

Supporting Cryptographic Migration with an IT Infrastructure Digital Twin

Daniel Herzinger, Christian Näther, and Stefan-Lukas Gazdag



AMiQuaSy

Agile Migration towards Quantum-Secure Systems

- Funded by German government
- 05/2023 - 10/2026
- Focus on practical strategies for PQC-migration and crypto-agility
- Special focus on crypto-agility tooling

「genua.

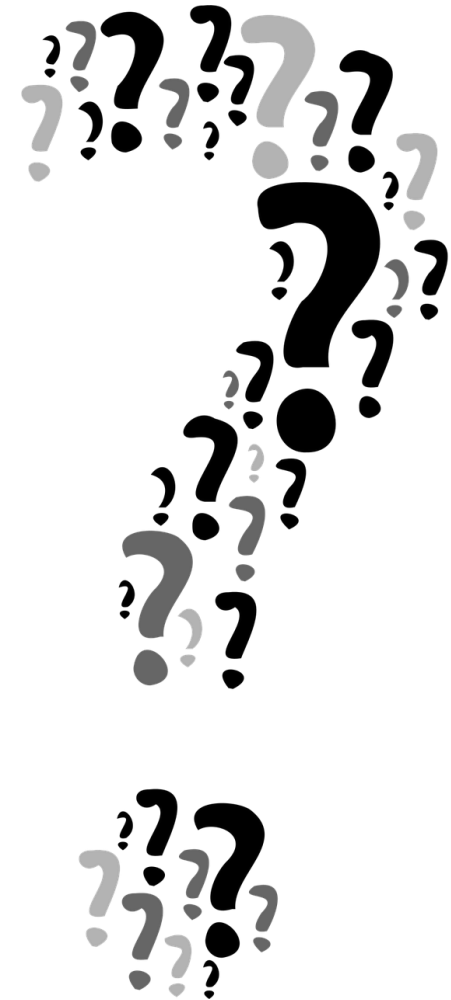
XITASO 



OTH
Amberg-Weiden

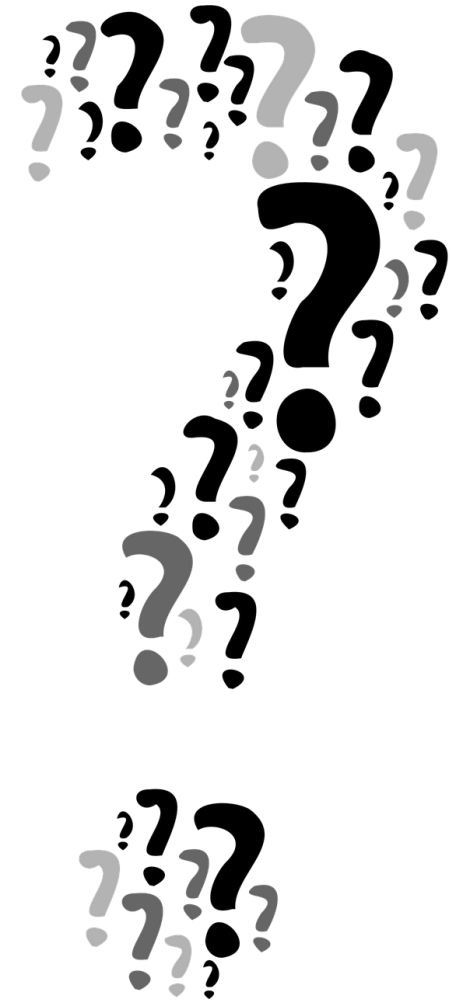
Crypto Inventory

- Cryptography
- Static keying material
- Context & Dependencies:
 - Host
 - Network
 - Software
 - Hardware
 - Regulation

