Cybersecurity @ Siemens

Der Siemens 5-Phasen Plan zur sicheren NIS2-konformen OT

SIEMENS

Gefährdungen existieren,
Risiken kann man managen!

SIEMENS

Risikoanalyse (mit Illustrationen)

Extremes Risiko

Eine Person betritt den Käfig und füttert den Löwen

Wahrscheinlichkeit	5
Auswirkung	5
Wahrscheinlichkeit x Auswirkung	25

Moderates Risiko

Eine Person mit Schutzausrüstung betritt den Käfig und füttert den Löwen

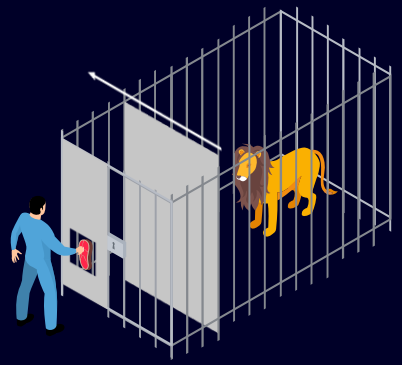
Wahrscheinlichkeit	5
Auswirkung	4
Wahrscheinlichkeit x Auswirkung	20

Tolerierbares Risiko

Eine Person füttert den Löwen durch eine speziell entwickelte Futteröffnung

Wahrscheinlichkeit	3
Auswirkung	3
Wahrscheinlichkeit x Auswirkung	9

Minimales Risiko



Eine Person füttert den Löwen in einem speziell konstruierten Futterkäfig

Wahrscheinlichkeit	1
Auswirkung	1
Wahrscheinlichkeit x Auswirkung	1

SIEMENS

Wie lange dauert es, ein Passwort zu ermitteln und was kostet das?

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Erforderliche Rechenleistung um

632.000.000.000

unterschiedliche Passwortkombinationen

pro Sekunde auszuprobieren kostet

EUR 25,-

SIEMENS

IT und OT - ähnliche Verantwortung andere Perspektive

IT (Informationstechnologie)

- Vertraulichkeit
- Integrität
- Verfügbarkeit

VS.

Priorisierung

OT (Operative Technologie)

- Verfügbarkeit
- Integrität
- Vertraulichkeit

SIEMENS

IT und OT - ähnliche Verantwortung andere Perspektive

IT (Informationstechnologie)

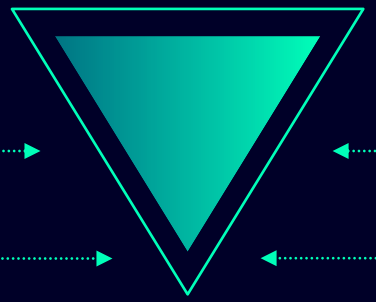
Vertraulichkeit

Integrität

Verfügbarkeit

- Starker Fokus auf Cybersecurity
- Gut bekannte und gelistete Assets
- Toleranz für Verzögerungen oder Ausfälle
- Erneuerung der Assets alle 3-5 Jahre
- Angreifer konzentrieren sich auf das Stehlen, Verschlüsseln oder Leaken von Daten

VS.



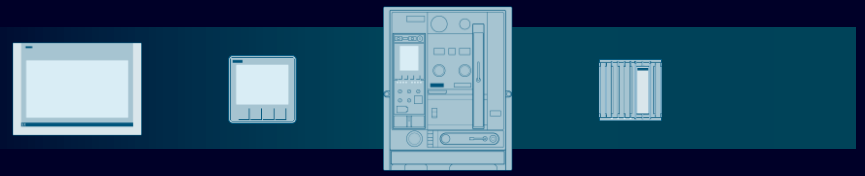
Priorisierung

OT (Operative Technologie)

Verfügbarkeit

Integrität

Vertraulichkeit



- (Noch) geringer Fokus auf Cybersecurity
- Viele Assets sind weder bekannt noch aufgeführt
- Keine Toleranz für Verzögerungen oder Ausfälle
- Erneuerung der Assets alle 15-20 Jahre
- Angreifer konzentrieren sich auf die Lahmlegung

SIEMENS

Gewohnheiten in der OT und ihre Auswirkungen auf den Schutz von Produktionssystemen

Gewohnheiten in der operativen Technologie

- **Systeme werden nur selten überprüft,** wenn kein konkreter Bedarf besteht
- **Fokus auf Komfort** und einfachen Zugang, um im Falle eines technischen Problems **schnell reagieren** zu können
- Betriebsfunktionen und Datenerfassung werden oft von **verschiedenen Personen** durchgeführt

"Solange es funktioniert - nicht anfassen!"

Schwächen vieler Produktionsanlagen

- **Kein Patch-Management**
- **Geringe Zugangsbarrieren**
- Verwendung von **Standardpasswörtern**
- Kein Logging
- Veraltete Hardware aufgrund langer Betriebsdauer

