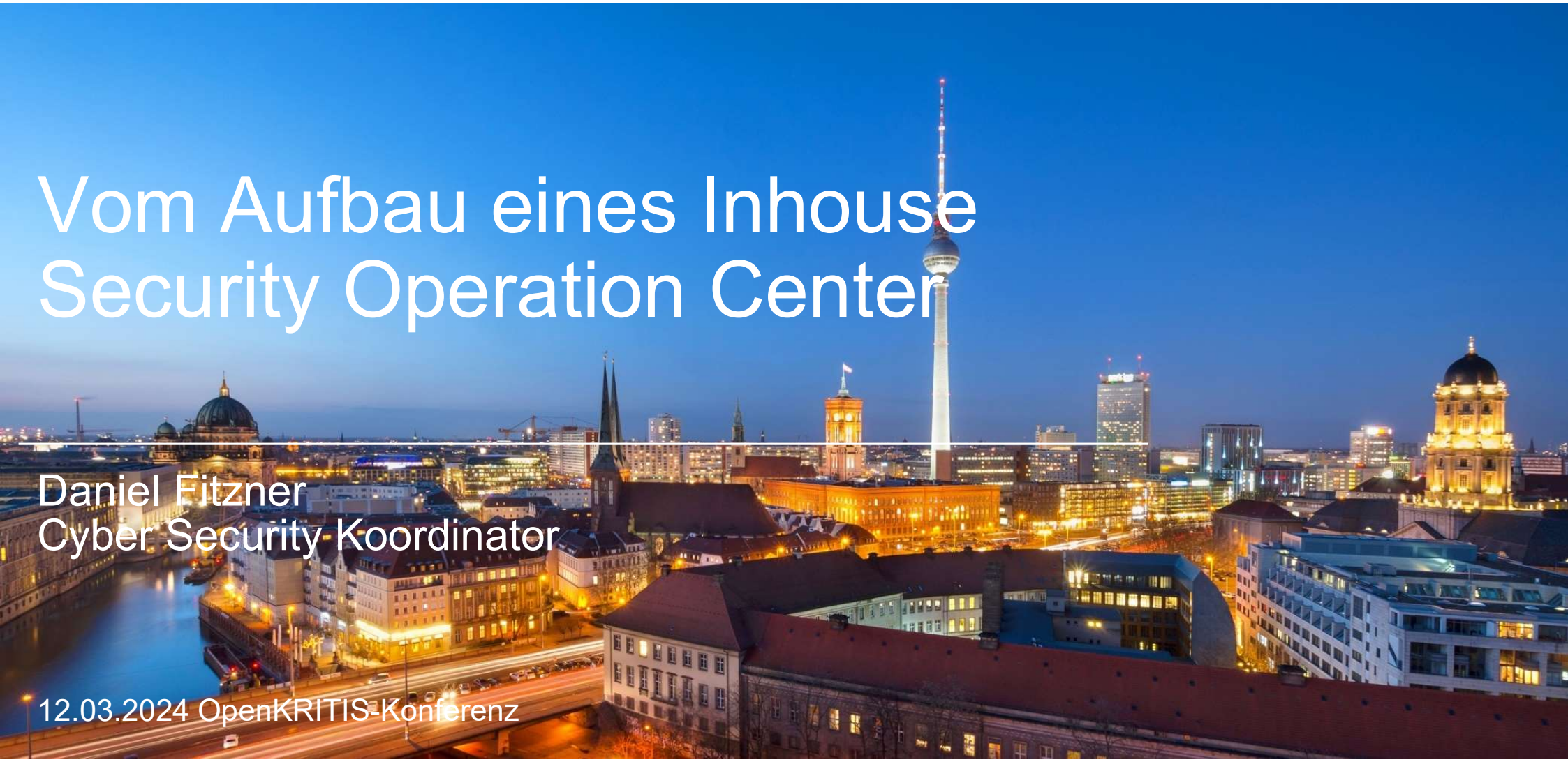
Vom Aufbau eines Inhouse Security Operation Center



