SerNet

Analyse des IT-Grundschutzstandards mit Graphendatenbanken

verinice.XP
23. Februar 2022

Alexander Koderman

SerNet GmbH, Berlin

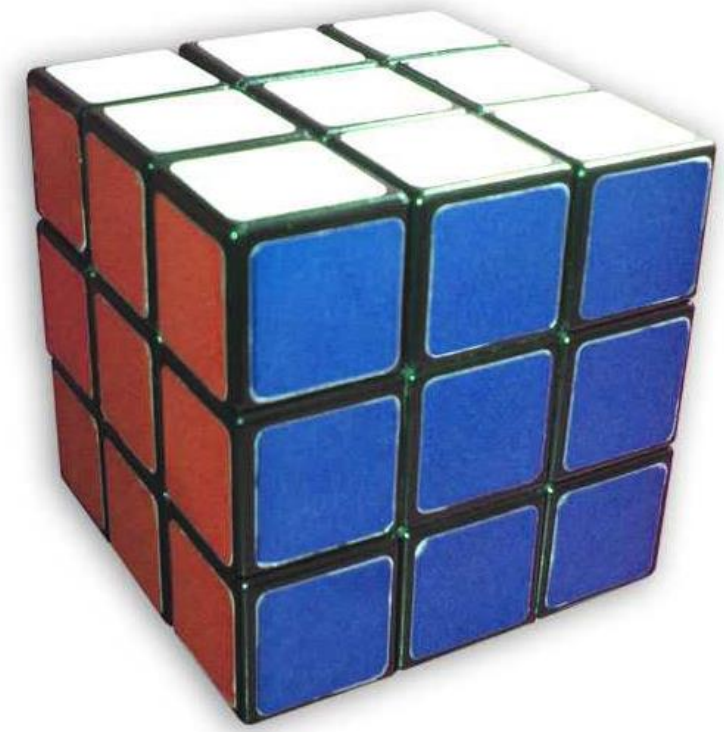
Inhalt

SerNet

- Automatisierung von Informationssicherheit
- Maschinenlesbare Formate (OSCAL, STIG, …)
- Graphendatenbanken für Implementierung & Compliance
- Graphendatenbanken für Audits & Assessments
- Die (nahe) Zukunft

Kombinatorik

SerNet



Beispiel: Compliance-Mappings

SerNet

- Arbeit mit mehreren Standards
  - IT-Grundschutz
  - Datenschutz (TOM)
  - Branchenspezifische Standards (B3S, ISO 27019…)
  - ISO 27001
  - PCI DSS
  - CoBIT
  - NIST 800-53
- Mapping:
  - existiert zwischen ITGS und 27001
  - existiert zwischen 27001 und PCI DSS
  - zwischen ITGS und PCI-DSS?

Beispiel: Compliance-Mappings

SerNet

- Annahme: 100 Maßnahmen mit je 10 Verknüpfungen
- Verknüpfungstabelle enthält 1.000 Einträge
- Existiert eine Verbindung zwischen Maßnahme B und A? (A → entspricht → B)
- Zwischen Maßnahme C und A? (A → entspricht → B → entspricht C)

	Zu untersuchende Pfade
A→B	1.000
A→…→C	1.000.000
A→…→D	1.000.000.000
A→…→E	1.000.000.000.000
A→…→F	1.000.000.000.000.000

Live Beispiel in Neo4J Graphendatenbank

SerNet

```
neo4j$ MATCH (n1)-[r:REQUIRED_BY_THREAT]→(t:BsiThreat) RETURN t.gsid, t.name, count(r) as numRequired ORDER by numRequired DESC…
```

