Implementing Knowledge Graphs at Center for Internet Security

Dalia Dahleh

November 2023

semantic arts

CIS Overview

- Community driven, non-profit
- Publishes security best practices
  - Controls: general recommendations
  - Benchmarks: vendor-specific, 25+ partners

semantic arts

Controls


CONTROL 01
Inventory and Control of Enterprise Assets
5 Safeguards
IG1 2/5
IG2 4/5
IG3 5/5
CONTROL 02
Inventory and Control of Software Assets
7 Safeguards
IG1 3/7
IG2 6/7
IG3 7/7
CONTROL 03
Data Protection
14 Safeguards
IG1 6/14
IG2 12/14
IG3 14/14
CONTROL 04
Secure Configuration of Enterprise Assets and Software
12 Safeguards
IG1 7/12
IG2 11/12
IG3 12/12
CONTROL 05
Account Management
6 Safeguards
IG1 4/6
IG2 6/6
IG3 6/6
CONTROL 06
Access Control Management
8 Safeguards
IG1 5/8
IG2 7/8
IG3 8/8
CONTROL 07
Continuous Vulnerability Management
7 Safeguards
IG1 4/7
IG2 7/7
IG3 7/7
CONTROL 08
Audit Log Management
12 Safeguards
IG1 3/12
IG2 11/12
IG3 12/12
CONTROL 09
Email and Web Browser Protections
7 Safeguards
IG1 2/7
IG2 6/7
IG3 7/7
CONTROL 10
Malware Defenses
7 Safeguards
IG1 3/7
IG2 7/7
IG3 7/7
CONTROL 11
Data Recovery
5 Safeguards
IG1 4/5
IG2 5/5
IG3 5/5
CONTROL 12
Network Infrastructure Management
8 Safeguards
IG1 1/8
IG2 7/8
IG3 8/8
CONTROL 13
Network Monitoring and Defense
11 Safeguards
IG1 0/11
IG2 6/11
IG3 11/11
CONTROL 14
Security Awareness and Skills Training
9 Safeguards
IG1 8/9
IG2 9/9
IG3 9/9
CONTROL 15
Service Provider Management
7 Safeguards
IG1 1/7
IG2 4/7
IG3 7/7
CONTROL 16
Applications Software Security
14 Safeguards
IG1 0/14
IG2 11/14
IG3 14/14
CONTROL 17
Incident Response Management
9 Safeguards
IG1 3/9
IG2 8/9
IG3 9/9
CONTROL 18
Penetration Testing
5 Safeguards
IG1 0/5
IG2 3/5
IG3 5/5

Controls and Safeguards

CONTROL 05 Account Management

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
5.1	**Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify	●	●	●
5.2	**Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Users	Protect	●	●	●
5.3	**Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Users	Respond	●	●	●
5.4	**Restrict Administrator Privileges to Dedicated Administrator Accounts** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	Users	Protect	●	●	●
5.5	**Establish and Maintain an Inventory of Service Accounts** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department	Users	Identify		●	●

semantic arts

Benchmarks

CIS Apple macOS 13.0 Ventura Benchmark

5.2.2 Ensure Password Minimum Length Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

A minimum password length is the fewest number of characters a password can contain to meet a system's requirements.

Ensure that a minimum of a 15-character password is part of the password policy on the computer.

Where the confidentiality of encrypted information in FileVault is more of a concern, requiring a longer password or passphrase may be sufficient rather than imposing additional complexity requirements that may be self-defeating.

Rationale:

Information systems that are not protected with strong password schemes including passwords of minimum length provide a greater opportunity for attackers to crack the password and gain access to the system.

Impact:

Short passwords can be easily attacked.

