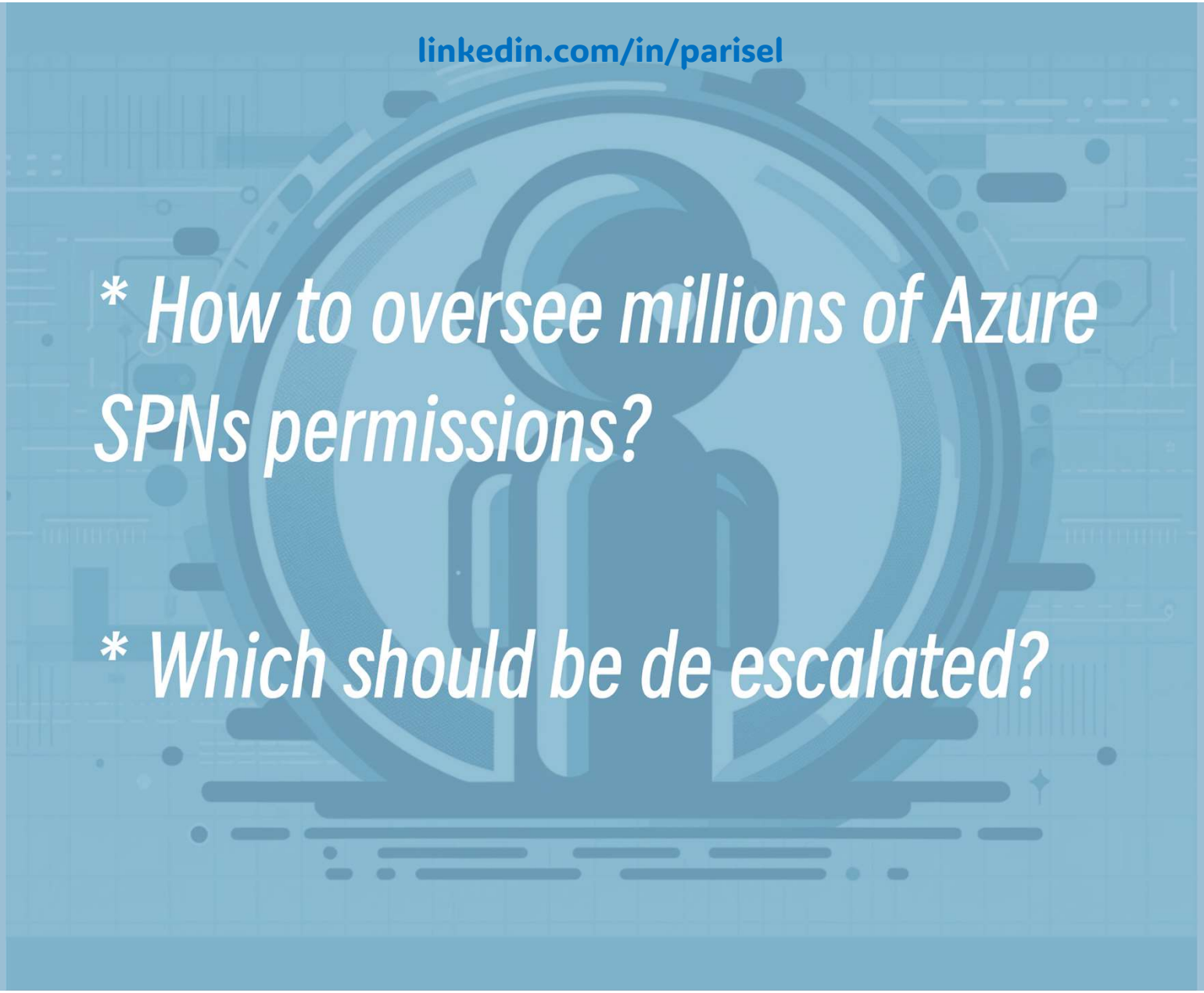
linkedin.com/in/parisel

Azure Silhouette

De escalate SPN permissions

linkedin.com/in/parisel




1) SPNs are grouped into relevant clusters with unsupervised Machine Learning

2) For each cluster, we collect permissions from the golden source (Azure Entra)