SIEMENS

Cybersecurity Services – Schritt für Schritt

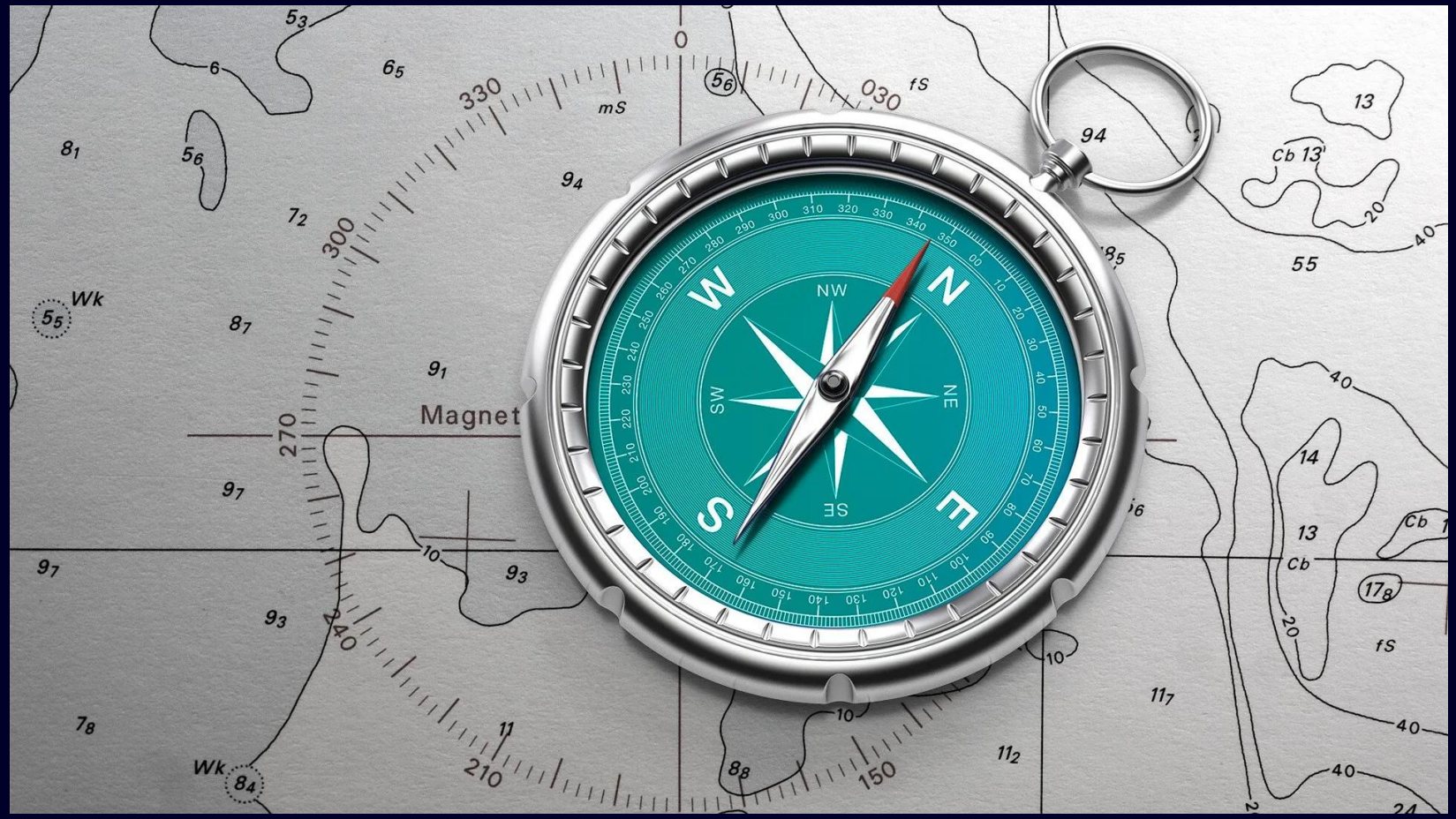
Phase 1
Wo stehe ich?
Wohin möchte ich?

Konzept
Strategie

Status Quo

Assessment
IEC 62443

Security Design
Workshop



Identifizieren Schützen

SIEMENS

Cybersecurity Services – Assessment

Phase 1
Wo stehe ich?
Wohin möchte ich?

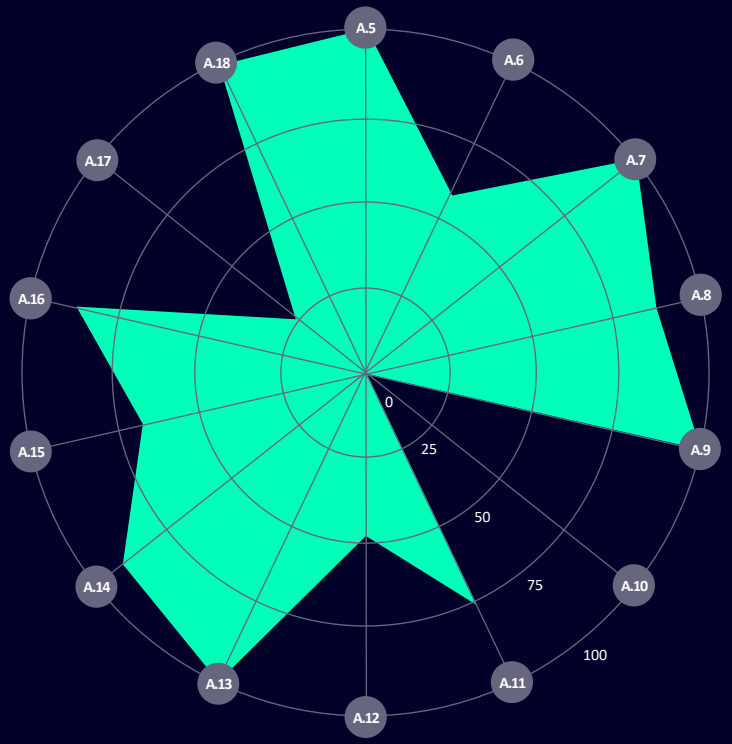
Konzept
Strategie

Status Quo

Assessment
IEC 62443

Security Design
Workshop

Report example



Radar Diagram
Compliance Coverage

Graphical Results IEC62443-2-2 (Establishing an industrial automation
and control security program)

Security Compliance Coverage Summary

Radar Chart showing in green the percent compliance to each category (A.5 – A.18) in the IEC62443-2-1 portion of the assessment.

The areas with the least compliance coverage represent the areas with least security policy coverage and should be prioritized in the implementation plan going forward.

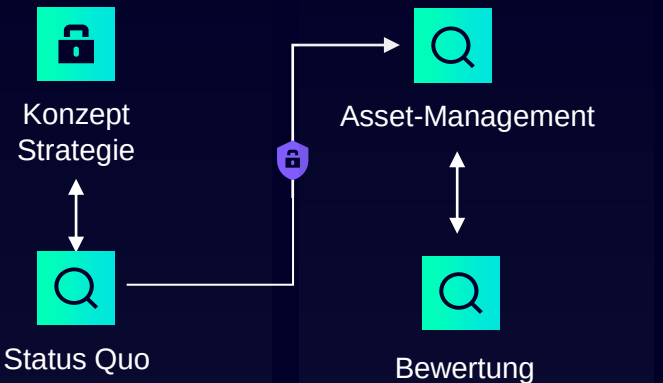
A.5 Information security policies
A.6 Organization of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 (text missing) acquisition, development and maintenenace
A.15 Supplier relationships
A.16 (text missing) security incident mgmt.
A.17 (text missing) aspects of business continuity mgmt.
A.18 Compliance

