Geprivilegieerd Toegangsbeheer

PAM as a Service: PAMaaS

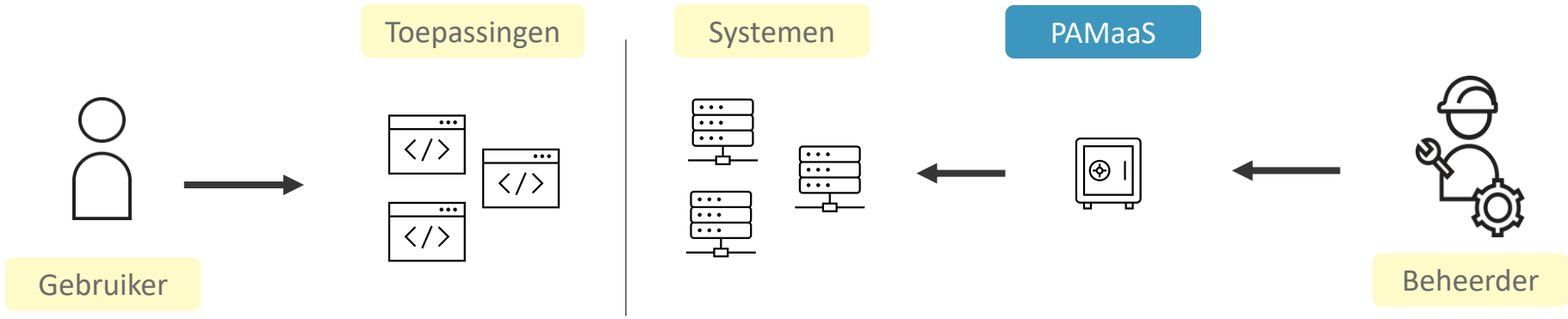
DIGITAAL VLAANDEREN

Vlaamse overheid

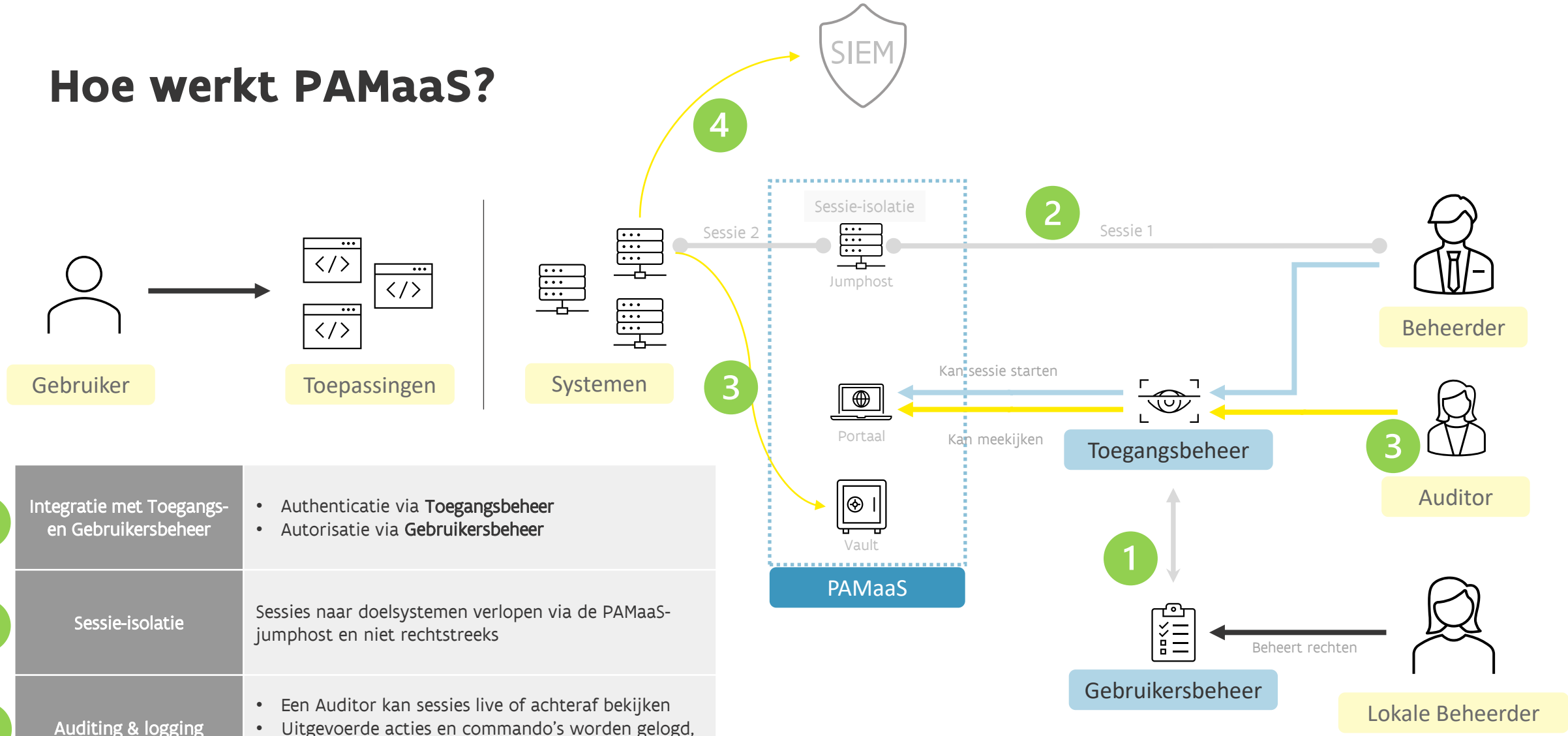
Wat is het Geprivilegieerd Toegangsbeheer (PAMAAS)?

