



Cybersecurity @ Siemens

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



Gefährdungen existieren,
Risiken kann man managen!

Risikoanalyse (mit Illustrationen)

<p>Extremes Risiko</p> 	<p>Moderates Risiko</p> 	<p>Tolerierbares Risiko</p> 	<p>Minimales Risiko</p> 
<p>Eine Person betritt den Käfig und füttert den Löwen</p> <p>Wahrscheinlichkeit 5</p> <p>Auswirkung 5</p> <p>Wahrscheinlichkeit x Auswirkung 25</p>	<p>Eine Person mit Schutzausrüstung betritt den Käfig und füttert den Löwen</p> <p>Wahrscheinlichkeit 5</p> <p>Auswirkung 4</p> <p>Wahrscheinlichkeit x Auswirkung 20</p>	<p>Eine Person füttert den Löwen durch eine speziell entwickelte Futteröffnung</p> <p>Wahrscheinlichkeit 3</p> <p>Auswirkung 3</p> <p>Wahrscheinlichkeit x Auswirkung 9</p>	<p>Eine Person füttert den Löwen in einem speziell konstruierten Futterkäfig</p> <p>Wahrscheinlichkeit 1</p> <p>Auswirkung 1</p> <p>Wahrscheinlichkeit x Auswirkung 1</p>

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,-

IT und OT - ähnliche Verantwortung andere Perspektive



IT und OT - ähnliche Verantwortung andere Perspektive



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



Schwächen vieler Produktionsanlagen

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

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

Cybersecurity Services – Assessment

Phase 1

Wo stehe ich?
Wohin möchte ich?



Konzept
Strategie

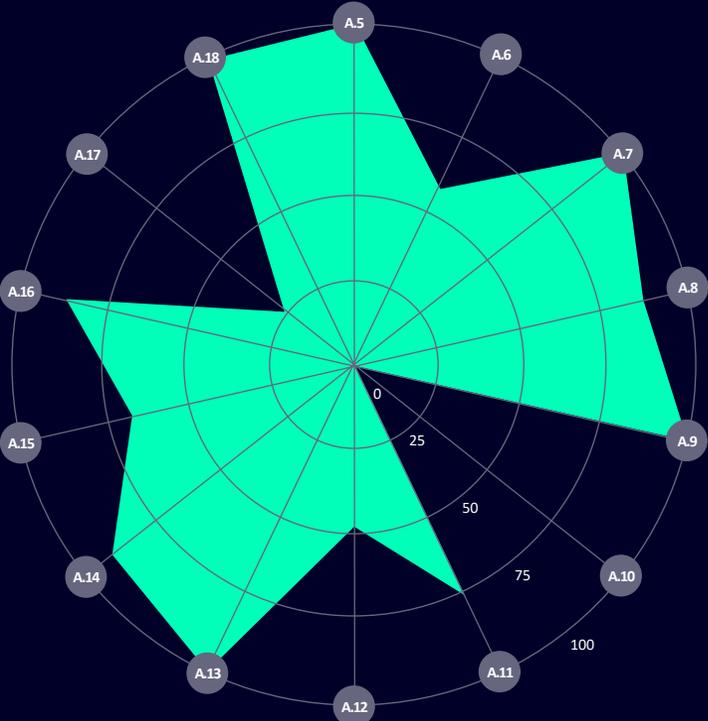


Status Quo

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 maintenance
- A.15 Supplier relationships
- A.16 (text missing) security incident mgmt.
- A.17 (text missing) aspects of business continuity mgmt.
- A.18 Compliance

Cybersecurity Services – Schritt für Schritt

Phase 1

Wo stehe ich?
Wohin möchte ich?



Konzept
Strategie



Status Quo

Phase 2

Was sind meine
(kritischen) Assets?



