Spring Cleaning

How AI took out a decade of Identity Debt

Manish Periwal & Stian Angvik

Stian Angvik

Cyber Security Engineer

Part of the Digital Identity team at NBIM.
Driving initiatives over the finish line without ever losing sight of the user experience

🛡️ Identity Security → 🔐 Access Management → 🤝 Communication → 🪪 Everything Identity

Manish Periwal

Senior Security Engineer

Indian-born, Norwegian citizen, now living in Singapore - **revoking access and securing systems wherever I go**.

🛡️ AppSec → ☁️ Cloud Security → ⚙️
DevSecOps → 🪪 **Everything Identity**

Microsoft® MVP Most Valuable Professional

Someone in the organization still has access which they haven’t used in more than [X] year.

The unused access is your attack surface and compliance risk.

Agenda

- ✓ **Decade of Identity Debt**
- ✓ **The Journey**
- ✓ **AI as force multiplier**
- ✓ **Some Demos**
- ✓ **Q&A**

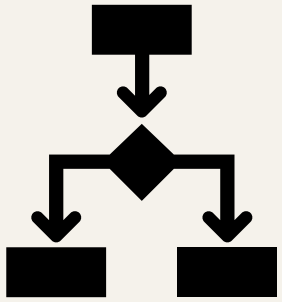
A decade of Identity Debt

Access & Entitlements

Entitlements granted over years, never revisited

Role Changes

People moved teams, projects, offices — access stayed



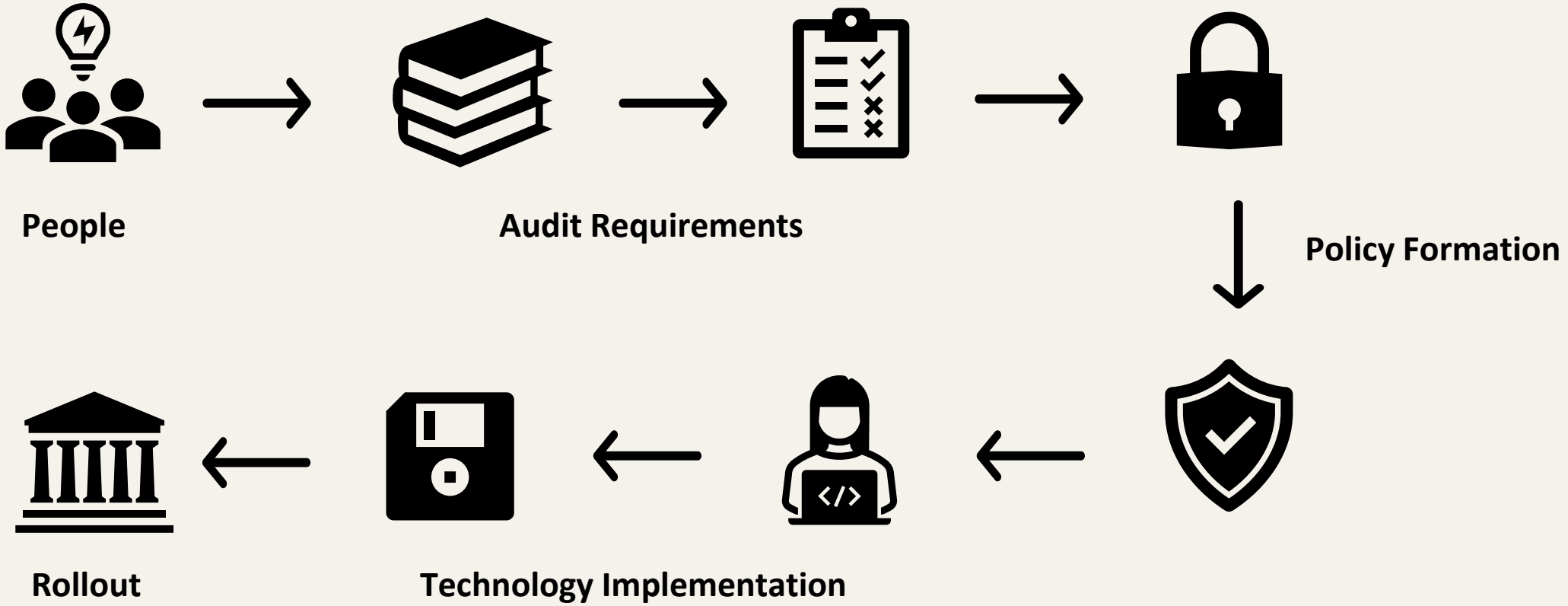
Multiple Sources

Access assigned through AD, apps, manual tickets, legacy systems, direct & indirect assignments

No Expiry

No time limits. No reviews. Access just accumulated.

