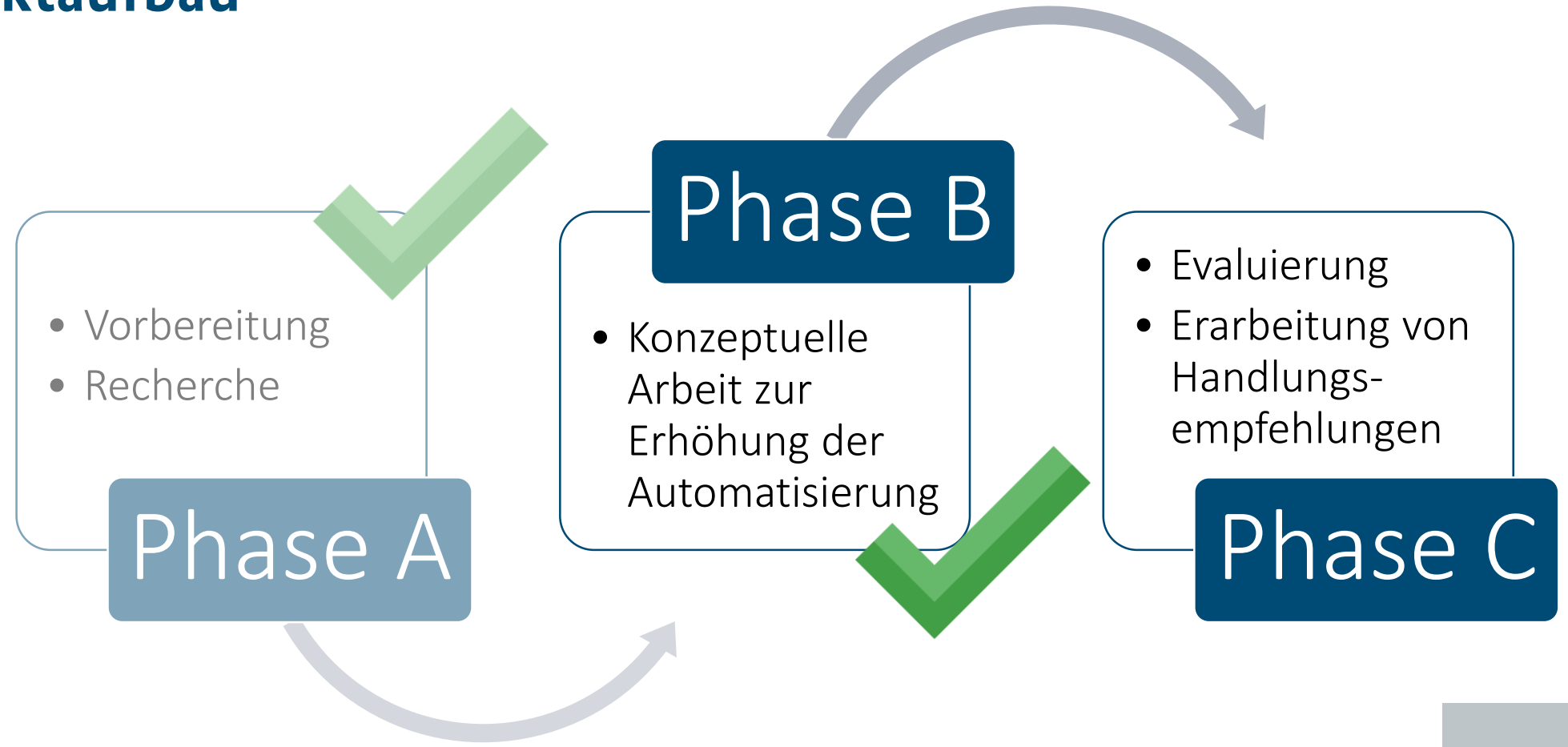
- **D**ie a**U**tomati**S**che digi**T**ale Nachweisführung zur Evaluierung von VS-IT
- Projektlaufzeit: 11/22 – 09/24
- Ziel
  - Erhöhung des Automatisierungsgrades im VS-IT Evaluierungsprozess

Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer AISEC

Fraunhofer IEM

Projektaufbau



Phase B – Konzeptuelle Arbeit

Automatisierung der aktuellen Nachweise

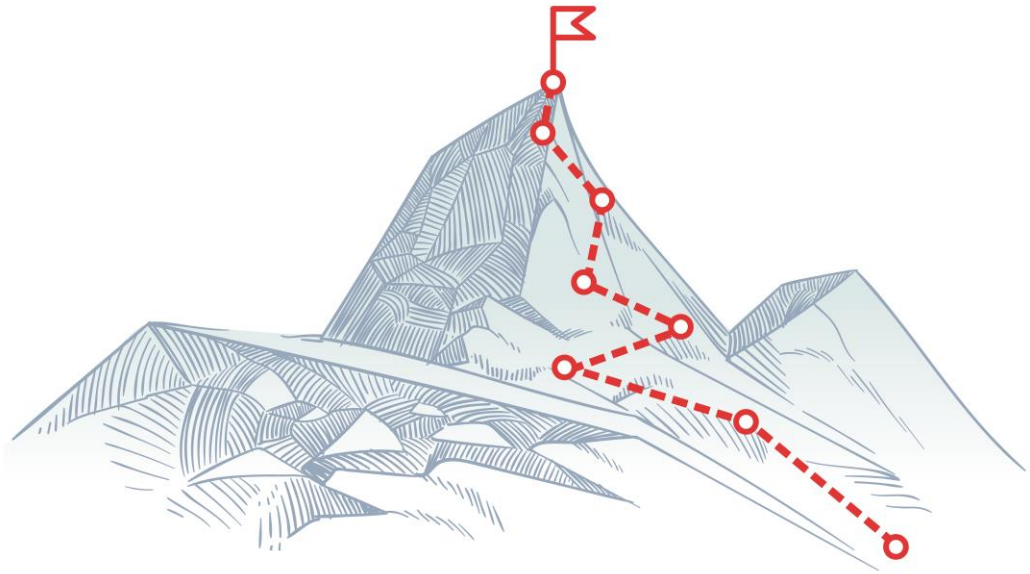
Erhöhung des Automatisierungsgrads durch kleine Änderungen an den aktuellen Nachweisen

Redesign des Nachweiskatalogs zur Maximierung des Automatisierungspotentials

Phase B – Konzeptuelle Arbeit

- Arbeitsschwerpunkte
  - Nachweiskatalog und Nachweisdokumente
  - Prozessbeschreibung als CI/CD-Pipeline
  - Automatisierung durch Werkzeuge

- Parallel Workshops vom BSI mit Herstellern und Prüfstellen



Phase B – Konzeptuelle Arbeit

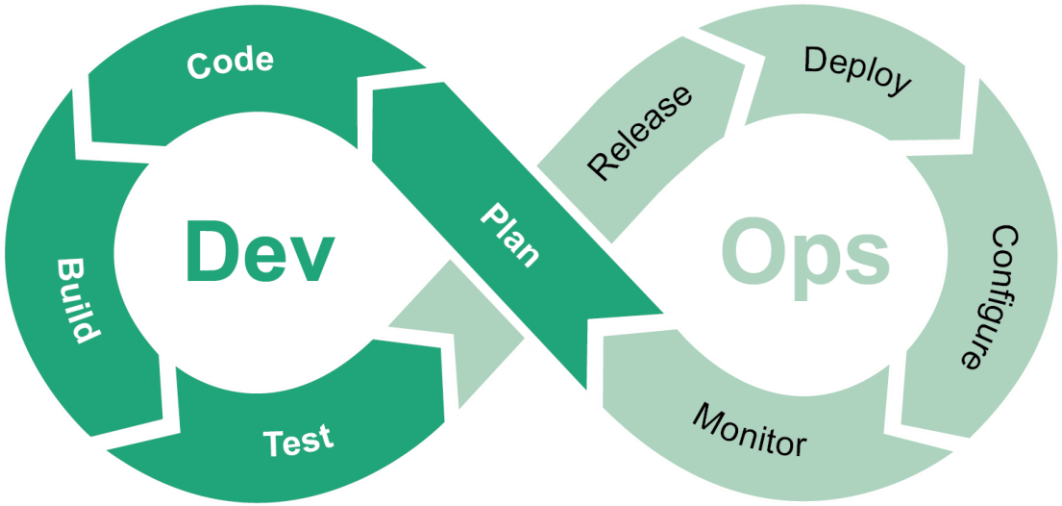
- Ist-Zustand
  - Anforderungen an die Form der Nachweise, wenige technische Anforderungen an das Produkt
  - Formate für Nachweiserbringung ⟷ Standardformate
  - Nachweiserbringung als Prosatexte ➔ Herausforderung für Automatisierung
- Vorschläge
  - Standardformate einsetzen ➔ strukturiertes Format
  - Zwischenergebnisse aus Entwicklung direkt nutzen
  - Fokus auf technische und konkrete Anforderungen an das Produkt (z.B. in VS-AP)