Asset-Management



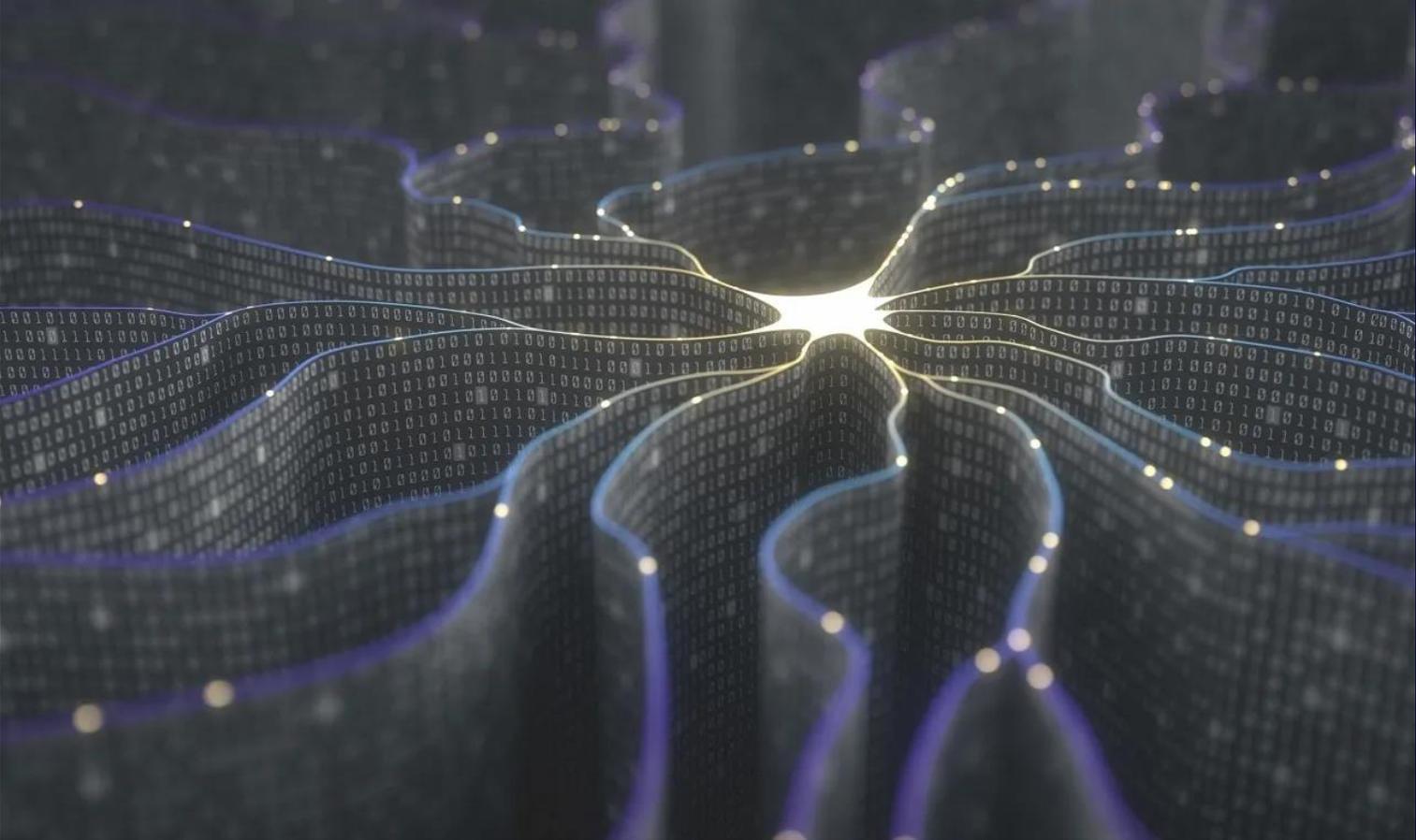
Bewertung
Schwachstellenanalyse

Assessment
IEC 62443

Security Design
Workshop

Asset Inventory
Scan

Vulnerability
Analysis



 Identifizieren  Schützen

 Training, Simulation und Schärfung
des Bewusstseins für Bedrohungen

Cybersecurity Services – Asset und Vulnerability Scan

Phase 1

Wo stehe ich?
Wohin möchte ich?



Konzept
Strategie



Status Quo

Phase 2

Was sind meine
(kritischen) Assets?



Asset-Management



Bewertung
Schwachstellenanalyse

Asset Inventory
Scan

Vulnerability
Analysis

Inventory High Level Stats			
		3,805 Devices	
3,519 Corporate		286 Guest ⓘ	
1,079 OT	1,714 IoT	1,012 IT	
2,431 Online	297 High Risk	11 Compromised	71 New this week

Identifizieren Schützen

Training, Simulation und Schärfung
des Bewusstseins für Bedrohungen

Cybersecurity Services – Netzwerkübersicht

Phase 1

Wo stehe ich?
Wohin möchte ich?