SIEMENS

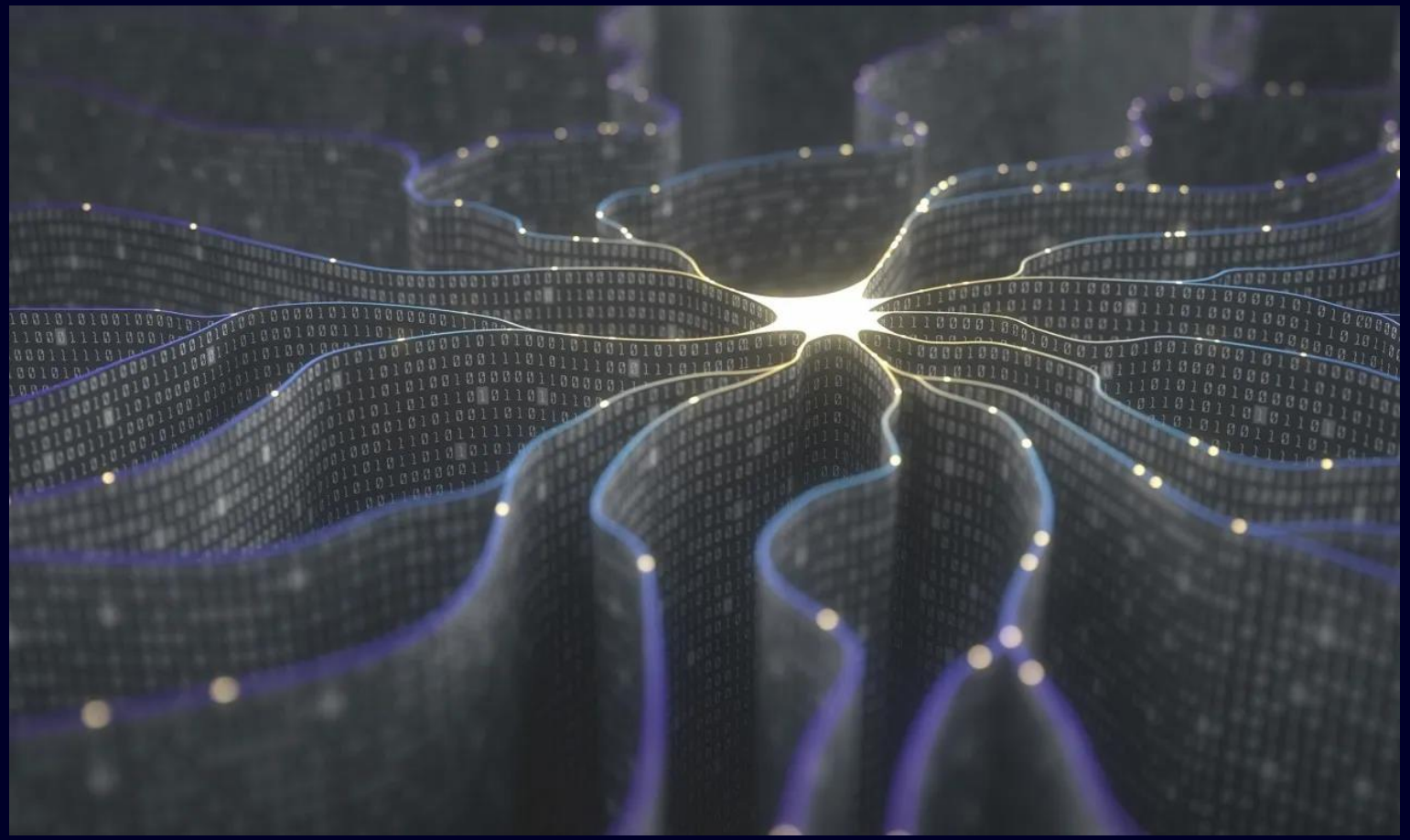
Cybersecurity Services – Schritt für Schritt

Phase 1
Wo stehe ich?
Wohin möchte ich?

Phase 2
Was sind meine
(kritischen) Assets?



- Assessment IEC 62443
- Security Design Workshop
- Asset Inventory Scan
- Vulnerability Analysis



Identifizieren | Schützen

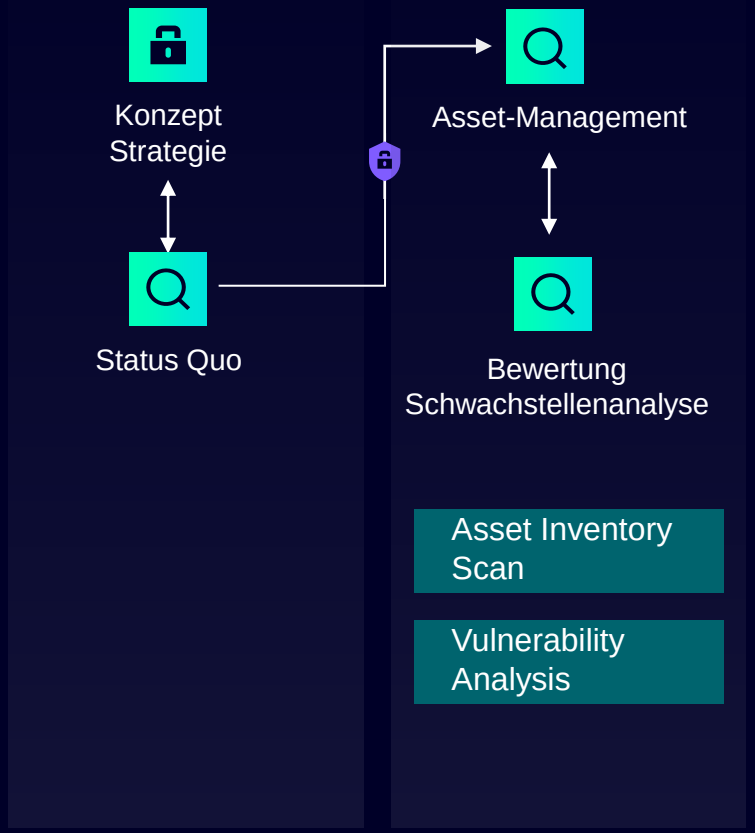
Training, Simulation und Schärfung des Bewusstseins für Bedrohungen

SIEMENS

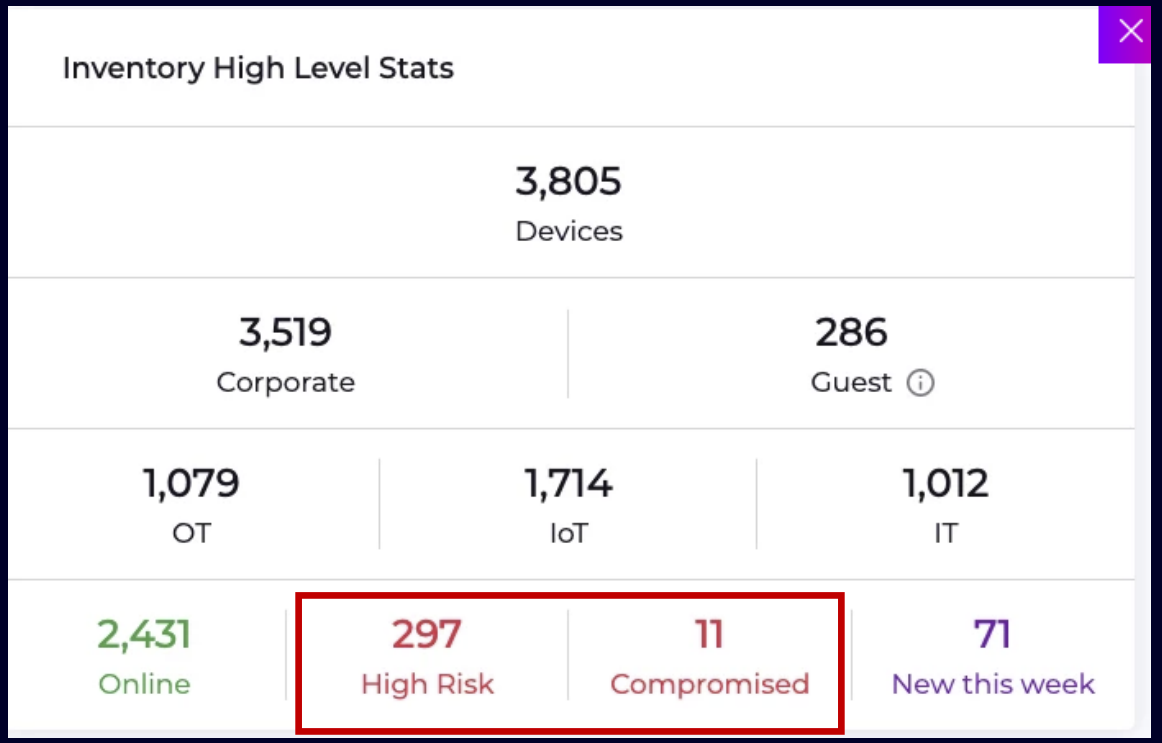
Cybersecurity Services – Asset und Vulnerability Scan