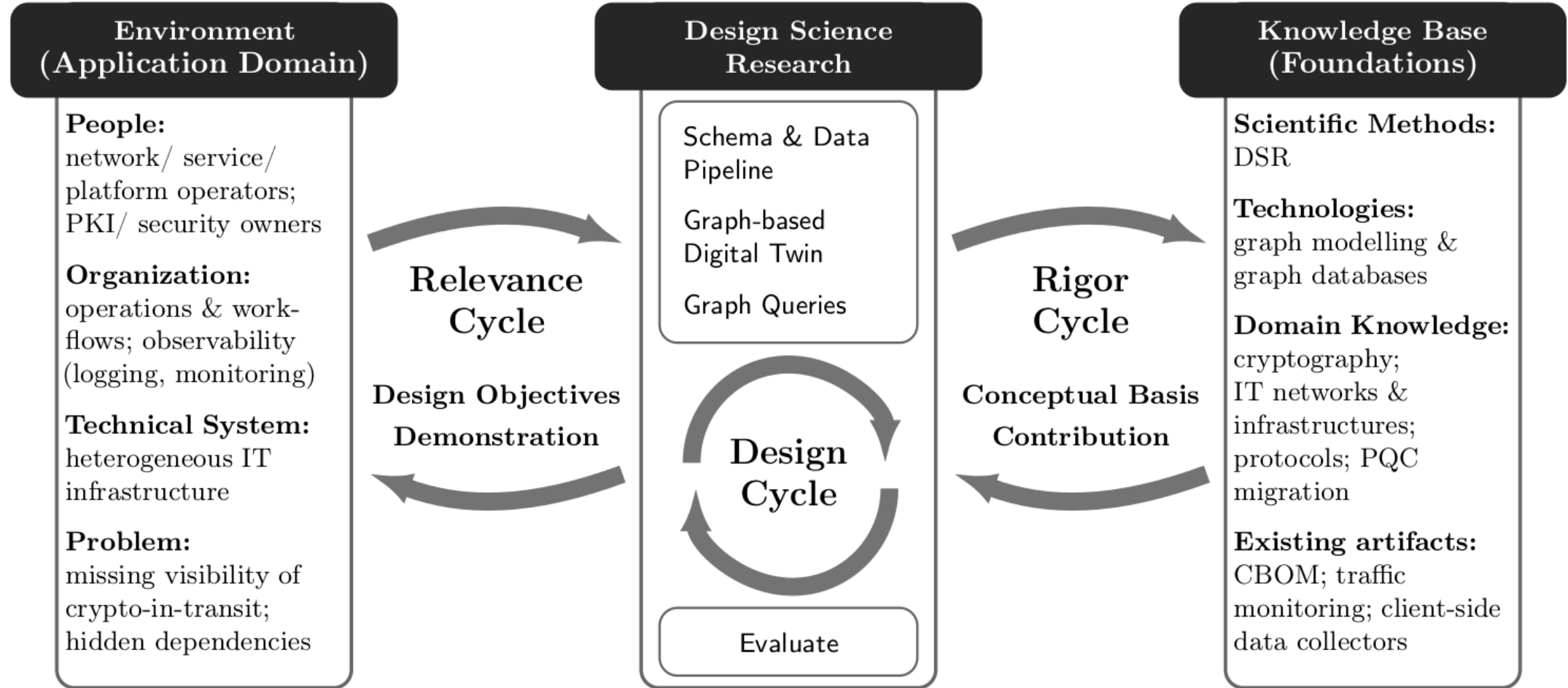


Crypto Inventory

- Cryptography
- Static keying material
- Context & Dependencies:
 - **Host**
 - **Network**
 - Software
 - Hardware
 - Regulation

