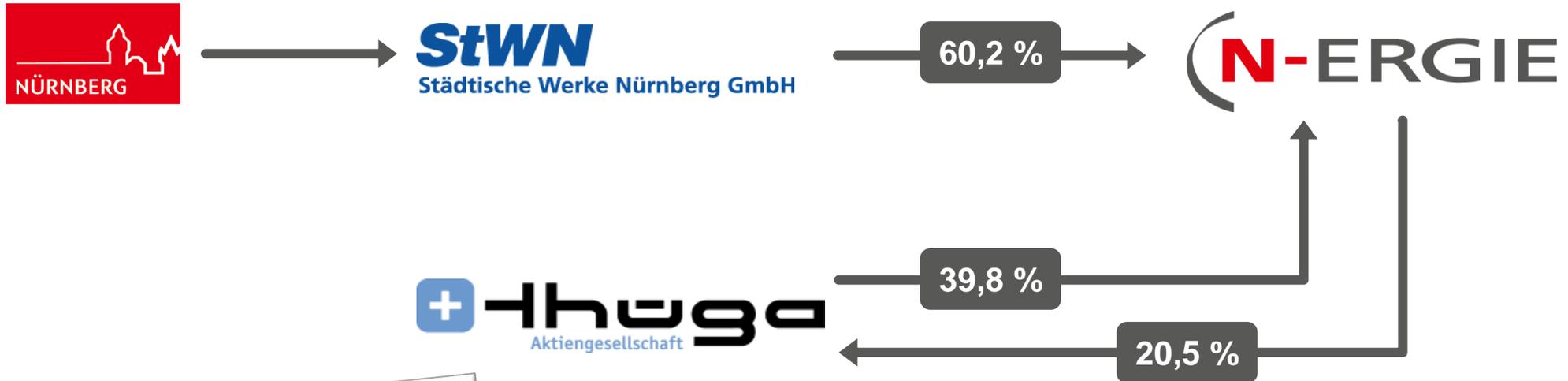


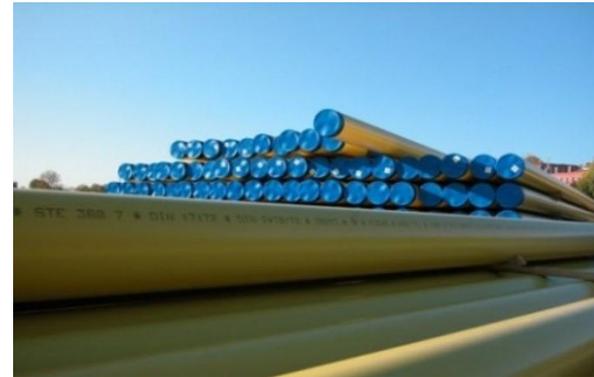
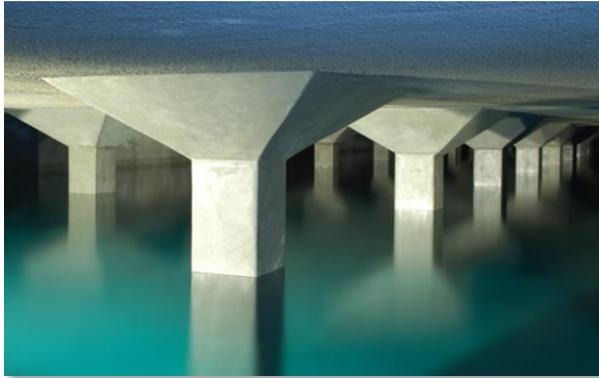
# **N-ERGIE's** Zukunftsstrategie für eine resilientere Cybersicherheit