Daniel Fitzner
Cyber Security Koordinator

12.03.2024 OpenKRITIS-Konferenz

Stromnetz Berlin

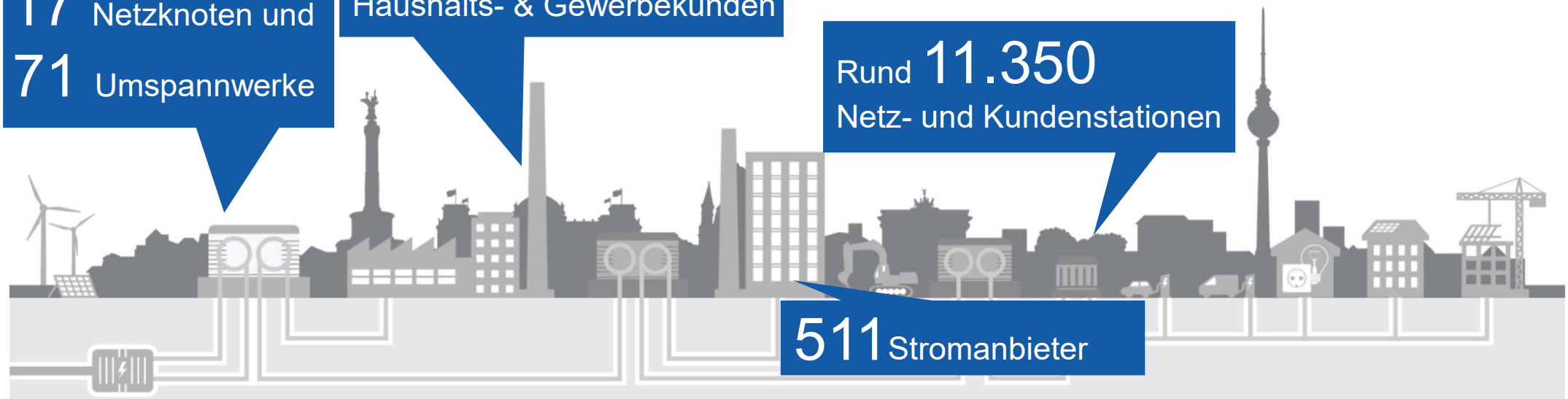
Das Berliner Netz in Zahlen*

Ca. 905.691 Wechselprozesse (Ein-/Auszug, Lieferantenanmeldung/-abmeldung)

Rund 2,41Mio. Haushalts- & Gewerbekunden

17 Netzknoten und
71 Umspannwerke

Rund 11.350 Netz- und Kundenstationen



511 Stromanbieter

Rund 99 % der insgesamt ca. 35.623 km Leitungen sind unterirdisch

*Stand 2022

Stromnetz Berlin

Der Auslöser

Diverse Herausforderungen…

1. Aufbau eines eigenständigen IT-Dienstleisters
2. Aufbau von Prozessen, Personal & Infrastruktur für den IT-Betrieb
3. Umzug von knapp 300 Business Anwendungen (konzernebene)
4. Parallel: Umsetzung Angriffserkennung ITSig2.0 (SzA)

…treffen auf einen ambitionierter Zeitstrahl.

ein … **der 1:1 Ansatz**

Stromnetz Berlin

SOC Aufbau
Handlungsfelder & Fragestellungen

Organisation & Governance

- Verortung: Nah am „Maschinenraum“ oder am CISO?
- integriertes oder eigenständiges Team?
- SLAs/KPI‘s vs. schaut der CISO in die Tools?

Service Portfolio

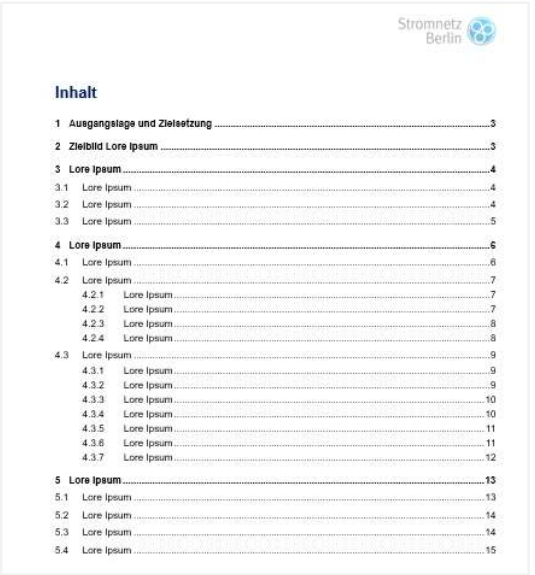
- Was sind die Kernservices?
- Partnering (Extern/Intern oder Hybrid)?
- Wieviel Support und Consulting?
- Rolle des IT SOC in der OT

Personal

- konkrete Erfahrung & Seniorität oder Ausbildung „on the job“?
- Wie halten wir die Mitarbeitenden langfristig?