Het Geprivilegieerd Toegangsbeheer is de bouwsteen voor de **controle** over de **beheerderstoegangen** tot je ICT-infrastructuur en/of toepassing.

Centraal beheer van logingegevens	De wachtwoorden en toegangssleutels worden **centraal** beheerd, automatisch periodiek **geroteerd** volgens het Toegangsbeleid, en eindgebruikers krijgen deze niet te zien.
Authenticatie en autorisatie	Gebruikers moeten **geauthentiseerd** en **geautoriseerd** zijn alvorens men geprivilegieerde accounts kan gebruiken.
Gemotiveerde toegang	Gevoelige toegang moet **gemotiveerd** worden via een change management proces.
Goedkeuring voor toegang	Uw organisatie behoudt de **controle** over *wie*, *wat*, en *wanneer*.
Sessieopname	Gebruikerssessies kunnen worden **opgenomen** voor auditing.



Hoe werkt PAMaaS?

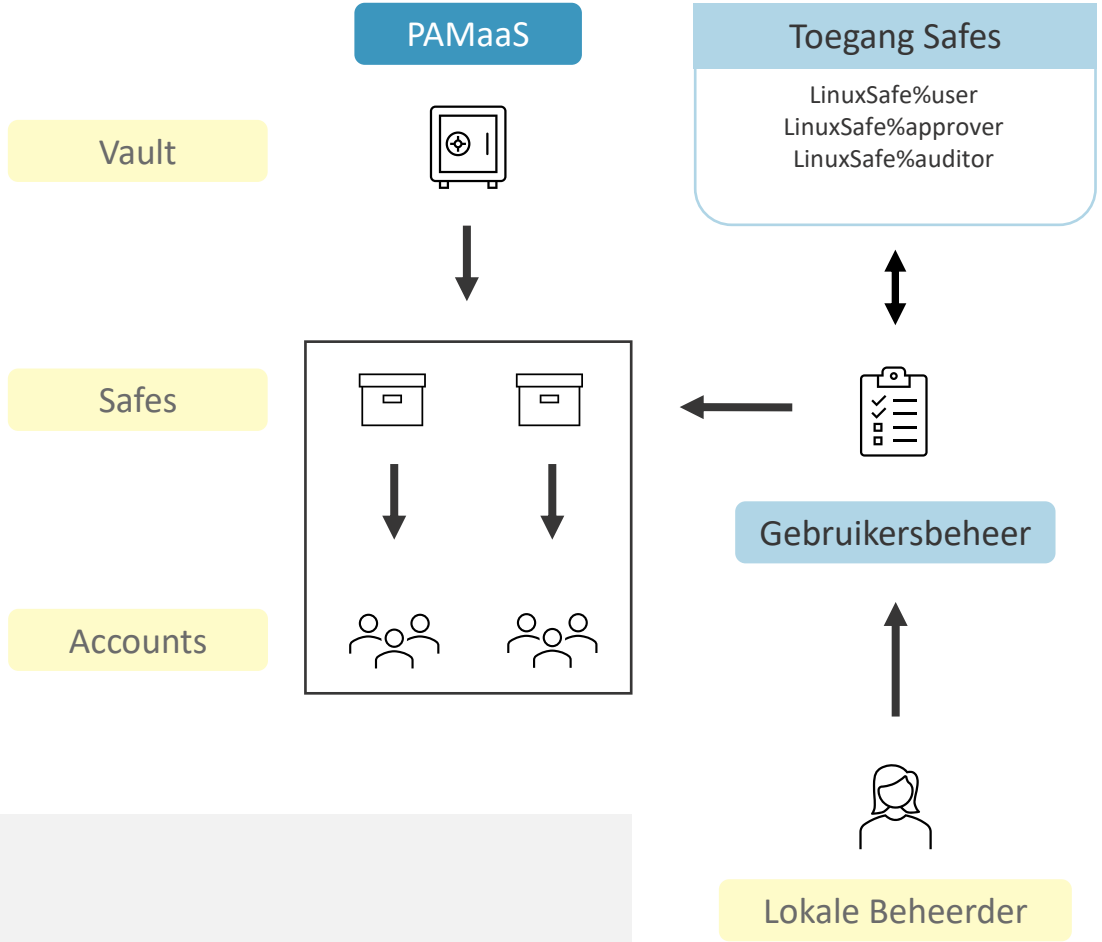


1	Integratie met Toegangs- en Gebruikersbeheer	• Authenticatie via **Toegangsbeheer** • Autorisatie via **Gebruikersbeheer**
2	Sessie-isolatie	Sessies naar doelsystemen verlopen via de PAMaaS-jumphost en niet rechtstreeks
3	Auditing & logging	• Een Auditor kan sessies live of achteraf bekijken • Uitgevoerde acties en commando's worden gelogd, en logs worden opgeslagen in de Vault.
4	SIEM-integratie	Het is mogelijk om de doelsystemen te integreren met de SIEM-oplossing, afhankelijk van het Toegangsbeleid. Meer informatie daarover vind je in de sectie rond *Rapportering en SIEM*.