## N-ERGIE: 100 Prozent kommunal



## Die N-ERGIE auf einen Blick



## Das Netzgebiet der N-ERGIE

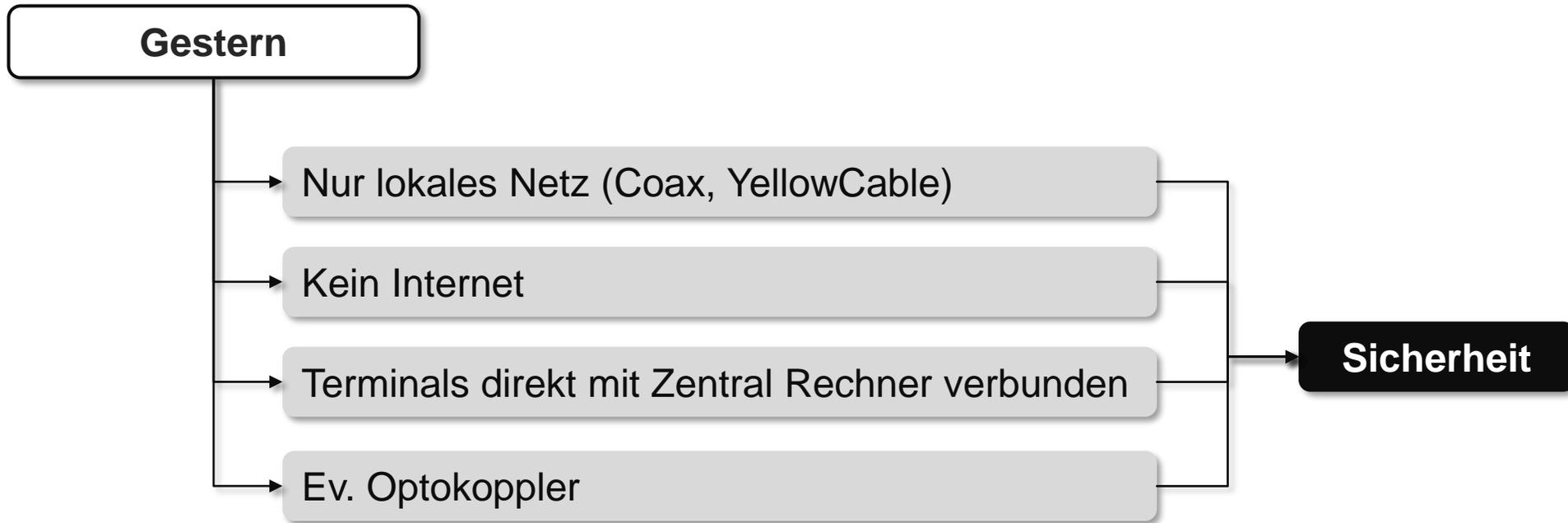


Das Netzgebiet der N-ERGIE hat eine Größe von rund 8.000 km<sup>2</sup>.

# Chronologie

Um zu wissen, wo ich hin will,  
muss ich wissen, wo ich herkomme.





Heute

### Unsere IT ist aufgebaut wie eine Burg

Alles zentral in der Mitte (Rechenzentren)

Rein und raus nur über eine Zugbrücke  
(Mail, Internet)

Alles, was rein kommt, wird gescannt  
und geschützt

Rechtevergabe macht die zentrale IT

### Werkzeuge

Virens Scanner

Firewalls

Gateways, Proxies

IDS (Intrusion Detektion System)

...

Morgen

**Alles ist homogen vernetzt, durchmengt**

O365 (Identitäten, Authentifizierung, Daten, Kommunikation...)

Dienste in der Cloud (Server, Services, Anwendungen...)

Rechtevergabe macht jeder User selber

ChatGPT

...

**Werkzeuge**

Datenklassifizierung, Labeling

Satayo, XM Cyber, Varonis, ...