People, Process & Technology



Design Principles

- ✓ **No Application Owners in Entra ID**
- ✓ **Identity team – Creates and Deletes Groups**
- ✓ **Each Group tagged to a system owner**
- ✓ **Only Security Groups in scope**
- ✓ **No Group owners assigned – everything must through IGA**

Winter before Spring Cleaning

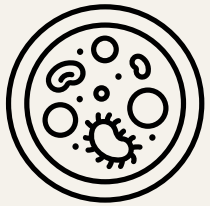
Accesses Expired

Not Enough Communication

March Madness

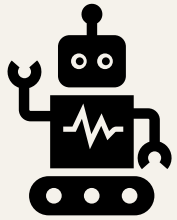
Communication is the Key

Communication across time zones is harder than the technical work



Culture eats access reviews for breakfast — get leadership buy-in first

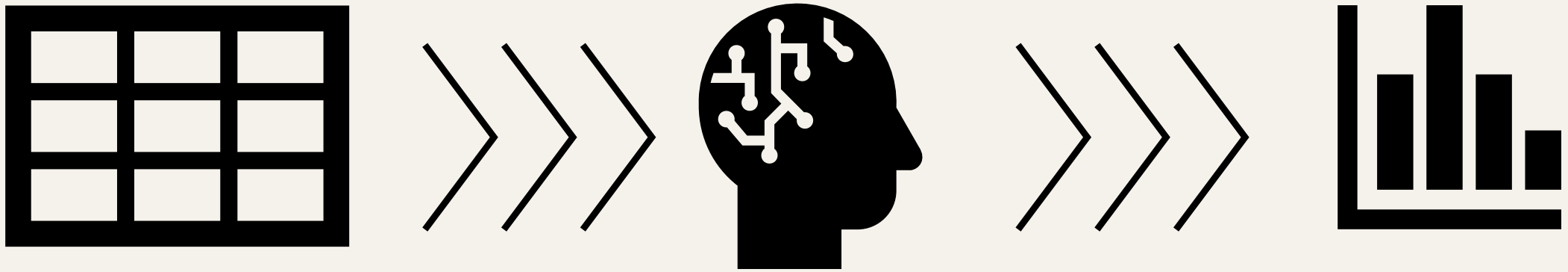
Explain *why* before asking anyone to act. Nobody likes losing access.



Automation without communication creates shadow IT, not security

Start with the most priority system first — everything else feels easy after that

Data to Information



AI as force multiplier

Vibe-coded Dashboards

Real-time access intelligence — built in days, not months

Claude Skills

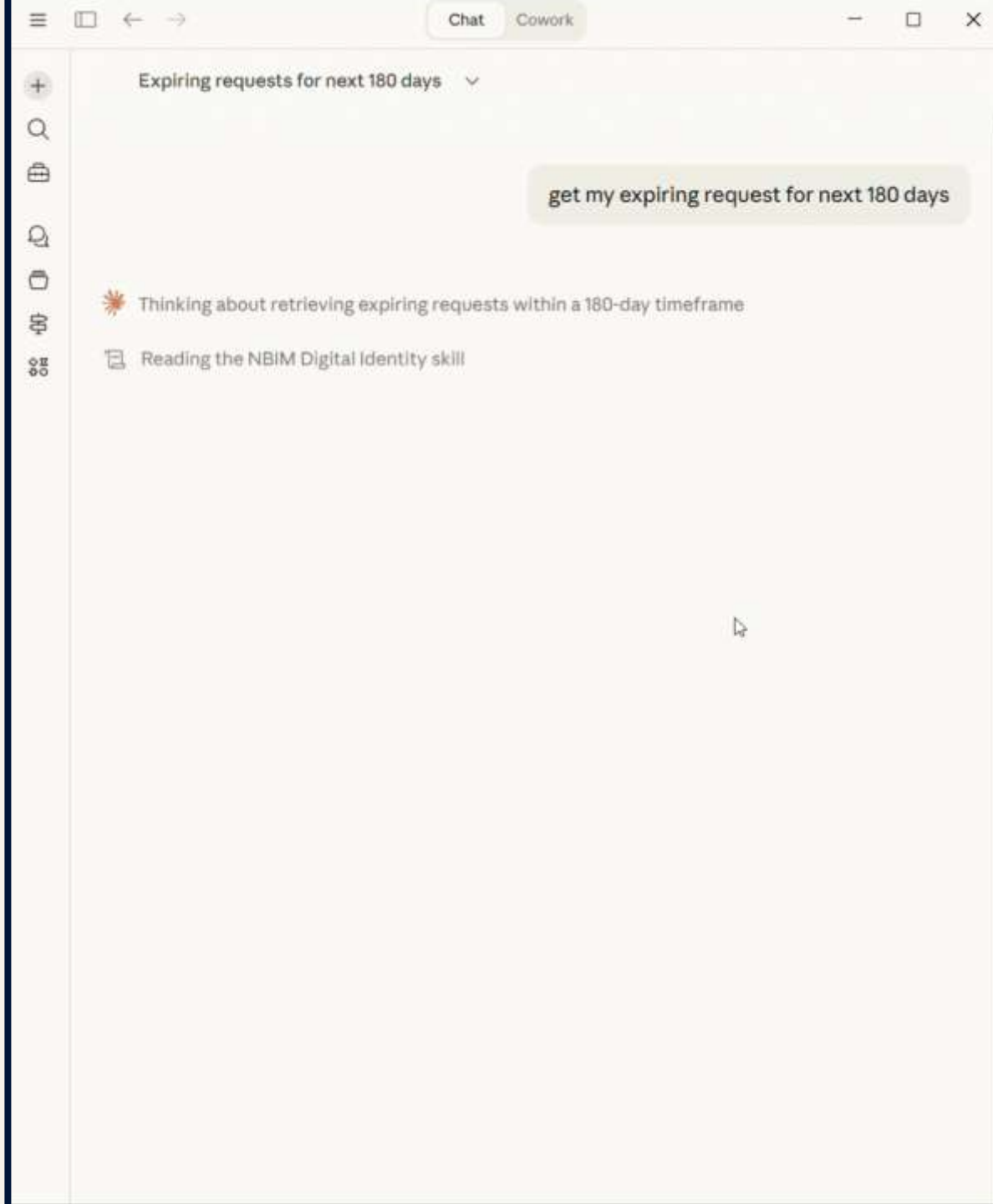
Step-by-step documentation for non-security staff to make access decisions

