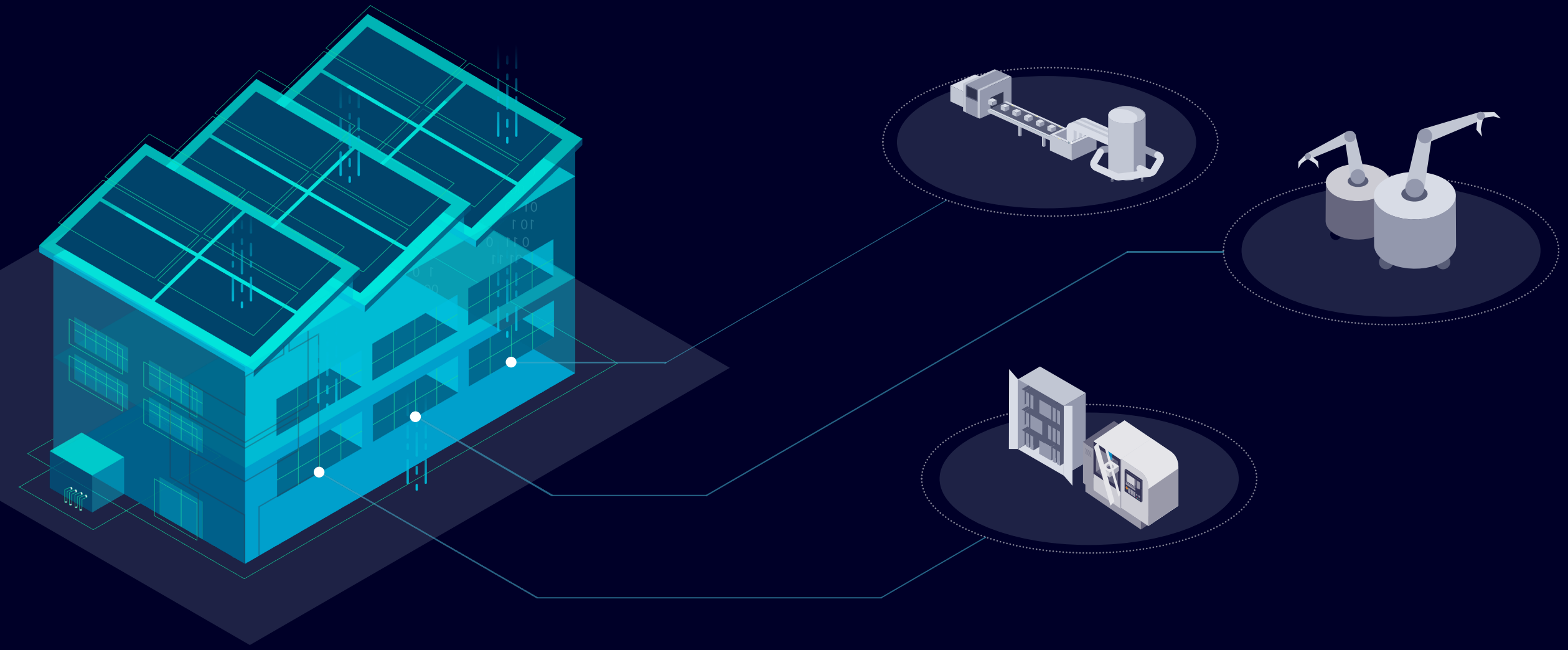
Industrial Cybersecurity

Challenge accepted

Frei verwendbar | © Siemens 2023 | Sandra Dominikus

SIEMENS

Früher gab es isolierte Kommunikationsinseln in der OT



Frei verwendbar | © Siemens 2023

SIEMENS

Heute ist alles miteinander vernetzt...