Phase 1
Wo stehe ich?
Wohin möchte ich?

Phase 2
Was sind meine (kritischen) Assets?



- Asset Inventory Scan
- Vulnerability Analysis



Identifizieren | Schützen

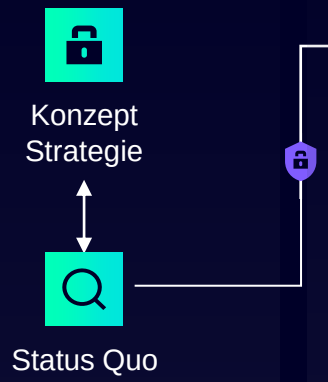
Training, Simulation und Schärfung des Bewusstseins für Bedrohungen

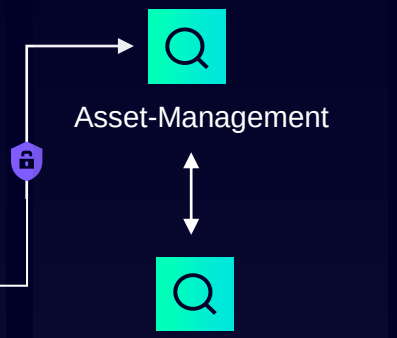
SIEMENS

Cybersecurity Services – Netzwerkübersicht

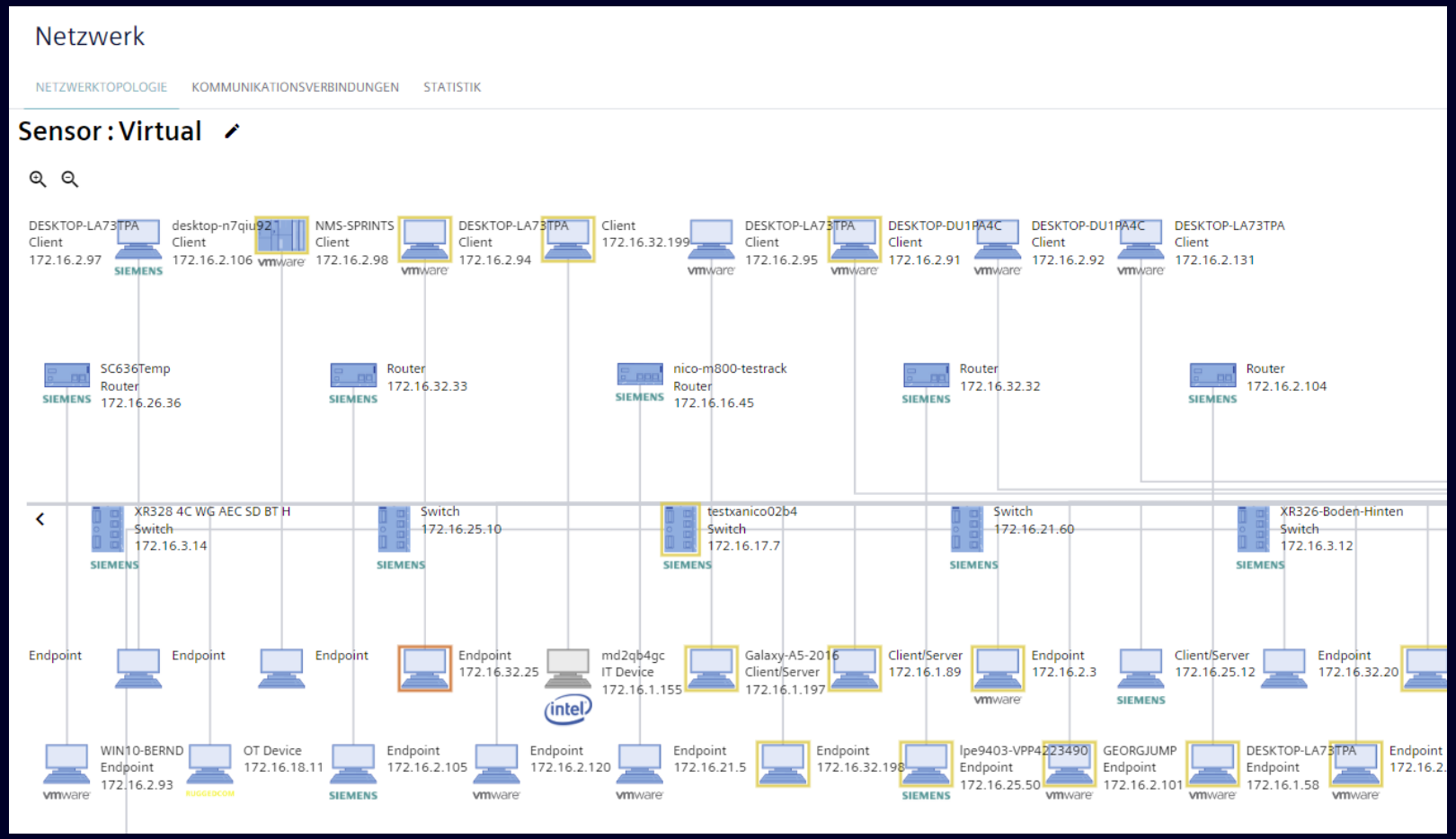
Phase 1
Wo stehe ich?
Wohin möchte ich?

Phase 2
Was sind meine (kritischen) Assets?





