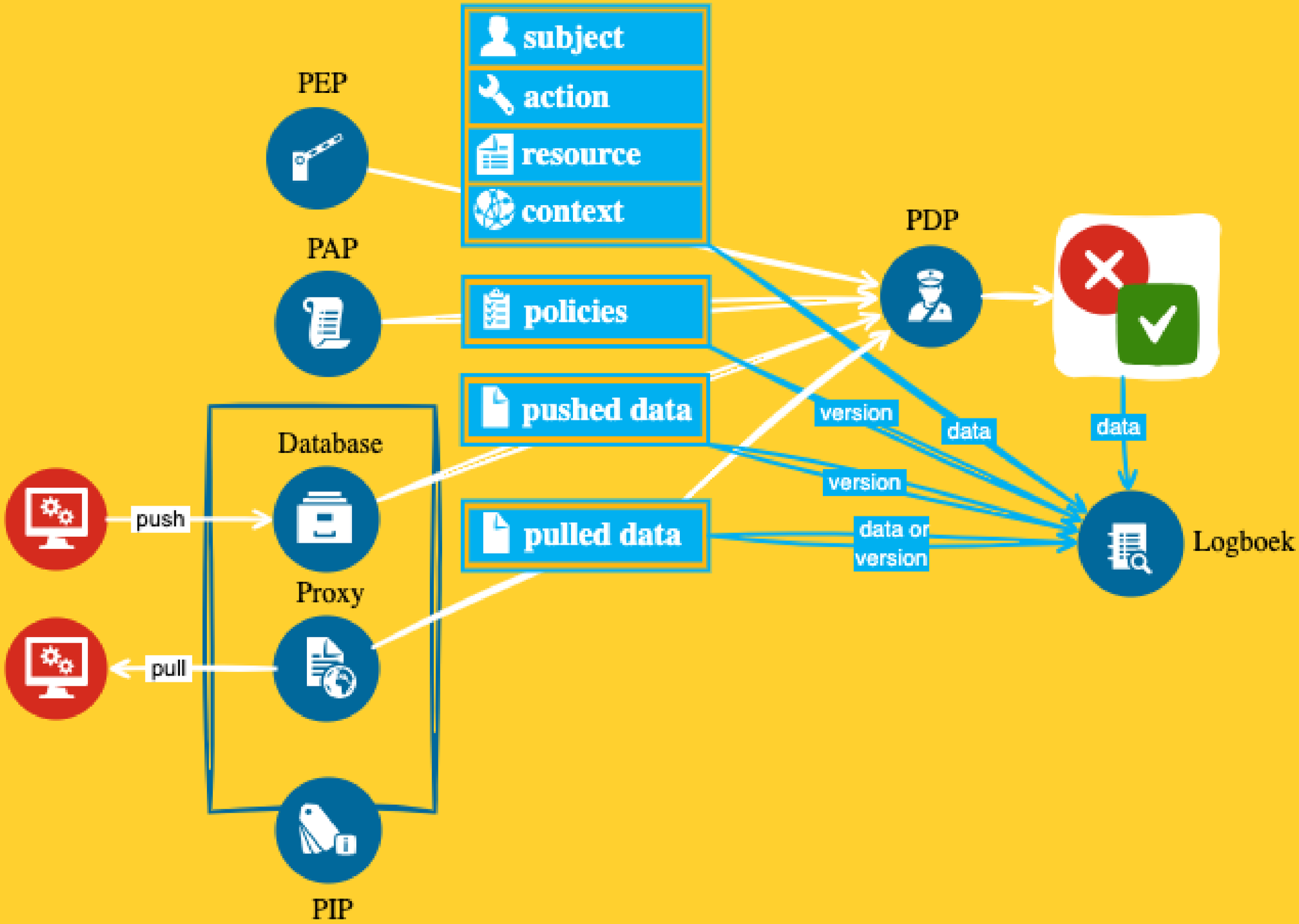
PEP
PAP
Database
subject
action
resource
context
policies
pushed data
pulled data
PDP
version
data
data
version
data or
version
Logboek
push
pull
Proxy
PIP

inzicht in logboek zal vaak juridisch bepaald zijn

richtlijnen over toegang voor SIEM/SOC

Definieren aan welke informatie-behoefte het logboek moet voldoen

hoe kunnen we betrouwbare bronnen gebruiken om duplicatie te voorkomen?

Wat ga je loggen voor welk doel (en welke doelgroep)

Moet de functionele grondslag ook worden vastgelegd. Of zit dit in de relaties? Bijvoorbeeld de policy

Toegang tot het logboek moet/mag/kan zelf ook weer achter een PEP

hoe gaan we om met aggregaties van het logboek (calls per type per dag)

Is er externe informatiebehoefte (en welke) door anderen/derden dan door de organisatie die de policiebeslissingen uitvoert.

hergebruik van huidige API's mogelijk?

Duidelijke scheiding van data log, applicatie log en toegangslog

Sterke afhankelijkheid en relatie met Logboek Dataverwerkingen maken

Relatie met FSC transactie log vastleggen

Verplichting van gebruik Logboek Toegangs-verzoeken (is opt-out mogelijk?)

logboek minder gevoelig maken door die buiten het log te laten (met eigen retention policies)

MVP: wat is het kleinste nuttige logboek

Hoe worden logboeken gecentraliseerd (en in welke mate)

Exporteer baarheid Logboek

Hoe maken we dit niet te zwaar?

Correlatie tussen logboek toegangsverzoek en van afnemer en aanbieder

Verschil / onderscheid tussen logboek toegangsverzoek en afnemer en aanbieder

Vastleggen van toegepaste Policy engine (versie)

Niet alleen een versie van de policy vastleggen, maar bijvoorbeeld ook een hash

Misschien zelfs certificeren van engines?

versie van de PxP's

alle version/identifier opnemen en bijv. in WARC definieren

Wie mag wat zien in het logboek en handelen we dit af (toegangsverlening)

De context encrypted opslaan

Sticky stack