UNIVERSITY OF TWENTE.

DReSC
Digital Resilience in Supply chains

https://dresc.nl/

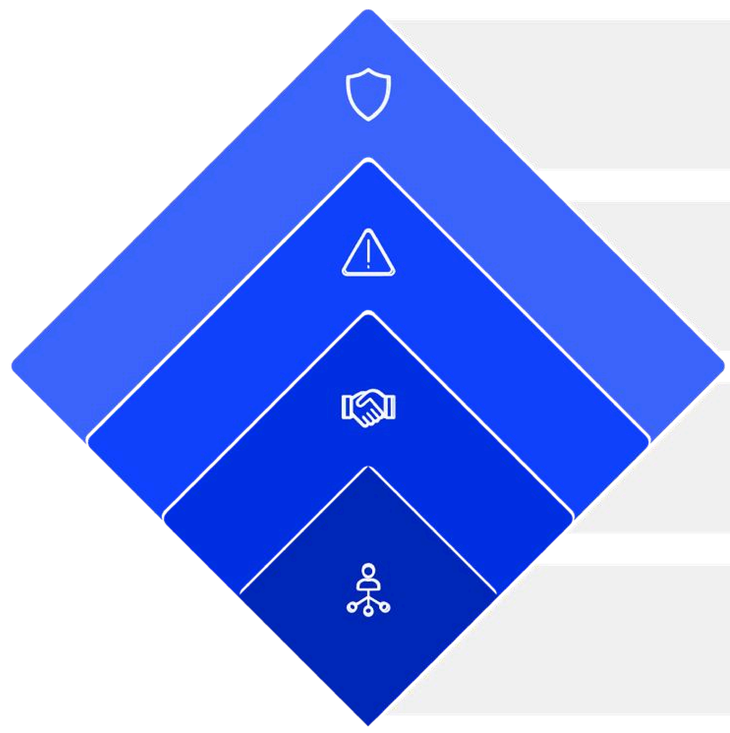
Description

Cyber-attacks can cripple global supply chains (e.g., Maersk, NHS) due to unpatched systems and low awareness.

Secure supply chains require joint effort: Supply chains are only as strong as their weakest link.

DReSC project: identifies risks, tests interventions (tech + human awareness), and designs incentives for partners to improve security together.

Goal: build resilient, secure, and collaborative supply chains.



Mitigate Impact
Prioritize controls and fixes

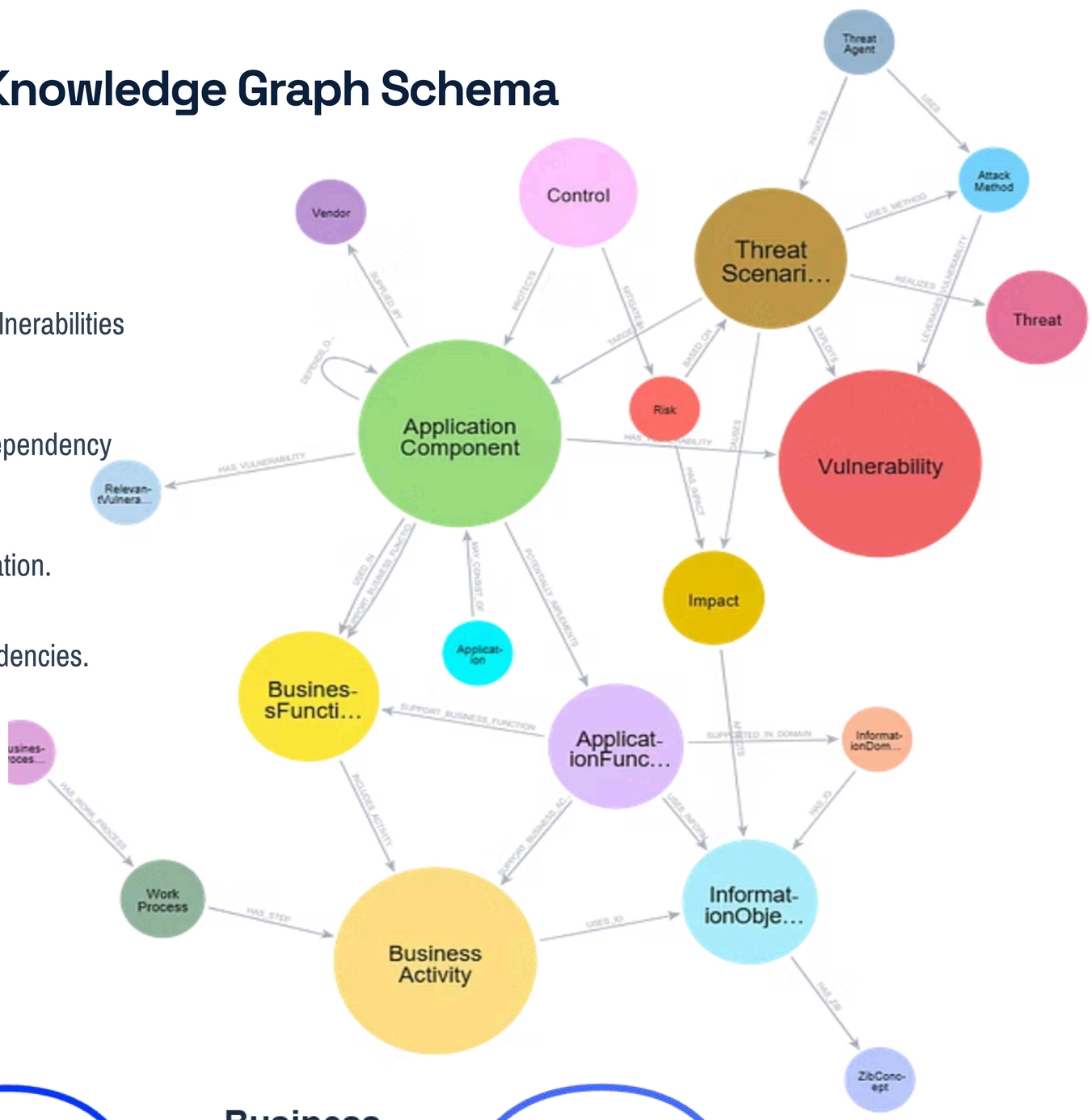
Link Suppliers
Connect external vendor paths