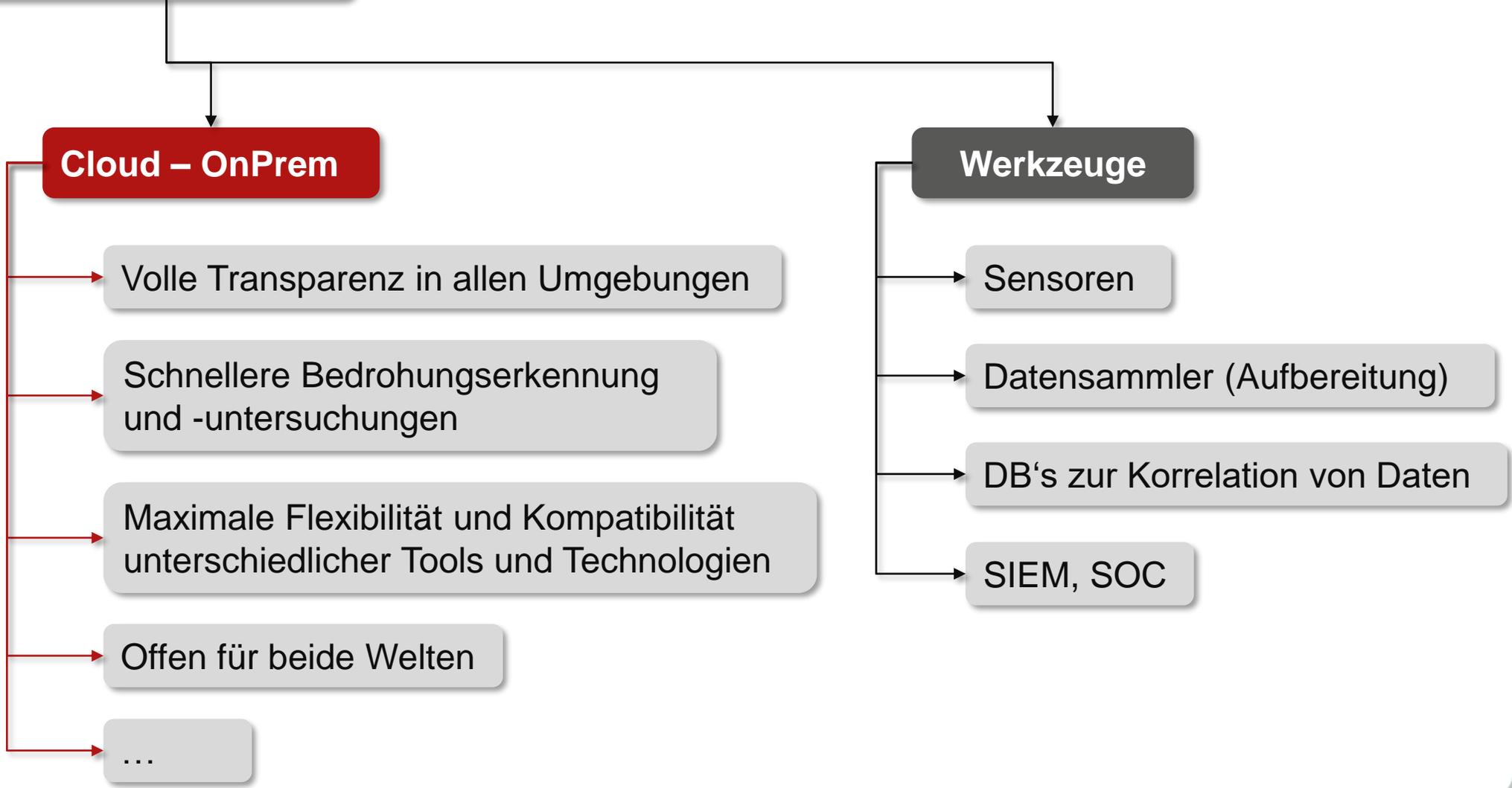
Neteye, NTOP, ...

MITRE ATTACK (Klassifizierungen)

Analysesysteme

DER, XDR

Was brauchen wir



Zauberwort

**Sichtbarkeit**



Wie gehen wir vor

Da sehr viele Systeme sowohl OnPrem als auch in der Cloud sind

→ Usecase definieren

→ Informationen, die benötigt werden separieren

→ Zusammenhänge aller Systeme aufzeigen

→ Dashboard definieren

→ Aktionen beschreiben

→ Meldewege definieren

→ SOC

## Zum Schluss

Wir benötigen ein offenes flexibles System, welches schnell an neue Technologien und Herausforderungen angepasst werden kann

Das Ganze ist ein Zusammenspiel von verschiedenen Produkten und Strategien, welche in ein "BigPicture" münden, ...

...um die SICHTBARKEIT aller Aktivitäten aufzuzeigen, ...

...diese zu bewerten und...

...daraus Aktionen abzuleiten.

**Vielen Dank!**

**Diskussion**

**Fragen**