Frei verwendbar | © Siemens 2023

SIEMENS

…und daher Cyber-Risiken ausgesetzt

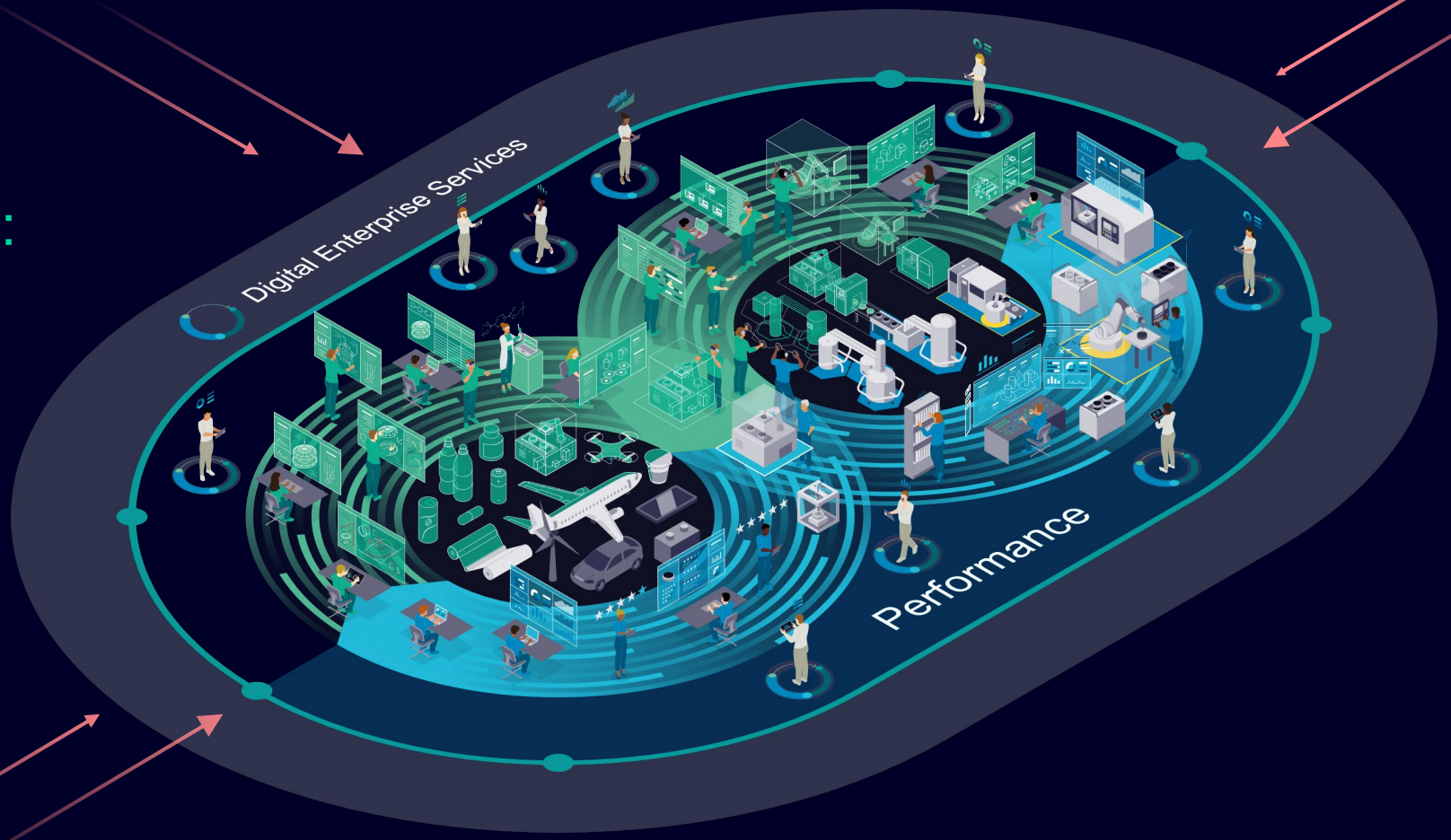
Frei verwendbar | © Siemens 2023

SIEMENS

Maschinen & Automatisierungssysteme sind Teil des IoT
Das bedeutet OT/IT-Integration in allen Ebenen

OT/IT-Konvergenz bedeutet:

- **Mehr Vernetzung**
- **Mehr Daten**
- **Neue Cyber-Risiken!**



Frei verwendbar | © Siemens 2023

SIEMENS

Die Bedrohung ist real und nimmt immer mehr zu

61%

der intelligenten Fabriken waren bereits von einen Cybersicherheits-vorfall betroffen

Quelle:
Fertigungsautomatisierung
Intelligente Fabriken sind zunehmend Cybersicherheitsrisiken ausgesetzt

33%

aller Cybersicherheits-vorfälle ereignen sich in der Fertigung

Quelle:
PMMI Whitepaper 2021 – Risikoeinschätzung
(PMMI 2021 Assess your risk white paper)

65%

aller Ransomware-Angriffe ereignen sich in der Fertigung

Quelle:
Dragos Jahresrückblick 2021 – Cybersecurity von ICS/OT-Systemen
(Dragos 2021 ICS/OT Cybersecurity year in review)

75%

der IT-Architekturen verfügten 2021 über externe Verbindungen zur Fertigungsebene

Quelle:
Dragos Jahresrückblick 2021 – Cybersecurity von ICS/OT-Systemen
(Dragos 2021 ICS/OT Cybersecurity year in review)