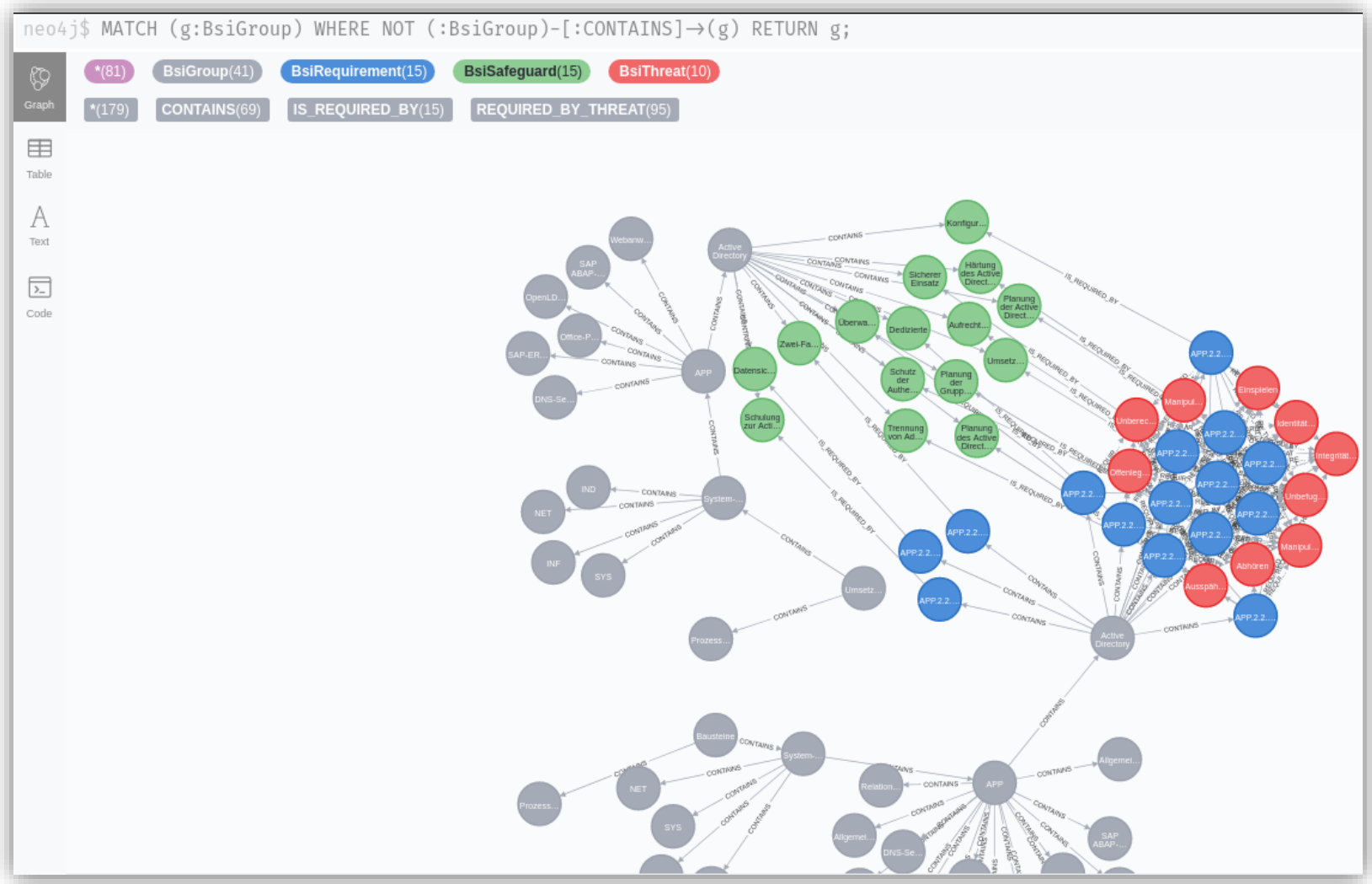
Table | Text | Code

	t.gsid	t.name	numRequired
1	"G 0.18"	"Fehlplanung oder fehlende Anpassung"	488
2	"G 0.19"	"Offenlegung schützenswerter Informationen"	487
3	"G 0.30"	"Unberechtigte Nutzung oder Administration von Geräten und Systemen"	375
4	"G 0.14"	"Ausspähen von Informationen (Spionage)"	353
5	"G 0.23"	"Unbefugtes Eindringen in IT-Systeme"	340
6	"G 0.22"	"Manipulation von Informationen"	331
7			

Started streaming 10 records after 5 ms and completed after 56 ms.

