SECURITY-BY-DESIGN IM MASCHINEN- UND ANLAGENBAU

Verantwortung für Security liegt im gesamten Team

Thorsten Koch

6. September 2023

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer
IEM

Sicherheitsvorfälle sind alltäglich geworden

Beispiele für Sicherheitsvorfälle im Bereich Industrial Control Systems

Anlagenbetreiber

Kritische Infrastruktur

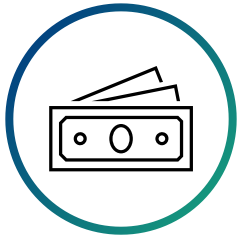
Schwachstellen in OT-Komponenten

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Fatale Folgen enstehen, wenn Security nicht ausreichend priorisiert wird

Eigen-schäden

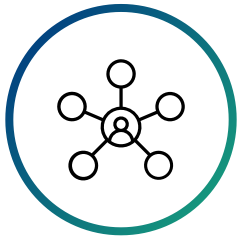


Finanzieller Schaden bis hin zur Insolvenz

Rechtliche Konsequenzen bis hin zu Freiheitsstrafen

Reputationsschäden bis hin zur Betriebsunfähigkeit

Fremd-schäden



Schäden an Kunden und Dritten

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Mehrere Gesetze, Normen und Standards sind im Bereich Security relevant

Ausgewählte Beispiele

Gesetze

DSGVO

Die DSGVO ist eine einheitliche Richtlinie zum Schutz privater und persönlicher Daten. Sie richtet sich an in- und ausländische Unternehmen und öffentliche Einrichtungen, die personen-bezogene Daten von EU-Bürgern speichern oder verarbeiten.

IT-Sicherheitsgesetz 2.0

Das IT-Sicherheitsgesetz (2.0) ist ein Gesetz, das Organisationen dazu verpflichtet, ein definiertes Mindestniveau an IT-Sicherheit einzuhalten. Zu diesem Zweck müssen technische und organisatorische Maßnahmen ergriffen und nachgewiesen werden. Das Gesetz richtet sich an Unternehmen aus der Telekommunikationsbranche, Anbieter von digitalen Diensten und Betreiber kritischer Infrastrukturen (KRITIS)

Normen

ISO 27001

Die ISO 27001 spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems. Die Norm umfasst insbesondere die Bewertung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation.

IEC 62443

Die IEC 62443 spezifiziert einen ganzheitlicher Ansatz für Betreiber, Integratoren und Komponentenhersteller zur Sicherstellung der Cybersecurity.

- Betreiber müssen die Maschinen / Anlagen entsprechend der Herstellervorgaben betreiben
- Integratoren muss sichere Komponenten einkaufen und zu einer Maschine / Anlage integrieren
- Komponentenhersteller entwickelt und fertigt sichere Komponenten

Kommende Gesetze und Richtlinien in der EU im Bereich Security

Gesetze

NIS 2 Directive

Die NIS2-Richtlinie ist die EU-weite Gesetzgebung zur Cybersicherheit. Sie enthält rechtliche Maßnahmen zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU. Unternehmen, die von den Mitgliedstaaten als Betreiber wesentlicher Dienste in den oben genannten Sektoren eingestuft wurden, müssen geeignete Sicherheitsmaßnahmen ergreifen und die zuständigen nationalen Behörden über schwerwiegende Vorfälle informieren.

EU Cyber Resilience Act

Der Cyber Resilience Act (CRA) soll die Rahmenbedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen festlegen, indem es dafür sorgt, dass Hardware- und Softwareprodukte mit weniger Schwachstellen auf den Markt kommen und dass die Hersteller die Sicherheit während des gesamten Lebenszyklus eines Produkts betrachten.

Radio Equipment Directive

Die Radio Equipment Directive (RED) schafft einen rechtlichen Rahmen für das Inverkehrbringen von Funkanlagen. Die Directive legt grundlegende Anforderungen für Sicherheit und Gesundheit, elektromagnetische Verträglichkeit und die effiziente Nutzung des Funkspektrums fest.

Richtlinien

Maschinenrichtlinie

Die Maschinenrichtlinie enthält verbindliche Anforderungen für Hersteller und andere Wirtschaftsakteure, die die funktionale Sicherheit von Maschinen regeln. Die Anforderungen in der neuen Verordnung betreffen neben der funktionalen Sicherheit u.a. die Cybersicherheit von Steuerungen.

Kommende Gesetze und Richtlinien in der EU im Bereich Security

Gesetze

NIS 2 Directive

Die NIS2-Richtlinie ist die EU-weite Gesetzgebung zur Cybersicherheit. Sie enthält rechtliche Maßnahmen zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU. Unternehmen, die von den Mitgliedstaaten als Betreiber wesentlicher Dienste in den oben genannten Sektoren eingestuft wurden, müssen geeignete Sicherheitsmaßnahmen ergreifen und die zuständigen nationalen Behörden über schwerwiegende Vorfälle informieren.