Frei verwendbar | © Siemens 2023

SIEMENS

Industrial Cybersecurity Konzept

Nur ein umfassendes Security-Konzept, das auf eine mehrschichtige Verteidigung basiert bietet effektiven Schutz gegen Cyber-Bedrohungen

Frei verwendbar | © Siemens 2023

SIEMENS

IT ≠ OT → Andere Anforderungen

Real-Time
Zykluszeiten < 1ms

Legacy
Alte Geräte in der Fertigung

Protokolle
Industrie Kommunikation
oft ohne Security

Lifecycle
Lebensdauer > 30 Jahre

Performance
weniger performante Geräte

Know-How
weniger Security Know-How
in der OT

Frei verwendbar | © Siemens 2023
SIEMENS

Industrial Security
Security-Konzepte für die Industrie

- Siemens hat ein **ganzheitliches Sicherheitskonzept** (HSC) für die Fertigung auf der Grundlage der Norm IEC 62443 definiert
- **Interne Sicherheitsmaßnahmen** bei Siemens basieren auf Anforderung der Norm **IEC 62443**
- Prozesse wie **PLM, SCM und CRM** werden bei Siemens den Anforderungen **nach IEC 62443** angepasst

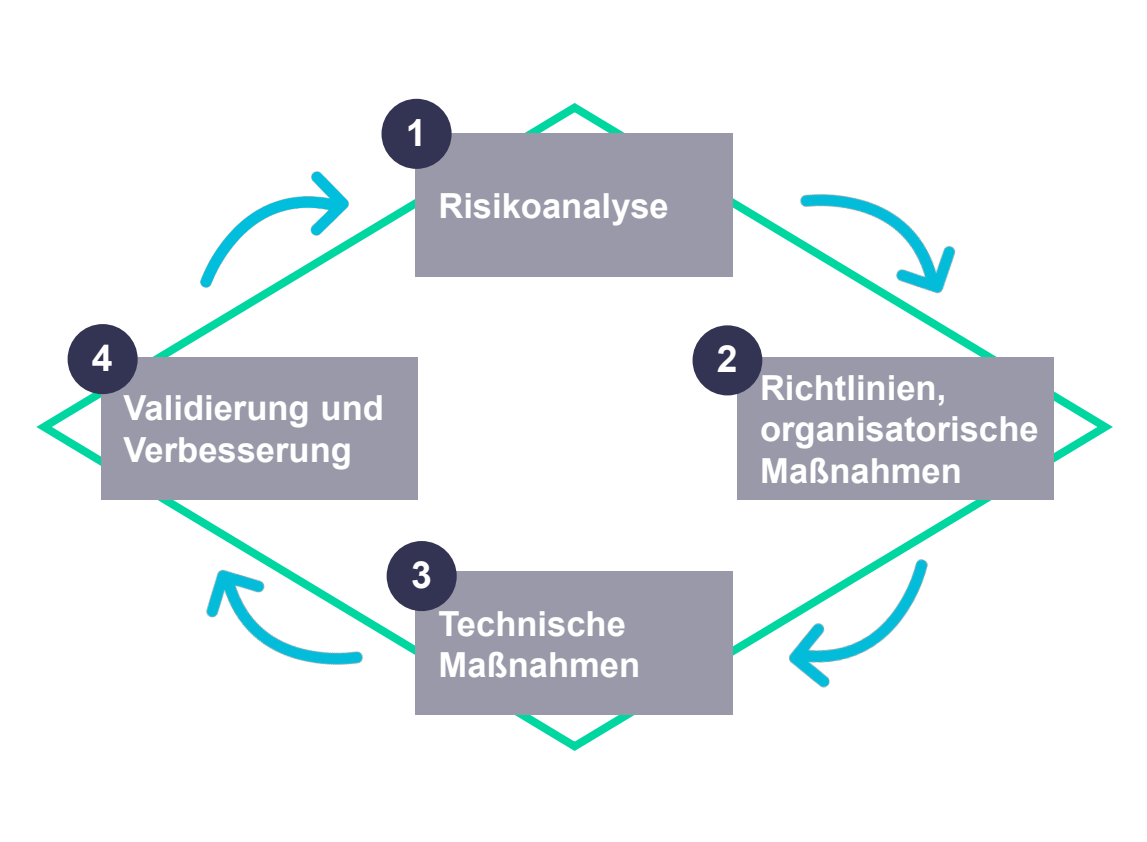
Frei verwendbar | © Siemens 2023

SIEMENS

Industrial Security
Security-Management

Security-Management-Prozess

- Risikoanalyse mit Definition von Risikominderungsmaßnahmen
- Festlegung von Richtlinien und Koordinierung organisatorischer Maßnahmen
- Koordination technischer Maßnahmen
- Regelmäßige/ereignisabhängige Wiederholung der Risikoanalyse