Phase B – Konzeptuelle Arbeit

- Einheitliches strukturiertes Nachweisdokument
  - Maschinelle Verarbeitung
  - Identifikatoren für Elemente → referentielle Integrität
  - Integration von Ergebnissen aus Werkzeugen
  - Validierung über Schema

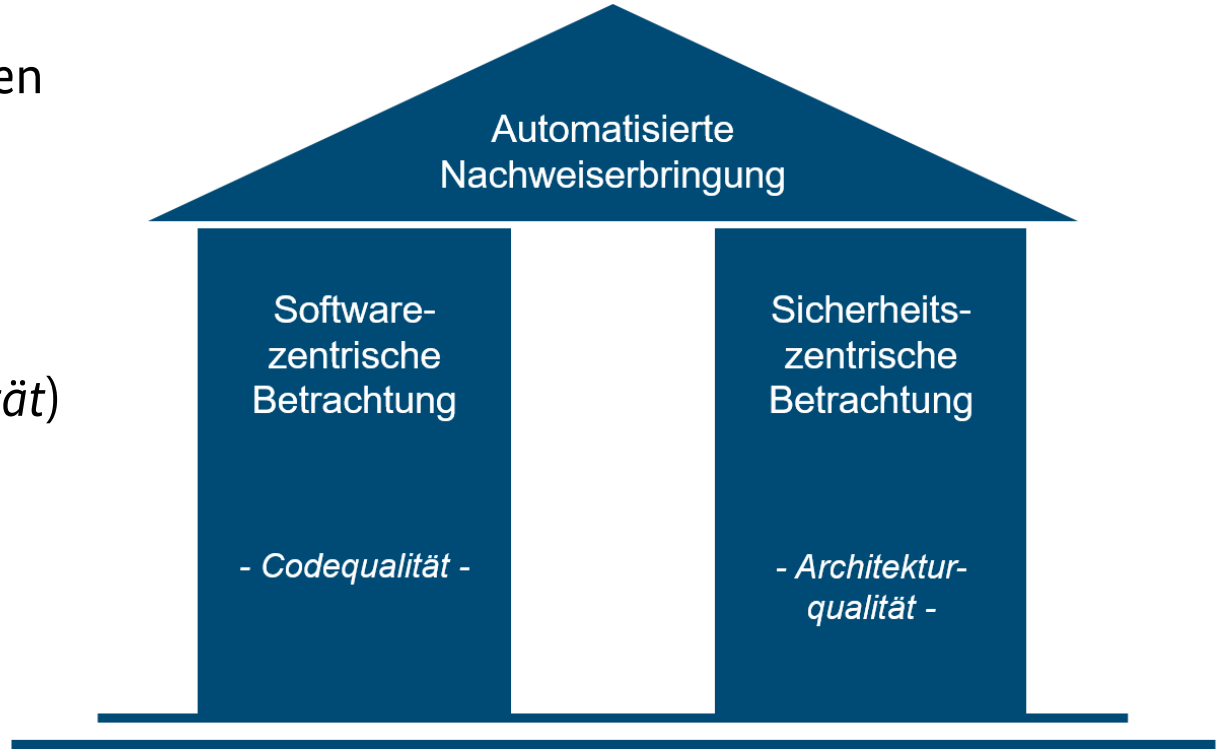
Phase B – Konzeptuelle Arbeit

- Orientierung an modernen Softwareentwicklungsprozessen
- Aufbauen auf existierender Automatisierung in CI/CD-Pipelines
- Fördern von Tool-basierten Analysen und Prüfungen
  - Etablierte Tools, Prozesse und Formate nutzen
  - Ergebnisse verwenden
- Reduzieren manueller Aufwände



Phase B – Konzeptuelle Arbeit

- Automatisierung durch Einsatz von Werkzeugen
  - Große Auswahl
  - Standardisierte Reportformate
- Vertrauen in Sicherheit durch
  - Softwarezentrische Betrachtung (*Codequalität*)
  - Sicherheitszentrische Betrachtungen (*Architekturqualität*)



Phase B – Konzeptuelle Arbeit

- Fragestellung ➔ Ist der Code frei von Fehlern und Schwachstellen?
- Etablierte Werkzeuge und Techniken
- Kategorien
  - Unit/Integration/System-Testing
  - Software Composition Analysis & SBOM
  - Static Application Security Testing