Trace Risks
Follow cyber-risk propagation

Map Systems
Identify IT and process nodes

Transforming complex hospital & supplier data into actionable cyber-risk intelligence

Knowledge Graph Schema



Results & Contribution

Dependency-aware cybersecurity model
A knowledge graph that connects business functions, application components, and vulnerabilities into a unified structure.

End-to-end impact traceability
Enables tracing from vulnerabilities to affected business operations through explicit dependency paths.

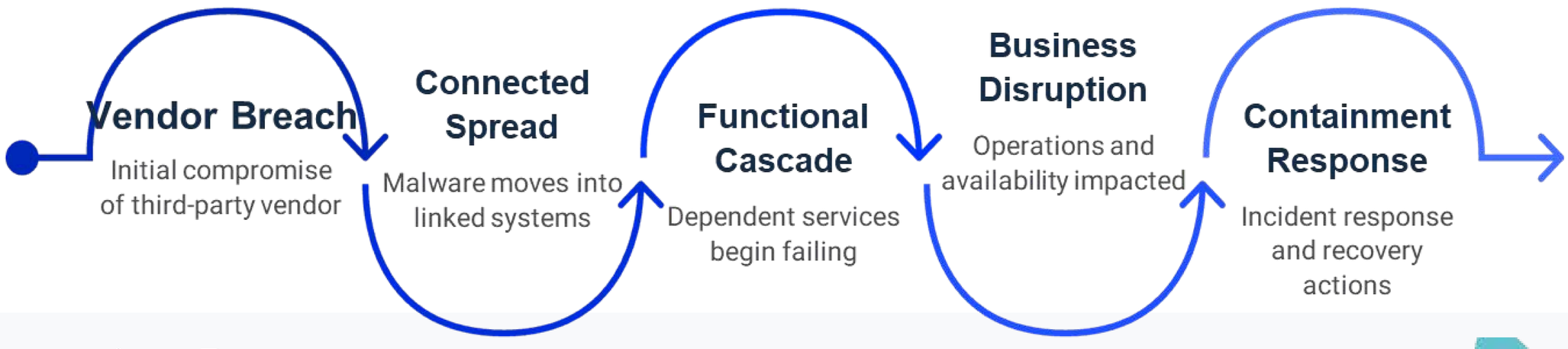
Interactive decision-support dashboard
Provides visual exploration of relationships, supporting risk interpretation and prioritization.

Contextualized vulnerability assessment
Moves beyond technical severity by incorporating business impact and system dependencies.

Sub Projects

- SBOM Generator Scorecard
- Knowledge Graph Driven GraphRAG AI Agent for Vulnerability Mapping in Supply Chains

Threat Propagation Simulation



Consortium Partners

JADS Jheronimus Academy of Data Science
Z-CERT
NORTHWAVE CYBER SECURITY
MST Medisch Spectrum Twente
port of Twente
AWARE WAYS
Emons
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid
TidalControl
Streekziekenhuis Koningin Beatrix
albert schweitzer