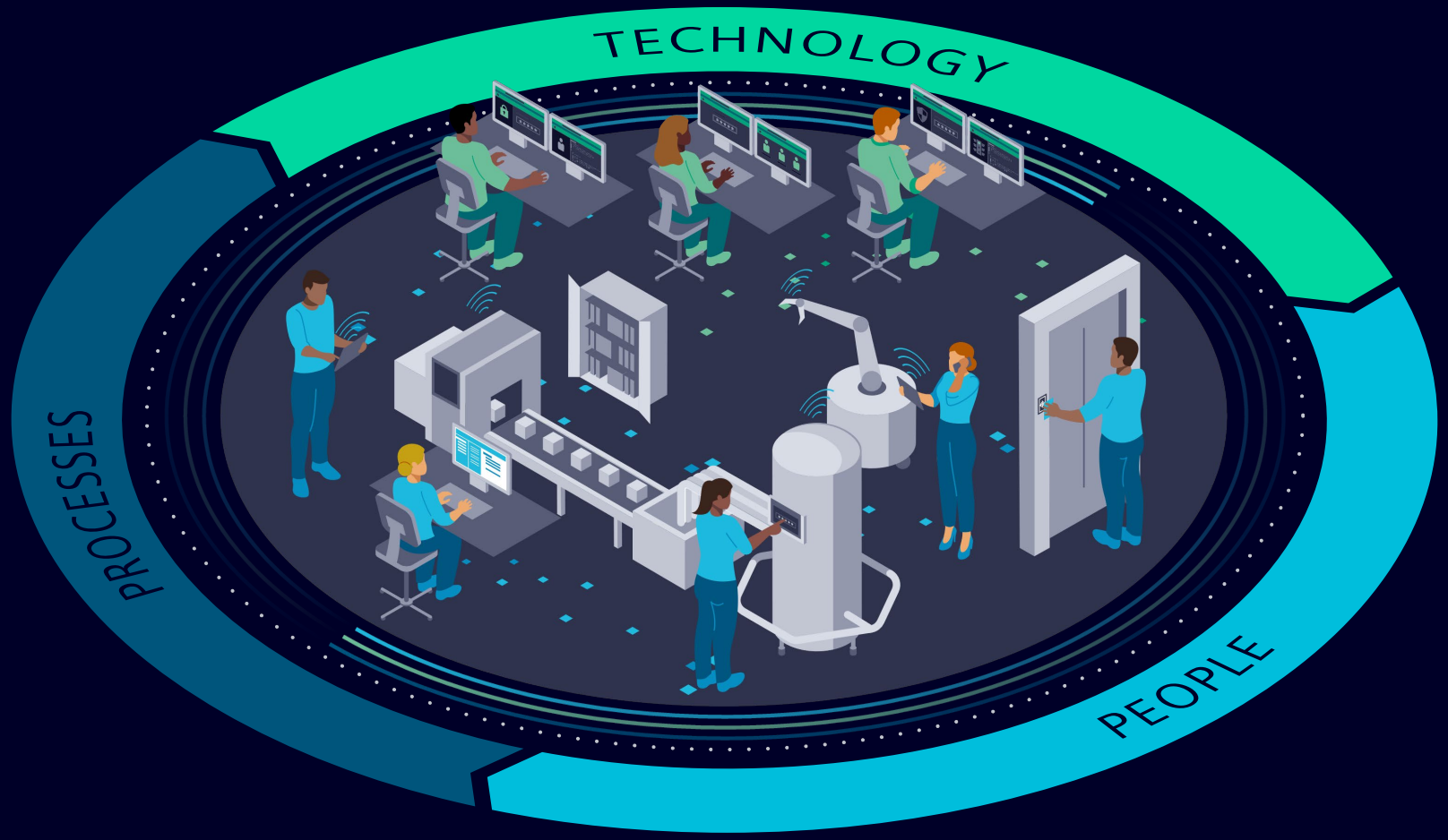


Security-Management ist unverzichtbar für ein durchdachtes Sicherheitskonzept

 Frei verwendbar | © Siemens 2023

SIEMENS

Ein ganzheitlicher Cybersecurity-Ansatz wird von drei Hauptsäulen geleitet: Menschen, Technologien und Prozesse



Richtlinien und Prozesse

Funktionale Cybersecurity-Maßnahmen

Kompetenz

 Frei verwendbar | © Siemens 2023

SIEMENS

Erfolgsfaktoren für ein Cybersecurity-System

Technische Umsetzung
Kompetenz
Vernetzung mit Experten

Management Kommittent
Prozesse
- Definieren
- Überprüfen
- Verbessern

Verantwortliche

Verantwortung
Kompetenz
Awareness

 Frei verwendbar | © Siemens 2023

SIEMENS

Danke!