- Asset Inventory Scan
- Vulnerability Analysis

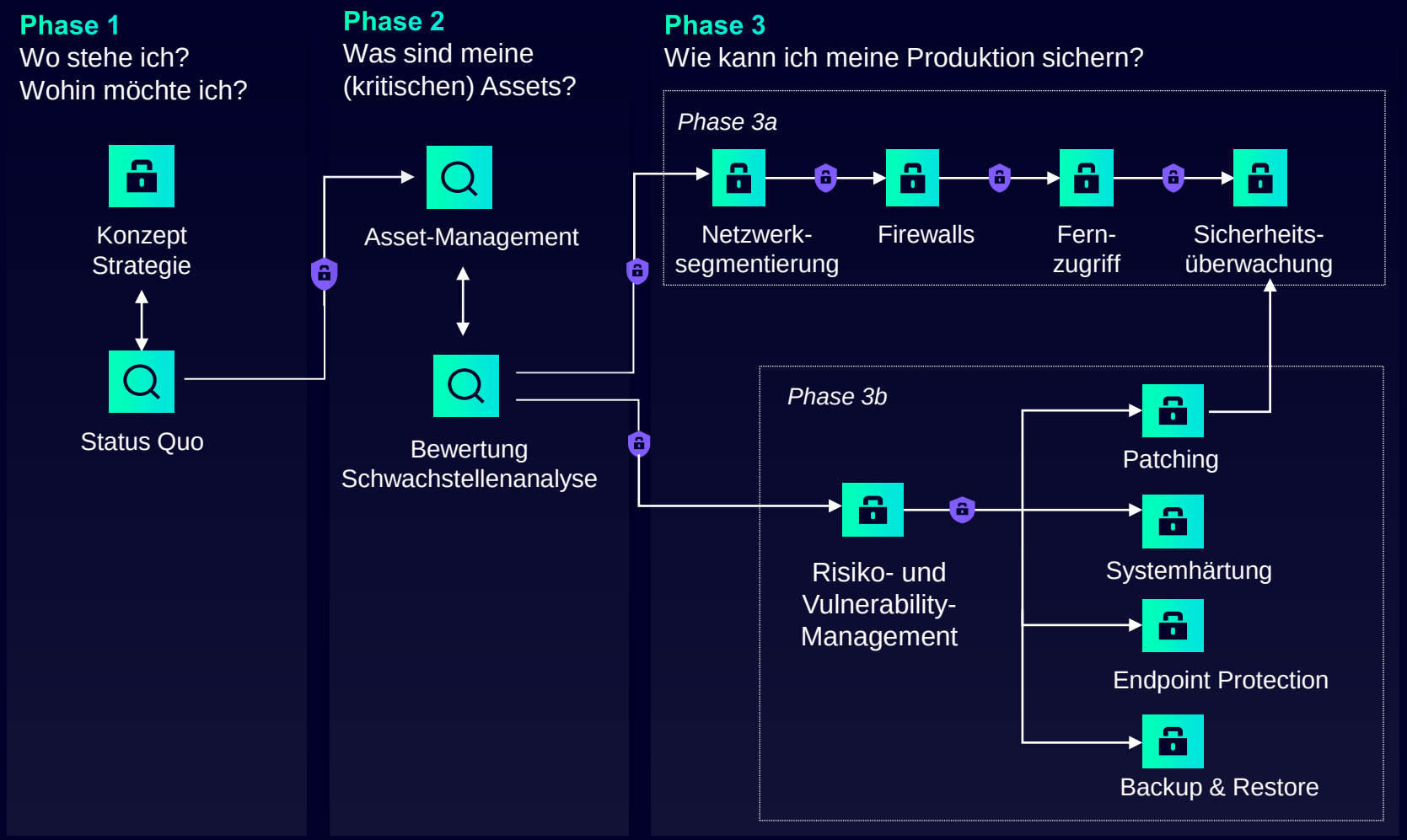


Identifizieren | Schützen

Training, Simulation und Schärfung des Bewusstseins für Bedrohungen

SIEMENS

Cybersecurity Services – Schritt für Schritt

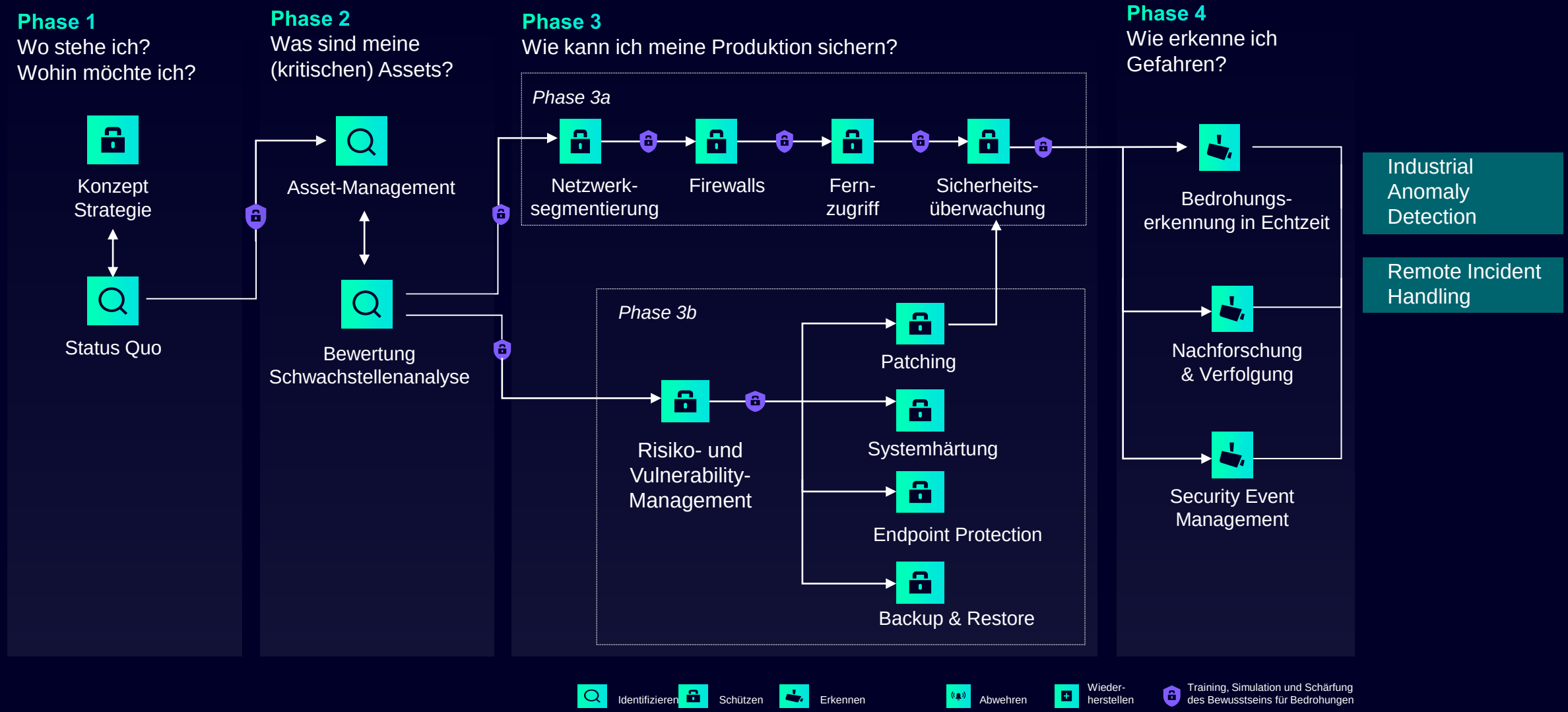


Netzwerk Design Workshop	Scalance Komponenten
Industrial Next Generation Firewall	Sinema RC
Industrial DMZ Infrastructure	Sinec NMS
Vulnerability Management Patch Management	User Management
Antvirus und Application Whitelisting	Simatic Hardening
Backup & Restore mit SIMATIC Infrastruktur	Automation Data Center

