DFN CERT

deutsches forschungsnetz

SOC-Connector

78. Betriebstagung | 28.03.2023

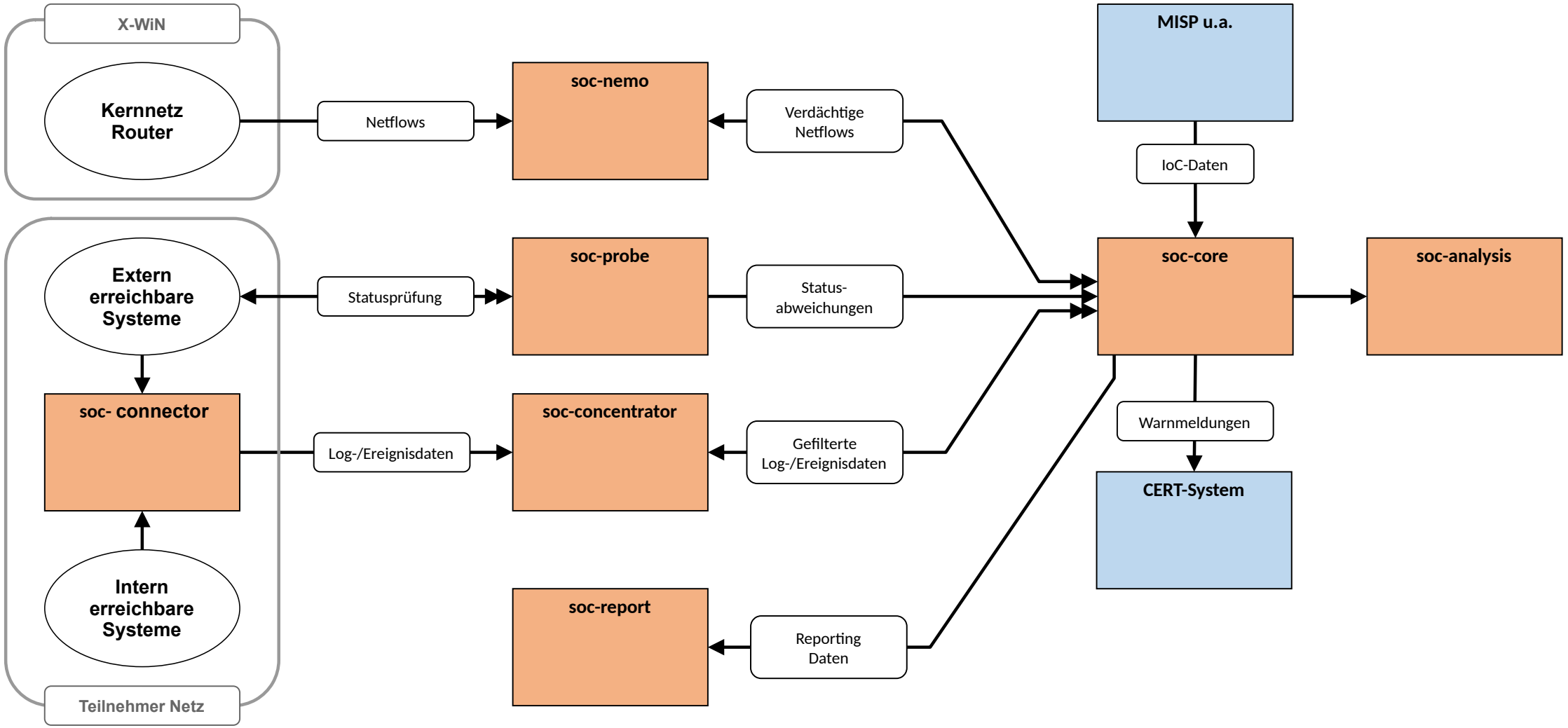
Reinhard Sell

Agenda