 Unrestricted | © Siemens 2023 | Sandra Dominikus

SIEMENS

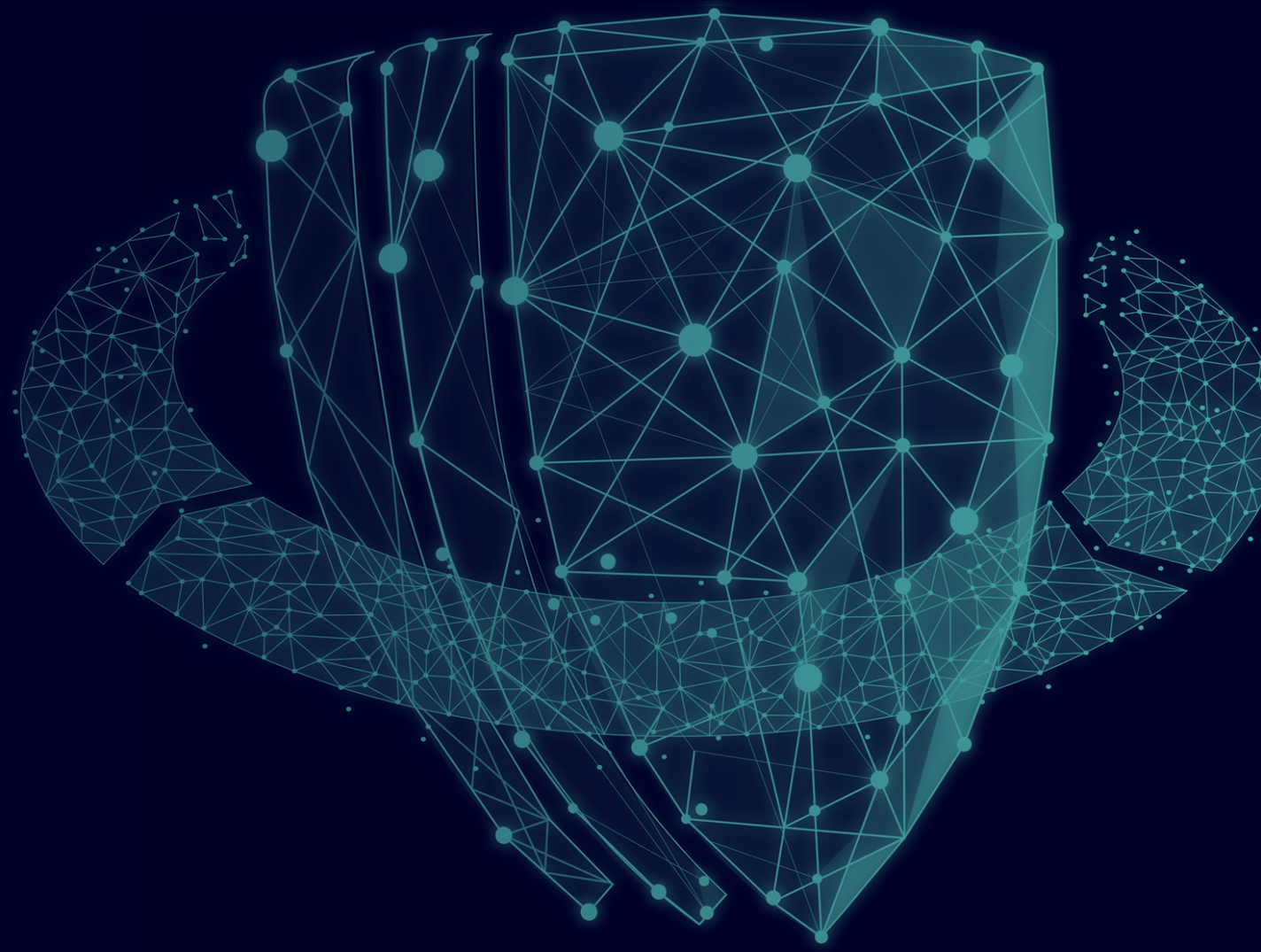
Contact

Published by Siemens 2023

Dr. Sandra Dominikus
Team Lead / Product Security Expert
DI FA SEA R&D-AT STI
Straßganger Straße 315
8054 Graz
Austria

Phone +43 80117-63844

E-mail sandra.dominikus@siemens.com



SIEMENS