The Top-25 Active Directory Privileged Access Reports

Paramount Defenses recommends that all organizations that operate on Active Directory (AD) accurately* identify and lockdown the number of individuals who possess *Domain Admin* equivalent privileged access in Active Directory.

The following 25 AD privileged access audit reports can help organizations fulfill this paramount cyber security need –

1. Who can replicate secrets i.e. password hashes from an AD domain?
2. Who can manage or control Domain Controllers (DCs), AD backups and AD admin workstations?
3. Who can promote a machine as a new DC in any AD domain in an AD forest?
4. Who can create (or modify) an inbound forest/external trust with another AD domain/forest or a Kerberos realm?
5. Who can change the security permissions on the domain root object in an AD domain?
6. Who can change the security permissions on the *Configuration* and *Schema* partition roots in AD?
7. Who can change the security permissions on the *AdminSDHolder* object in an AD domain?
8. Who can change the security permissions on all administrative accounts and groups in AD?
9. Who can change the security permissions on domain computer accounts of all DCs and AD admin workstations?
10. Who can change the security permissions on all top-level Organizational Units (OUs) in an AD domain?
11. Who can change the security permissions on the default *Users*, *Builtin* and *System* containers in an AD domain?
12. Who can change the default *Domain* group policy or the default *Domain Controllers* group policy in an AD domain?
13. Who can link a group policy object (GPO) to the domain root or to the *Domain Controllers* OU in an AD domain?
14. Who can change the membership of all administrative groups in an AD domain?
15. Who can reset the passwords of all administrative accounts in an AD domain?
16. Who can disable the requirement of Smartcards for interactive logon on all administrative accounts in an AD domain?
17. Who can modify critical configuration data contents in the Configuration and Schema partitions in an AD forest?
18. Who can change LDAP query policies, quotas and FSMO role-holder assignments in an AD forest?
19. Who can change the *Trusted for Unconstrained Delegation* setting on all domain computer accounts in AD?
20. Who can manage the OUs in which the domain computer accounts of all AD admin workstations reside?
21. Who can link a GPO to the OUs in which the domain computer accounts of all AD admin workstations reside?
22. Who can disable administrative accounts in an AD domain, or modify their account settings (e.g. logon script)?
23. Who can read and change the LAPS password on domain accounts that avail of the LAPS protection feature?
24. If SID History is enabled, who can change the *SID History* attribute on all domain user and computer accounts?
25. Who is delegated what privileged access domain-wide in AD so as to be able to create, manage and delete OUs, user accounts, computer accounts, security groups, service connection points, containers, mailboxes etc. in AD?

* For AD privileged access reports 5 – 11 above, additionally one may also wish to consider who can change the ownership of these objects.

***** The accurate identification of who has what privileged access in Active Directory requires the precise determination of exactly who has what Active Directory Effective Permissions on various pertinent objects inside Active Directory.