AI Chatbot Interface

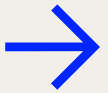
Self-service access insights — anyone can query identity data in plain English

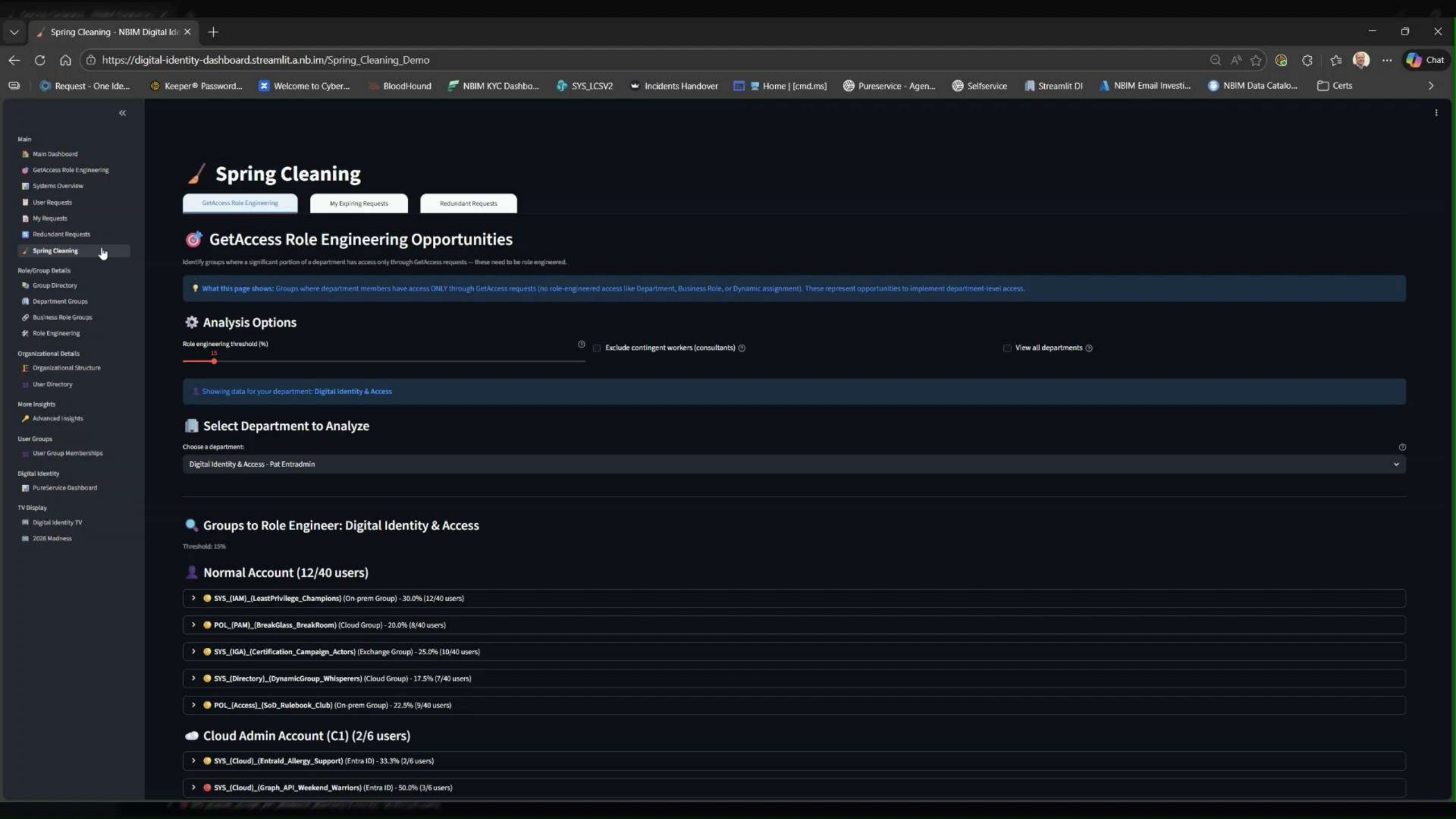
MCP Integrations

Model Context Protocol for real-time Sentinel, Entra ID & identity data querying



Demo




Spring Cleaning - NBIM Digital Ide
https://digital-identity-dashboard.streamlit.a.nb.im/Spring_Cleaning_Demo
Chat
Request - One Ide...
Keeper® Password...
Welcome to Cyber...
BloodHound
NBIM KYC Dashbo...
SYS_LCSV2
Incidents Handover
Home | [cmd.ms]
Pureservice - Agen...
Selfservice
Streamlit DI
NBIM Email Investi...
NBIM Data Catalo...
Certs
Main
Main Dashboard
GetAccess Role Engineering
Systems Overview
User Requests
My Requests
Redundant Requests
Spring Cleaning
Role/Group Details
Group Directory
Department Groups
Business Role Groups
Role Engineering
Organizational Details
Organizational Structure
User Directory
More Insights
Advanced Insights
User Groups
User Group Memberships
Digital Identity
PureService Dashboard
TV Display
Digital Identity TV
2026 Madness
Spring Cleaning
GetAccess Role Engineering
My Expiring Requests
Redundant Requests
GetAccess Role Engineering Opportunities
Identify groups where a significant portion of a department has access only through GetAccess requests — these need to be role engineered.