Identifizieren | Schützen | Erkennen | Abwehren | Wieder-herstellen | Training, Simulation und Schärfung des Bewusstseins für Bedrohungen

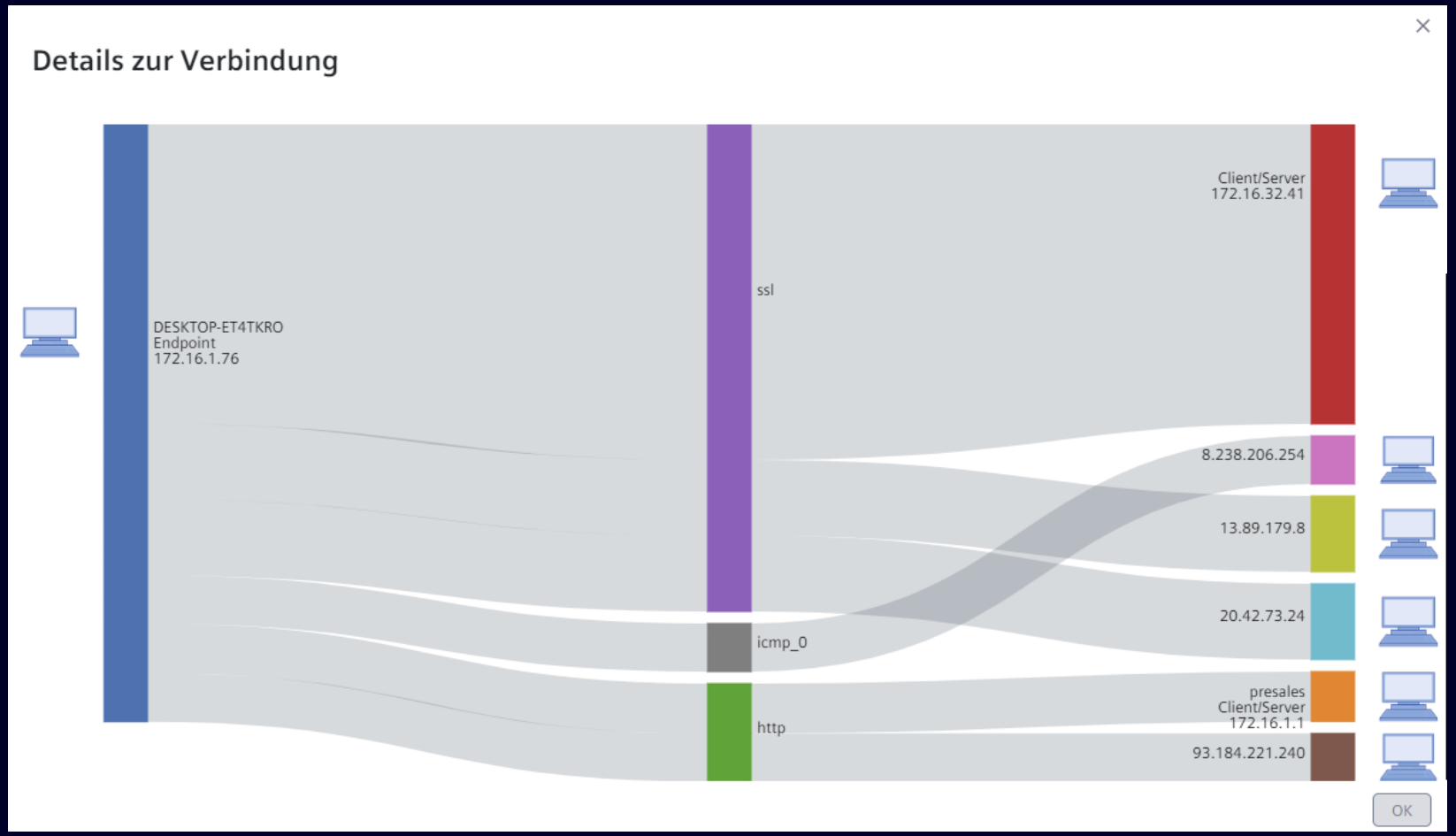
SIEMENS

Cybersecurity Services – Schritt für Schritt



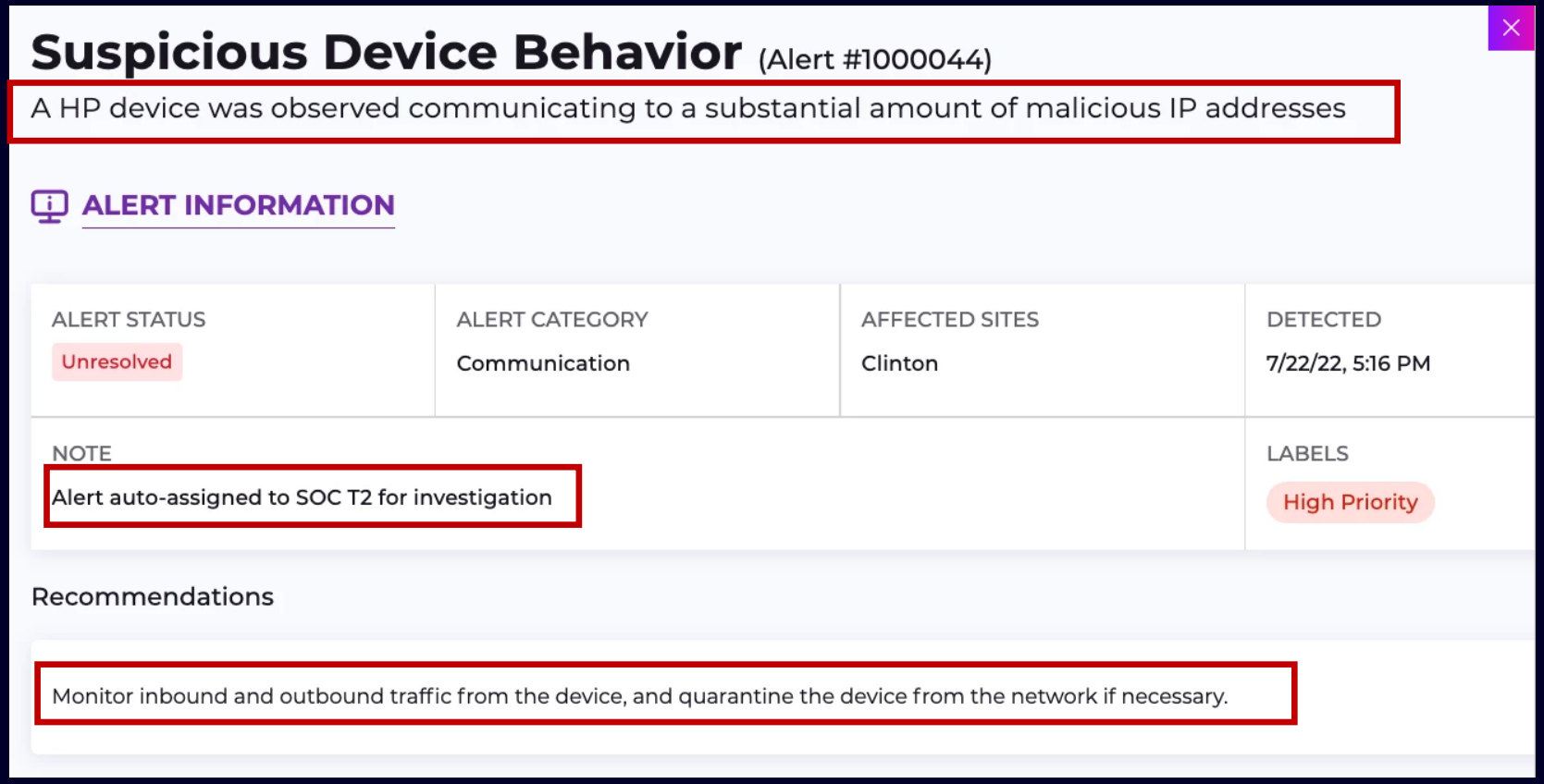
SIEMENS

IP Verkehr – Wer redet mit wem über welches Protokoll



SIEMENS