3) We calculate a score, the « outer silhouette » of each cluster

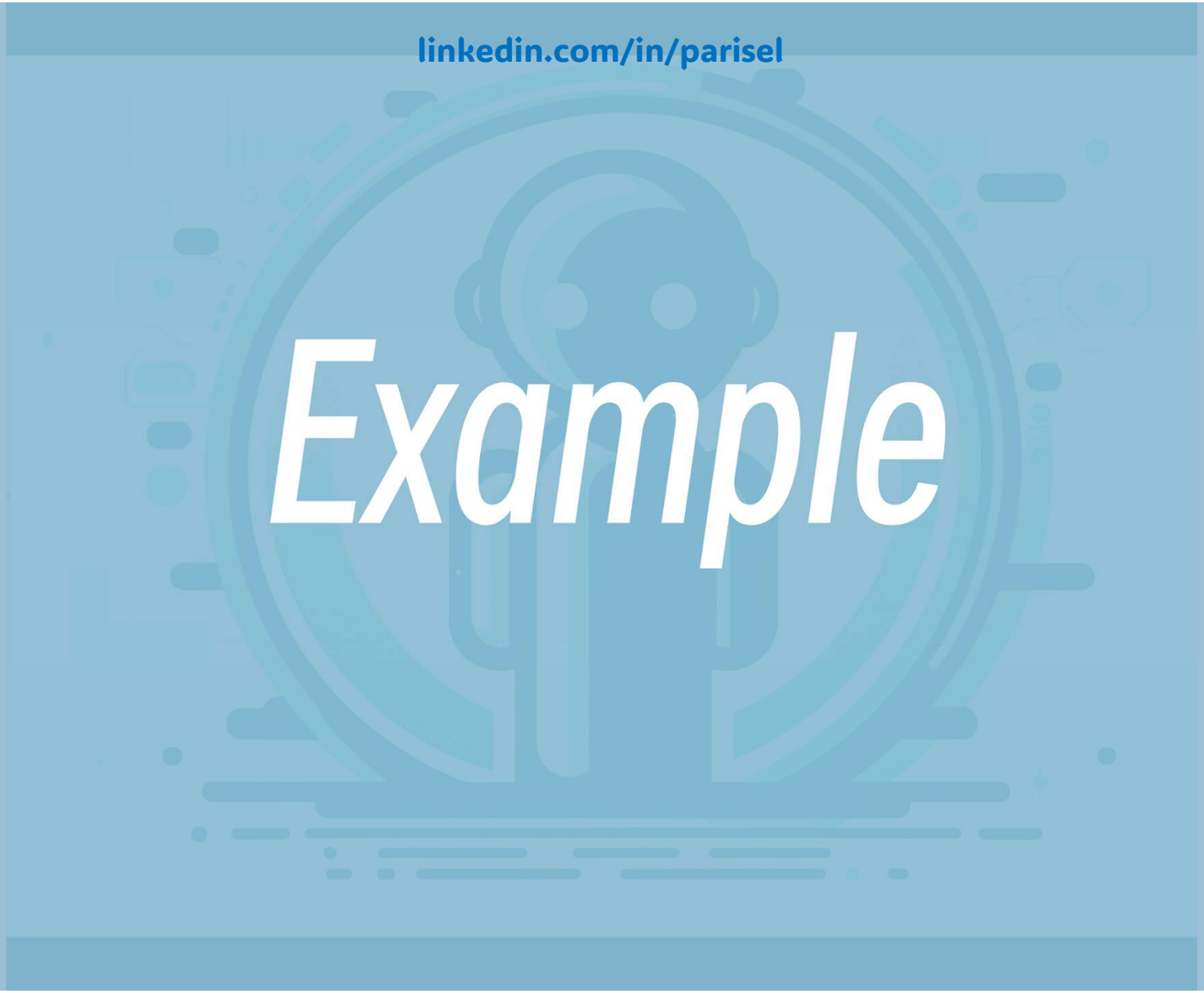
4) For each cluster, we collect permissions from the ground truth (Azure Log Analytics)