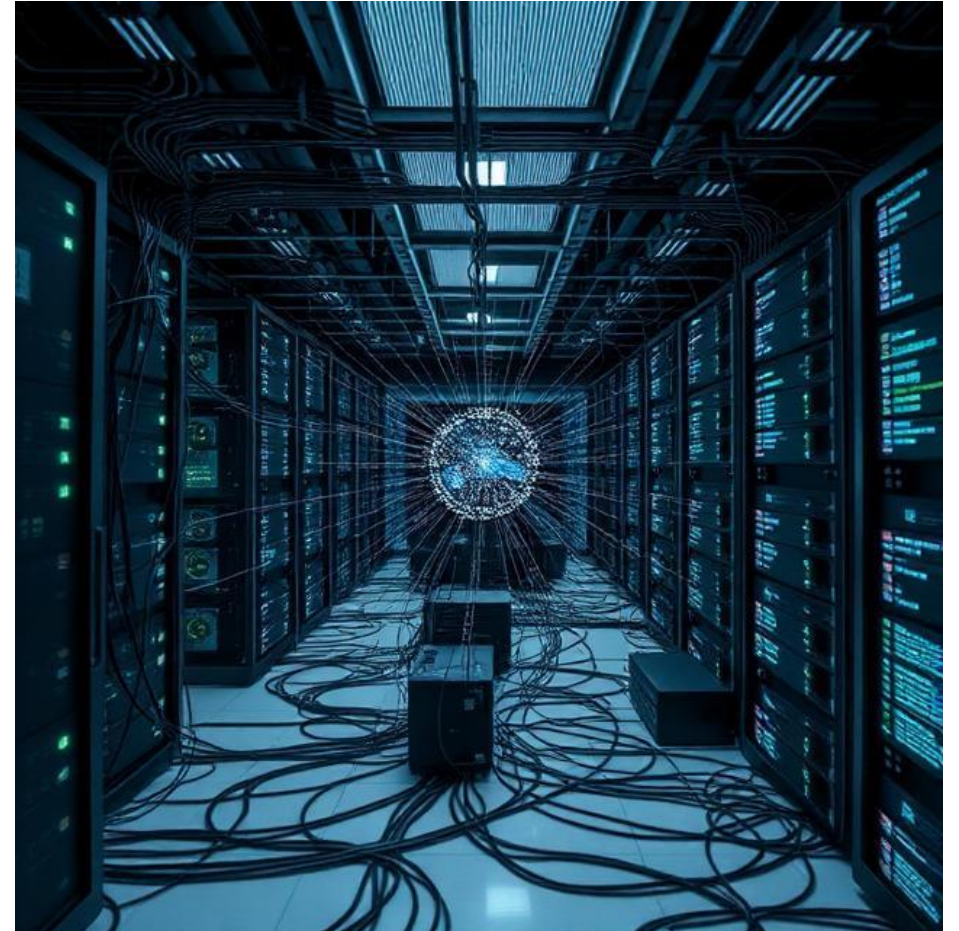


Design Science Research Approach

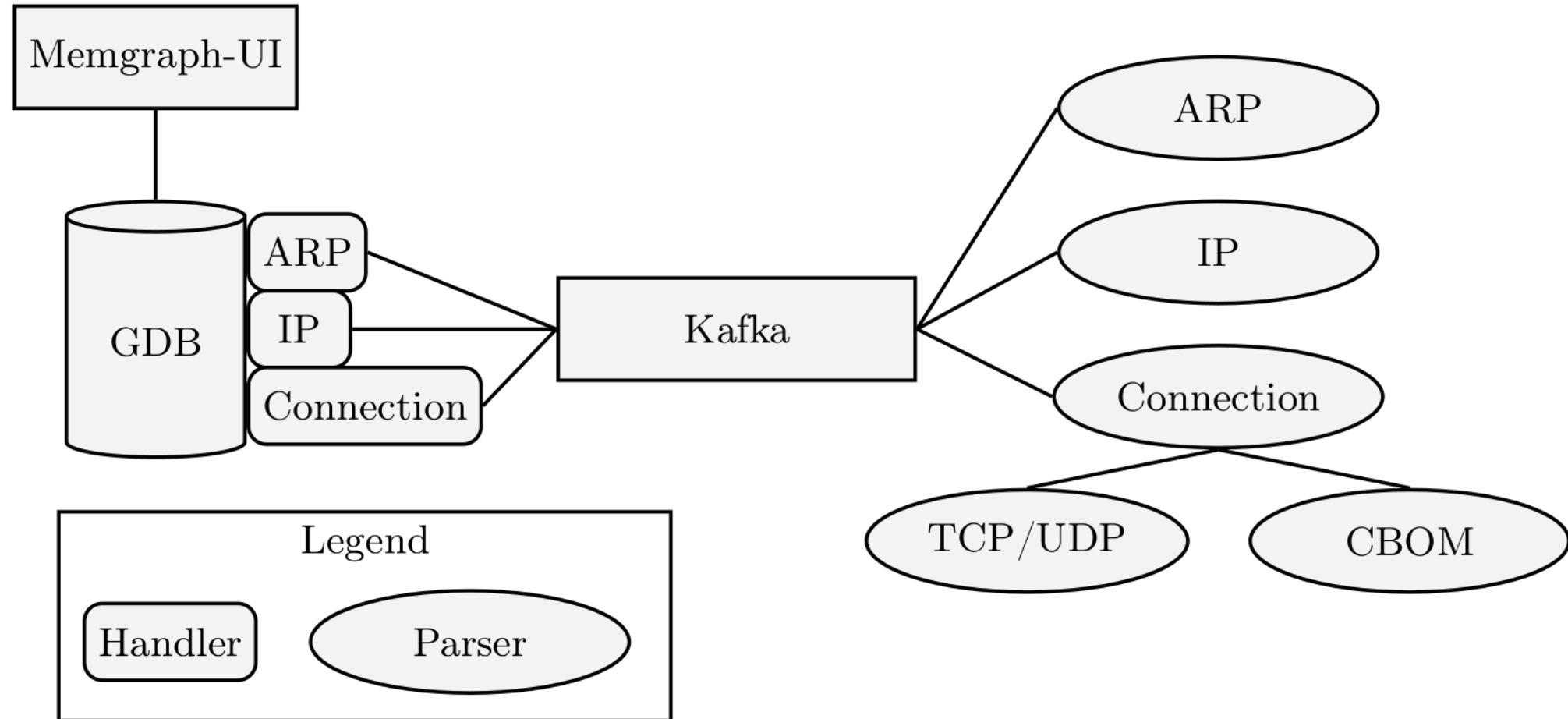


IT-Infrastructure Digital Twin – Idea

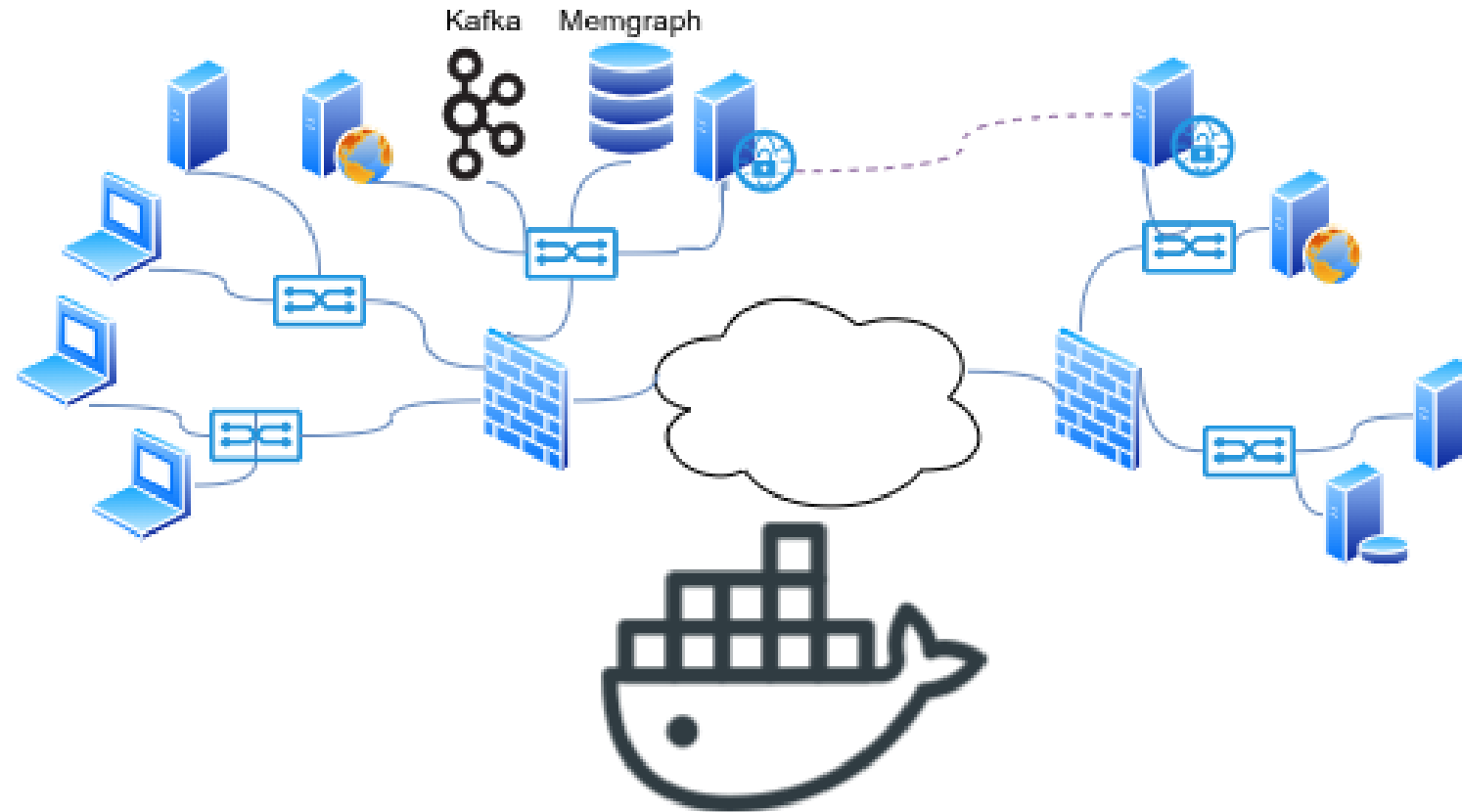
- Crypto-inventory + network context
- DPI scanners and host-based scripts as sensors
- Data processing pipeline
- Data visualization and querying
- Extensible with additional sensors



