Resources

https://bloodhound.readthedocs.io/en/latest/index.html

https://github.com/BloodHoundAD/BloodHound

BloodHound

BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. As of version 4.0, BloodHound now also supports Azure. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment.

BloodHound Enterprise is an Attack Path Management solution that continuously maps and quantifies Active Directory Attack Paths. You can remove millions, even billions of Attack Paths within your existing architecture and eliminate the attacker’s easiest, most reliable, and most attractive techniques.