WARNING!!!

The following presentation displays an unsettling addiction to the Power Platform and the MCU Avengers

Viewer discretion is advised
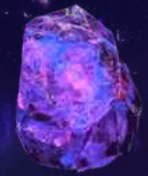
Power Platform Avengers

The Infinity Stones of Security

Security Concepts

- Users
- Business Units
- Teams
- Security Roles
- Record Ownership
- Hierarchy Models
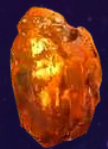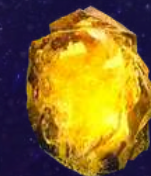
Environment Security Groups

Entra ID Security Groups

Security group for developers

Security group for testers

Security group for end users

Development Environment

Testing Environment

Production Environment

AAD Users

AAD Users

AAD Users
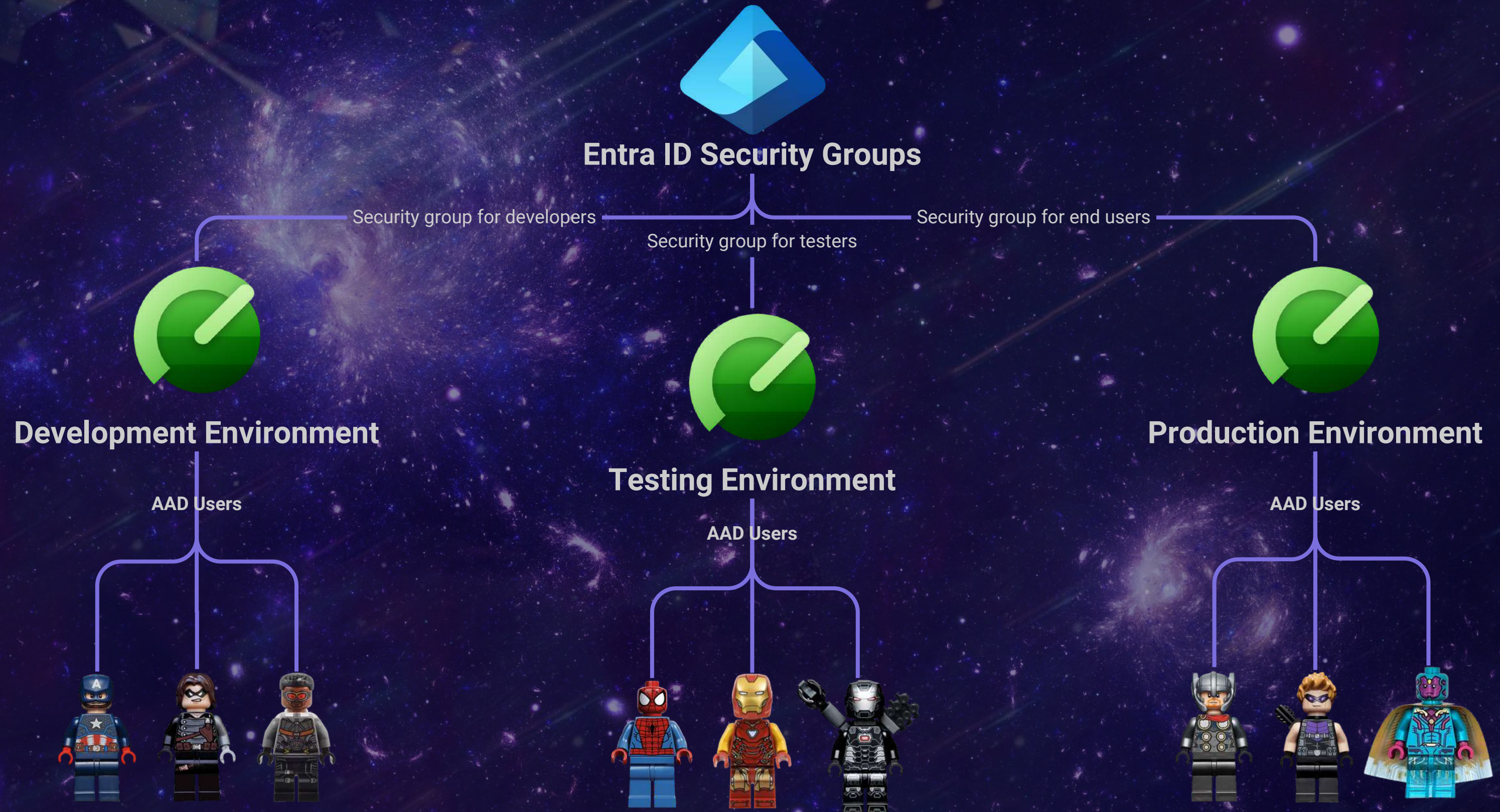
Force Sync User

When a group member is added or removed

* Group Id

Apply to each

* Select an output from previous steps

body ✕

Force Sync user

* Environment

The Avengers

* ObjectId

User Id ✕

Show advanced options ⌄

⊤ Add an action

Entra ID Security Groups **+** **New user**

Trigger Force Sync User action