Bedrohungserkennung durch Anomalie – Erkennung

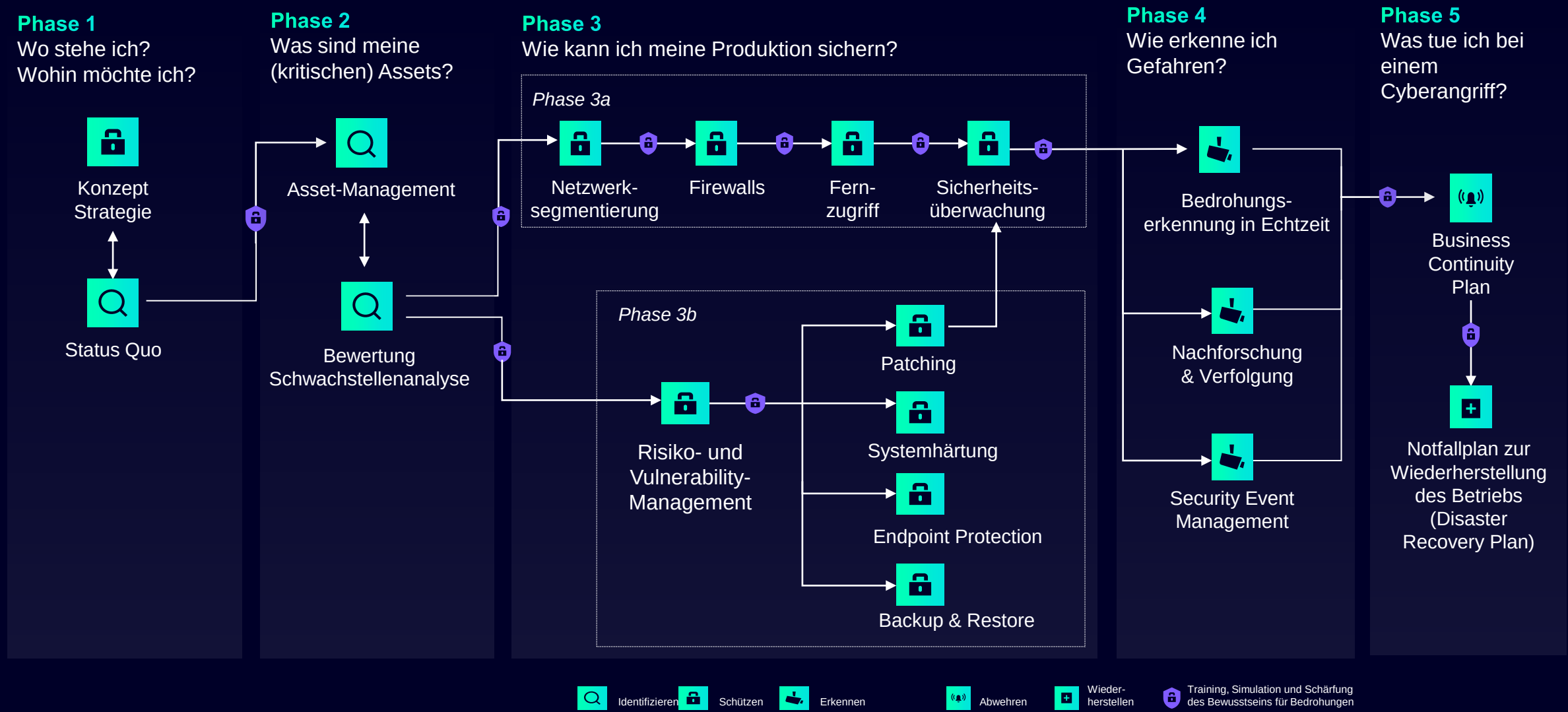


SIEMENS

Security Events - automatische Ereigniserstellung auf Basis von Regeln

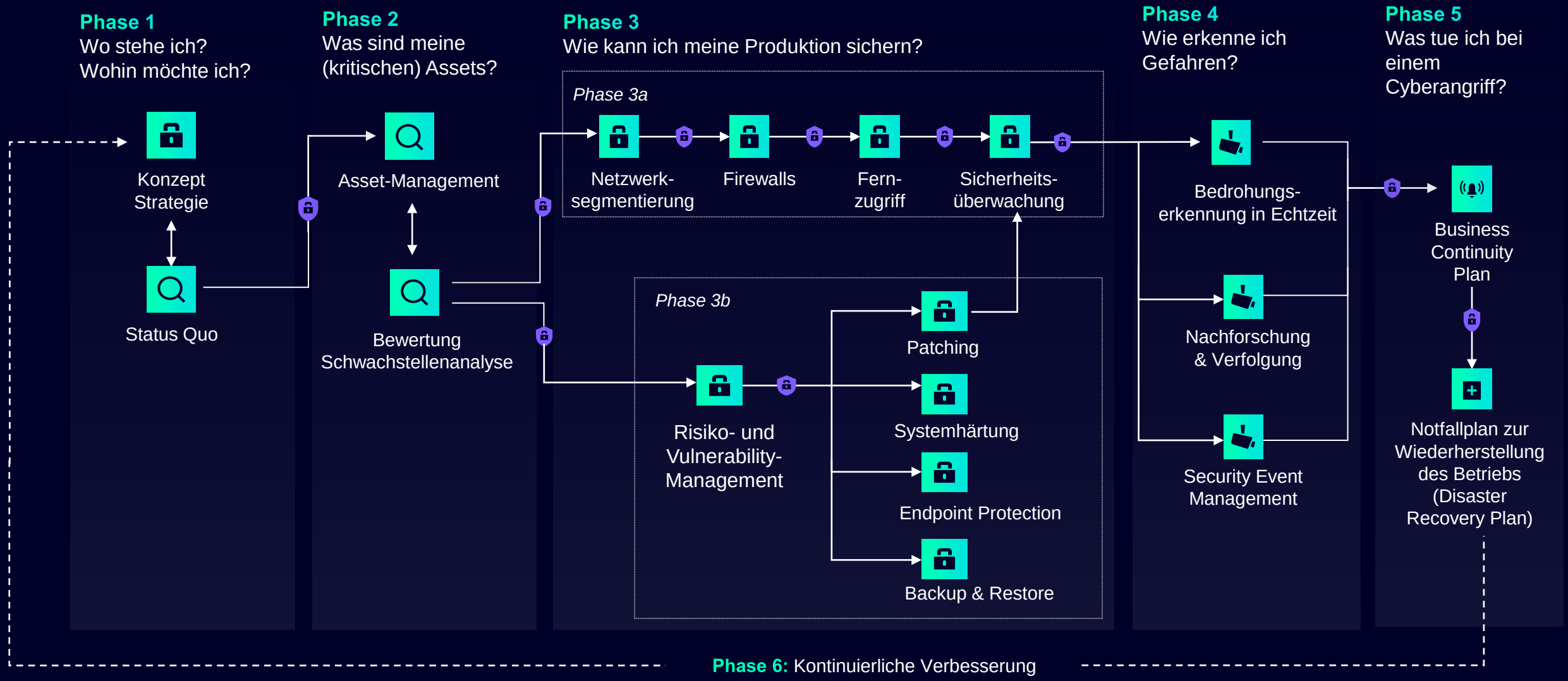
SIEMENS

Cybersecurity Services – Schritt für Schritt



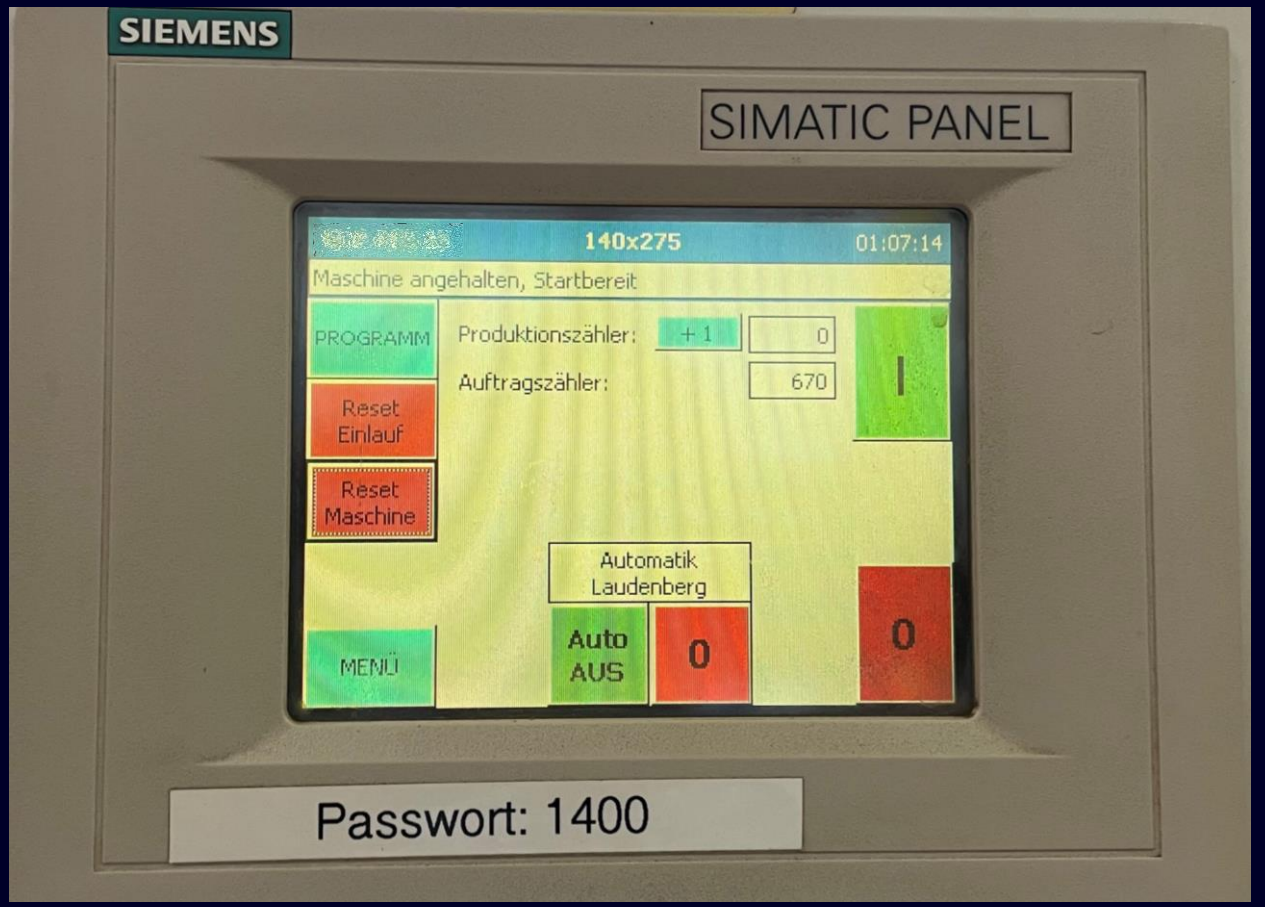
SIEMENS

Cybersecurity Services – Schritt für Schritt



SIEMENS

Fazit: „Ein bisschen“ Cybersecurity ist nutzlos



SIEMENS

Vielen Dank

SIEMENS

Kontakt

Dipl.-Ing. Adrian Pinter, COSM
Head of Horizontal Cyber Security AT + LCB
Cybersecurity for Industry

Siemens Aktiengesellschaft Österreich
Strassgangerstraße 315
8054 Graz
Österreich

Mobil +43 (664) 88552673
E-Mail adrian.pinter@siemens.com

SIEMENS