Secure Privileged Access with ESAE Model

blog.netwrix.com/2017/12/26/secure-privileged-access-with-esae-model

Russell Smith

Ensuring that systems are patched and that defense-in-depth security protections are working effectively, top the list of concerns for IT departments. But despite these efforts, security breaches are still on the rise because operational issues are commonly ignored.

Best practice dictates that privileged groups should remain empty most of the time. In practice, that means groups like Domain Administrators, BUILT-INAdministrators, and Enterprise Administrators, should only be populated when an approved change is being applied to Active Directory. But the reality is that many organizations issue IT staff with accounts that are members of one of the above groups, or members of other privileged AD groups.

In this blog post, we'll talk about a tiered administration model which ESAE is based on to smarter restructure the assigning processes of privileged access in your organization.

Analyzing Security Dependencies

But failing to grant privileges just before access is required, and for a limited time, isn't the only mister meaner. The clean source principle states that *a system can be dependent on a higher trust system but not on a lower trust system*. If IT staff log in to their notebooks, which they use for everyday tasks like browsing the Internet and reading email, with domain admin rights, then the clean source principle has been broken because the security of users' accounts rely on the security of the devices they log in to.

Compromised devices put the accounts of users that log in at risk. Hackers often target user workstations with the aim of getting access to privileged Active Directory accounts. Once a hacker has access to a domain-joined device, credentials can be harvested to get access to other devices on the network, eventually leading to a domain controller.

Because security dependencies can endanger the domain, domain admin accounts should be used only to log in to domain controllers or devices that are configured to the same level of trust as domain controllers. To achieve this goal, set up PCs that are specially configured for the purposes of managing domain controllers. Jump servers also break the clean source principle because they are dependent on the security of the device from where remote desktop sessions are initiated.

If budgets are tight or you don't want to deploy devices specifically for managing domain controllers, another option is to configure IT staffers' PCs to the same level as your domain controllers and deploy guest virtual machines (VMs) on the PCs. The VMs can be used perform everyday computing tasks. But deploying VMs for managing domain controllers breaks the clean source principle because the security of the VMs is dependent on the host.

Separation of Administration According to the ESAE Microsoft Model

As part of the Active Directory ***Enhanced Security Administrative Environment*** **(ESAE)** model or the so-called Red Forest in Active Directory, Microsoft recommends using tiered administration to create zones that separate administration of high-risk end-user devices and critical business systems. AD objects, including user accounts and computers, should be categorized into three tiers. With tier 0 representing the highest level of trust, and tier 2 the lowest.

Domain administrator accounts, privileged AD groups, domain controllers, and domains that have direct or indirect administrative control of the AD forest, should be categorized as tier 0. These objects can manage assets across all three tiers but can only log in interactively to tier 0 assets, which again means that domain administrators should never log in interactively to end-user devices.

Domain member servers, applications, systems that host sensitive business data, and accounts used to manage these systems, are categorized as tier 1 objects. Tier 1 user accounts can access and manage tier 1 objects. Tier 1 user accounts can access tier 0 objects using the network logon type but cannot log in to tier 0 devices interactively. They can manage tier 1 and tier 2 objects but can only log in interactively to tier 1 devices.

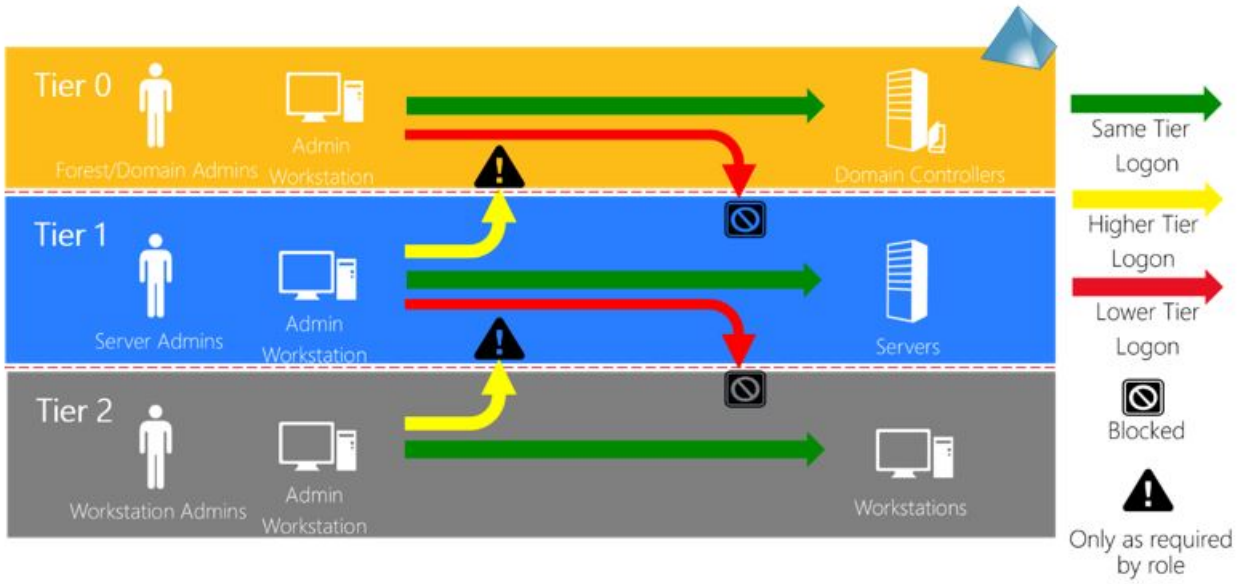

Figure 1 (Image Credit: Microsoft)

Tier 2 is reserved for end-user PCs and notebooks. In addition to end-users, IT helpdesk staff are also categorized as tier 2 objects and can perform network logons to devices in all tiers but are limited to managing tier 2 devices. Similarly, tier 2 users can also log in interactively to tier 2 devices.

To help enforce the tiered model, security controls like the Protected Users group can be used to prevent users with domain admin privileges logging in to tier 0 devices. Other security controls, like authentication policies and silos can provide more granular control.

For more information on how to use the Protected Users group, see Add Sensitive User Accounts to the Active Directory Protected Users Group on the Netwrix blog.

Privileged Access Management

Organizations need to be much more stringent with how administrative privileges are assigned to users, where those privileges are used, and what they are used for. Lateral movement across networks can be prevented by implementing privileged account management best practices, such as not using the same local administrator password on every device, not using domain admin accounts to log in to end-user devices, categorizing assets using a tiered administration model and performing continuous user activity monitoring.

The ESAE based on the tiered administration model isn't difficult to implement with some planning. It's not only important to consider the privileges assigned to users, but also whether they are using those privileges to access or manage resources. And if you can't implement automated IT administration, set up a manual process for managing access to privileged AD groups.

Russell Smith
IT consultant and author specializing in management and security technologies. Russell has more than 15 years of experience in IT, he has written a book on Windows security, and he coauthored a text for Microsoft's Official Academic Course (MOAC) series.