What are Tier 0 Admins

Who are the Tier 0 (Zero) Admins?

The smallest circle of administrators on a domain, these accounts are the most vital in an organization. They contain the permissions required to view all the user passwords.

> Guard these accounts with a sense of shear ferocity

Why does tier 0 have the least number of administrators?

Tier 0 administrators have the ability to access the ntds.dit file on a Domain Controller. If someone or something can access to the ntds.dit file, that person or service is considered a Tier 0 administrator.

> *Any part* of the environment that has access to control the domain controllers is considered part of Tier 0.

What is the ntds.dit file

The ntds.dit file is the data store for all the user names and passwords in an active directory domain. This ntds.dit file is so important because it holds all the users and all the passwords of an organization.

Whoever controls this file, controls all the users, all the accounts, all the access to everything inside an organization.

This file is the one thing that rules the domain. People that control this file can get to any type of data: Research data, PII, trade secrets. The people that can access this file can read every single email inside an organization.

> **The number of people that can access this file needs to be as small as possible. This file needs to be secured.**

Secure Tier 0 Systems in an Environment

Access to Observed Systems

Access to the ntds file can come on many different manners: applications installed the servers, agents or services running on the servers, scheduled task or scheduled jobs, hard disk administrators, backup administrators. The list goes on.

This reference picture above is a great place to start to understand how many Tier 0 administrators, *not just domain administrators*, an organization might have. By focusing on all the separate areas that control this precious file, an organization can begin to identify areas he or she needs to protect.

Tier 0 Security Roadmap

Where to begin

Get an understanding of the Active Directory Administrator, Domain Administrator, and Enterprise Administrator Groups

Active Directory Administrators / DA / EA

Dive into lesser known privileged groups that control Active Directory

Active Directory Built In Groups

Get an understanding on how to dive into those "other systems" that control tier 0

Identify and Secure Tier 0 Services, Systems, and Hardware