Add users to environment

BUSINESS UNITS

MCU

Midgard

Heroes
Weapons
Threats

Asgard

Heroes
Weapons
Threats

The Dynasty

Heroes
Weapons
Threats
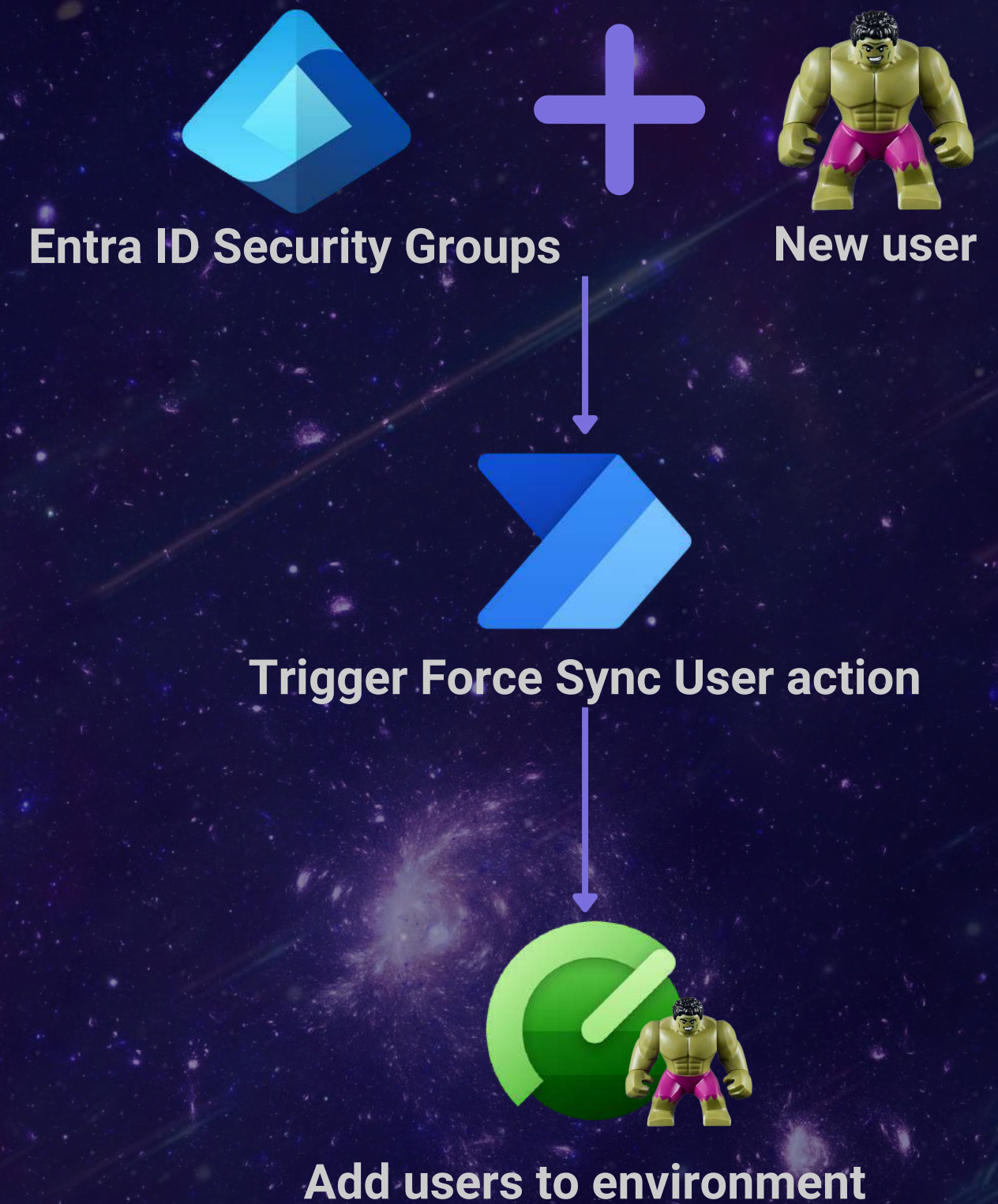
Business Units

MCU
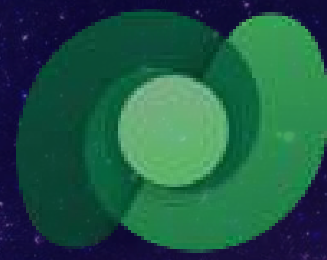
Midgard   **Asgard**   **The Dynasty**

Midgard
Heroes
Weapons
Threats

Asgard
Heroes
Weapons
Threats

The Dynasty
Heroes
Weapons
Threats

Teams

Owner Team

Owns records created by users assigned to that team and thus has full privilege rights to its owned records. Members can inherit the security role assigned to an owner team

Access Team

Will not own any records its members create but rather allow its members to share records with the team, which then allows other members to have read, write, and append privileges. Members are dependant on their own security roles.

Entra Security Team

Driven by Entra ID Security Groups or Entra Office Groups. When an Entra group team is associated with either a security group or office group, the security group or office group controls member access.

