~~access cer~~

identity over entitled users.

→ Role-mining

→ Unusual activity

→ User Entity behavioral analytics

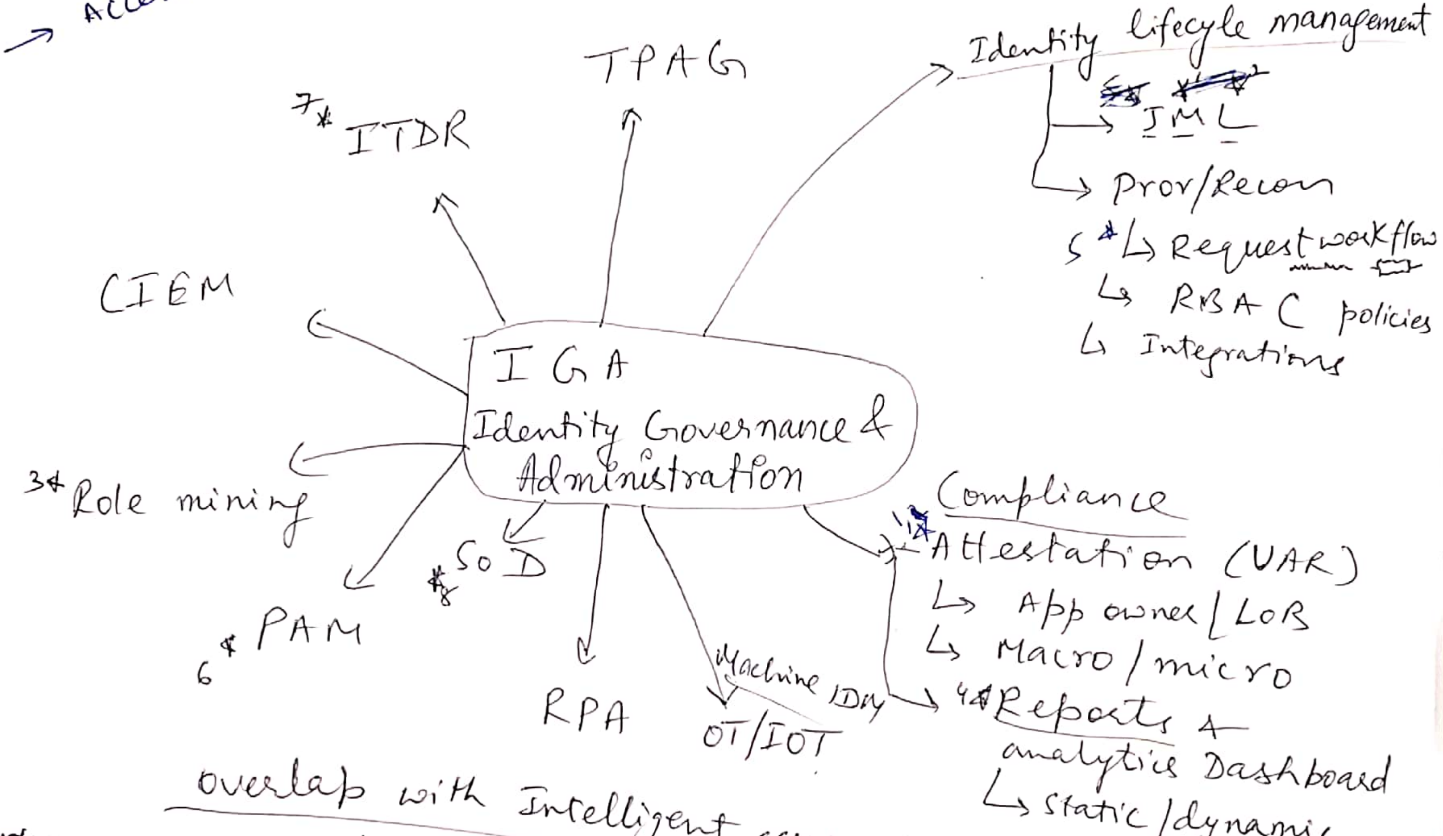
→ Access recomendation

SBOM

Dev Ops

Cloud data security + Governance

Secrete Management



IGA
Identity Governance & Administration

Identity lifecyle management
- ~~5* 1*~~ JML
- Prov/Recon
- 5* Request workflow
- RBAC policies
- Integrations

TPAG

7* ITDR

CIEM

3* Role mining

6* PAM

8* SoD

RPA

Machine IDM

OT/IOT

Compliance

1* Attestation (UAR)
- App owner / LoB
- Macro / micro

4* Reports + analytics Dashboard
- static / dynamic

overlap with Intelligent access Governance?

* ~~A~~ML usecases

1) Contageous situation due to accrued entitlements (bottom-up approach), ML + ongoing, Anomaly / outlier detection at user level & IGA role level, hypothesis of whether a role is relevant for a job position or entitlement to role connection (obsolescense).

~~2)~~ 2) ML based automation for access removal, ongoing process for leavers + ML, identify dormant accounts, orphan accounts

3) Role mining [Top down approach can miss over entitlement, iterations of ML based bottom-up, access certification, and then top down] [peer groups)

4) Threat detection → Identity defn unusual changes, access polibies, Role defn
- Misuse of access [~~ov~~ exfiltration]
- obsolete entitlement

Recomendations, Risk score

5) Recomendations ~~of~~ on access requests [what does the user need?]

6) ML on Privileged access (assignment, usage, dormant)

7) Anomaly detection [Identity definition - SOD policies, Role defns ... under threat] Cloud IAM policies

8) Based on historical data (frauds), recomendation while SOD policy creation.

TODO: Can access data be used to ~~ide~~ catch SOD violation? Rule versus ML?