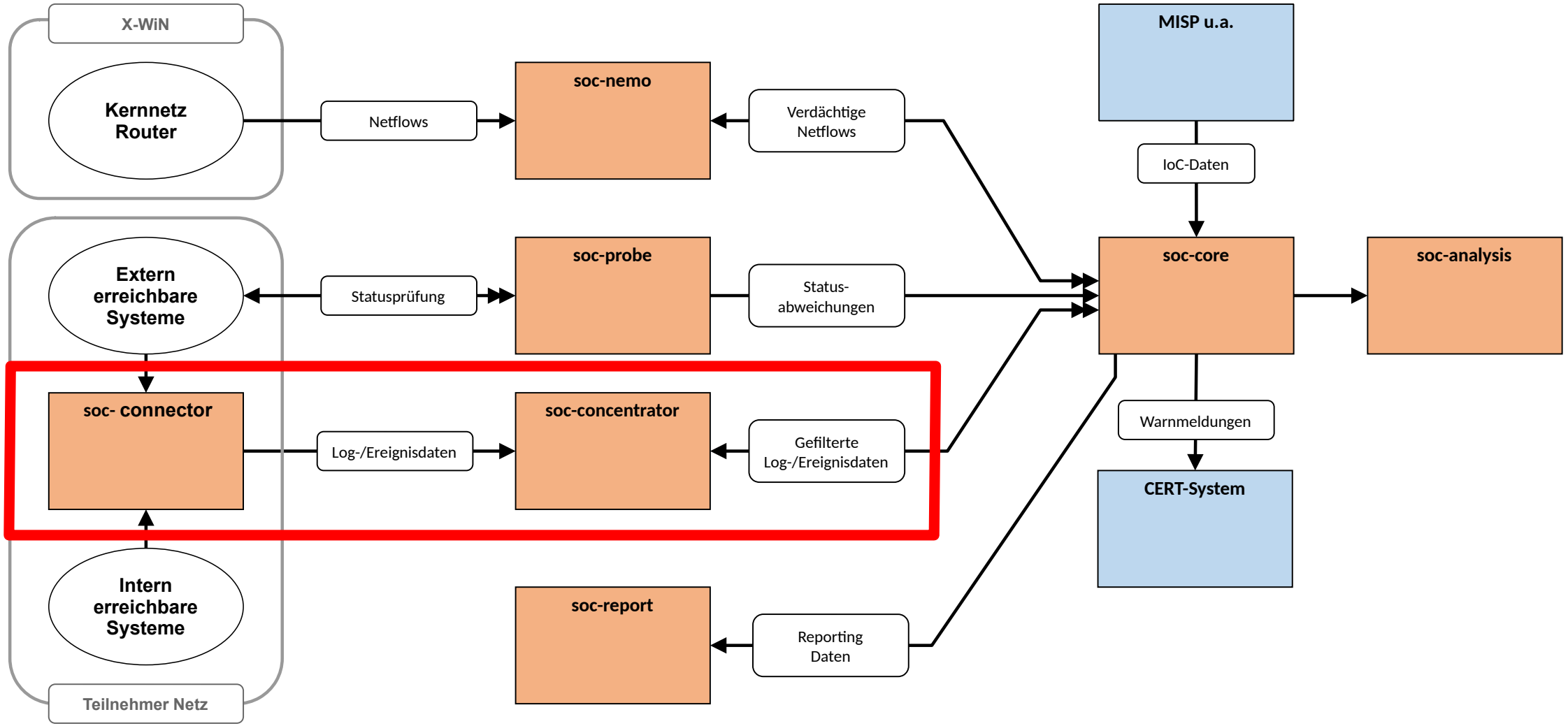
1. Architektur
2. Funktionsweise
3. Installation und Inbetriebnahme
4. Technische Details und Alternativen
5. Zusammenfassung