EU Cyber Resilience Act

Der Cyber Resilience Act (CRA) soll die Rahmenbedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen festlegen, indem es dafür sorgt, dass Hardware- und Softwareprodukte mit weniger Schwachstellen auf den Markt kommen und dass die Hersteller die Sicherheit während des gesamten Lebenszyklus eines Produkts betrachten.

Radio Equipment Directive

Die Radio Equipment Directive (RED) schafft einen rechtlichen Rahmen für das Inverkehrbringen von Funkanlagen. Die Directive legt grundlegende Anforderungen für Sicherheit und Gesundheit, elektromagnetische Verträglichkeit und die effiziente Nutzung des Funkspektrums fest.

Richtlinien

Maschinenrichtlinie

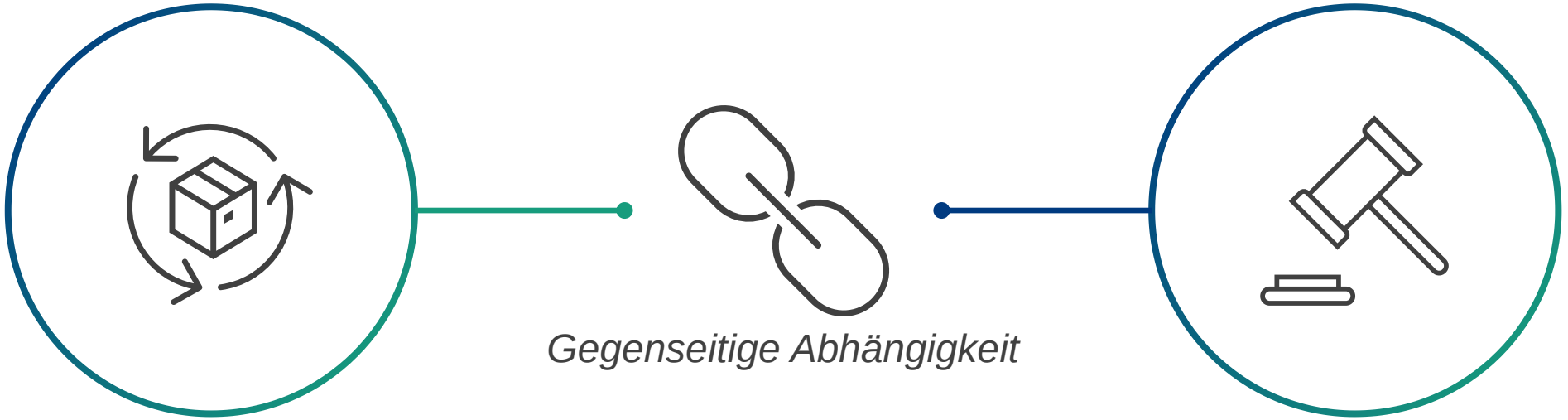
Die Maschinenrichtlinie enthält verbindliche Anforderungen für Hersteller und andere Wirtschaftsakteure, die die funktionale Sicherheit von Maschinen regeln. Die Anforderungen in der neuen Verordnung betreffen neben der funktionalen Sicherheit u.a. die Cybersicherheit von Steuerungen.

Die rechtlichen Anforderungen an die Security werden in den kommenden Jahren deutlich steigen. Unternehmen müssen sich daher frühzeitig mit der systematischen Betrachtung von Security beschäftigen.

Das Produktteam und die Rechtsabteilung müssen im Bereich Security zusammenarbeiten

