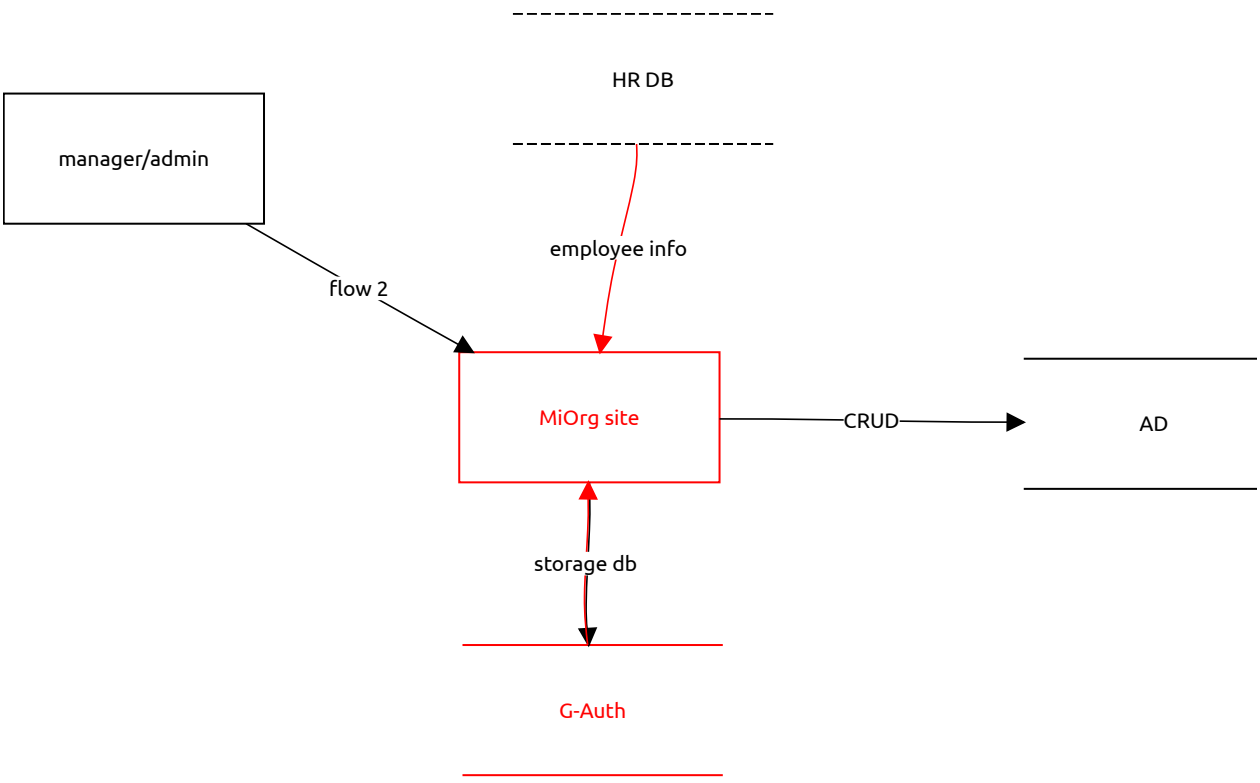
Threat model report for MiOrg-

Owner:
Dileep Gurazada
Reviewer:
Josh
Contributors:

High level system description

Application is used for managing an employee lifecycle

Infrastructure/backend data flow- MiOrg



manager/admin (External Actor)

No threats listed.

MiOrg site (External Actor)

sensitive data leakage

Information disclosure, Open, High Severity

Description:
Service account to talk to AD is in github config file encrypted. easy to decrypt as many knows the endpoint and have access.
Mitigation:
Remove the account credentials and save it in server env variable till Vault is used

possible elevated privilige account

Elevation of privilege, Open, Medium Severity

Description:
Whether the service account to talk to AD is of least privilege or not
Mitigation:
identify right account and provision it to App. service account type 'Account operator', Members of this group can create and modify most types of accounts, including those of users, local groups, and global groups, and members can log in locally to domain controllers

possible access to different role in CAS and Ops portal

Elevation of privilege, Open, Low Severity

Description:
User roles can be replicated from employees, cant be sure as each domain has multiple users with different roles based on their daily work. Multiple roles are allowed to access MiOrg Including Directors so for an employee they can choose manager access instead of regular previlige.
Mitigation:
Atleast audit should be happening continuously. We have logs being stored in Miorg db.

flow 2 (Data Flow)

No threats listed.

G-Auth (Data Store)

sensitive information

Information disclosure, Open, Low Severity

Description:
Database has encrypted password of new employee
Mitigation:
passwords are encrypted AES 256.

(Data Flow)

No threats listed.

storage db (Data Flow)

Can have encrypted password during transit

Information disclosure, Open, Low Severity

Description:
miorg app to DB is on http. It is low because non of our apps does encrypt the traffic to DB.
Mitigation:
https

employee info (Data Flow)

Probable PII

Information disclosure, Open, Low Severity

Description:
Employee info is gathered from HR DB and moved to Gauth DB
Mitigation:
encrypt PII in rest?

AD (Data Store)

No threats listed.

CRUD (Data Flow)

No threats listed.

HR DB (out of scope Data Store)

Out of scope reason:
not a miorg entity