SOC-Connector - Architektur

DFN.Security - SOC-System



DFN.Security - SOC-System



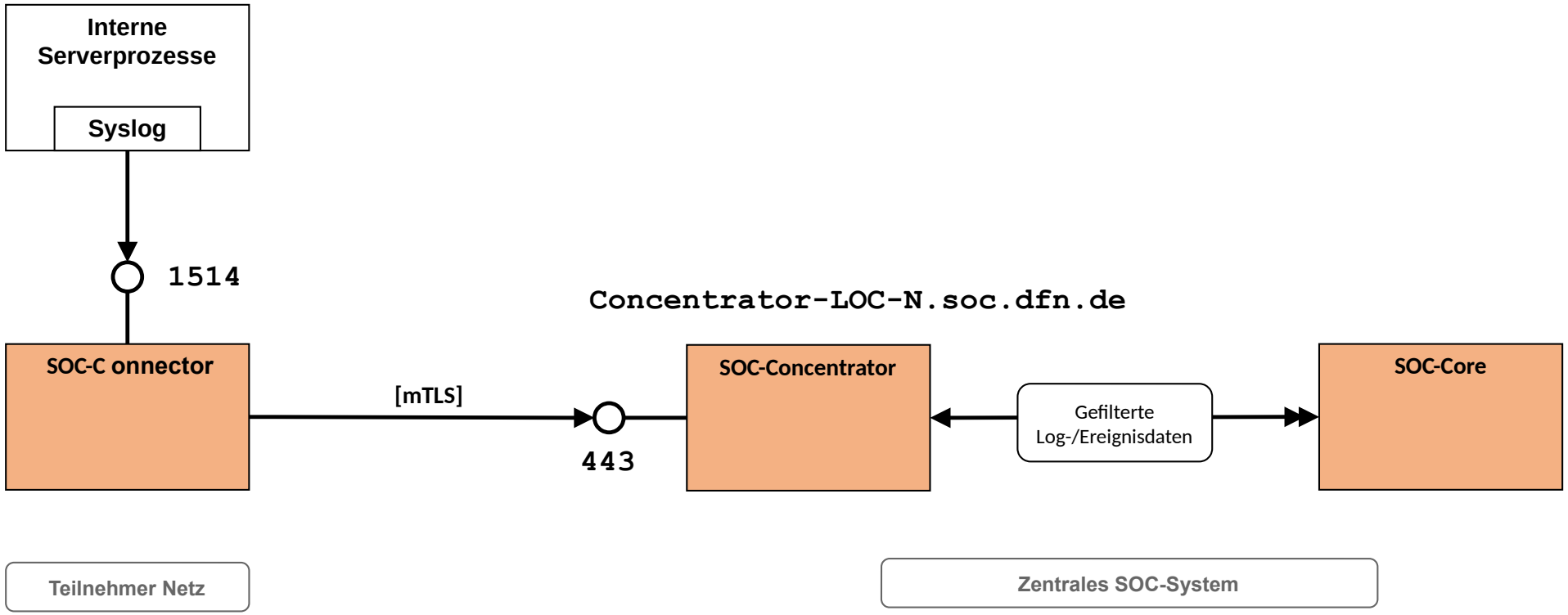
SOC-Connector - Übersicht

- Software-Komponente zur Übertragung von Log-Daten
  - Muss im lokalen Netz des Teilnehmers installiert und betrieben werden
  - Soll soweit möglich ohne manuellen Support seitens DFN-CERT auskommen
  - Kann von (öffentlich) zugänglicher Website heruntergeladen werden
  - Zur Verwendung wird ein Teilnehmer-spezifisches TLS-Client-Zertifikat benötigt

- Steht ab sofort zur Verfügung
  - Für Teilnehmer, die die Basisleistungen nutzen, stellt der SOC-Connector die einzige, offiziell unterstützte Variante dar, Logdaten einzuliefern.
  - Für Teilnehmer, die die erweiterten Leistungen nutzen, wird der SOC-Connector in Zukunft durch den umfassenderen SOC-Agent abgelöst.
  - Interaktiver Test-Modus läuft gegen Incubator-System, um Funktionsweise genau prüfen zu können ohne Daten ins Produktionssystem einliefern zu müssen.