Manager, Product Owner, und Produktteam

Rechtsabteilung

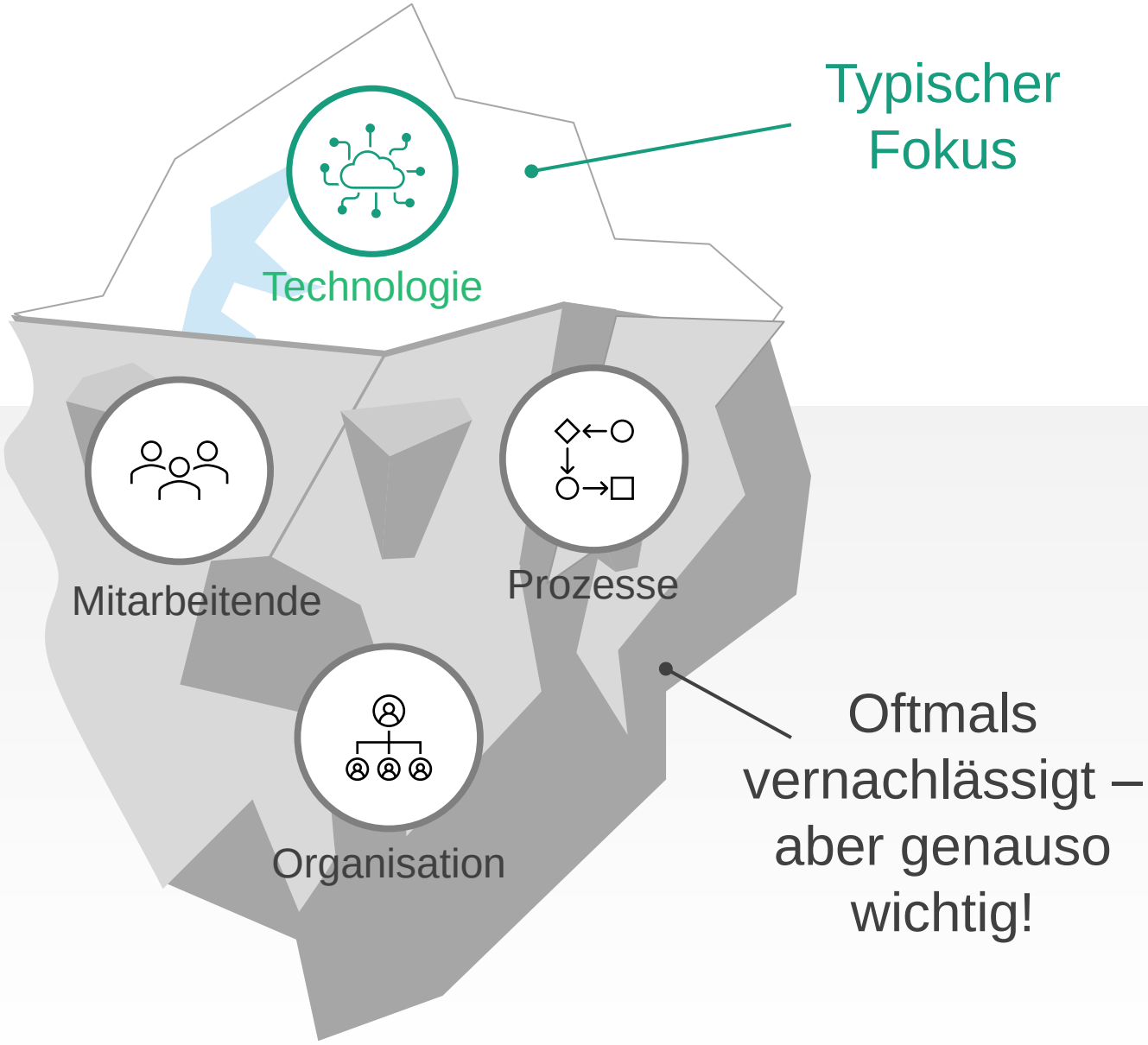


Gegenseitige Abhängigkeit

Manager, Product Owner und das Produktteam sollten in der Lage sein, zu verstehen, welche Gesetze für sie gelten (mit Hilfe der Rechtsabteilung) und diese umzusetzen.

Die Rechtsabteilung sollte in der Lage sein, die wichtigsten Anforderungen und Gesetzesänderungen zu vermitteln.

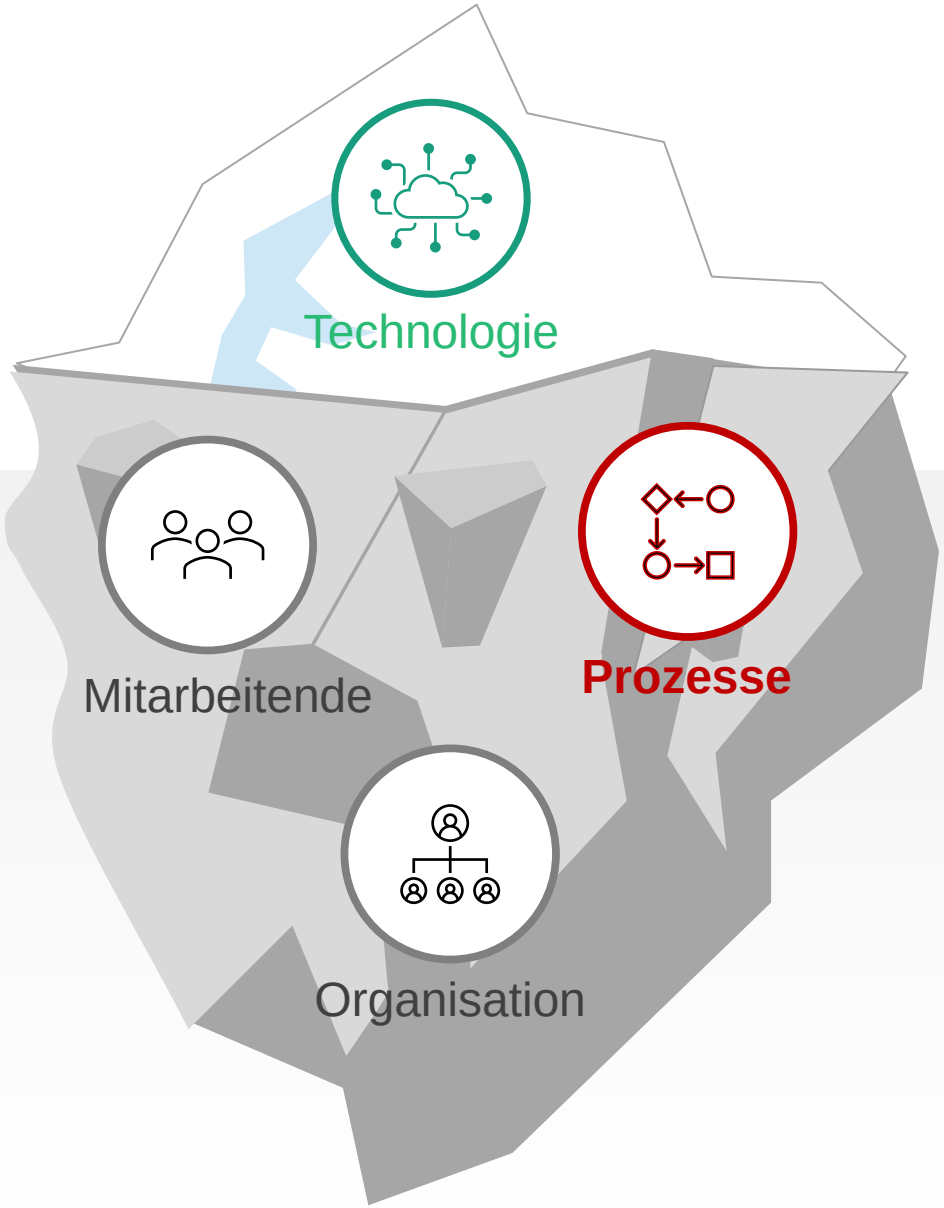
Security muss ganzheitlich betrachtet werden