Konzept
Strategie



Status Quo

Phase 2

Was sind meine
(kritischen) Assets?



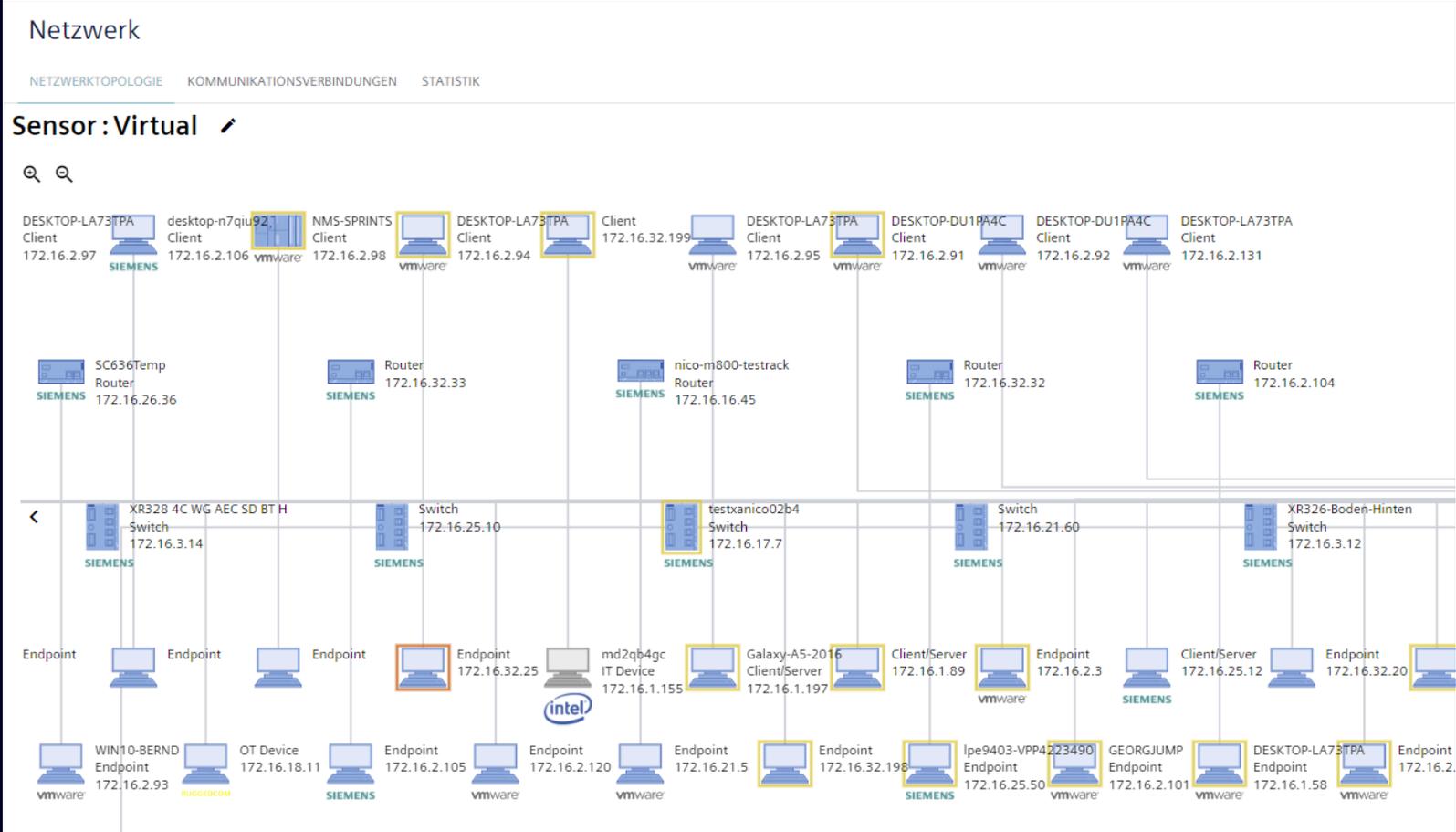
Asset-Management



Bewertung
Schwachstellenanalyse

Asset Inventory
Scan

Vulnerability
Analysis



Identifizieren Schützen

Training, Simulation und Schärfung
des Bewusstseins für Bedrohungen

Cybersecurity Services – Schritt für Schritt

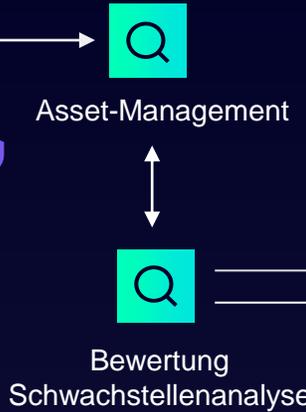
Phase 1

Wo stehe ich?
Wohin möchte ich?