5) We calculate a second score, the « inner silhouette » of each cluster

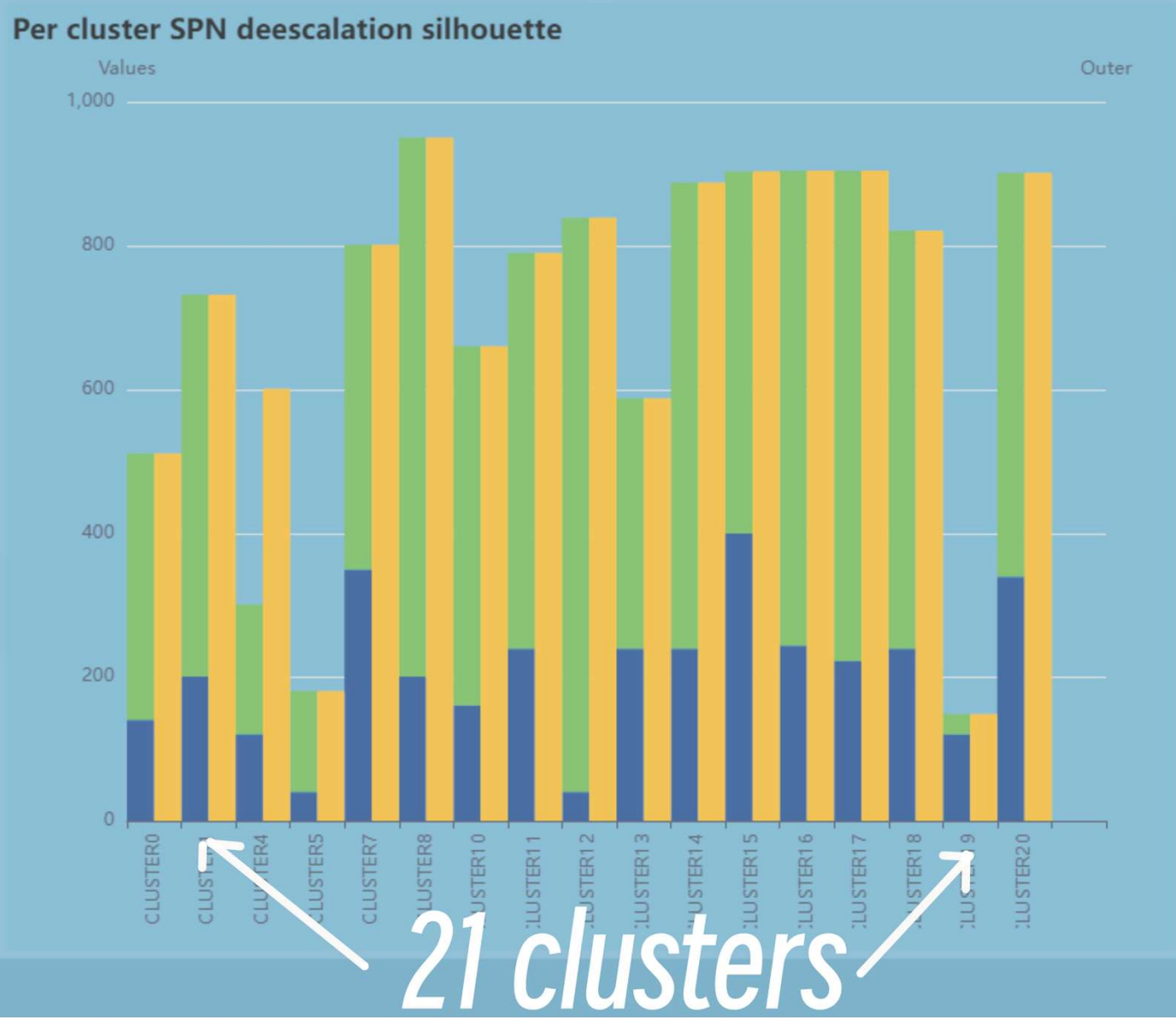
6) We define a metrics distance between silhouette scores

