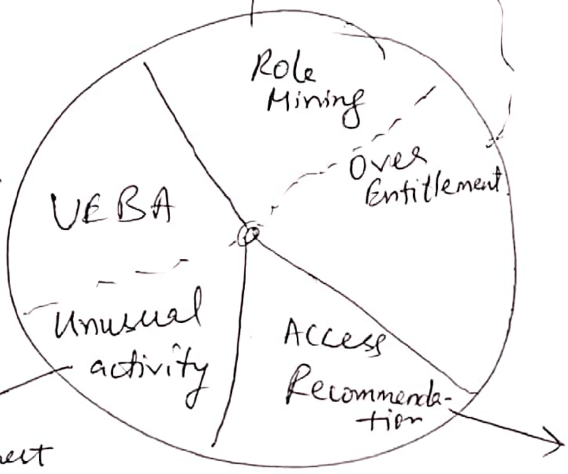
Periodic activity

Iterations of unsupervised learning + Human

Identify similar Users, density clusters

→ Graph, Cluster, use edges to identify over-ent nodes

SIEM + UEBA



IsolationForest
LOF
Gaussian Mixtures clusters or MCD
PCA
[One-class svm for select cases]

→ hybrid
~~Content based & collaborative~~
Rule based, contextual access
Radomforest /gradientbos
feedback from access reviews & user decisions
underentitled

Use cases

UEBA/ Unusual ITDR

- → Identity outlier/anomalous Changes in identity defn.
- → User behavior (loginfreq/volume/location/geovelocity/ peer / user agent usual activity)
- → Anomalous sequence
- → Risk scoring [dashboard with dynamic control on further profiling for riskiest]
- → Anomaly in any entity behavior
- → Risk scoring for users, accounts, access, workload
- → Request approval mapped to UEBA results/summary
- → Micro certification campaign