UW-Madison VPN Usage Approval via Manifest (Grouper)

A use case on using Grouper's composite groups to create a two-person approval system for a service

With the deployment of our new VPN service at UW-Madison, we wanted to control access by Grouper groups (managed through our Manifest interface). This new VPN system allowed for multiple contexts each with specific goals for accessing systems. A more general purpose (just put me on a campus network) VPN is authorized to all users based on the data-driven status of being student, faculty, or staff. Another of these contexts is a HR VPN used to access restricted HR system resources. Our Security group on campus required that people complete a training and were approved to the use the VPN, but we also did not want them to be the sole responsibility for adding and removing access for someone. We set up a system where a team, independent of security, could add people that should use the VPN while security maintains a list of people who are authorized to use the VPN based on completion of training, hasn't been compromised etc. This allows security to remove a person if their account is compromised, but also allows the HR team to remove a person when they quit their job and not have to rely on security removing them in a timely manner. One of the groups that drives HR VPN users is even data-driven based on employment status so their use is removed automatically when they quit their job. If they took a job elsewhere on campus, their training is still relevant potentially and they are still part of that group maintained by security but won't have HR VPN access until someone adds them as someone who needs that access again. This system was accomplished with some simple group math as shown below. A composite group makes up who can use the HR VPN by requiring membership in both the Security Authorizations group and the HR VPN users group. If security authorizations ever choses to only ban naughty users (instead of full on authorization), the composite can be changed to a NOT and everything will continue to work as is. Note that "HR Users" is made up of groups maintained by HR officers all around campus as there is not a clear data-driven defined way to see who is relevant to the HR VPN system.