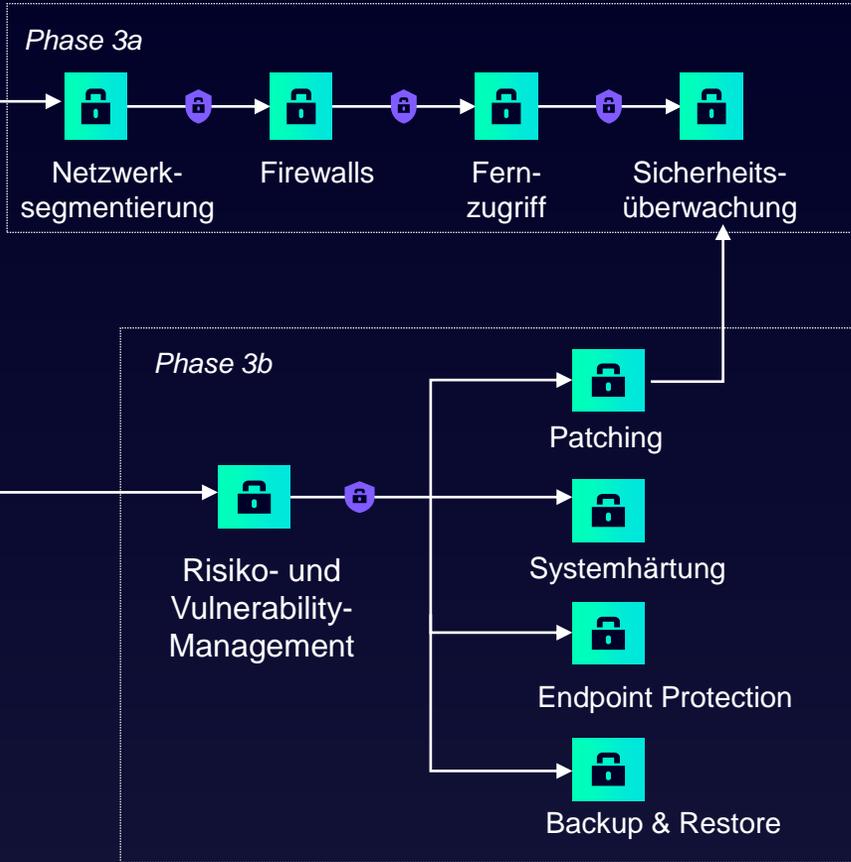
Phase 2

Was sind meine
(kritischen) Assets?



Phase 3

Wie kann ich meine Produktion sichern?



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

Identifizieren
 Schützen
 Erkennen
 Abwehren
 Wiederherstellen
 Training, Simulation und Schärfung des Bewusstseins für Bedrohungen

Cybersecurity Services – Schritt für Schritt

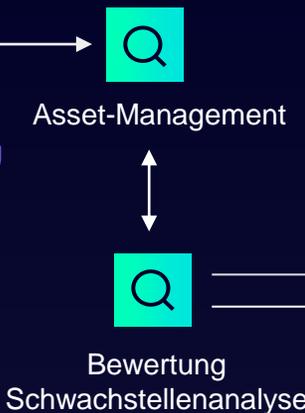
Phase 1

Wo stehe ich?
Wohin möchte ich?