  - Dynamic Application Security Testing & Fuzzing
- Bereits im Einsatz
- Mehrwert durch automatisierte Reduzierung der Angriffsfläche über Erhöhung der Codequalität

Phase B – Konzeptuelle Arbeit

- Herausforderungen
  - Bewertung von Werkzeugen
  - Synergien zwischen Werkzeugen
  - Konsolidierung von Ergebnissen
  - Nachvollziehbarkeit von Ergebnissen (Chain of Reasoning)
- Opt-out ermöglichen
- Handlungsempfehlung
  Erarbeitung von Kriterien in Zusammenarbeit zwischen BSI, Herstellern und Prüfstellen

  ➔ Ihre Erfahrungen und Anregungen sind uns wichtig!

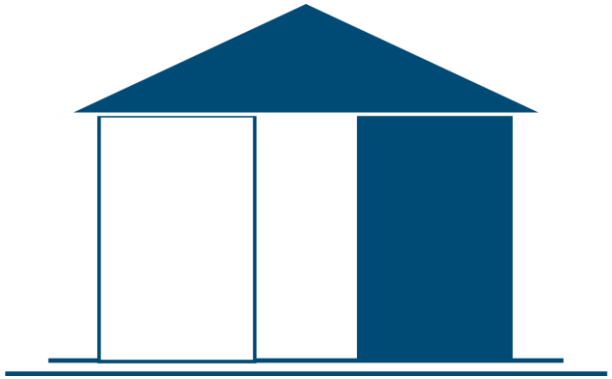
Phase B – Konzeptuelle Arbeit

- Fragestellung ➔ Erfüllt die Software alle (Sicherheits-)Anforderungen?
- Aktuelle Forschung
- Beispiel: Verwendung kryptographischer Bibliotheken gemäß BSI TR-02102
  - Wie werden kryptographische Bibliothek richtig (Implementierung) und nach den Vorgaben vom BSI (Anforderungen) verwendet?
  - CogniCrypt und CrySL (Fraunhofer IEM) https://github.com/CROSSINGTUD/CryptoAnalysis
  - Codyze und MARK (Fraunhofer AISEC) https://www.codyze.io/
- Mehrwert durch (teil-)automatisierte Bewertung der Sicherheitsarchitektur