Safes en rollen

Safes en rollen

- PAMaaS bewaart de wachtwoorden van geprivilegieerde accounts in een **centrale Vault**
- Deze Vault is onderverdeeld in verschillende **Safes** waarin de accounts opgeslagen worden.
- Hoe krijg je **toegang** tot een safe?
  - De toegang wordt altijd beheerd via het **Gebruikersbeheer**.
  - Gebruikers krijgen in het Gebruikersbeheer het PAMaaS-recht toegekend samen met een “context”, een combinatie van een Safenaam en een Rol.

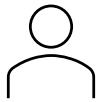


Voorbeeld

Situatie: een persoon krijgt in het Gebruikersbeheer het PAMaaS-recht met context *LinuxSafe%User* :

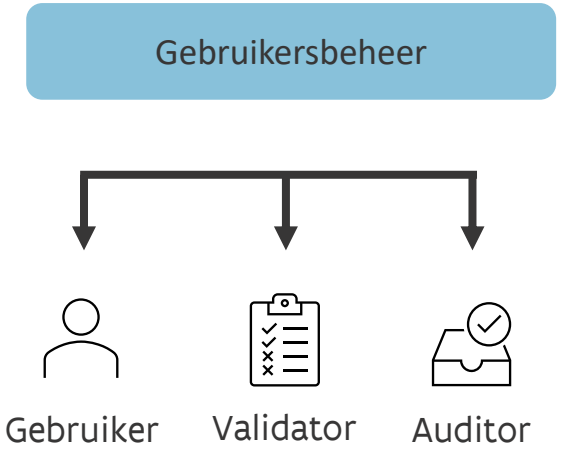
Resultaat: deze gebruiker krijgt **toegang** tot de safe *LinuxSafe* en zal de accounts in de safe kunnen **gebruiken** door ermee aan te melden.

Welke rollen bestaan er?

 Gebruiker *User*	Een **Gebruiker** kan geprivilegieerde accounts gebruiken door er een sessie mee te starten.
 Validator *Approver*	Een **Validator** kan toegangen die een Gebruiker aanvraagt goed- of afkeuren.
 Auditor *Auditor*	Een **Auditor** heeft inzage in de logs en opnames van de sessies van Gebruikers, en kan deze live of achteraf raadplegen.

Rollen <-> Toegangsbeleid

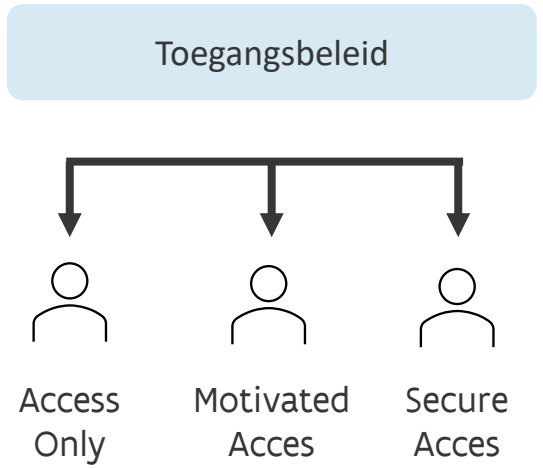
De rollen: “Gebruiker, Validator en Auditor” worden toegewezen via het Gebruikersbeheer.