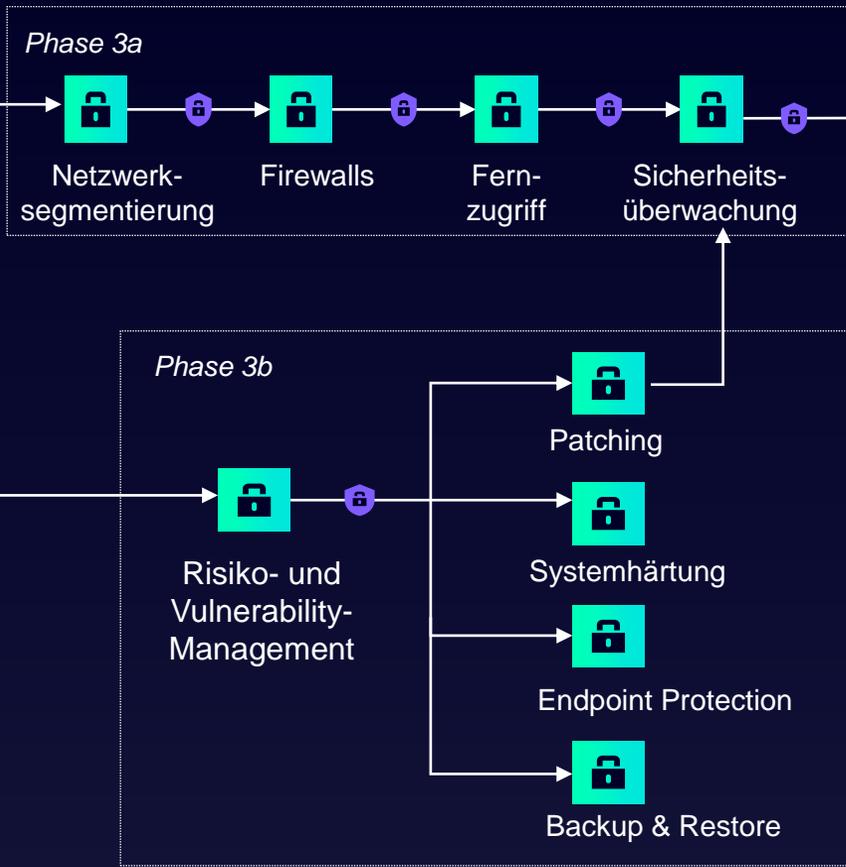
Phase 2

Was sind meine
(kritischen) Assets?



Phase 3

Wie kann ich meine Produktion sichern?



Phase 4

Wie erkenne ich
Gefahren?