Live Beispiel in Neo4J Graphendatenbank

SerNet



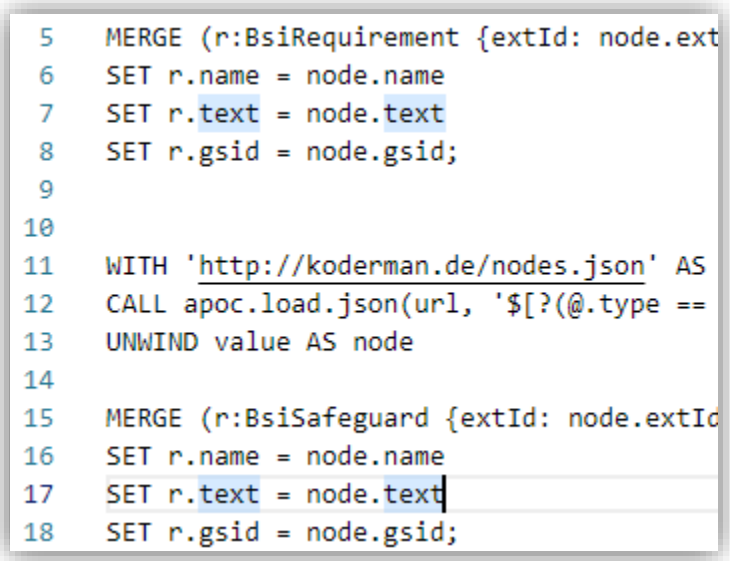
Maschinell lesbare Maßnahmenkataloge

SerNet

- IT-Grundschutz, vom BSI veröffentlicht als
  - PDF (Dokumentenformat)
  - DOCX (Dokumentenformat)
  - Docbook (Dokumentenformat)

- Behelfslösung: verinice.xml → Konvertierung → Import
  - https://github.com/Agh42/IT-Grundschutz4Neo4J

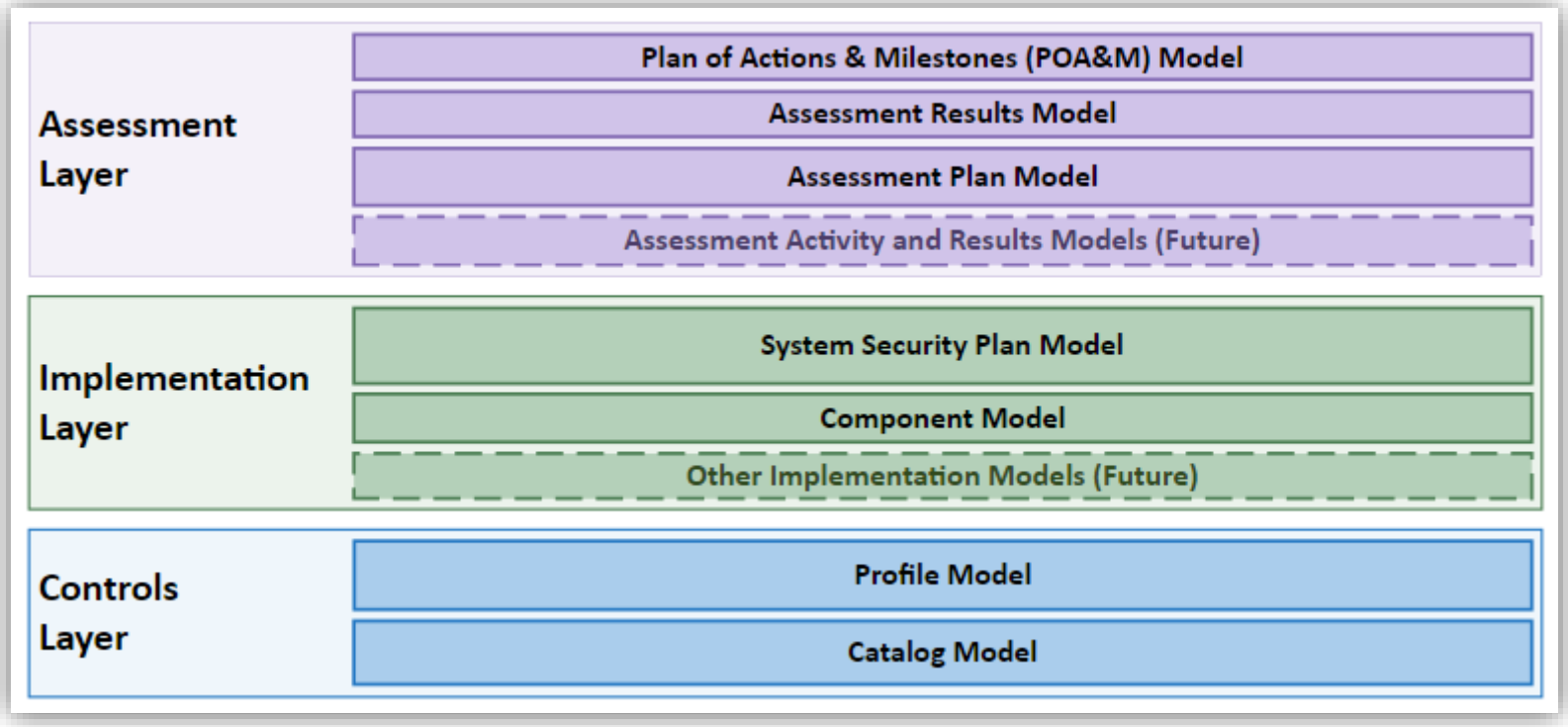
verinice.xml



```
5   MERGE (r:BsiRequirement {extId: node.ext
6   SET r.name = node.name
7   SET r.text = node.text
8   SET r.gsid = node.gsid;
9
10
11  WITH 'http://koderman.de/nodes.json' AS
12  CALL apoc.load.json(url, '$[?(@.type ==
13  UNWIND value AS node
14
15  MERGE (r:BsiSafeguard {extId: node.extId
16  SET r.name = node.name
17  SET r.text = node.text
18  SET r.gsid = node.gsid;
```