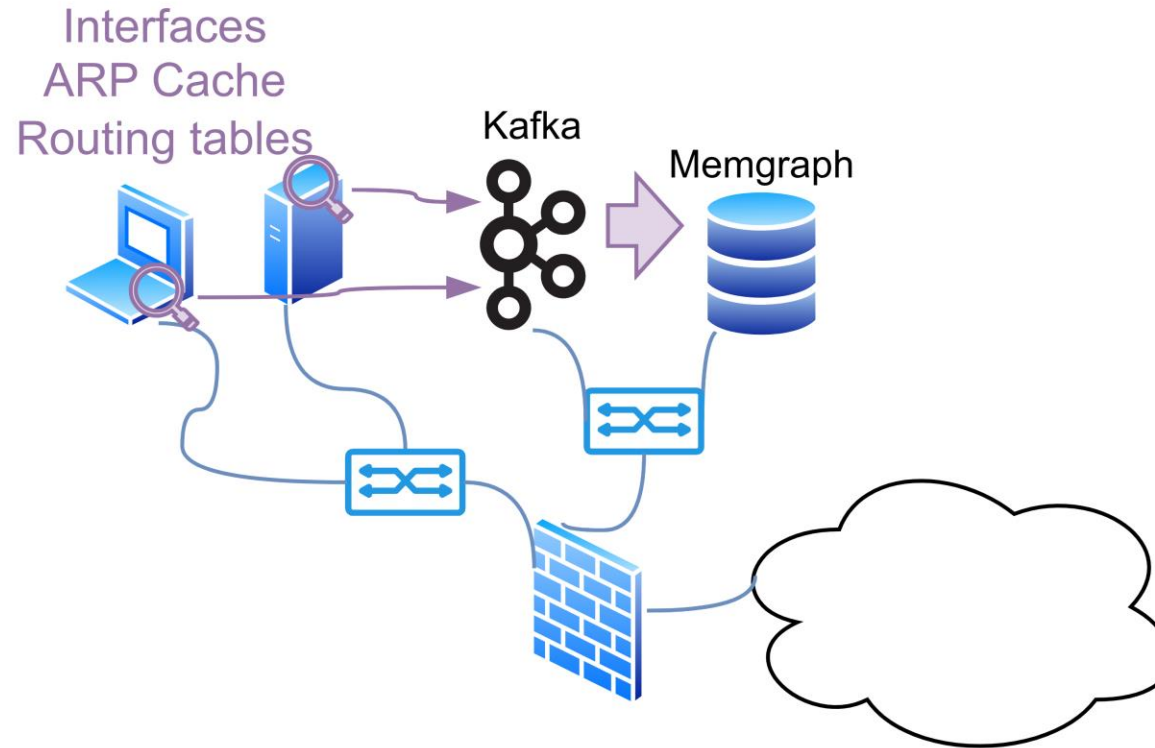
IT-Infrastructure Digital Twin – Architecture



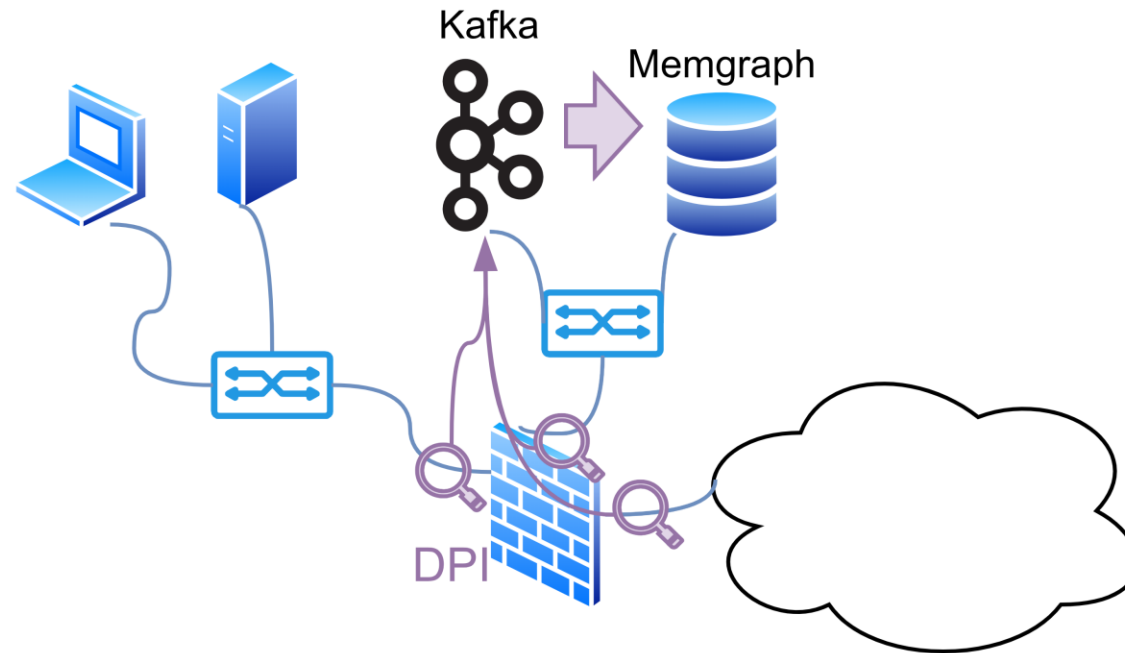
IT-Infrastructure Digital Twin – Exemplar



