Dienstenbeschrijving

Privileged Identity Management

rawworks

PORTAL TO AUTOMATION

VERSIE	0.1
AUTEUR	Gerjon Kunst
STATUS	Eerste opzet
CLASSIFICATIE	**Intern**

INHOUD

PRIVILIGED IDENTIY MANAGEMENT

Bij Privileged Identity Management (PIM) as a service wordt een dienst geleverd waarbij op basis van een PowerApp gebruikers van de IT-omgeving beheerders rechten via de Active Directory van de on-premisses omgeving kunnen aanvragen.

Doel van deze tool is het onder controle houden van het aantal beheerders en het kunnen aantonen wie, wanneer beheerders rechten heeft aangevraagd. De rechten zijn onder te verdelen in verschillende gradaties en types. Deze worden in overleg met de klant ingeregeld via het security model.

WELKE PROBLEMEN LOST DEZE DIENST OP?

- Beperken van het aantal (domain) administrator accounts bij klanten
- Traceerbaar wie wanneer rechten heeft aangevraagd waarvoor en wie heeft goedgekeurd
- Aanvragen via powerapp/micro-app
- Dienst per maand opzegbaar
- Koppeling met SOC/Siem dienst mogelijk
- Accounts worden aangemaakt en verwijderd dus geen vervuiling

VOOR WELKE TYPE KLANTEN IS DEZE DIENST INTERESSANT

Voor bedrijven of instellingen die:

- Degene die nog een on-premisses (Microsoft) IT omgeving hebben
- Degene die geen IAM tooling (of onvoldoende) in place hebben voor beheeraccounts
- Degene die auditing van beheer accounts niet (of onvoldoende) op orde hebben

DELIVERY VORMEN

PIM as a service wordt in twee vormen geleverd:

- Als dienst vanuit de omgeving van RawWorks.
  De service draait in de beveiligde cloudomgeving van RawWorks en wordt centraal beheerd en gepatched
- Als dienst vanuit de klantomgeving (tegen meerprijs)
  De service draait in de cloudomgeving van de klant. Hiervoor is aanschaf extra licenties en extra kosten voor beheer (ivm decentraal beheer) noodzakelijk

Verwante diensten:
Bovenop deze dienst werken we vanuit de

- Cloud Tribe aan
  - een IaC Landing Zone in Azure (straks ook in AWS)
  - OneSecure
  - Competence as a service
- Workspace Tribe aan
  - een IaC Workspace (die noemen we de DevOps Workspace).
- Digital aan
  - Een datalake-as-a-Service,

INHOUD VAN DE DIENST

Bij Privileged Identity Management wordt een beheerschil om het beheren van de diverse soorten beheer (administrator) accounts gelegd. Hierdoor kunnen medewerkers die beheerrechten benodigd zijn op de on-premisses omgeving deze aanvragen via een PowerApp/Micro-app

Vooraf worden met de klant de rollen besproken en in het security model gezet. Hierdoor is duidelijk wie welke rol kan aanvragen en wie deze kan goedkeuren (indien nodig). De borging van dit proces wordt in het model opgenomen en op basis hiervan wordt de tooling ingericht.

De aanvraag wordt gedaan via een micro-app/powerapp. Deze trapt onderwater via een pipeline de benodigde scripts af waar via parameters is aangegeven vanuit het security model wat de rollen zijn en wie deze aan mag vragen. Er wordt in de active directory op basis van een templateaccount een nieuw administrator account aangemaakt. De logingegevens van het account worden via mail (en wachtwoord via bijv. sms) verstuurd

Indien nodig is het ook mogelijk om bestaande beheeraccounts aan en uit te zetten (voor bijvoorbeeld toegang tot andere beheerportalen van bijvoorbeeld firewalls welke aan ad gekoppeld zijn).

In geval van storingen binnen de Azure infrastructuur of internet is het verstandig een “break the glass” account in de kluis te leggen zodat beheer toch mogelijk blijft.

VOORDELEN VAN DE DIENST

- Als dienst af te nemen en per maand opzegbaar
- Controle en audit op wie wanneer beheersrechten benodigd is
- Minimalisatie van attack surface op beheer accounts

-

INVESTERING

Delivery Vorm	Afrekenmodel
Services – Project	Fixed Price (op basis van statement of work) Nacalculatie (125 euro per uur, indicatief)
Managed Service	Prijs per maand (gebaseerd op value)