NIST OSCAL -
Open Security Controls Assessment Language:
Format speziell für Cybersecurity-Controls

SerNet



NIST OSCAL - Open Security Controls Assessment Language: Format speziell für Cybersecurity-Controls

SerNet

- Import
  - OSCAL4NEO4J
- Mit weiteren Tools verlinkt bei:
  - https://github.com/usnistgov/OSCAL/blob/develop/docs/content/tools/_index.md)
  - https://github.com/oscal-club/awesome-oscal

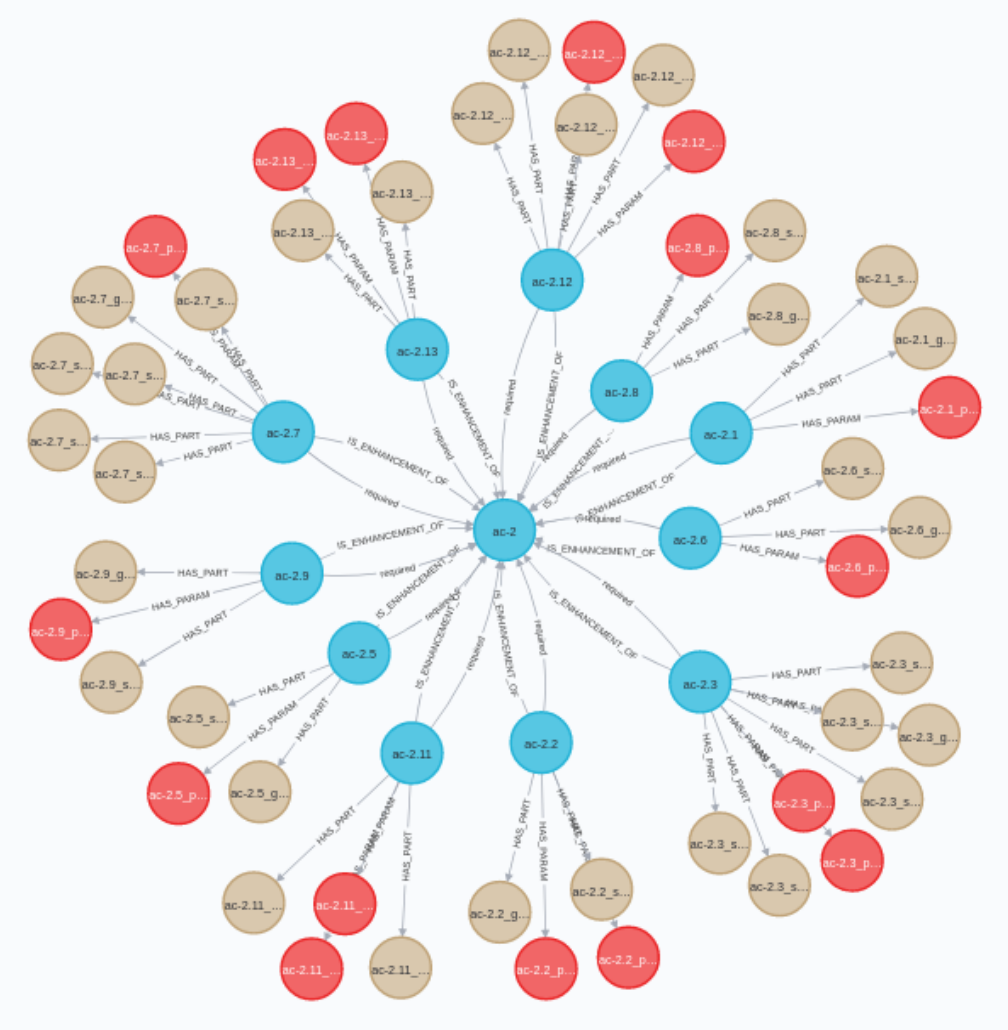
Tools

- Alex Koderman's oscal4neo4j: a collection of scripts in Neo4j's Cypher query language to load OSCAL catalog data in JSON format into its graph database, potentially for use with the Red Team Project's Security Control Knowledge Graph.
- Brian Ruf's OSCAL-GUI: an example PHP web interface developed by @brian-ruf of former FedRAMP fame. It has core presentation logic, file import, format conversion, and working profile resolution.
- CivicActions's compliance-io library for composable functions for conversion from OpenControl to OSCAL.
- CivicActions's ssp-toolkit is a suite of command line utilities in Python to mediate the creation of system security