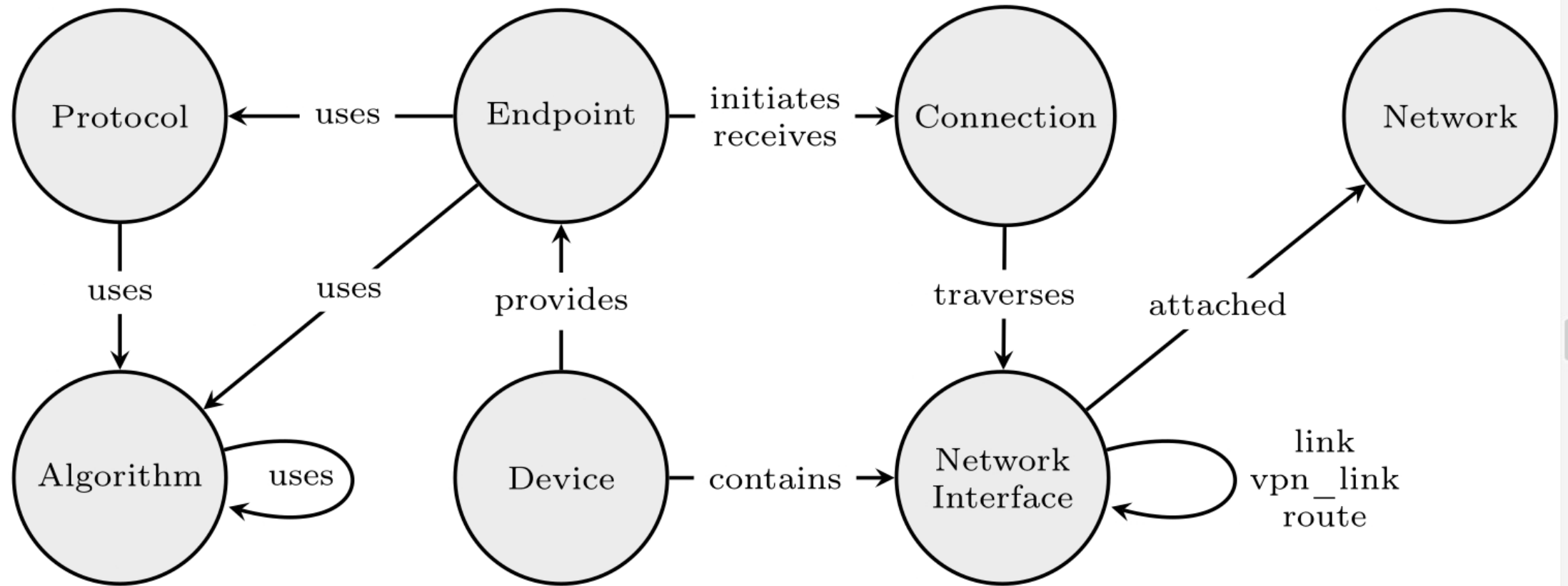
IT-Infrastructure Digital Twin – Scanner



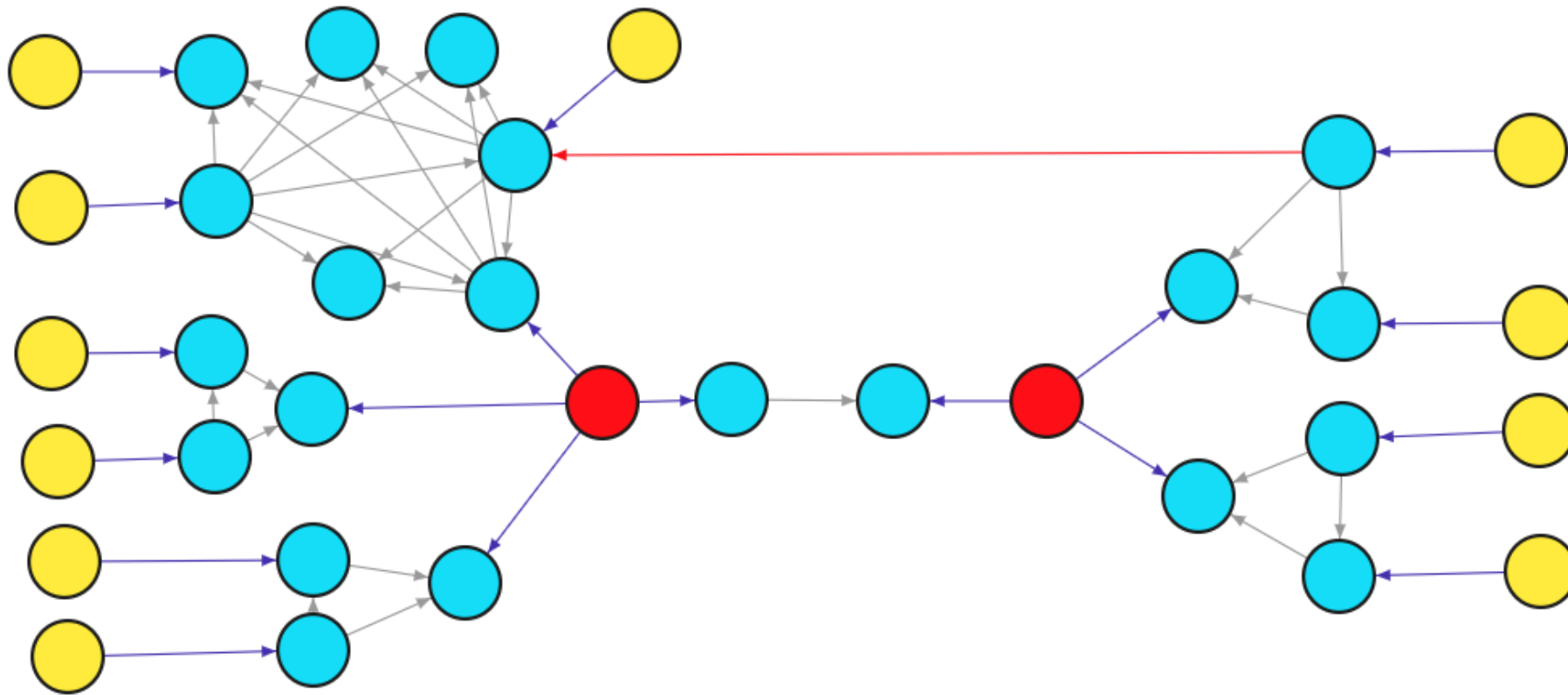
IT-Infrastructure Digital Twin – Scanner