Teams-Owner

Owner Team
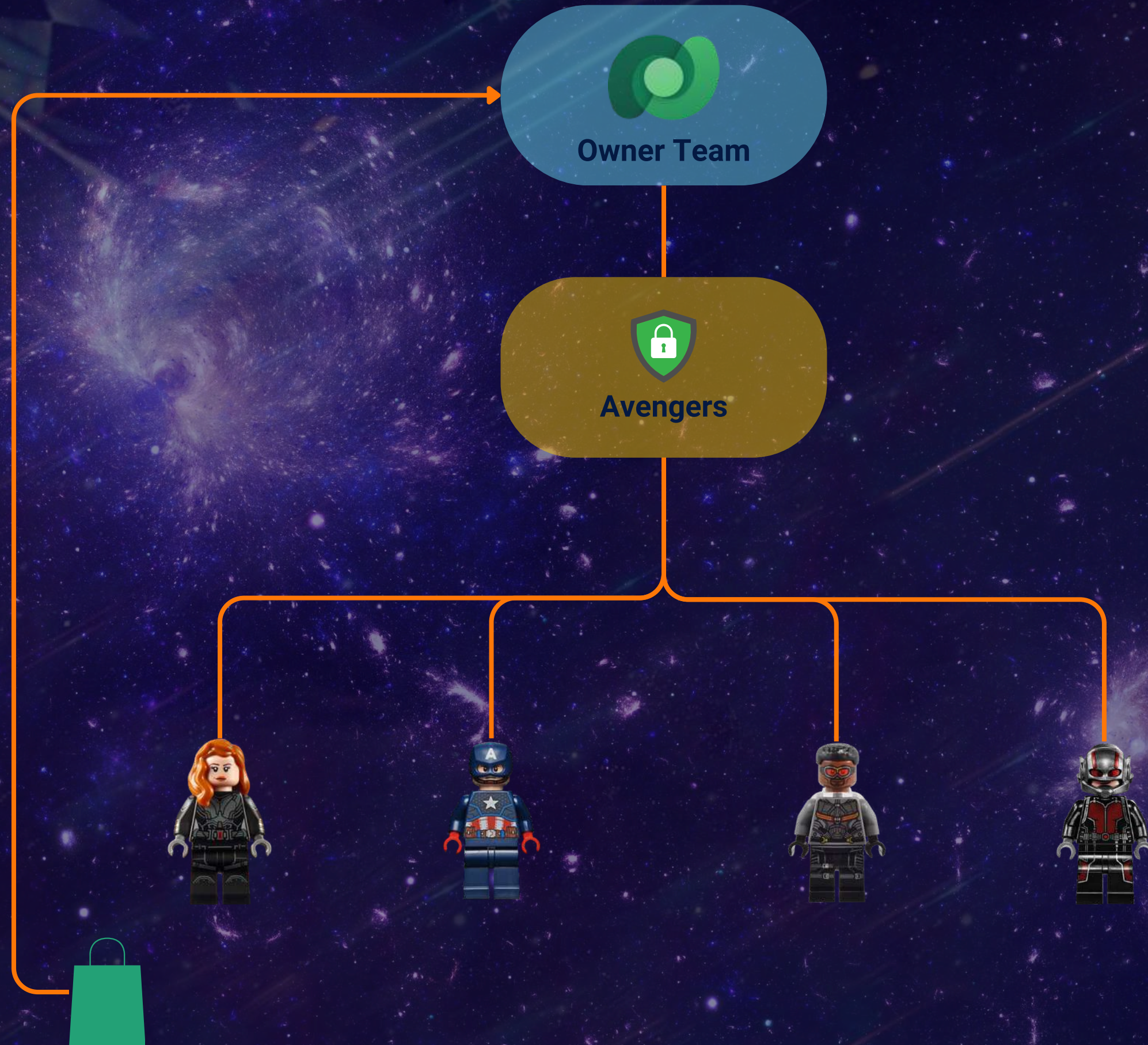