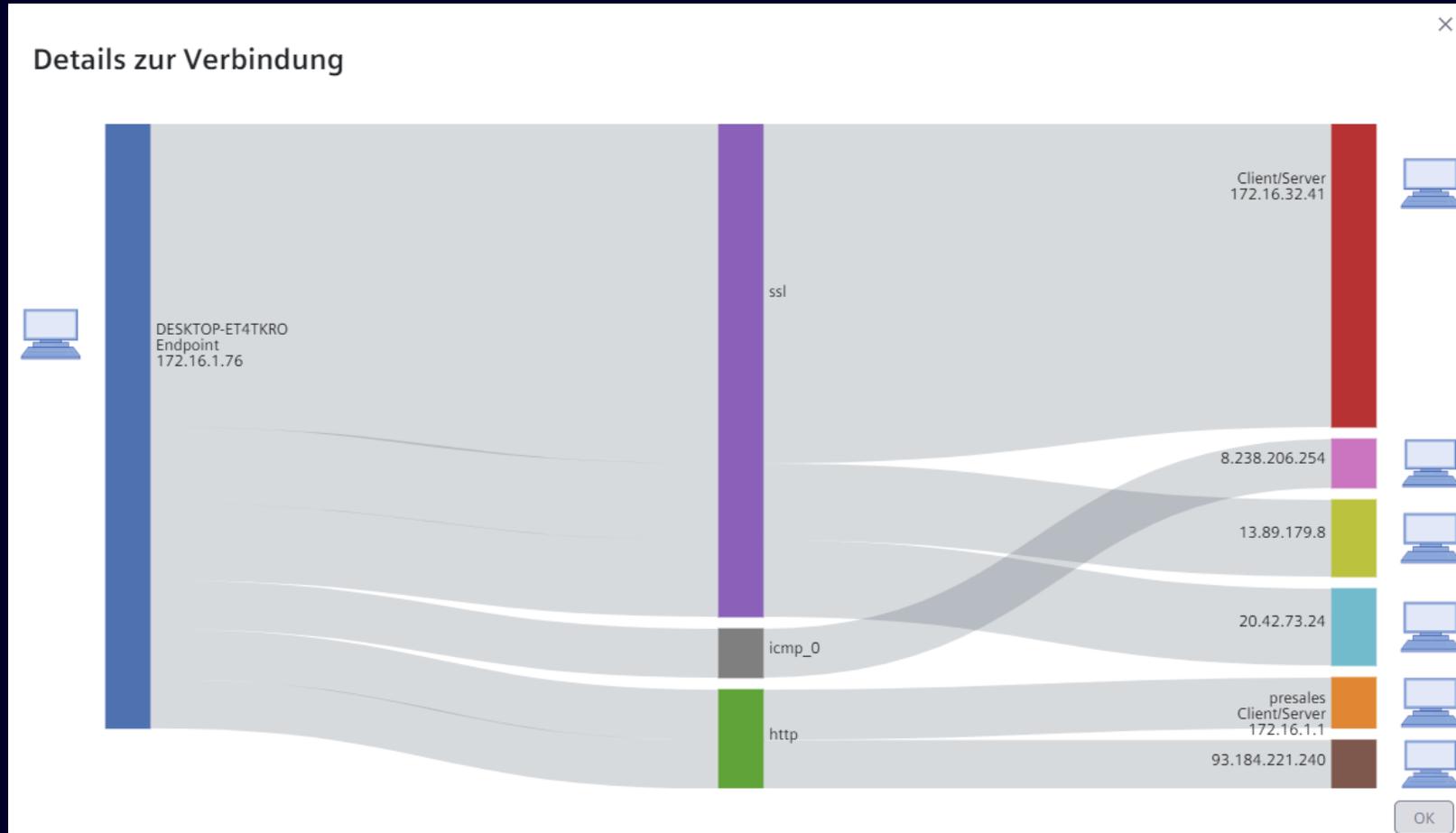


Industrial Anomaly Detection

Remote Incident Handling

Identifizieren
 Schützen
 Erkennen
 Abwehren
 Wiederherstellen
 Training, Simulation und Schärfung des Bewusstseins für Bedrohungen

IP Verkehr – Wer redet mit wem über welches Protokoll



Bedrohungserkennung durch Anomalie – Erkennung

Suspicious Device Behavior (Alert #1000044)

A HP device was observed communicating to a substantial amount of malicious IP addresses

ALERT INFORMATION

ALERT STATUS Unresolved	ALERT CATEGORY Communication	AFFECTED SITES Clinton	DETECTED 7/22/22, 5:16 PM
NOTE Alert auto-assigned to SOC T2 for investigation			LABELS High Priority

Recommendations

Monitor inbound and outbound traffic from the device, and quarantine the device from the network if necessary.