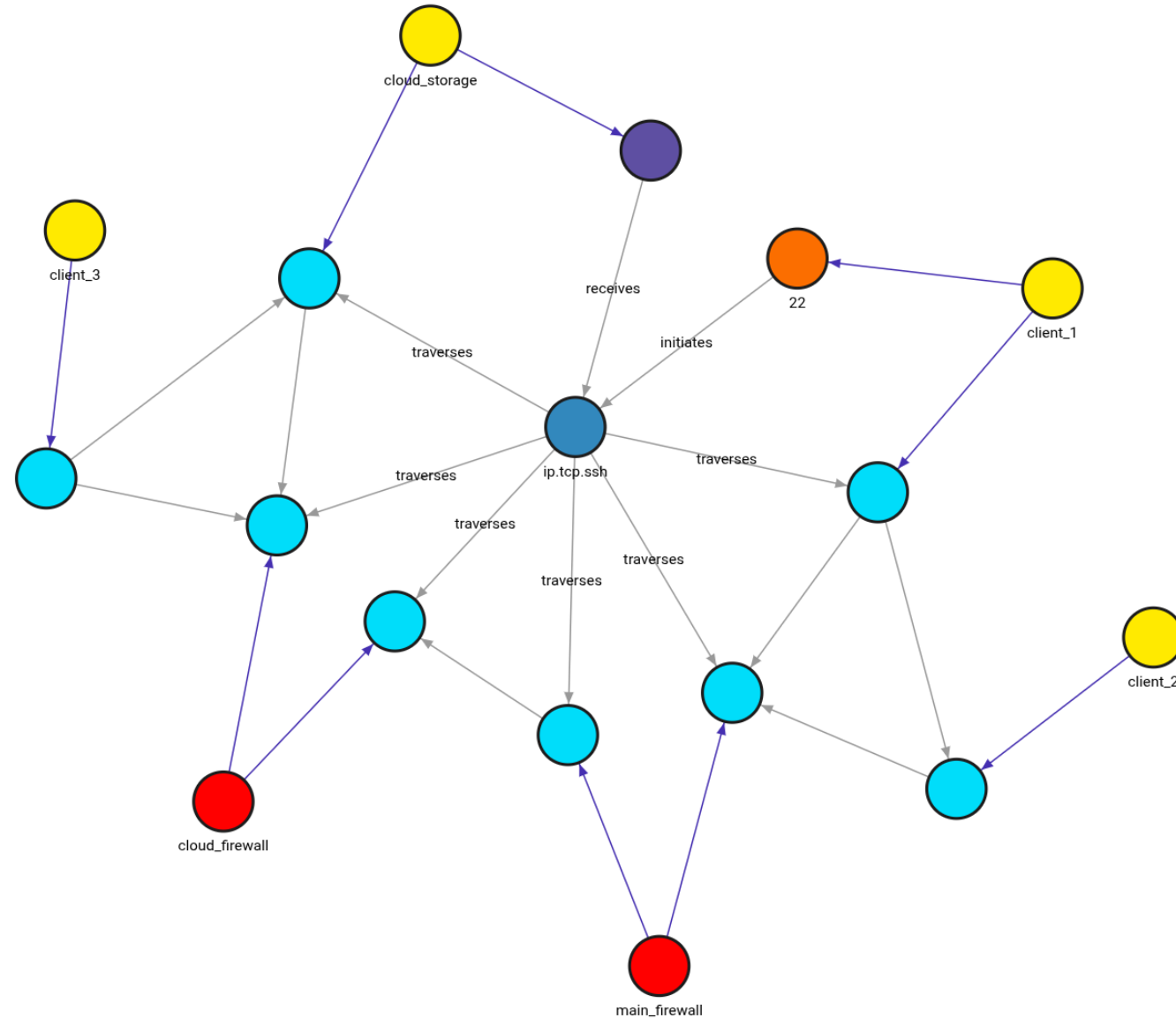
IT-Infrastructure Digital Twin – Data Scheme