Hoe de “Gebruiker” toegang heeft tot een geprivilegieerd account wordt bepaald via het toegangsbeleid.

Tijdens het onboardingsproces bepaal je de soorten toegangen die er mogelijk zijn tot je geprivilegieerde accounts.

Meer informatie volgt in de sectie rond *Toegangsbeleid*



Toegangsbeleid

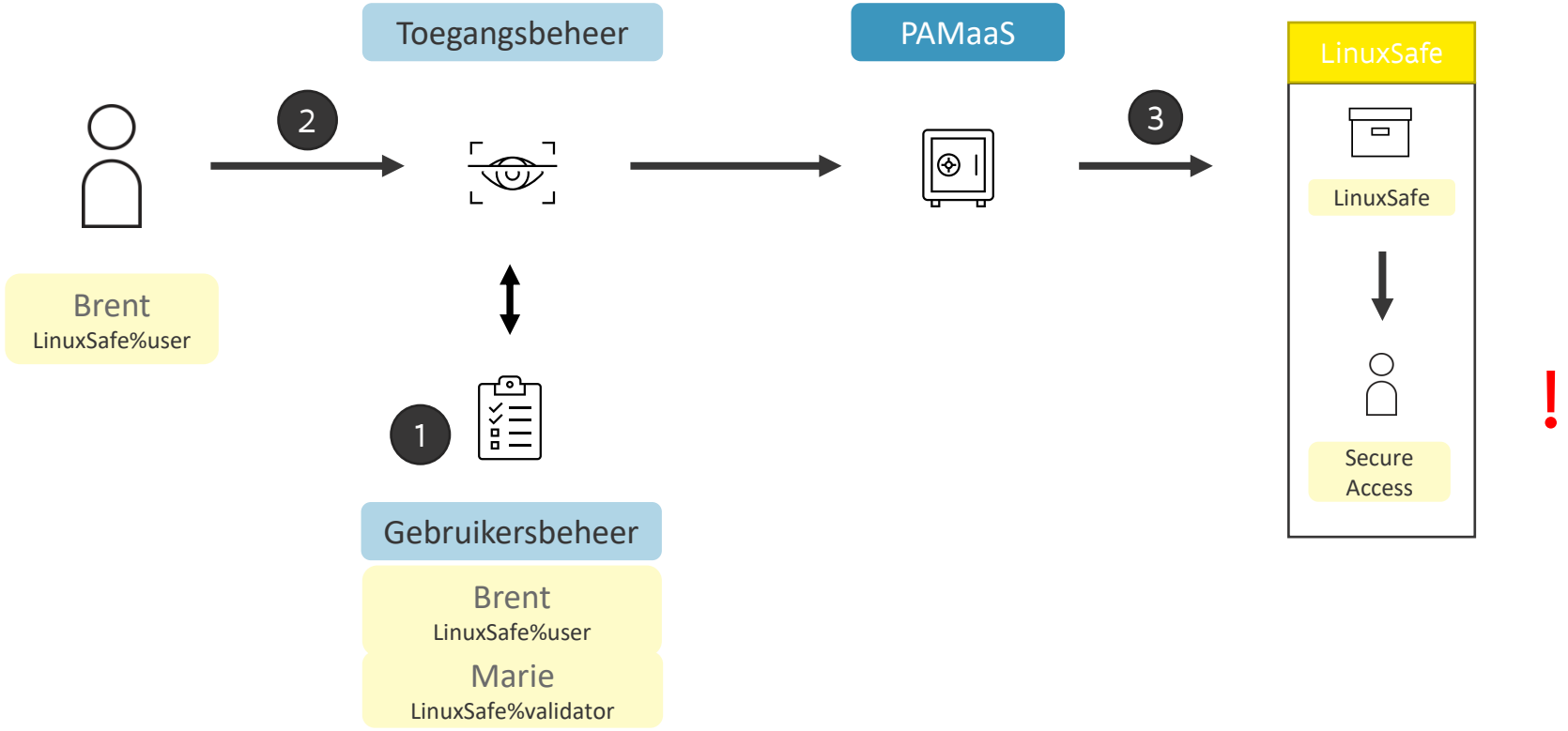
Toegangsbeleid om accounts te beveiligen

Met PAMaaS kan je accounts beveiligen op basis van drie niveaus die we het **Toegangsbeleid** noemen. Deze zorgen voor een toenemende **mate van controle** een account.