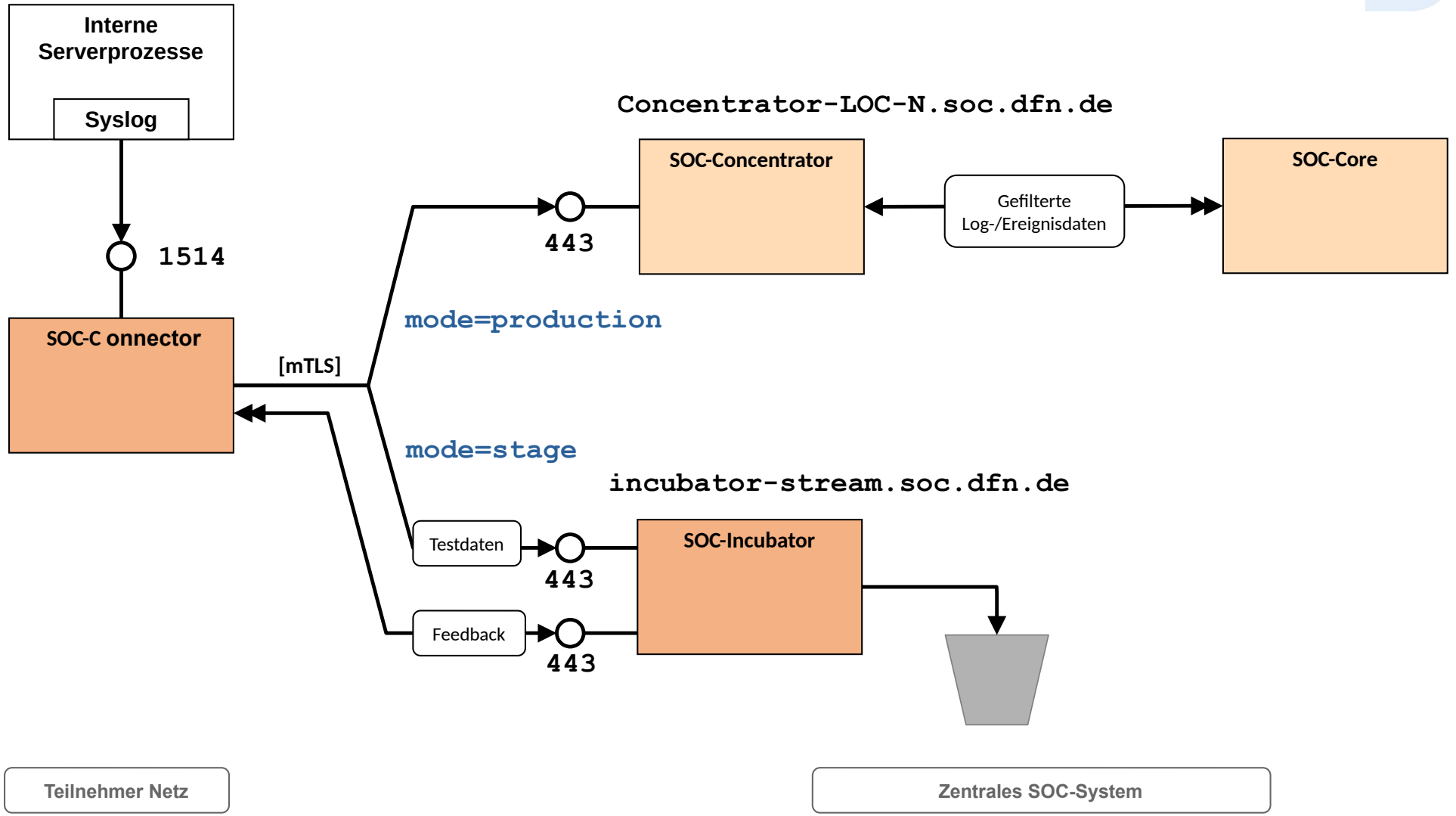
SOC-Connector - Funktionsweise

Funktionsweise - Produktion



- Meldungen werden lokal auf Port 1514 in Syslog-Format angenommen.
- Meldungen werden an den zentralen SOC-Concentrator weitergeleitet.
- Übertragung erfolgt über authentifizierten und verschlüsselten Kanal.

Funktionsweise - Stage



SOC-Connector – Installation und Inbetriebnahme

Installation

- Voraussetzungen
  - Kleiner Server-Host (oder VM)
  - Linux (z.B. Debian 11), bash-Shell + Standard-Tools („sed“)
  - Podman oder Docker als Container-Manager
- Benötigte Artefakte
  - Das Script soc-connector.sh
  - Teilnehmer-Zertifikat und zugehöriger Schlüssel

```
my-host:/home/soc/soc-connector # ls -l
    total 56
        -rw-r--r-- 1 soc soc  2013 Nov  9 09:53 <UUID>-cert.pem
        -r-------- 1 soc soc  1679 Nov  9 09:53 <UUID>-key.pem
        -rwxr-xr-x 1 soc soc 45729 Nov  9 09:53 soc-connector.sh
```

Inbetriebnahme

- Einfache Kommandos für Setup und Betrieb

```
# ./soc-connector.sh help
# ./soc-connector.sh setup
# ./soc-connector.sh start
# ./soc-connector.sh status
# ./soc-connector.sh test
# ./soc-connector.sh stop
# ./soc-connector.sh deploy
# …
```