Atlasity: Continuous Compliance Automation	C2 Labs	Atl dev Pla Atl	
control_freak	Risk Redux	This refe fro OS	
OSCAL4NEO4J	The OSCAL4NEO4J Project	This project features a set of Neo4J cypher scripts which will import OSCAL catalogs and profiles directly from the official Github-repositories into a Neo4J database. Once imported, the information can be queried to gain insight into the structure of those catalogs and baselines. The project aims to add tool support for the implementation and assessment layers by allowing generation of component definitions, system security plans, assessment-plans, assessment-results and POA&Ms.	open source

Graphendarstellung von OSCAL Daten:
Control AC-2 „ACCOUNT MANAGEMENT “

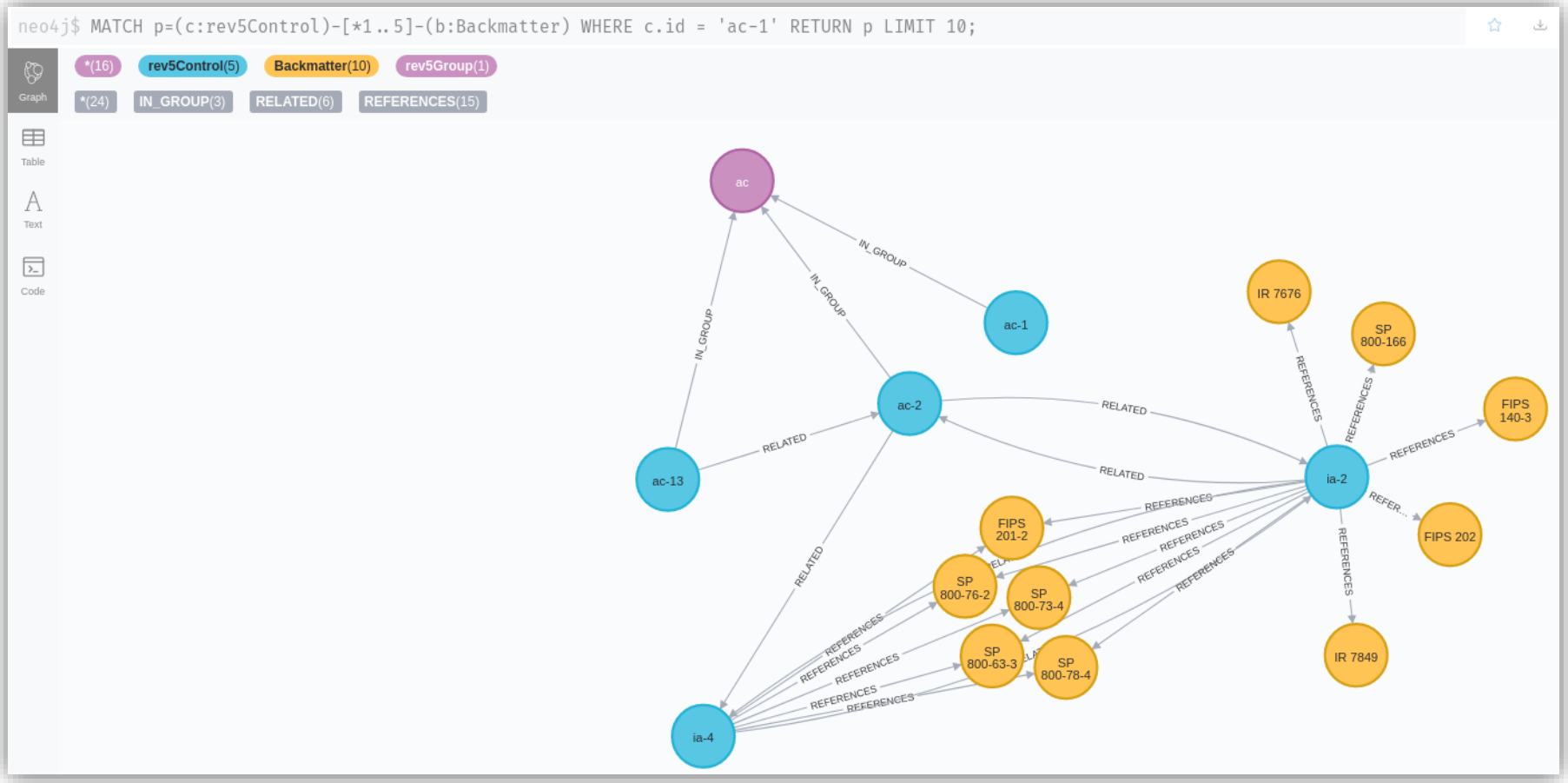
SerNet



Graphendarstellung von OSCAL Daten:

„Backmatter“: verknüpfte Standards

SerNet



Graphendarstellung von OSCAL Daten: Assessment-Objectives

SerNet

```
1 MATCH p=(c:rev5Control)-[:HAS_PART*]→(part)
2 WHERE c.id='ac-2.1'
3 WITH p, c, part
4 MATCH (part)-[:HAS_PROP]→(prop)
5 OPTIONAL MATCH (part)-[:HAS_PART]→(subpart)
6 RETURN c.id, c.title, part.name, part.prose, prop.value, subpart.name, subpart.prose
7 ORDER BY c.id, part.prose, part.name, subpart.name;
```

neo4j$ MATCH p=(c:rev5Control)-[:HAS_PART*]→(part) WHERE c.id='ac-2.1' WITH p, c, part MATCH (part)-[:HAS_PROP]→(prop) OPTIONA…

Table | Text | Code

	c.id	c.title	part.name	part.prose	prop.value	subpart.name	subpart.prose
1	"ac-2.1"	"Automated System Account Management"	"assessment-objective"	"the management of system accounts is supported using {{ insert: param, ac-02.01_odp }}."	"AC-02(01)"	*null*	*null*
2	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"AC-02(01)-Interview"	"assessment-objects"	"Organizational personnel with account management responsibilities system/network administrators organizational personnel with information security with information security responsibilities system developers"
3	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"INTERVIEW"	"assessment-objects"	"Organizational personnel with account management responsibilities system/network administrators organizational personnel with information security with information security responsibilities system developers"
4	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"AC-02(01)-Test"	"assessment-objects"	"Automated mechanisms for implementing account management functions"