Toegangsbeleid	Reden voor toegang	Changenummer ingeven	Sessieopname	SIEM-integratie	Toegang beperkt in tijd	Goedkeuring nodig?*
Access Only	✓	✗	✗	✗	✗	✗
Motivated Access	✓	✓	✓	✓	✗	✗
Secure Access	✓	✓	✓	✓	✓	✓

* De gebruiker krijgt pas toegang na goedkeuring door een validator

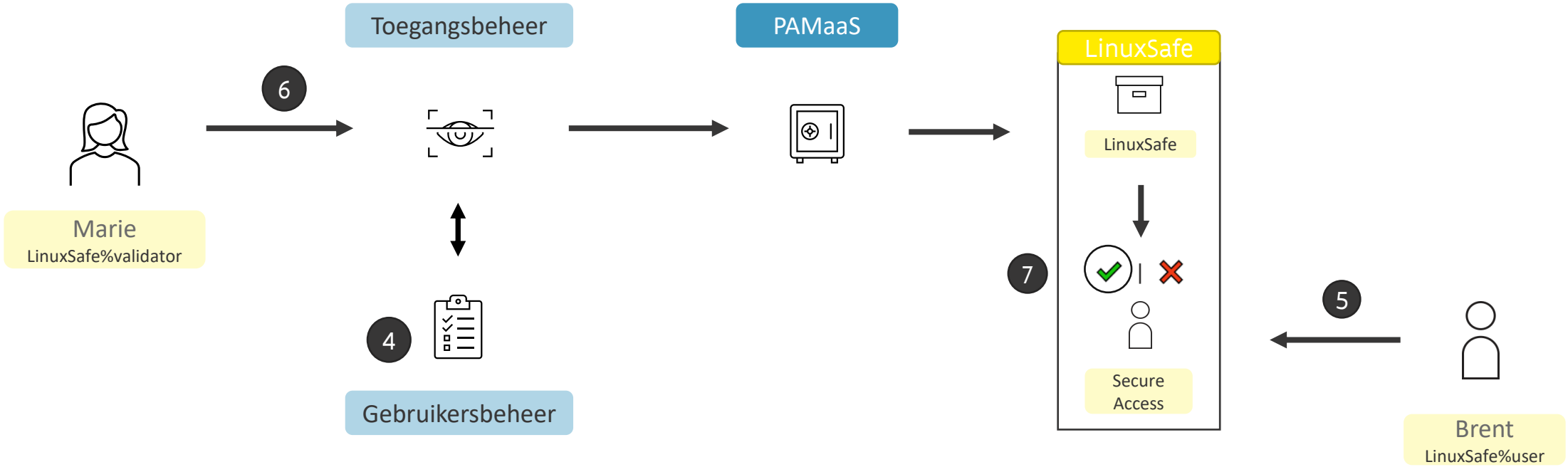
Goedkeuringsproces bij het “Secure Access” Toegangsbeleid



1. De gebruiker **Brent** heeft via het Gebruikersbeheer door zijn Lokale Beheerder het PAMaaS-recht met context LinuxSafe%User gekregen.
2. Brent **meldt aan** op het PAMaaS-portaal via het Toegangsbeheer.
3. Eenmaal aangemeld kan Brent een sessie starten om zo de accounts in de ‘LinuxSafe’ te gebruiken.

! MAAR: voor accounts met Toegangsbeleid Secure Access moet de sessie eerst **goedgekeurd** worden.

Goedkeuringsproces bij het “Secure Access” Toegangsbeleid



4. Marie is geautoriseerd als Validator in de LinuxSafe door de Lokale Beheerder
5. Wanneer Brent als gebruiker een **aanvraag** indient om een sessie te starten zal Marie als Validator een **melding** krijgen per mail.
6. Marie meldt aan op PAMaaS via het Toegangsbeheer.
7. Op het PAMaaS-portaal kan Marie de door Brent aangevraagde sessie **goed- of afkeuren**. Brent krijgt een mailtje met de een melding van Maries keuze. Enkel als de sessie goedgekeurd werd kan Brent de sessie starten.

Technologieën

Welke technologieën worden standaard ondersteund?

Technologie	Wat kan je onboarden?	Hoe werkt dit in de praktijk?
Windows	Windows Local accounts	RDP-sessie via PAMaaS-jumphost
	Windows Domain accounts	RDP-sessie via PAMaaS-jumphost
Unix/Linux	Unix/Linux accounts	SSH-sessie via PAMaaS-jumphost
AWS	AWS IAM User/Role-combinatie	• Browser (https://console.aws.amazon.com) • AWS CLI
Azure	Azure Active Directory (AAD) users	Browser (http://portal.azure.com/, inclusief CloudShell)

De volledige lijst van standaard ondersteunde technologieën vind je hier

Rapportering en SIEM

Welke rapportering wordt er aangeboden?