Avengers
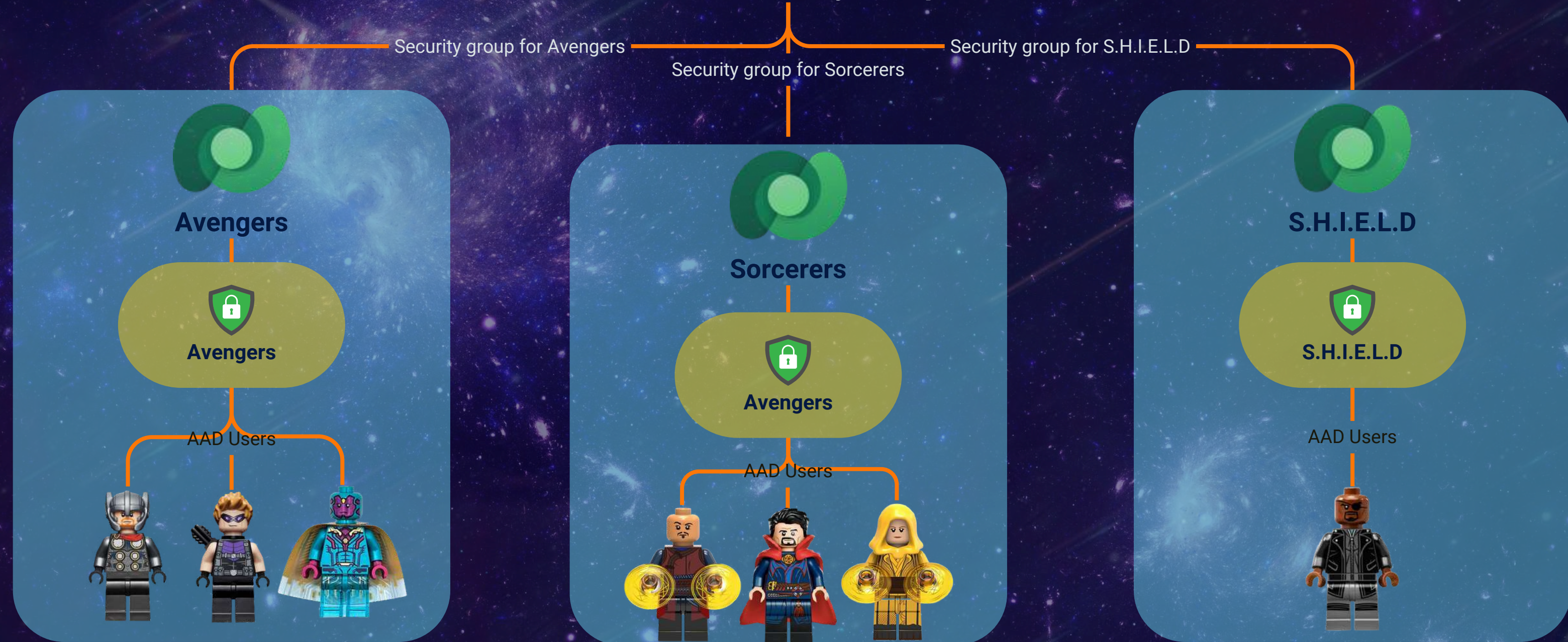
Security Roles