5	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"TEST"	"assessment-objects"	"Automated mechanisms for implementing account management functions"
6	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"EXAMINE"	"assessment-objects"	"Access control policy procedures for addressing account management system design documentation system configuration settings and associated documentation

Started streaming 7 records after 18 ms and completed after 19 ms.

Graphendarstellung von OSCAL Daten: Alle Interviewpartner für *Access Control*

SerNet

```
1 MATCH (g:rev5Group {id: 'ac'})←[:IN_GROUP]-(c:rev5Control)←[:IS_ENHANCEMENT_OF]-(ce:Enhancement)-[*1..3]→(pp:PartProp {value:
  'INTERVIEW'})
2 WITH pp,c,ce
3 MATCH (pp)←[:HAS_PROP]-(cp:ControlPart)
4 WITH cp,c,ce
5 MATCH (cp)-[:HAS_PART]→(part)
6 WHERE part.name = 'assessment-objects'
7 RETURN DISTINCT c.id, c.title, ce.id, ce.title, part.prose
8 order by c.id, ce.id;
```

neo4j$ MATCH (g:rev5Group {id: 'ac'})←[:IN_GROUP]-(c:rev5Control)←[:IS_ENHANCEMENT_OF]-(ce:Enhancement)-[*1..3]→(pp:PartProp …

Table | Text | Code

	c.id	c.title	ce.id	ce.title	part.prose
1	"ac-11"	"Device Lock"	"ac-11.1"	"Pattern-hiding Displays"	"System/network administrators organizational personnel with information security responsibilities system developers"
2	"ac-12"	"Session Termination"	"ac-12.1"	"User-initiated Logouts"	"System/network administrators organizational personnel with information security responsibilities system developers"
3	"ac-12"	"Session Termination"	"ac-12.2"	"Termination Message"	"System/network administrators organizational personnel with information security responsibilities system developers"
4	"ac-12"	"Session Termination"	"ac-12.3"	"Timeout Warning Message"	"System/network administrators organizational personnel with information security responsibilities system developers"
5	"ac-14"	"Permitted Actions Without Identification or Authentication"	"ac-14.1"	"Necessary Uses"	"System/network administrators organizational personnel with information security responsibilities"
6	"ac-16"	"Security and Privacy Attributes"	"ac-16.1"	"Dynamic Attribute Association"	"System/network administrators organizational personnel with information security and privacy responsibilities system developers"

Started streaming 336 records after 16 ms and completed after 719 ms.