7) for each cluster, the de-escalation effort equals the distance between outer and inner scores

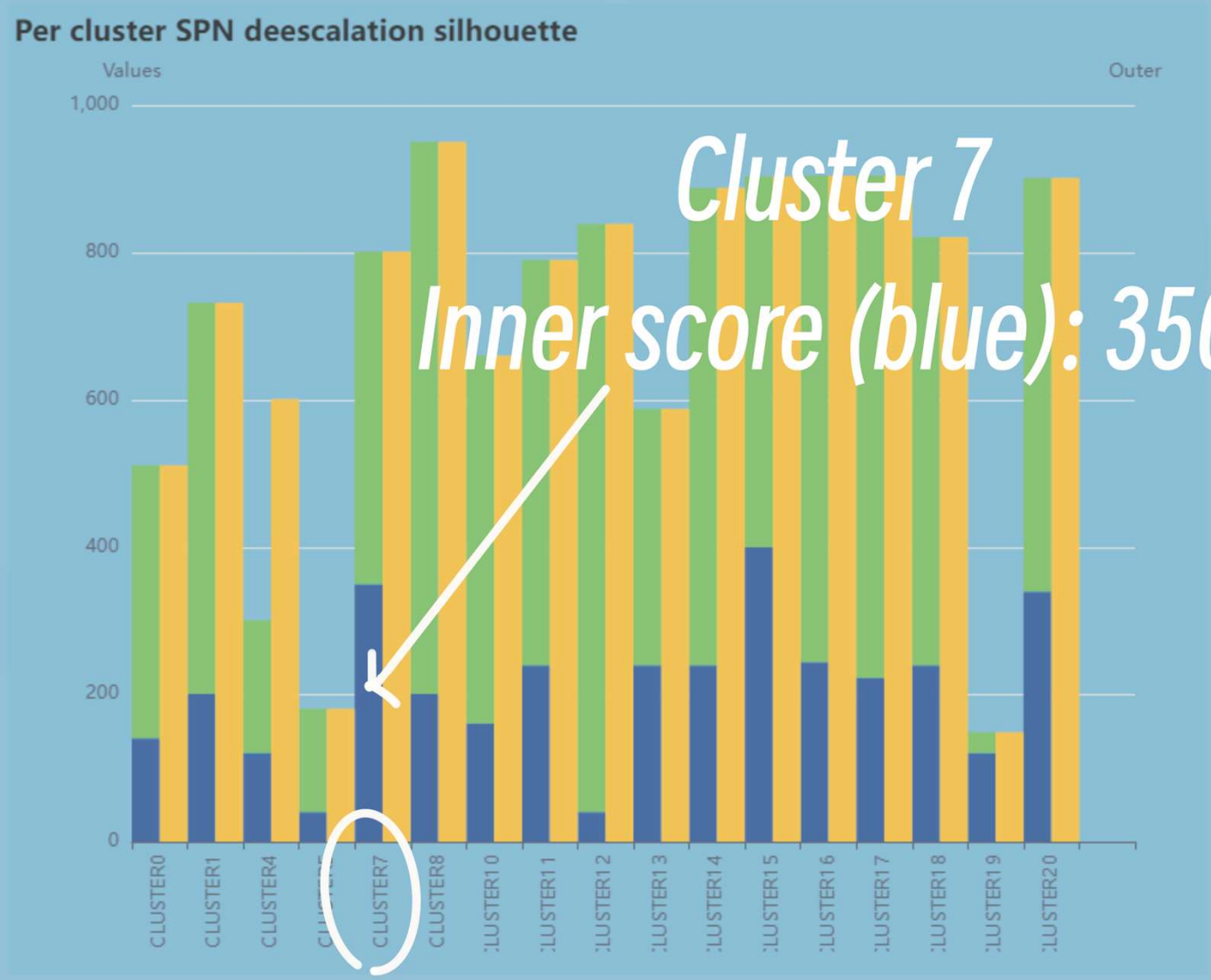
linkedin.com/in/parisel