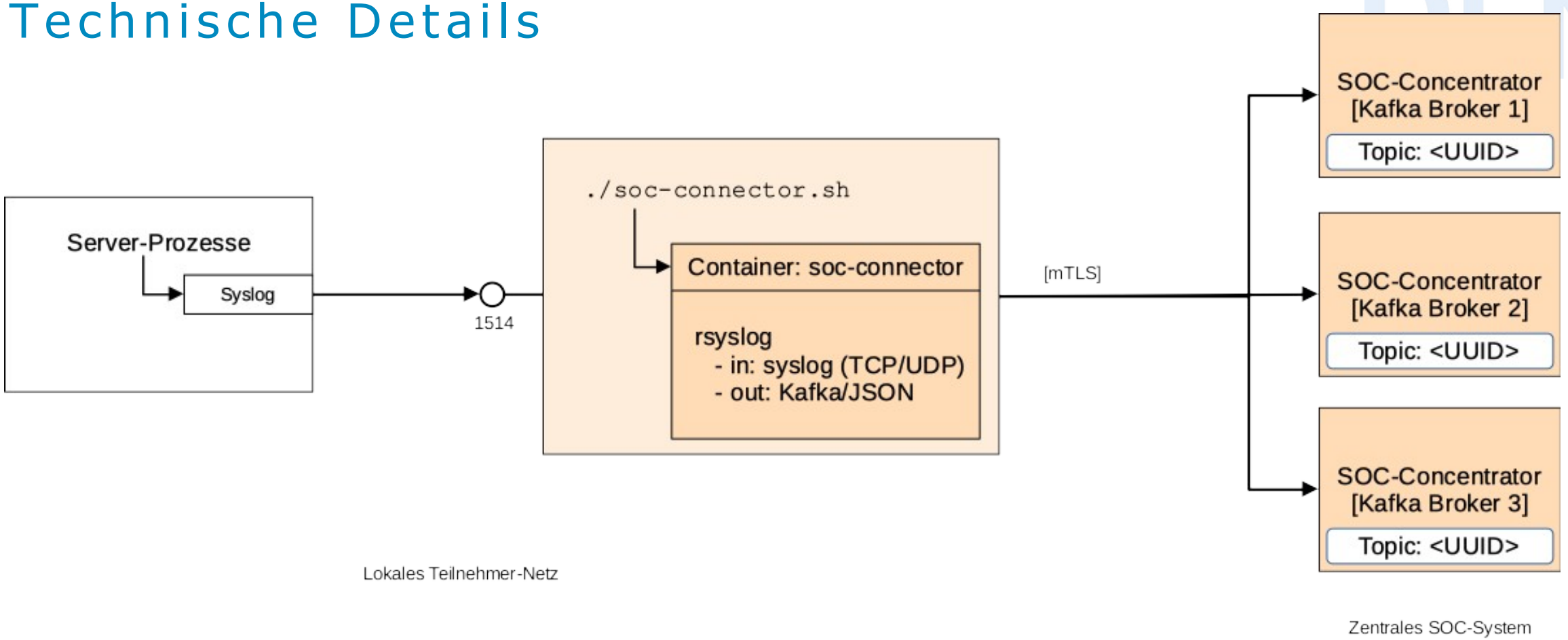
- Setup wenn nötig mit angepasster Konfiguration, z.B.:

```
# ./soc-connector.sh setup --port 514 --docker --sudo
```

- Tests laufen gegen das SOC-Incubator-System
  - Sofortige Rückmeldung
  - Daten werden nach kurzer Zeit gelöscht und nicht weiter verarbeitet

SOC-Connector -
Technische Details und Alternativen

Technische Details



- Im Container läuft ein rsyslog-Prozess
- Daten werden in JSON-Format an ein Kafka-Cluster geschickt
- Daten landen in Teilnehmer-spezifischem Kafka-Topic

Alternativen (erweiterter Dienst)

- Eigener Rsyslog-Prozess
  - Mit entsprechend konfiguriertem Kafka-Client (omkafka)
  - Mit TLS-Client-Zertifikat für gegenseitige Authentifizierung
- Eigener Kafka-Client
  - Übertragung in JSON-Format mit entsprechend gesetzten Feldern
  - Mit TLS-Client-Zertifikat für gegenseitige Authentifizierung
- Kafka Output-Plugin für ElasticSearch/Logstash (o.a.)
  - (Noch nicht getestet)

SOC-Connector - Zusammenfassung

Zusammenfassung

- Komponente SOC-Connector zum Übertragen von Log-Daten steht zur Verfügung
- Eine ausführliche und eine kurze Anleitung zur Inbetriebnahme stehen zur Verfügung
- Authentifizierte und verschlüsselte Kommunikation an SOC-Concentrator
- Test-Modus gegen Incubator-System vorhanden
- Alternative Einlieferungsmöglichkeiten im Rahmen der erweiterten Leistungen möglich

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?