Security Events - automatische Ereigniserstellung auf Basis von Regeln

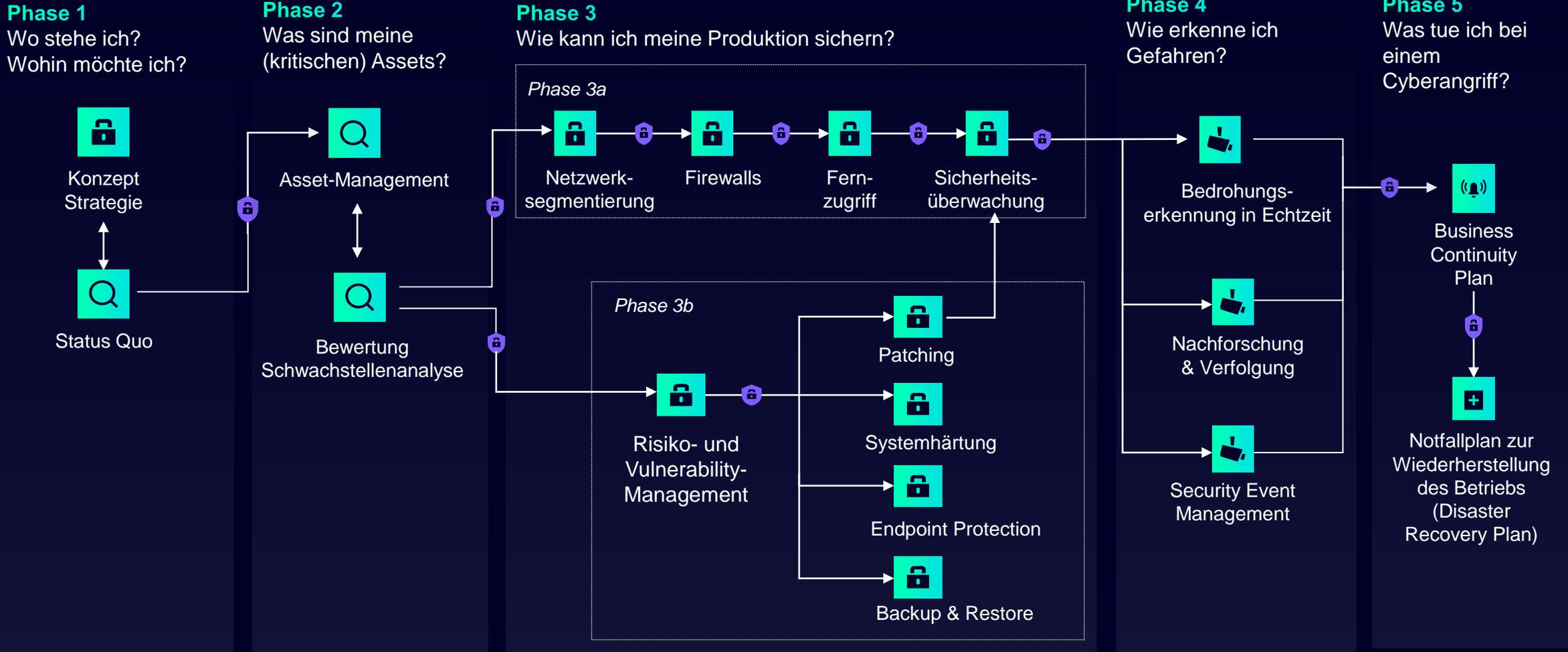
The screenshot shows the Siemens SINEC Security Monitor interface. On the left is a navigation sidebar with options: DASHBOARD, ASSETS, SECURITY-EREIGNISSE (highlighted), Risikolage, Security-Ereignisse, and Logs. The main area displays 'Security-Ereignisse' with a search bar and filters. A table lists three events, all with a 'Nicht bearbeitet' status and 'Warnung' level. The events are 'New APP Flow' detected on 2023-10-04 at 17:06:00 from a virtual source at 172.16.32.199. The first event is detected between src host 172.16.32.199 and dst host 172.16.21.2. The second is detected between src host 172.16.32.199 and dst host 20.54.24.69. The third is detected between src host 172.16.32.199 and dst host 172.16.2.101.

Status	Zeitstempel	Ereignis-ID	Ereignistyp	Ereignisname	Datenquelle	Hostname	Anmerkungen
Nicht bearbeitet	2023-10-04 17:06:00	204	Warnung	New APP Flow	Virtual	172.16.32.199	New application communication (APP Flow) tcp_7680 is detected between src host 172.16.32.199 and dst host 172.16.21.2.
Nicht bearbeitet	2023-10-04 17:06:00	204	Warnung	New APP Flow	Virtual	172.16.32.199	New application communication (APP Flow) tcp_443 is detected between src host 172.16.32.199 and dst host 20.54.24.69.
Nicht bearbeitet							New application communication (APP Flow) tcp_7680 is detected between src host 172.16.32.199 and dst host 172.16.2.101.

SINEC Security Monitor
CYBERSECURITY REPORT

Report Period: Aug 01, 2023 ~ Aug 31, 2023
Generated by: admin
Time: Sep 01, 2023
Classification: Confidential

Cybersecurity Services – Schritt für Schritt



🔍 Identifizieren
🔒 Schützen
🚒 Erkennen
🚒 Abwehren
🛠️ Wiederherstellen
🛡️ Training, Simulation und Schärfung des Bewusstseins für Bedrohungen

Cybersecurity Services – Schritt für Schritt

Phase 1

Wo stehe ich?
Wohin möchte ich?



Konzept Strategie



Status Quo

Phase 2

Was sind meine
(kritischen) Assets?



Asset-Management



Bewertung
Schwachstellenanalyse

Phase 3

Wie kann ich meine Produktion sichern?