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Security muss ganzheitlich betrachtet werden

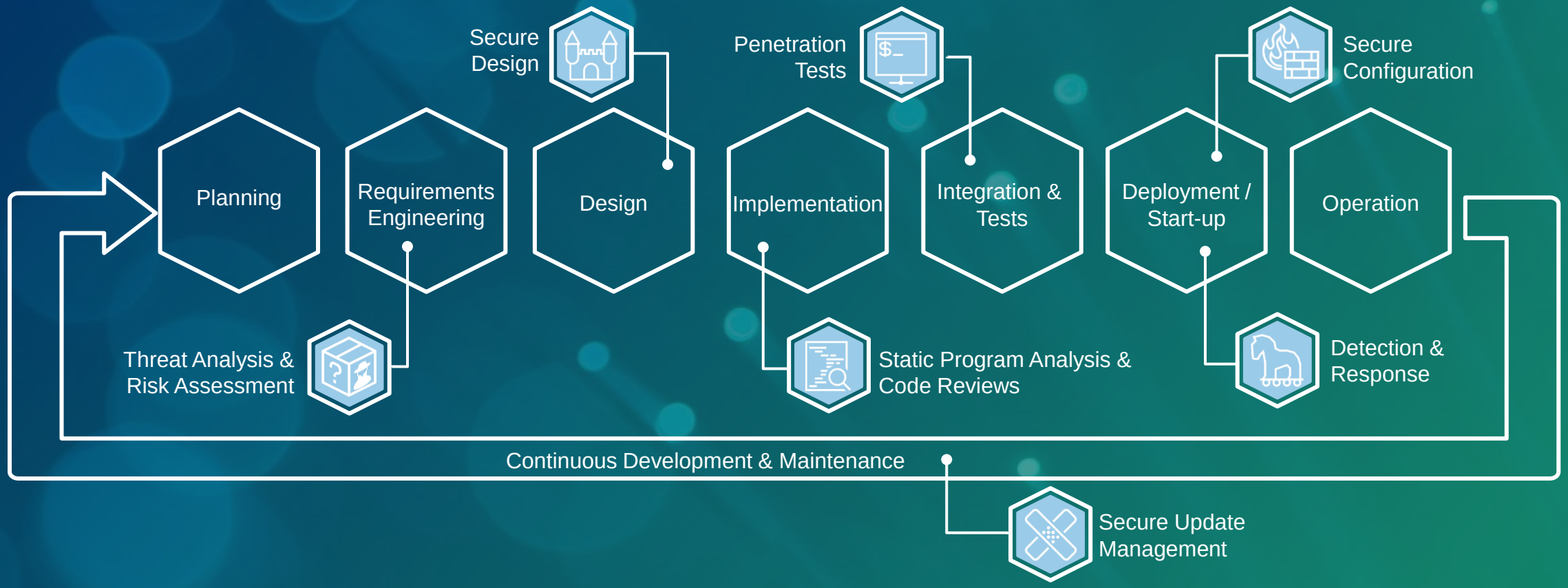


HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