Tools & Methoden

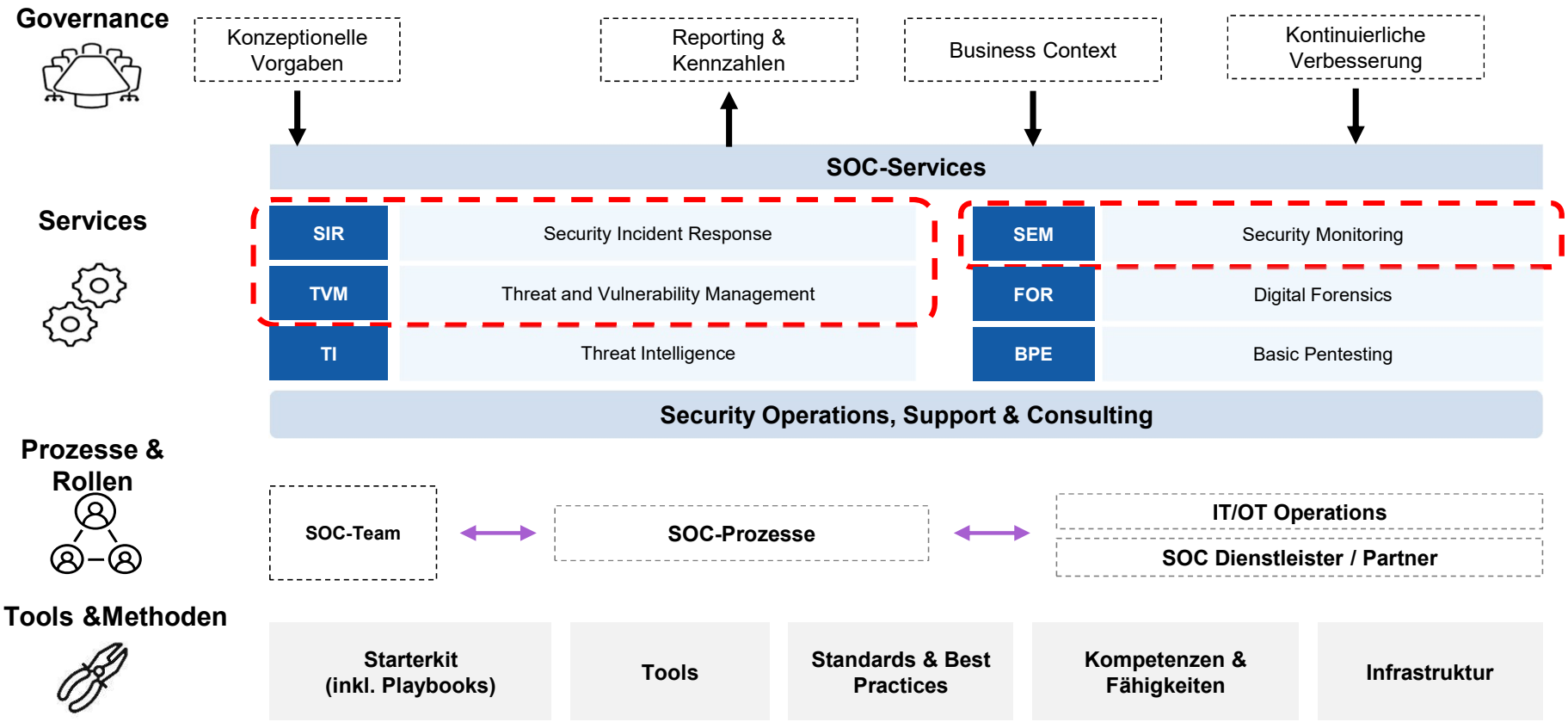
- Welche Tools und Anwendungen?
- Welche Standards existieren?
- OT: Monokultur & Synergien vs. Produktdiversifikation?


Stromnetz Berlin

Inhalt

Stromnetz Berlin

Leistungsportfolio SNB SOC



„Kernprozesse“ des SOC

Stromnetz Berlin

Wie war das mit dem Bau des ersten  ?

Organisation & Governance

- Nähe zum Betrieb war erfolgskritisch
- ein messbares Reifegradmodell fehlte
- Regulatorik frühzeitig berücksichtigen (Nachweise)
- Erfahrungsaustausch mit anderen Kritis Betreibern suchen
- Inhouse vs. Extern: Vorsicht vor Vergleich von Äpfeln mit Birnen

Service Portfolio

- Der operative Support ist der größte Mehrwert eines Inhouse SOC
- SOC „bezahlt“ die Qualitätsprobleme anderer Prozesse
- alles - was möglich ist - automatisiert Messen : Umsetzungsgrad, Aufwand pro Services, Qualität-KPIs
- regelmäßiger Blick von „außen“

Personal

- Cybersecurity ist attraktiv
- Karrierepfade vorhalten
- 24/7 ist ein Thema
- Ein eigenständiges Team ist von Vorteil
- frühzeitig (zunächst interne) RedTeamings, praktische Schulungen, Notfallübungen etc.

Tools & Methoden

- MITRE ATT&CK Framework hat für uns funktioniert
- konsequente(re) Automatisierung
- frühzeitig (interne) RedTeamings, Schulungen, Notfallübungen planen

Stromnetz Berlin

Ausblick und Hausaufgaben

- Strategie und Zielbild weiterentwickeln (inkl. Roadmap)
- Scoping, Ziele und SLAs der Services überprüfen
- Ressourcen anpassen
- Automatisierung weiter ausbauen
- Übungen & Tests fest verankern
- Vernetzung vorantreiben

Stromnetz Berlin

Vielen Dank für Ihre Aufmerksamkeit

...

Zeit für **Fragen**

Vielfalt leben – weil wir unterschiedlich sind.

Stromnetz Berlin