ROLES	CANVAS APPS	CLOUD FLOWS	CONNECTORS	GATEWAYS DATAFLOWS	DATAVERSE	MODEL-DRIVEN APP	SOLUTION FRAMEWORK	AI BUILDER
Environment Maker	✔	✔	✔	✔		✔	✔	
Environment Admin	✔	✔	✔	✔				
System Customiser	✔	✔	✔		✔	✔	✔	✔
System Admin	✔	✔	✔	✔	✔	✔	✔	✔

Principle of Least Privilege - PoLP

- Limit user access to the minimum necessary.
- Grant minimal permissions for specific tasks.
- Group privileges into layers.
- Implement granular release layers.

Principle of Least Privilege - PoLP

Hero Security Role

TABLES	CREATE	READ	WRITE	DELETE	APPEND	APPEND TO	ASSIGN	SHARE
Heroes	None	Organisation	None	None	Business Unit	Business Unit	None	None
Weapons	User	User	User	User	User	User	User	User
Threats	Business Unit	Business Unit	Business Unit	None	Business Unit	Business Unit	None	None
Ships	Organisation	Organisation	Organisation	Organisation	Organisation	Organisation	Organisation	Organisation

Role Privileges

- Organisation
- Parent : Child Business Unit
- Business Unit
- User
- None

Security Role-Threats

Midgard

Avenger Captain

Avenger

Avenger

Avenger

Asgard

Realm God

Andromeda

Guardian of the Galaxy Captain

Guardian of the Galaxy

Guardian of the Galaxy

Guardian of the Galaxy

Hero Security Role

TABLES	CREATE	READ	WRITE	DELETE	APPEND	APPEND TO	ASSIGN	SHARE
Heroes	None	Organisation	None	None	Business Unit	Business Unit	None	None
Weapons	User	User	User	User	User	User	User	User
Threats	Business Unit	Business Unit	Business Unit	None	Business Unit	Business Unit	None	None
Ships	Organisation	Organisation	Organisation	Organisation	Organisation	Organisation	Organisation	Organisation

Role Privileges

- 🟢 ORGANISATION
- 🟢 (with triangle) PARENT : CHILD BUSINESS UNIT
- 🟡 BUSINESS UNIT
- 🟡 (quartered) USER
- ⭕ NONE

Security Role - Weapons

Midgard

Asgard

Andromeda

Avenger Captain

Realm God

Guardian of the Galaxy Captain

Avenger

Avenger

Avenger

Guardian of the Galaxy

Guardian of the Galaxy

Guardian of the Galaxy

Security Role - Weapons

Midgard

Asgard

Andromeda

Avenger Captain

Realm God

Guardian of the Galaxy Captain

Avenger

Avenger

Avenger

Guardian of the Galaxy

Guardian of the Galaxy

Guardian of the Galaxy

S.H.I.E.L.D Security Role

TABLES	CREATE	READ	WRITE	DELETE	APPEND	APPEND TO	ASSIGN	SHARE
Heroes	🟢	🟢	🟢	🟢	🟢	🟢	🟢	⭕
Weapons	⭕	⭕	⭕	⭕	⭕	⭕	⭕	⭕
Threats	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Ships	◓	◓	◓	◓	◓	◓	◓	◓