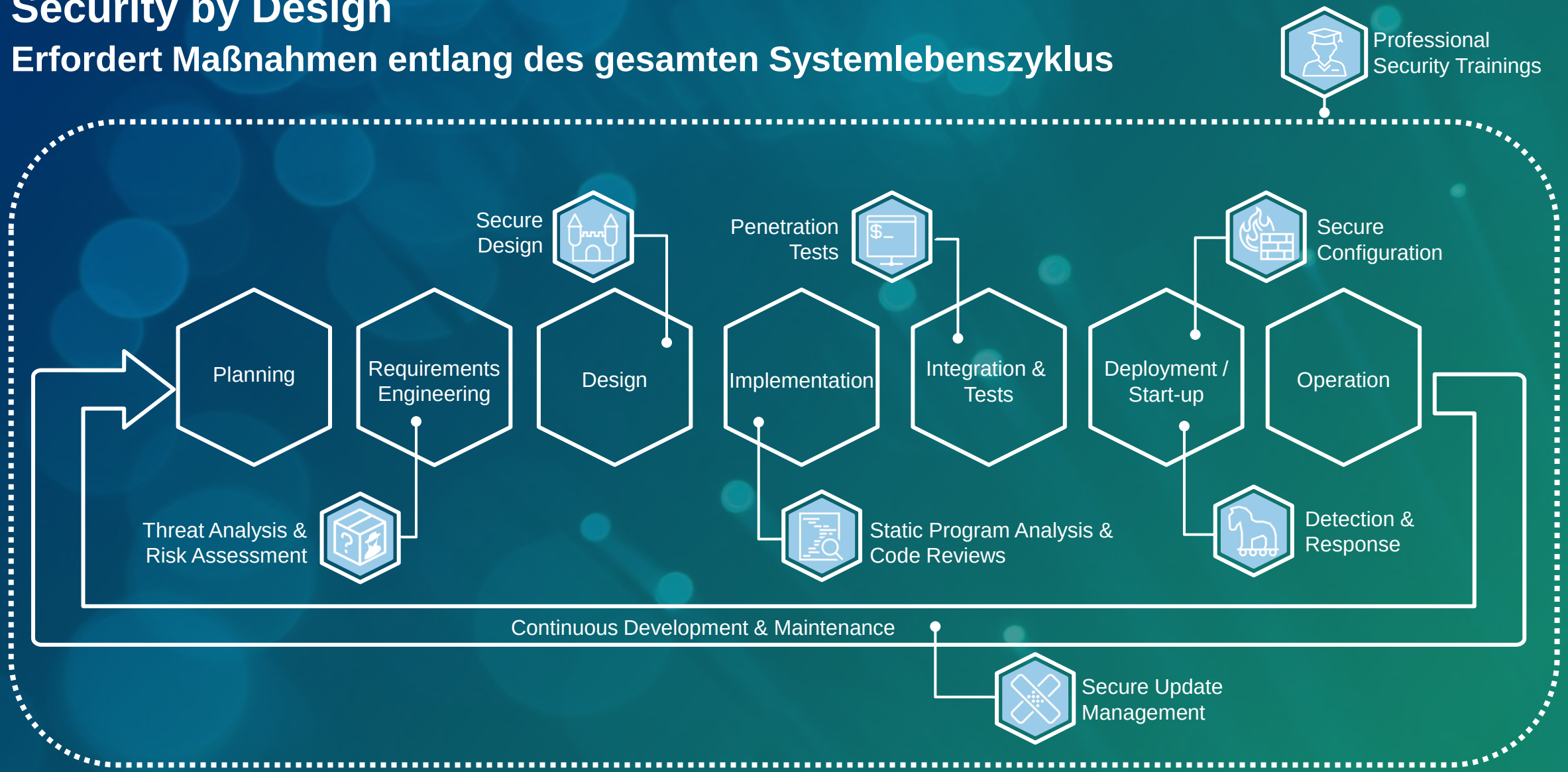
Security by Design

Erfordert Maßnahmen entlang des gesamten Systemlebenszyklus

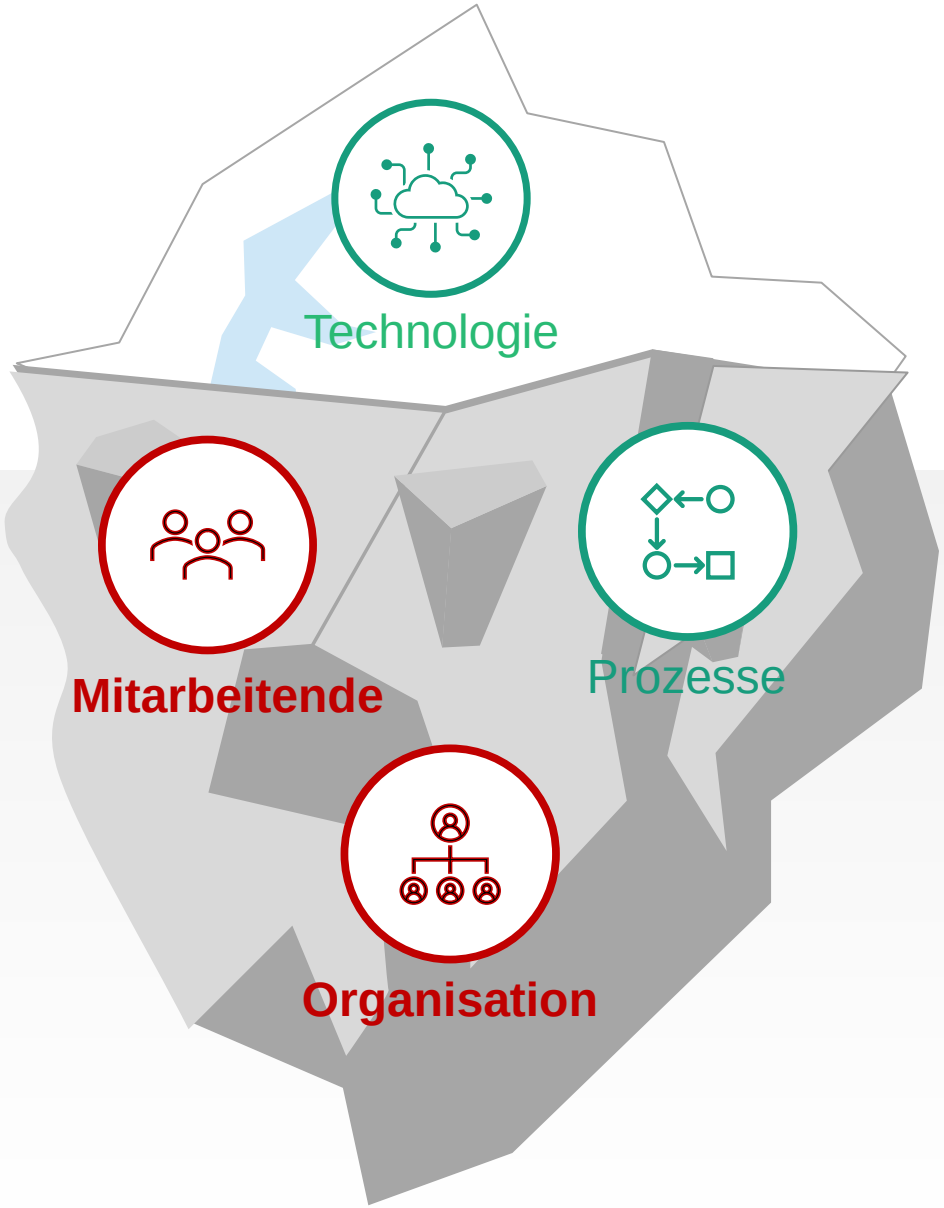