What this page shows: Groups where department members have access ONLY through GetAccess requests (no role-engineered access like Department, Business Role, or Dynamic assignment). These represent opportunities to implement department-level access.
Analysis Options
Role engineering threshold (%)
15
Exclude contingent workers (consultants)
View all departments
Showing data for your department: Digital Identity & Access
Select Department to Analyze
Choose a department:
Digital Identity & Access - Pat Entradmin
Groups to Role Engineer: Digital Identity & Access
Threshold: 15%
Normal Account (12/40 users)
SYS_(IAM)_(LeastPrivilege_Champions) (On-prem Group) - 30.0% (12/40 users)
POL_(PAM)_(BreakGlass_BreakRoom) (Cloud Group) - 20.0% (8/40 users)
SYS_(IGA)_(Certification_Campaign_Actors) (Exchange Group) - 25.0% (10/40 users)
SYS_(Directory)_(DynamicGroup_Whisperers) (Cloud Group) - 17.5% (7/40 users)
POL_(Access)_(SoD_Rulebook_Club) (On-prem Group) - 22.5% (9/40 users)
Cloud Admin Account (C1) (2/6 users)
SYS_(Cloud)_(Entra1d_Allergy_Support) (Entra ID) - 33.3% (2/6 users)
SYS_(Cloud)_(Graph_API_Weekend_Warriors) (Entra ID) - 50.0% (3/6 users)

Data to Information

Rolling Remediation

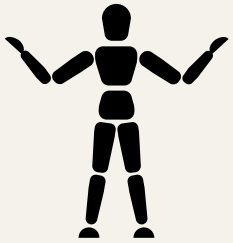
Uphill task!

Not everything was smooth

Follow ups & frequent Communication

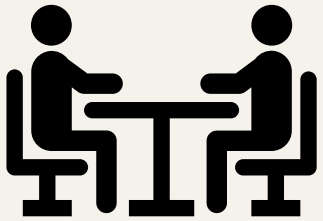
Escalation

Resistance



Self-Action

The Outcome



Access Review Program which works!

Time based memberships

Role Engineering & Dynamic Assignments

Compliant & Audited Accesses

AI Goes Beyond!

Thank you!