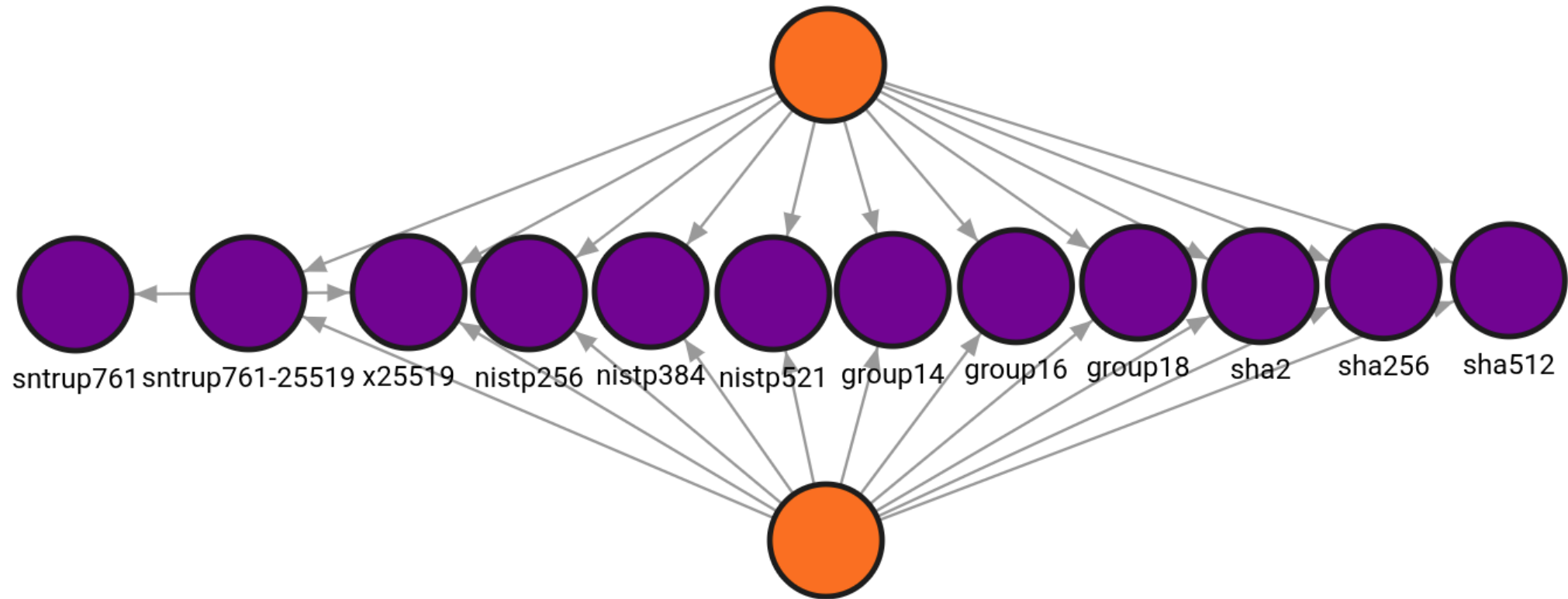
IT-Infrastructure Digital Twin – L2 Topology



IT-Infrastructure Digital Twin – Connection Route



IT-Infrastructure Digital Twin – Cryptography



Bringing It All Together

- Extensible architecture of a digital twin, including the following contexts:
 - Host information
 - Network topology
 - Network connections
 - Network security zones
 - Cryptography
- Answers questions like:
"Which hosts use deprecated cryptography to protect the infrastructure's most critical network connections."

Limitations and Future Work

- Limitations:
 - Compatibility of sensors with infrastructure
 - Real-world corner cases
- Future Work:
 - Testing in large scale environments
 - Adding different contexts & sensors
 - Forgetting old information