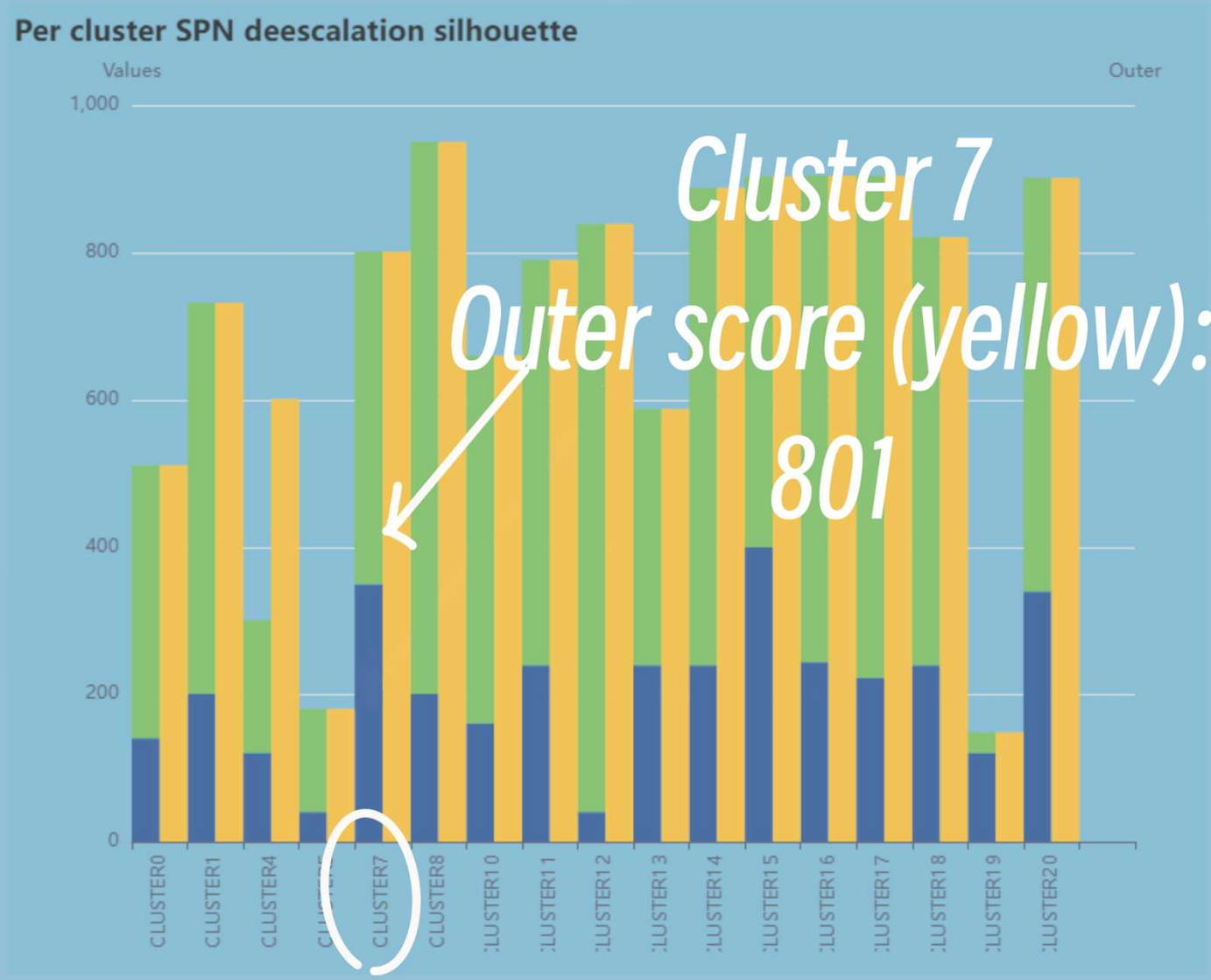
linkedin.com/in/parisel



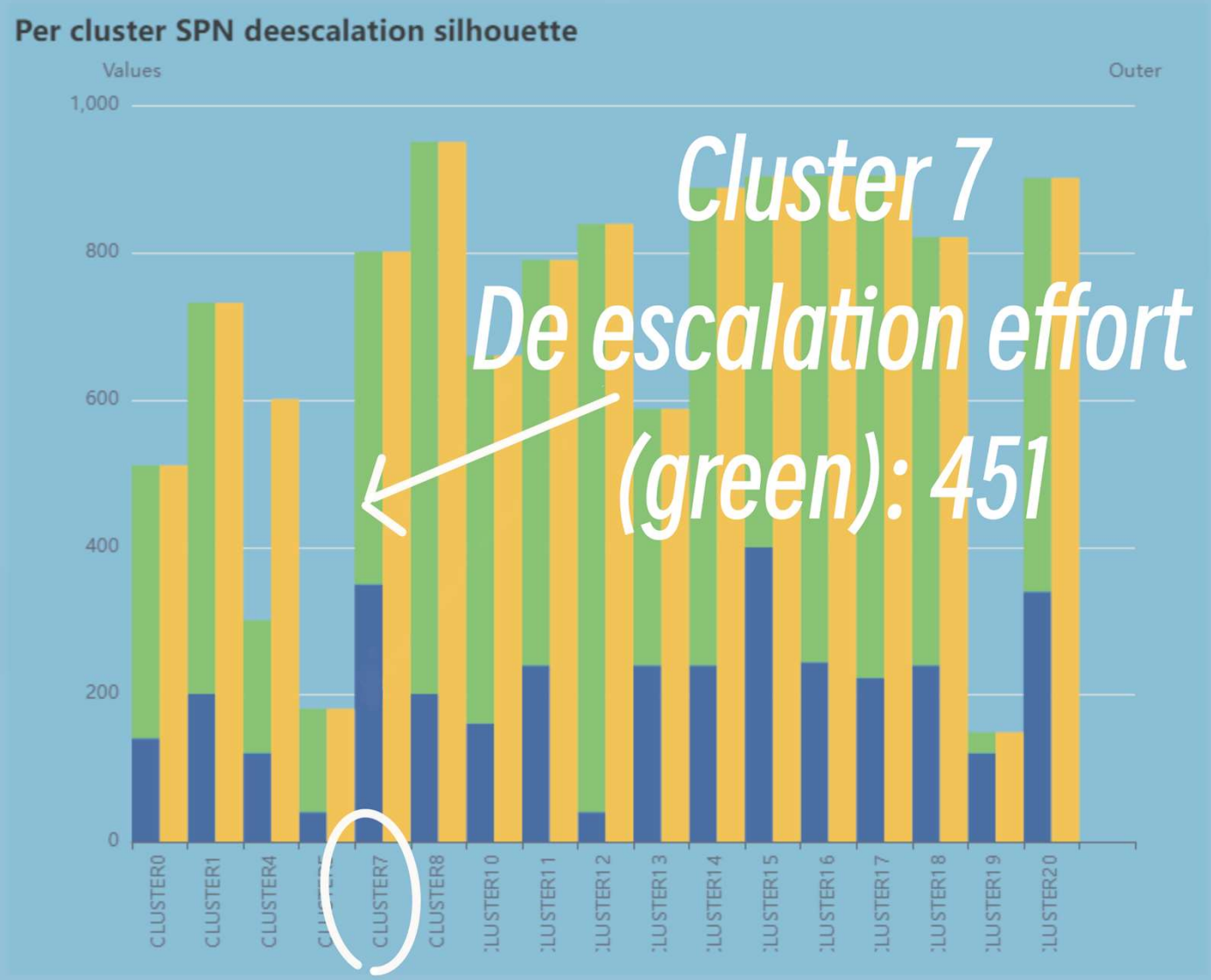
linkedin.com/in/parisel

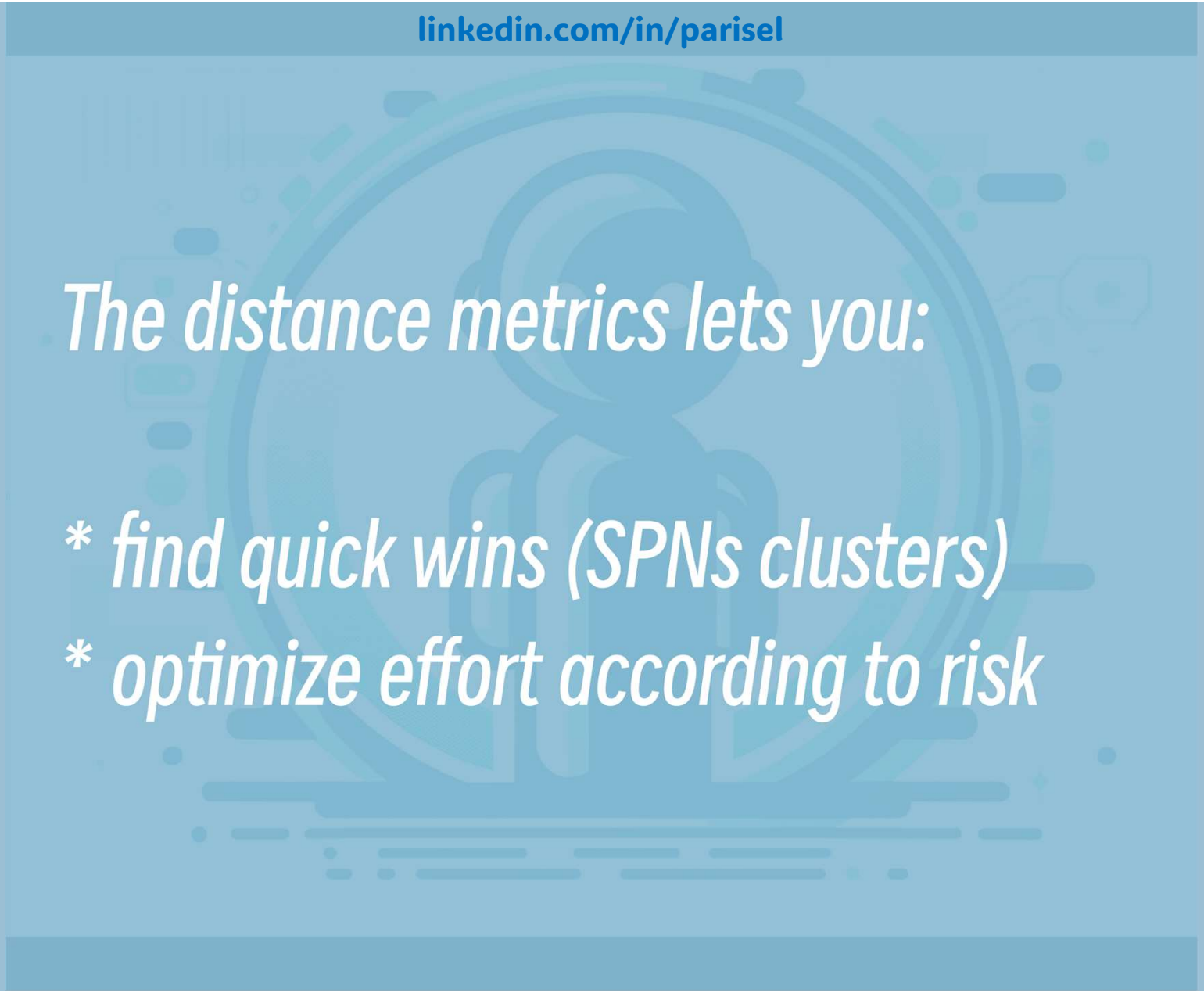