Role Privileges

🟢 ORGANISATION ◓ PARENT : CHILD BUSINESS UNIT ◑ BUSINESS UNIT ◔ USER ⭕ NONE

TRIPLE THREAT

Entra ID Security Groups

Security group for Avengers Team

MCU

Avengers

Midgard

The Dynasty

Andromeda

Hierarchy Models

- **Configured per environment**
- **Not AAD driven**
- **Set access depth**
- **Aligned with selected table**
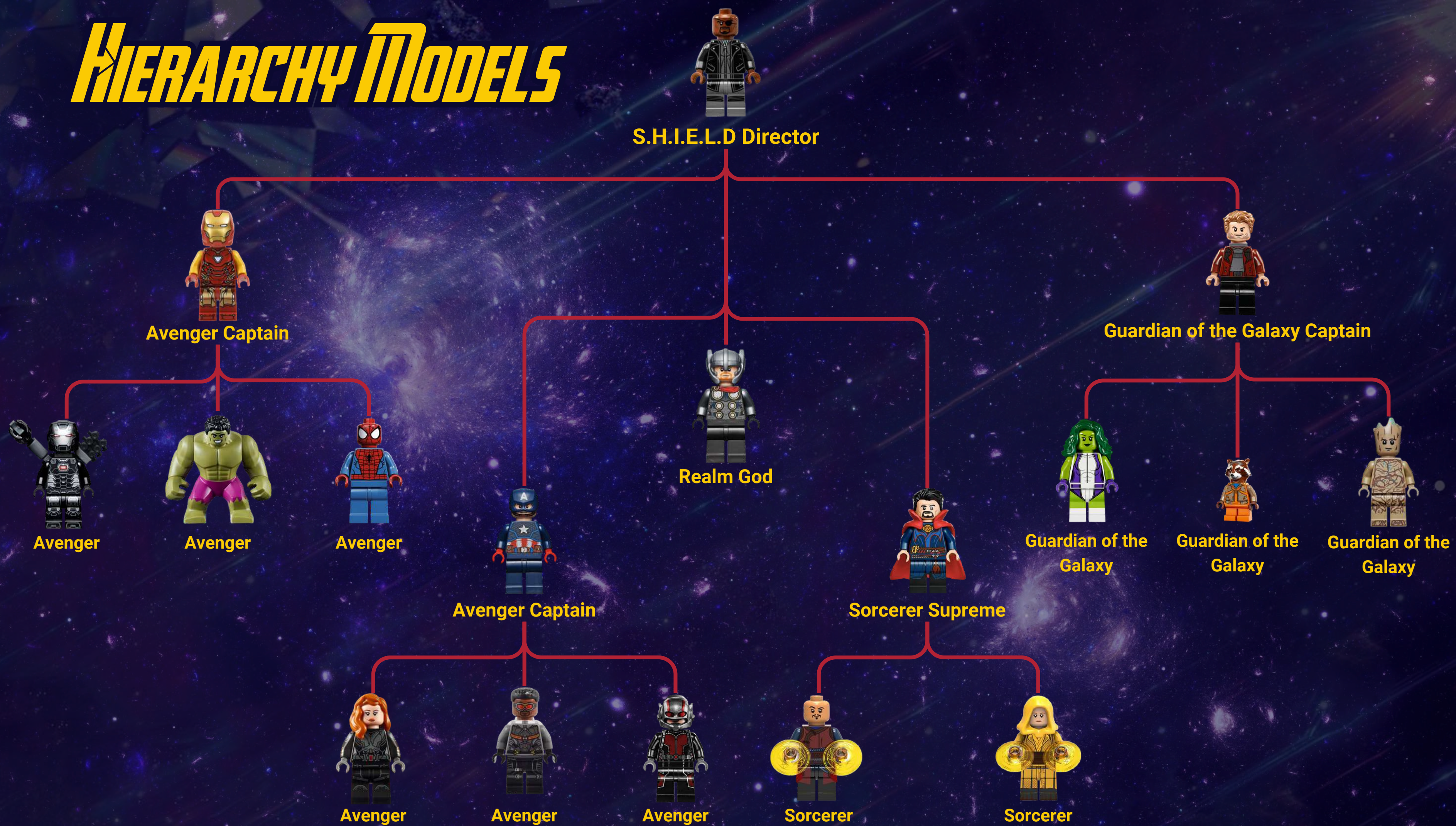
HIERARCHY MODELS

Manager

- **Users assigned manager**
- **Based on Users table**

Position

- **Configure positions**
- **Users assigned to position**
- **Based on Users table and Position table**