Phase 3a



Netzwerk-
segmentierung



Firewalls



Fern-
zugriff



Sicherheits-
überwachung

Phase 3b



Risiko- und
Vulnerability-
Management



Patching



Systemhärtung



Endpoint Protection



Backup & Restore

Phase 4

Wie erkenne ich
Gefahren?



Bedrohungs-
erkennung in Echtzeit



Nachforschung
& Verfolgung



Security Event
Management

Phase 5

Was tue ich bei
einem
Cyberangriff?



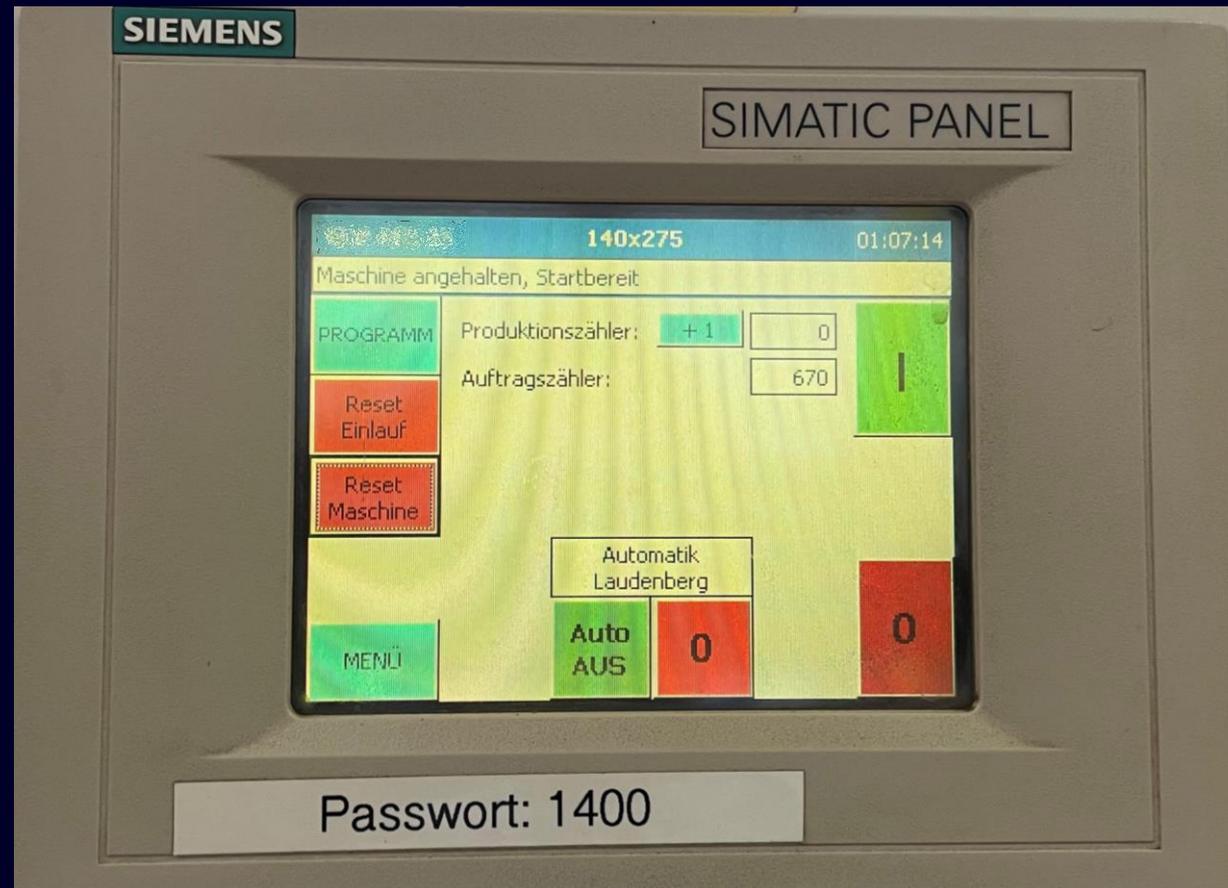
Business
Continuity
Plan



Notfallplan zur
Wiederherstellung
des Betriebs
(Disaster
Recovery Plan)

Phase 6: Kontinuierliche Verbesserung

Fazit: „Ein bisschen“ Cybersecurity ist nutzlos





Vielen Dank

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