Security by Design

Erfordert Maßnahmen entlang des gesamten Systemlebenszyklus



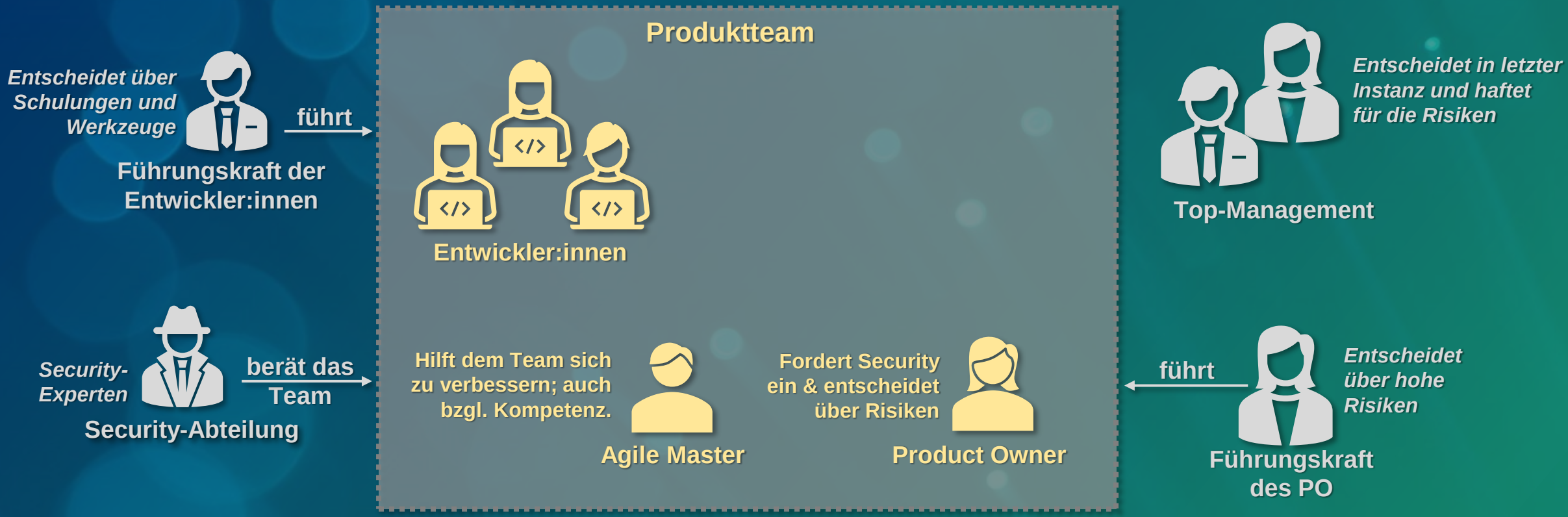
Security muss ganzheitlich betrachtet werden