Toegangsbeleid	Rapport		
	Change management (CR709)	Ongeoorloofde toegang tot accounts (CR117)	Ongeoorloofde toegang tot bronsystemen (CR118)
	Dit rapport geeft aan of een **toegang tot een targetsysteem** door een PAM-gebruiker conform de afspraken werd verschaft.	Dit rapport geef aan of er login-activiteiten hebben plaatsgevonden op PAM-targetsystemen door **accounts die niet onder controle van PAM staan.**	Dit rapport geeft aan of er login-activiteiten hebben plaatsgevonden op PAM-systemen met PAM-accounts **vanuit een bronsysteem dat niet gekend is binnen PAM.**
Access Only	✗	✗	✗
Motivated Access	✓	✓	✓
Secure Access	✓	✓	✓

Hoe werkt de integratie met SIEM?

Voorwaarden

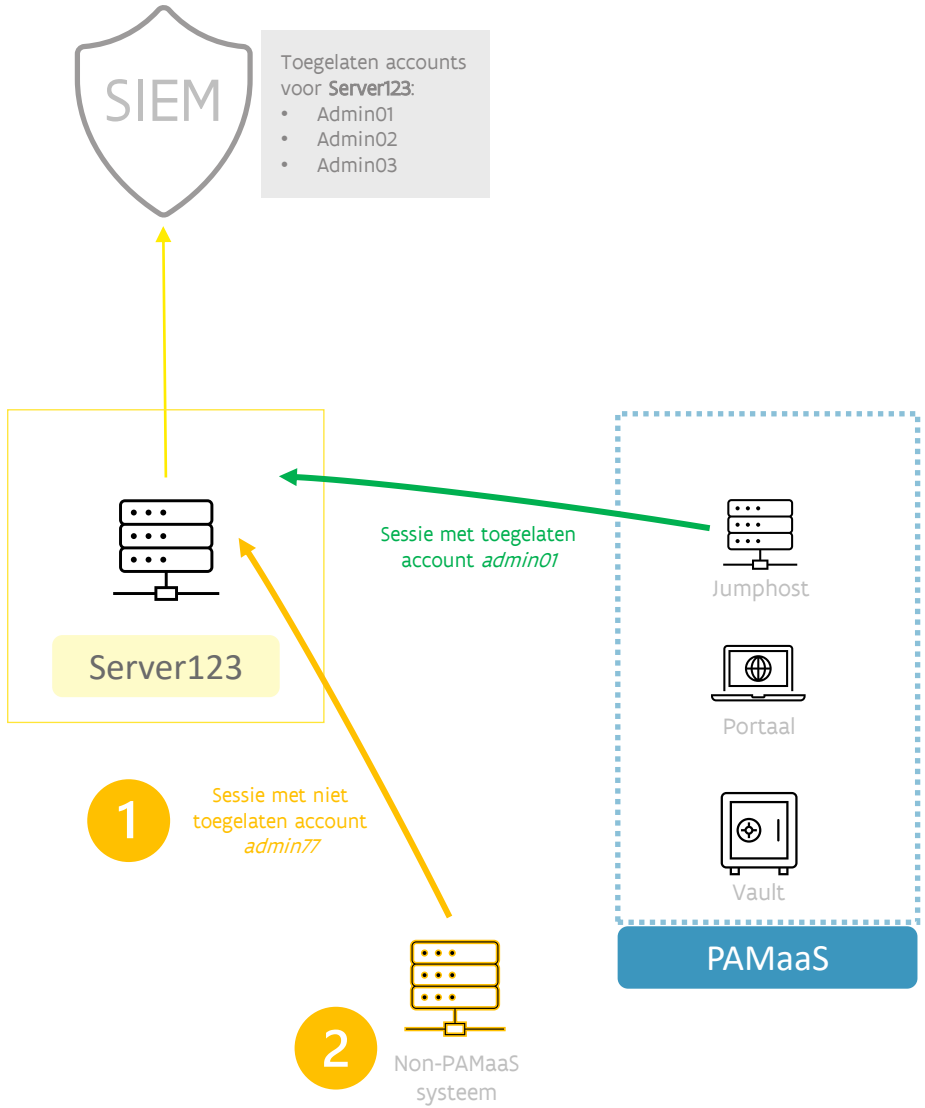
- De **SIEM-client software** moet geïnstalleerd zijn op het targetsysteem
- Het SIEM-team moet voor dit targetsysteem een **lijst van toegelaten geprivilegieerde accounts** definiëren

SIEM use cases

Er zijn twee SIEM use cases actief:

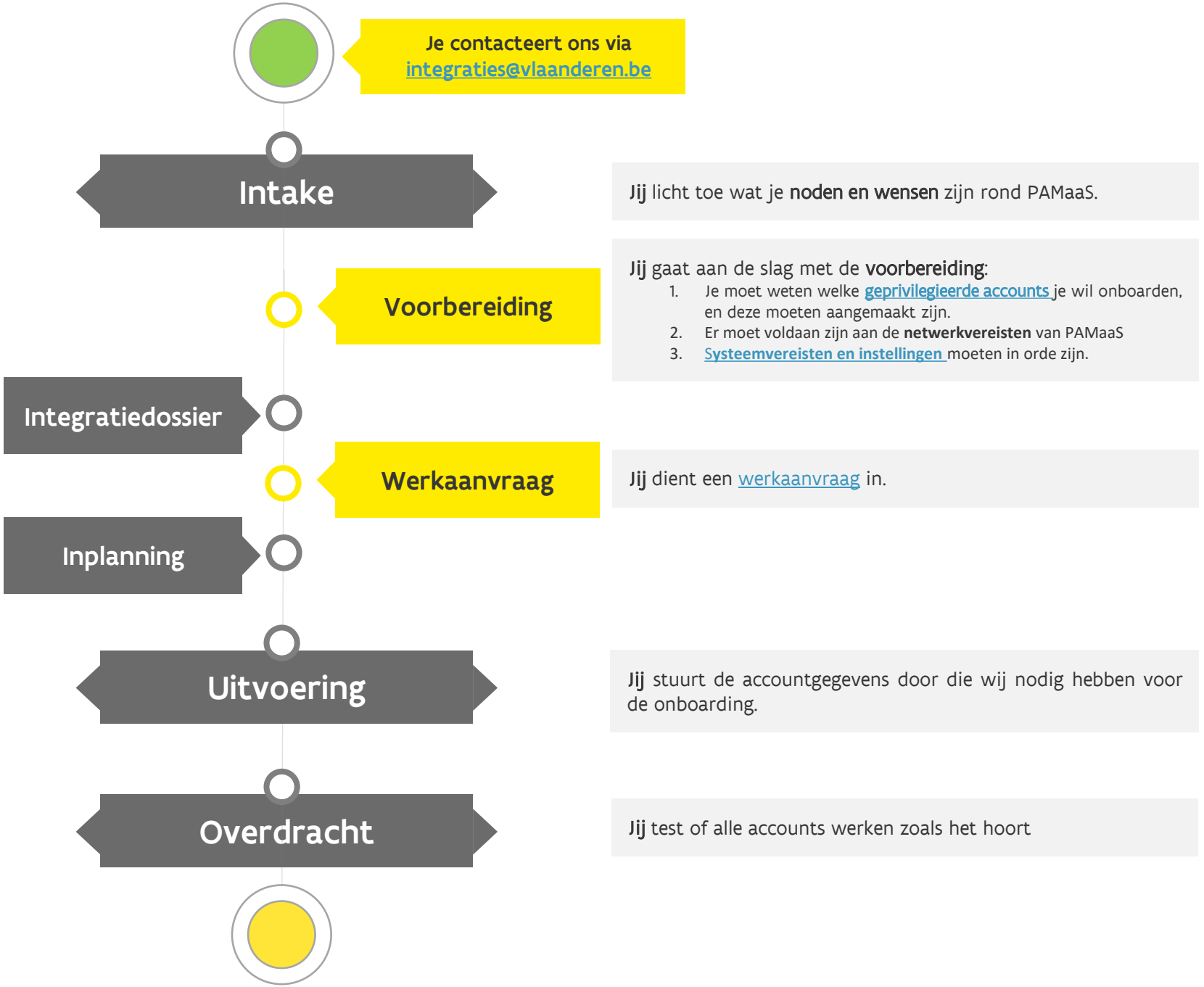
1. Wanneer er wordt aangemeld op een targetsysteem met een geprivilegieerd account dat ***niet*** in de lijst met **toegelaten geprivilegieerde accounts** voorkomt
2. Wanneer er wordt aangemeld op een targetsysteem vanop een ***ander*** systeem dan de PAMaaS jumphost (PSM of PSMP)

Telkens wanneer er een use case getriggerd wordt zal er een **incident** worden aangemaakt en opgenomen door het SOC-team.



Standaardonboarding

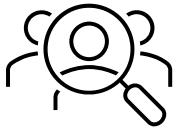
Integratieproces



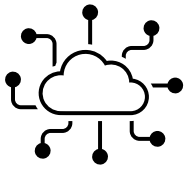
Het integratieteam plant een **intakegesprek** met jou:
Wij lichten volgende zaken toe:

- Functionaliteiten en ondersteunde technologieën.
- Vereisten, voorwaarden en proces standaardonboarding.
- Niet-standaardonboarding.
- Prijsmodel

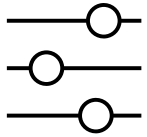
Waar ben ik als klant zelf verantwoordelijk voor?