Audit:

Graphical Method:
Perform the following steps to ensure that the Password Account Threshold is set to greater than or equal to 15:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `Min Password Length` set to ≥ `15`

Remediation:

Terminal Method:
Run the following command to set the password length to greater than or equal to 15:

```
$ /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"minChars=<value≥15>"
```

example:

```
$ /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"minChars=15"
```

Profile Method:
Create or edit a configuration profile with the following information:

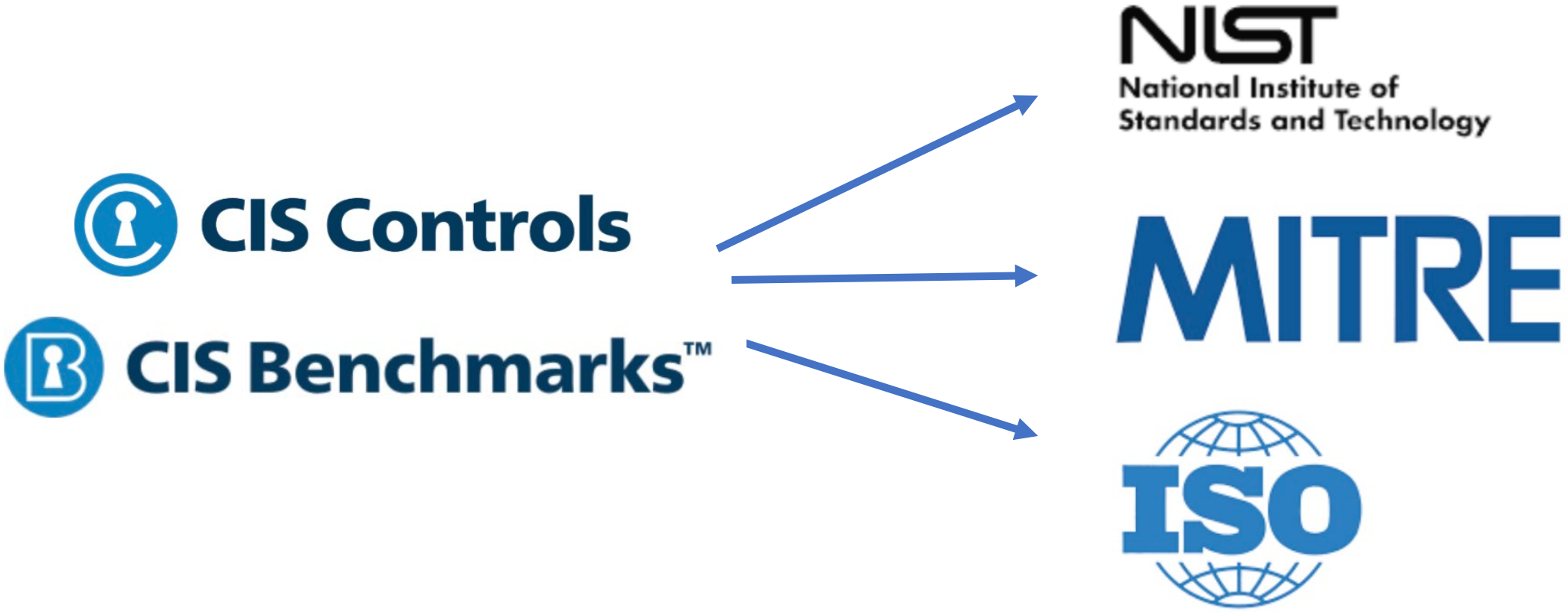
1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `minLength`
3. The key must be set to `<integer><value≥15></integer>`

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

CIS Controls:

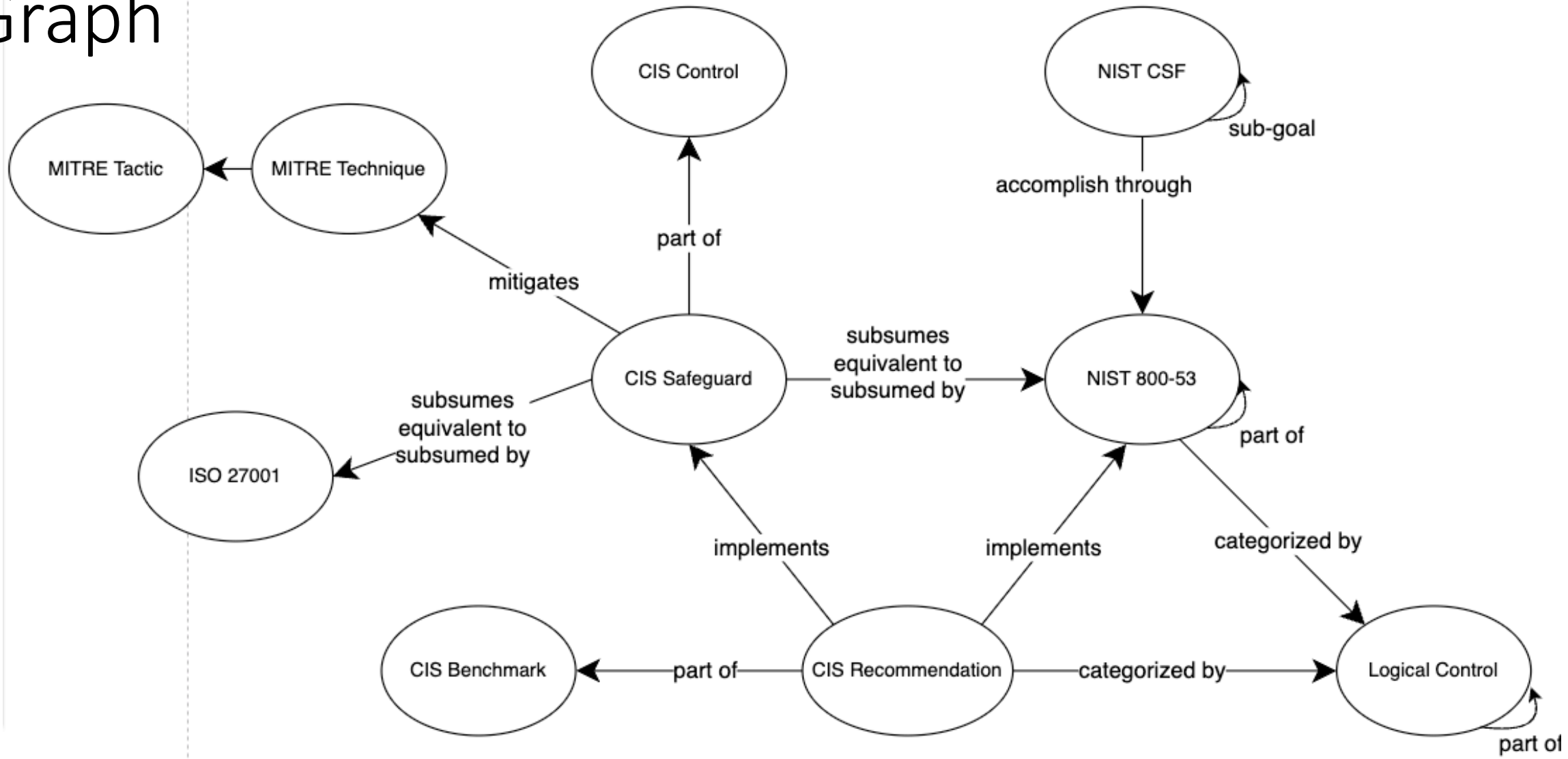
Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Mappings to External Frameworks



semantic arts

Knowledge Graph



Populating the Graph

csv file → transformation script → graph representation

Recommendation	800-53r5
1.1.1	IA-5(1)
1.1.2	IA-5(1)
1.1.3	IA-5(1)
1.1.4	IA-5(1)
1.1.5	IA-5(1)
1.1.6	IA-5(1)
1.1.7	IA-5(1), SC-28, SC-28(1)