Graphendarstellung von OSCAL Daten:
Alle abfragbaren Controls für einen Interviewpartner

SerNet

```
1 MATCH (g:rev5Group {id: 'ac'})<-[*1..2]-(c:rev5Control)-[*1..3]->(pp:PartProp {value: 'INTERVIEW'})
2 WITH c, pp as ip
3 MATCH (ip)<-[:HAS_PROP]-(cp:ControlPart)-[:HAS_PART]->(part)
4 WHERE part.name = 'assessment-objects'
5 RETURN DISTINCT  replace(part.prose, "\n\n", " / ") AS InterviewPartners, collect(distinct(c.id + " " + c.title)) as Controls
6 ORDER by Controls;
```

neo4j$ MATCH (g:rev5Group {id: 'ac'})<-[*1..2]-(c:rev5Control)-[*1..3]->(pp:PartProp {value: 'INTERVIEW'}) WITH c, pp as ip MATC…

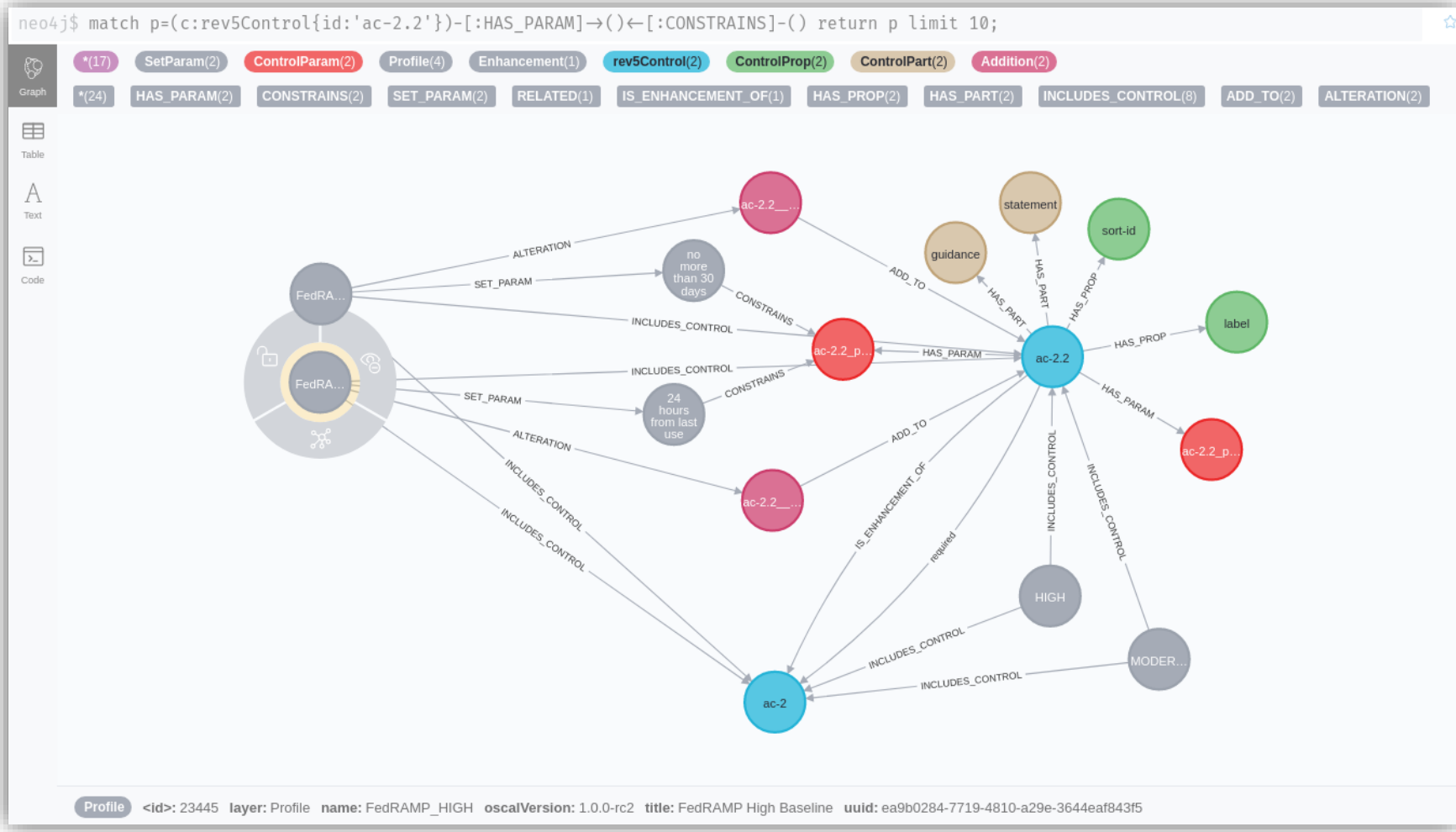
Table | Text | Code

	InterviewPartners	Controls
	responsibilities / system developers"	
12	"Organizational personnel approving the use of alternate work sites / organizational personnel using alternate work sites / organizational personnel assessing controls at alternate work sites / organizational personnel with information security and privacy responsibilities"	["ac-17 Remote Access", "pe-17 Alternate Work Site"]
13	"Organizational personnel with responsibilities for implementing or monitoring remote access to the system / system users with knowledge of information about remote access mechanisms / organizational personnel with information security responsibilities"	["ac-17.6 Protection of Mechanism Information"]