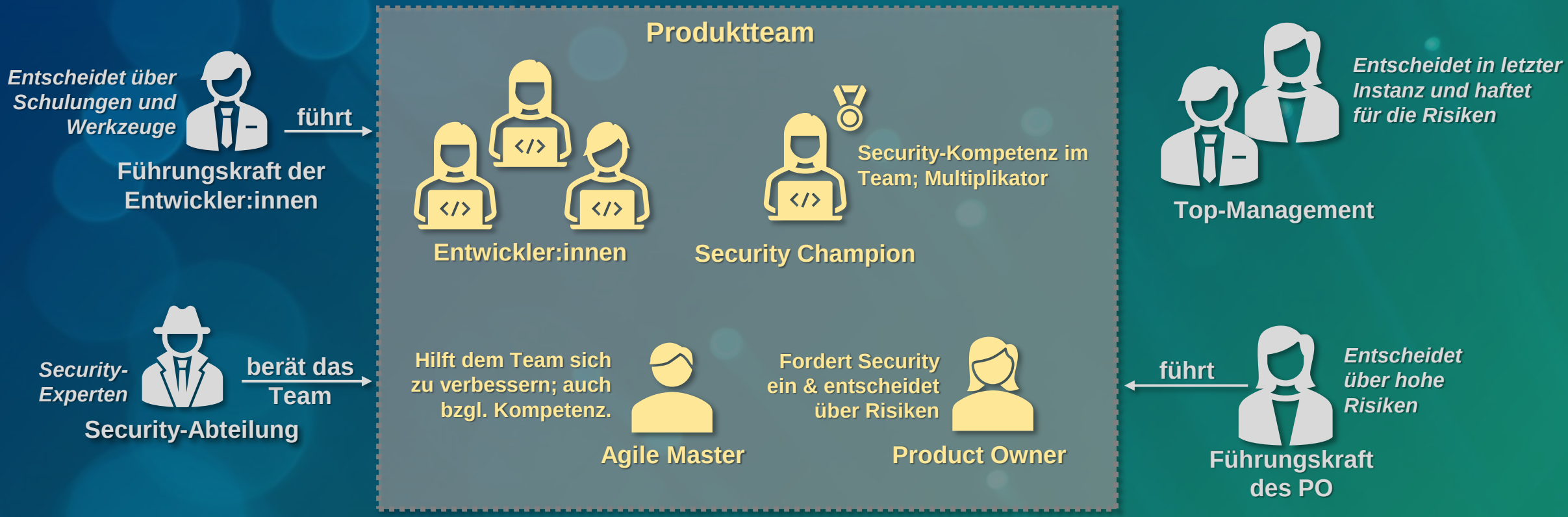
HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

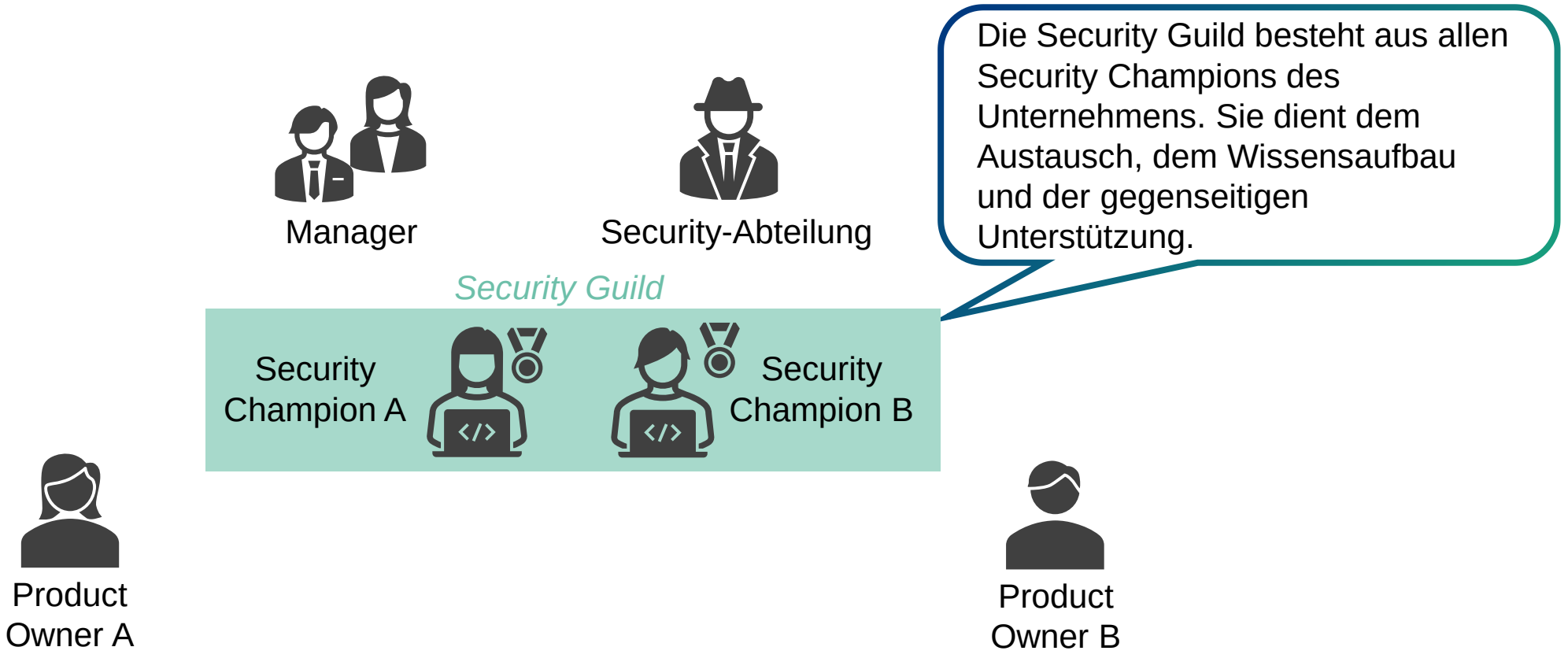
Um die Security der Produkte zu gewährleisten, müssen alle Beteiligten ihre Rolle kennen und die hierfür notwendigen Kompetenzen haben