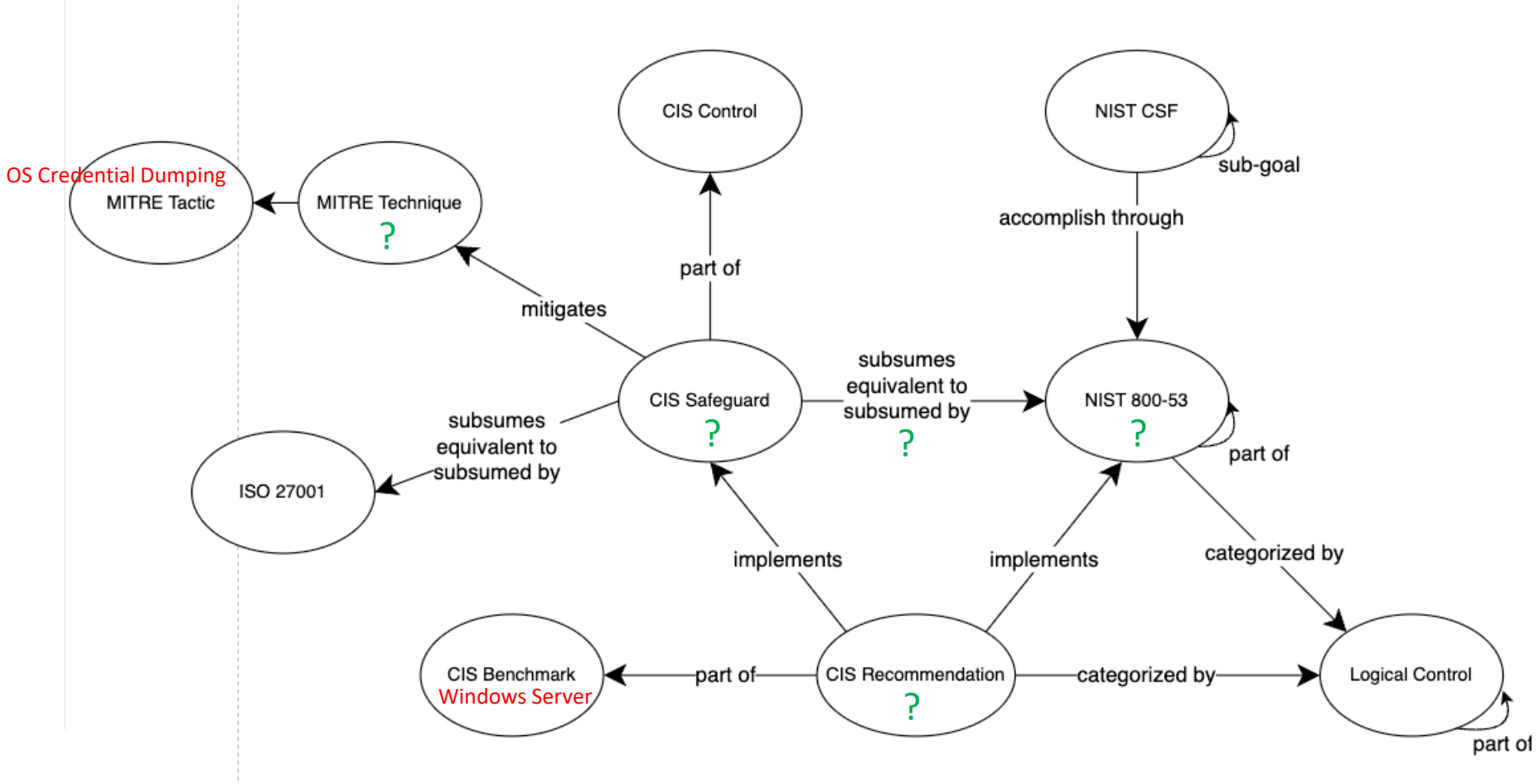
```
CONSTRUCT {

  ?recommendation cis:implements ?control .
}
WHERE {
  SERVICE <system-states-800-53-bins.csv> {
    [] xyz:Recommendation ?recommendation ;
       xyz:800-53r5 ?control ;
     .
    }
}
```

```
cis:471892  cis:implements  nist:IA-5.1 .

cis:471893  cis:implements  nist:IA-5.1 .

cis:471894  cis:implements  nist:IA-5.1 .

cis:471895  cis:implements  nist:IA-5.1 .

cis:471896 cis:implements  nist:IA-5.1 .

cis:471897 cis:implements  nist:IA-5.1 .

cis:471898  cis:implements  nist:IA-5.1, nist:SC-28, nist:SC-28.1.
```

semantic arts

Querying the Graph

Which Windows Server recommendations help to mitigate OS Credential Dumping?



semantic arts

Current and future work

- Meaningful stable IDs and resolvable URIs
- Mapping UI powered by the knowledge graph
- Automating mapping process

semantic arts