14	"Organizational personnel with access enforcement responsibilities / system/network administrators / organizational personnel with information security responsibilities"	["ac-17.7 Additional Protection for Security Function Access", "ac-3.10 Audited Override of Access Control Mechanisms", "ac-3.13 Attribute-based Access Control", "ac-3.12 Assert and Enforce Application Access"]

Started streaming 277 records after 11 ms and completed after 10327 ms.

Graphendarstellung von OSCAL Daten:
Profile für mittleren / hohen Schutzbedarf

SerNet



Die (nahe) Zukunft

SerNet

- Tool-Unterstützung für maschinenlesbare Formate (wie OSCAL) für Kataloge, Component Definitions, System Security Plans, Assessment-Plans & -Results, SBOM[1]…
- Fachspezifischer Austausch von Daten im IS-Management zwischen Prüfer, Auditor, Lieferanten…
- Stärkere Verzahnung von technischen Maßnahmen auf Systemebene und Managementebene
- Automatisierung von Prüfungshand-lungen
- Steigende Prüfungsfrequenz, bis zum Continuous Assessment

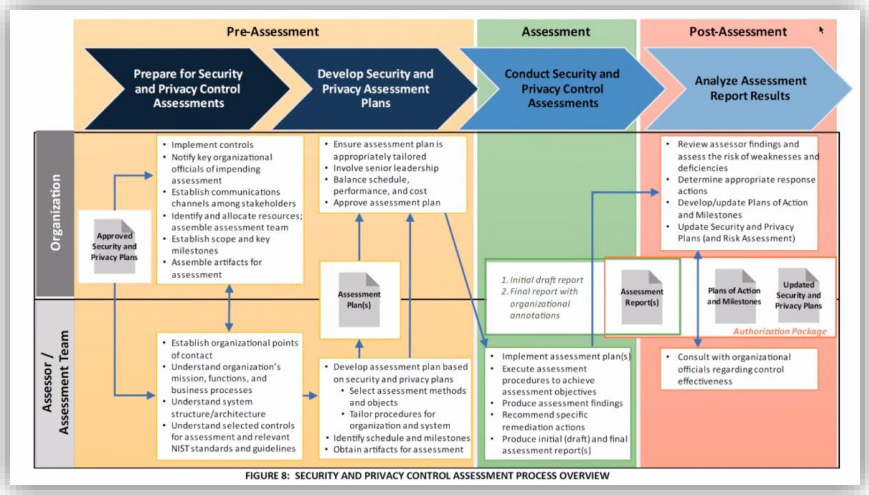


FIGURE 8: SECURITY AND PRIVACY CONTROL ASSESSMENT PROCESS OVERVIEW

1. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Kontakt

SerNet

Alexander Koderman, AK@sernet.de

SerNet GmbH
Bahnhofsallee 1b
37081 Göttingen

+49 551 370000-0
+49 551 370000-9

https://www.sernet.de
kontakt@sernet.de

SerNet GmbH
Torstraße 6
10119 Berlin

+49 30 5 779 779 0
+49 30 5 779 779 9

SerNet Inc.
101 Montgomery St.
San Francisco, CA 49104

+1 (415) 248-7818

https://www.sernet.com
contact@sernet.com