HIERARCHY MODELS

S.H.I.E.L.D Director

Avenger Captain

Guardian of the Galaxy Captain

Avenger

Avenger

Avenger

Realm God

Avenger Captain

Sorcerer Supreme

Guardian of the Galaxy

Guardian of the Galaxy

Guardian of the Galaxy

Avenger

Avenger

Avenger

Sorcerer

Sorcerer

Position Hierarchy Model

S.H.I.E.L.D Director

S.H.I.E.L.D Director

Avengers Captain

Avenger Captain

Avenger Captain

Avengers

Avenger

Avenger

Avenger

Avenger

Avenger

Avenger

The End Game

RBAC's Model

USERS	ENTRA ID SECURITY GROUPS	TEAMS + SECURITY ROLES	BUSINESS UNITS	HIERARCHY MODEL
	Avengers	Avengers	Midgard	Manager
	Sorcerers	Sorcerers	The Dynasty	Avengers
	Guardians	Guardians	Andromeda	
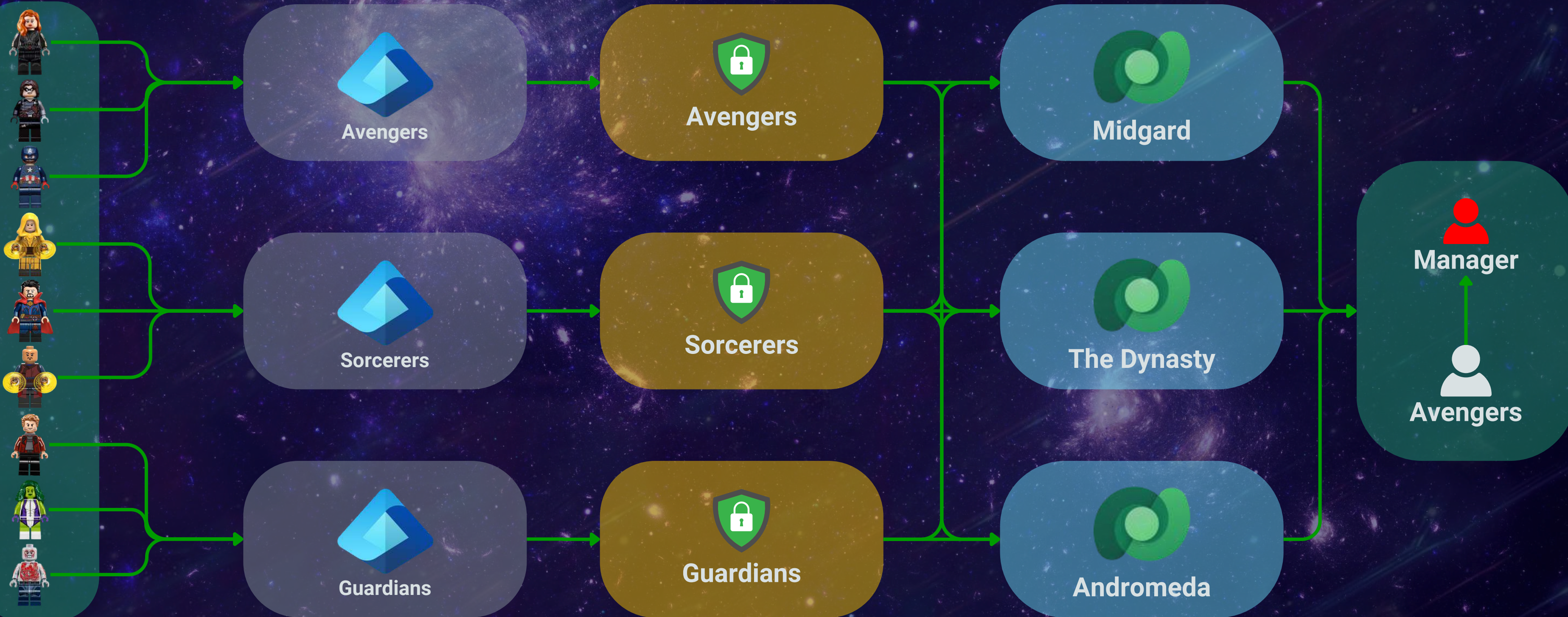
RBAC's Model

Avengers Security Role

User-level read access SR

User-level read access SR

Record Owner: User-level read access SR

MIDGARD

THE DYNASTY

ANDROMEDA

Summary

In realms where data flows, secure and strong,
Business Units guard us all day long.
Security Roles define what each can see,
Dataverse Teams work in harmony.
Hierarchy Models pass power down,
Ensuring data's safe, without a frown.

Nathan Rose
#ChallengeAccepted