**User Provisioning - Fight against Zombie Accounts**

The Walking Dead – is not a fiction anymore. Zombies are real. For now, even though they are trapped in the digital ecosystem, their impact is oh so real.

It is a never-ending game between bad actors and the defenders. Bad Actors, always trying to cause all kinds of havoc and disrupt the system. As defenders, it is a battle to keep our digital assets, infrastructure and information secure. As attackers, it is the next set of credentials, PII or information that you can leverage for your own personal gain – or just to watch the world burn by deploying Ransomwares, Exposing state secrets, cause financial crisis, bring about the apocalypse.

How about using knowledge of both worlds to secure what we can i.e. our applications?

It is well known that we may have the best, cutting-edge infrastructure and applications built on the latest, cool tech stacks and snazzy user interfaces and having colossal security products attempting to protect the data and assets. However, it takes just a tiny section of code, one vulnerability that we knowingly or unknowingly introduce, that can be the Achilles heel.

We’ve been developing this solution for the past 2 years, and it is finally ready to unleashed – in a good way – onto the world.

This submission aims at presenting the threat that digital zombies pose to the real world. Having uncancelled, unused, but still active accounts in the system, can come to bite us in the arse.

Through the course of the session, we will go through what came to be as a User Life Cycle Management Solution. We will also touch upon very real attacks that have happened as a result of threat actors taking advantage of ghost or zombie accounts.

**Key Takeaways**

The session aims at using at using User Lifecycle Management as a solution for mitigating ghost account cyber attacks, by having automated provisioning and deprovisioning of user accounts.