De analyse rond en het aanmaken van de **geprivilegieerde accounts** die je wil onboarden in PAMaaS.



Er moet voldaan zijn aan de **netwerkvereisten** van PAMaaS: gebruikers en systemen moeten de nodige verbindingen kunnen maken naar het portaal en de PAMaaS-jumphost(s).



De systemen waarvan accounts geonboard worden moeten voldoen aan bepaalde technische **systeemvereisten en instellingen**.

Prijsmodel voor standaardonboardings

VOORBEELD

Voor jouw organisatie wil je het volgende onboarden:

- 16 Windows Local accounts
- 2 Linux accounts
- 2 AWS IAM user/roles

Je organisatie telt **vier** systeembeheerders.

Je onboarding zal volgende kost (incl. BTW) hebben:

- Eenmalige kosten: € 1.651,74 + € 2.052,20 = **€ 3.703,94**
- Maandelijkse kosten: 4 mensen x € 20,84 / maand = **€ 83,36 per maand**

EENMALIGE KOSTEN	
Opstartkosten	
Vaste kost (incl. BTW)	**€ 1.651,74 / onboardingstraject**

Geprivilegieerde accounts		
Technologie	**Aantal**	**Eenheidsprijs (incl. BTW)**
Windows Domain account	0	€ 102,61 / account
Windows Local account	16	
Unix/Linux account	2	
AWS IAM user/role	2	
Azure AD accounts	0	
TOTAAL	**20**	**€ 2.052,20**

MAANDELIJKSE KOSTEN	
Licentie- en onderhoudskosten	
Kostprijs (incl. BTW)	**€ 20,84** per gebruiker* per maand
Aantal	4
TOTAAL	**€ 83,36 / maand**

* Elke persoon die aanmeldt op PAMaaS is een gebruiker. Deze prijs is per persoon (=mens), en is onafhankelijk van het aantal rollen of applicaties waarvoor men gemachtigd is

Prijsmodel voor standaardonboardings

WAT IS NIET INBEGREPEN?

Als klant sta je zelf in voor volgende zaken:

- De analyse van welke gedeelde **geprivilegieerde accounts** je nodig hebt en het (laten) aanmaken ervan.
- Het opstellen en inregelen van de vereiste **datastromen** voor de onboarding.
- Het inregelen van de **SSL-VPN-verbinding** voor PAMaaS-gebruikers die geen toegang hebben tot het Vonet-netwerk.
- SIEM-integratie zit **niet** in het onboardingsproces maar kan additioneel worden afgenomen.
- De facturatie verloopt via het **facturatieproces van P5**.

Niet-standaardonboarding

Integratieproces

Je contacteert ons via
integraties@vlaanderen.be

Intake

Jij licht toe wat je **noden en wensen** zijn rond PAMaaS.

Het integratieteam plant een **intakegesprek** met jou:
Wij lichten volgende zaken toe:

- Functionaliteiten en ondersteunde technologieën.
- Vereisten, voorwaarden en proces standaardonboarding.
- Niet-standaardonboarding.
- Prijsmodel

Voorbereiding

Jij gaat aan de slag met de **voorbereiding**:

- Je beschrijft gedetailleerd wat je nodig hebt en stuurt dit door naar integraties@vlaanderen.be

Onderzoek en inschatting

Wij onderzoeken je de haalbaarheid van je aanvraag en stemmen af met jou over een inschatting van de kosten.

Beslissing

Jij beslist of je de niet-standaardonboarding wilt:

- Je stemt in met de te nemen kosten en beslist om de onboarding te doen.

Integratiedossier

Wij vullen samen met jou het **integratiedossier** in, het document dat alle informatie voor jouw onboarding moet bevatten.

Volgend zoals standaardonboarding

Prijsmodel voor niet-standaardonboardings

Wat is een niet-standaardonboarding?

Elke onboarding die afwijkt van een standaardonboarding is een **niet-standaardonboarding**, bijvoorbeeld:

- Je wilt geprivilegieerde accounts onboarden van een technologie die nog niet ondersteund wordt door PAMaaS.
- Je wilt een decentrale PAMaaS-opzet implementeren met eigen PAM-componentservers (PSM, PSMP, CPM) in je netwerk.
- …

Prijsmodel

Prijzen voor niet-standaardonboardings worden bepaald op basis van een **offerte op maat**. Om deze te kunnen opstellen hebben we voldoende informatie nodig.

Heb je interesse?

Bezorg ons een gedetailleerde beschrijving van je noden en wensen via integraties@vlaanderen.be, dan komen we daar zo snel mogelijk op terug.

Heb je vragen, wil je gebruik maken van deze bouwsteen?

Contactformulier

integraties@vlaanderen.be

DIGITAAL VLAANDEREN

Vlaamse overheid