CogniCrypt

Codyze

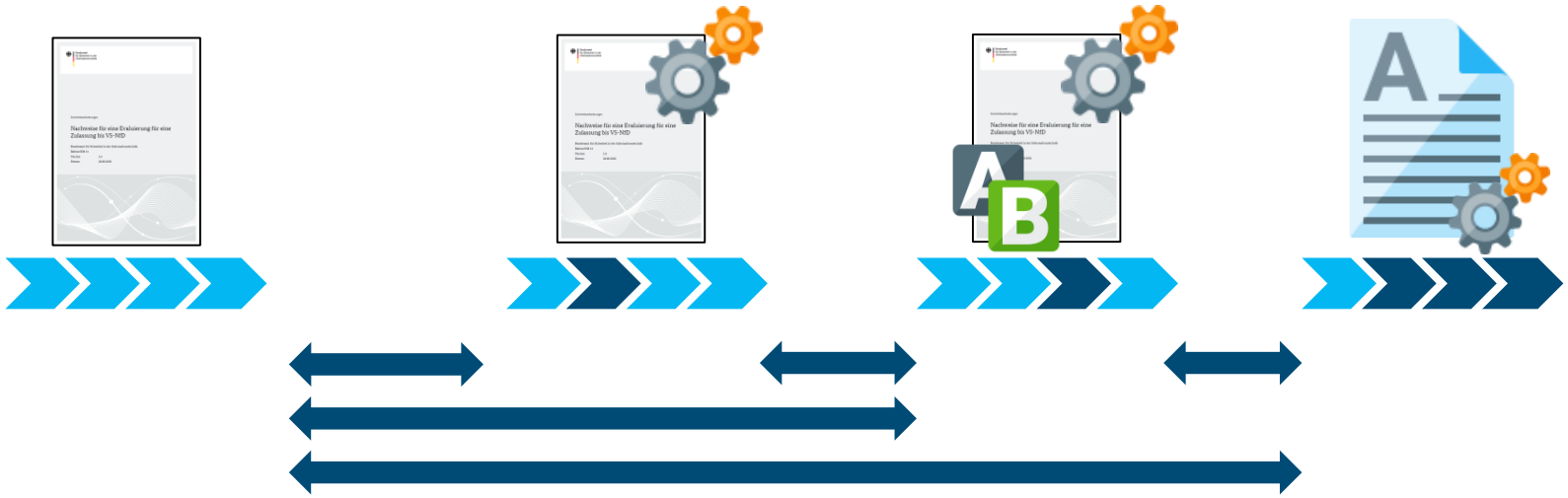
Phase B – Konzeptuelle Arbeit



- Herausforderungen
  - Erstellen von Prüfregeln für Anforderungen (z.B. VS-AP)
  - Modellieren möglicher Implementierungen
  - Pflege und Wartung von Regeln und Modellierungen
  - Entwicklung von Tools zur Überprüfung der Regeln
- Einschätzung
  - Geringes bis mittleres Automatisierungspotential
  - Bewertung der Chancen in Zusammenarbeit mit Herstellern und Prüfstellen

➔ Ihre Erfahrungen und Anregungen sind uns wichtig!

Phase C - Evaluierung



Analyse und Vergleich der Änderungen im Evaluierungsprozess

Mockup und Testlauf

Vergleich der Ergebnisse und Empfehlungen

Ausblick

- Was bedeutet das für Sie?
  - In Zukunft: Weniger repetitive manuelle Tätigkeiten
  - Diskussion in nationalen und internationalen Communities
  - Standardisierung von Tools und Schnittstellen
  - Agilere Produktentwicklung für den VS-Markt
  - Einsatz von Tools (CI/CD-Pipeline)

Haben Sie Interesse an einer Zusammenarbeit?

Nur gemeinsam schaffen wir das!

gp-dust@bsi.bund.de

Kontakt

Deutschland
Digital•Sicher•BSI•

Jan Sinkewitz, BSI

Evaluator
Referat KM 26 – Sichere stationäre VS-IT
Jan.sinkewitz@bsi.bund.de
Tel. +49 228 99 9582 5638

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de / www.bsi-fuer-buerger.de

Florian Wendland, Fraunhofer AISEC

Wissenschaftlicher Mitarbeiter
Service & Application Security
florian.wendland@aisec.fraunhofer.de
Tel. +49 89 3229986 177

Fraunhofer AISEC
Lichtenbergstraße 11
85748 Garching bei München
www.aisec.fraunhofer.de

Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer AISEC

Fraunhofer IEM