linkedin.com/in/parisel

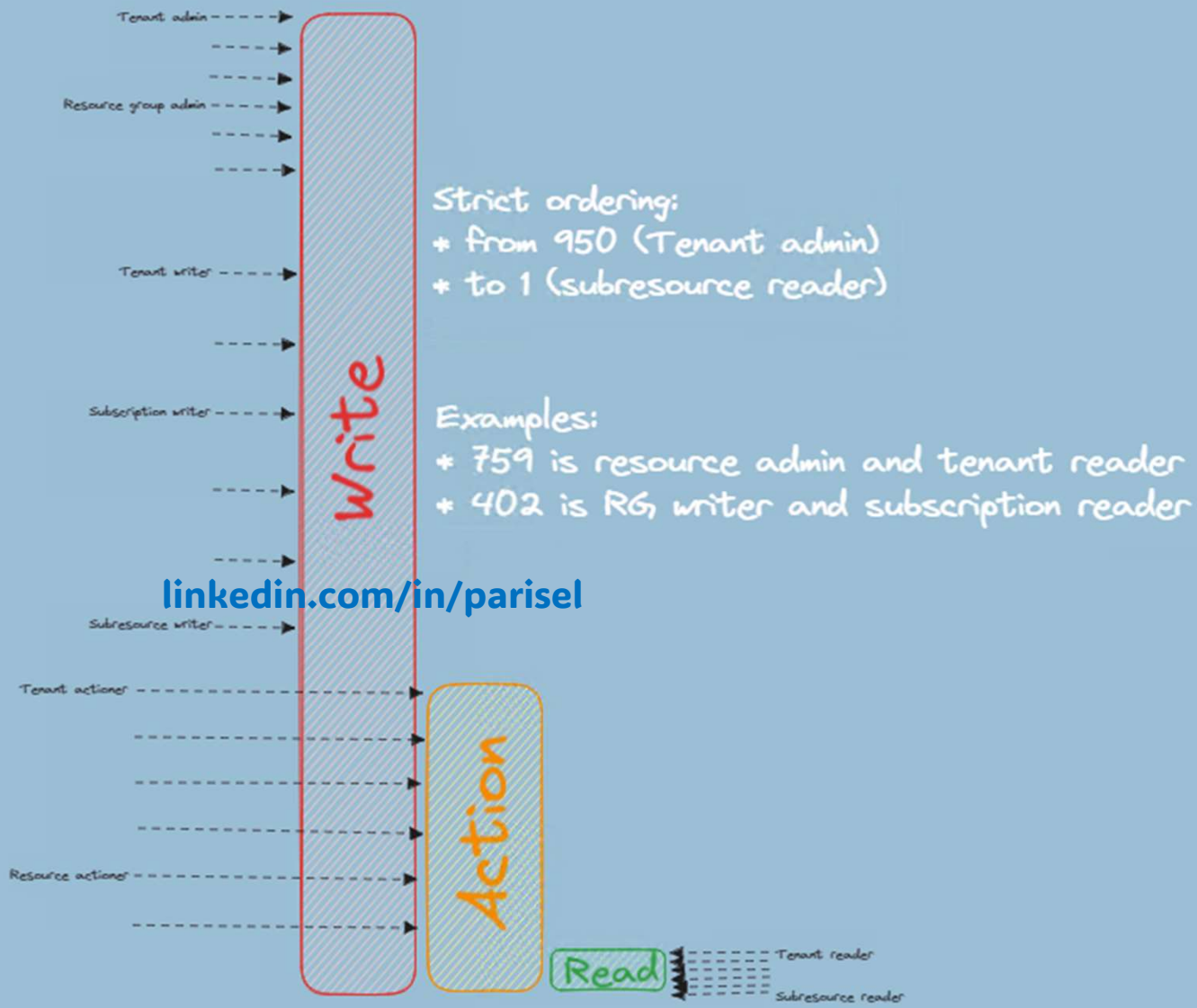


linkedin.com/in/parisel




The distance metrics lets you:
* find quick wins (SPNs clusters)
* optimize effort according to risk

Permissions hierarchy in the silhouette metrics



Strict ordering:
* from 950 (Tenant admin)
* to 1 (subresource reader)

Examples:
* 759 is resource admin and tenant reader
* 402 is RG writer and subscription reader

linkedin.com/in/parisel

Get it for free:

https://github.com/labyrinthinesecurity/silhouette