Security Champions bringen Security-Kompetenzen in das Produktteam



Security Champions sind das fehlende Bindeglied zwischen dem Produktteam und dem Management



Kompetenzen eines Security Champions

Ein Security Champion ...

... inspiriert und motiviert das Team, einschließlich des PO, im Bereich Security besser zu werden und sensibilisiert dafür, dass Security gemacht werden muss (Leader)

… liefert dem Team Argumente, warum Werkzeuge und -Methoden im Team eingesetzt werden müssen und Schwachstellen behandelt werden müssen (Sparring Partner).

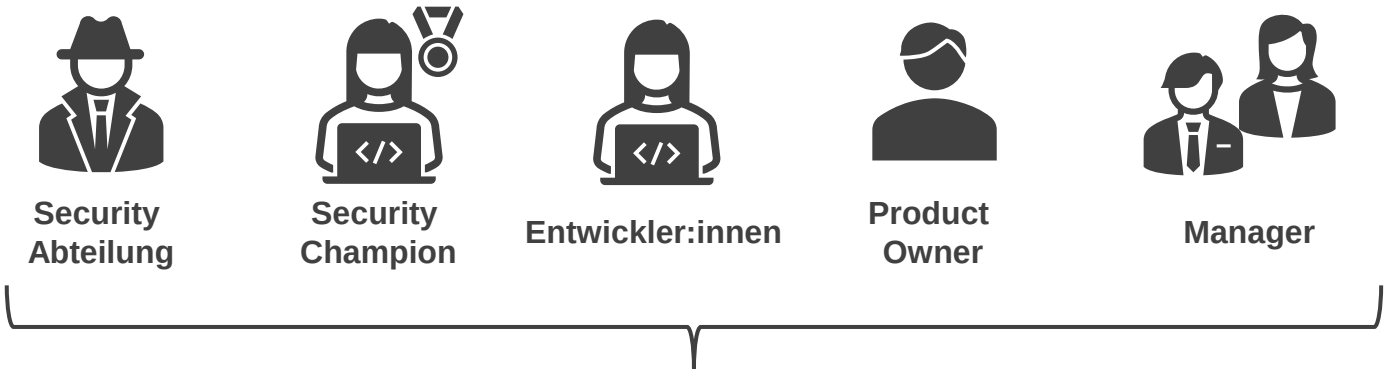
... verfügt über die entsprechenden Fachkenntnisse und Fähigkeiten für die Position (Expert).

... teilt sein Fachwissen mit dem Team, einschließlich des PO und der Organisation (Multiplier).

... ist immer noch Teil des Teams(developer).

Based on: Neumann, M.: Projekt Safari- Das Handbuch für Souveränes Projektmanagement. Campus Verlag GmbH, Frankfurt am Main, 2012

Die Verantwortung für Security liegt im gesamten Team



Alle an der Entwicklung beteiligten Personen müssen ihre Rolle kennen und die hierfür notwendigen Kompetenzen haben

Rollenspezifische Schulungen und Coachings helfen dabei, die notwendigen Kompetenzen effizient zu vermitteln

Beginnen Sie frühzeitig, damit Security ganzheitlich und systematisch in ihrem Unternehmen zu verankern.

Thorsten Koch

Fraunhofer IEM, Germany

thorsten.koch@iem.fraunhofer.de

thorsten-koch

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM