BDO

AUDIT • ADVISORY • TAX

ALICE

A DIGITAL AUDIT SOLUTION, BROUGHT TO YOU BY BDO

BASIC SECURITY HYGIENE ASSESSMENT

OVERVIEW

A large portion of data breaches and system compromises are as result of breakdowns in basic security hygiene disciplines. Using ALICE, we are able to assess the hygiene of your basic security control environment quickly, cost-effectively and remotely.

WHAT CONTROLS ARE TESTED, WHERE APPLICABLE?

User Administration

1. Identification of duplicate usernames in a system.
2. Identification of multiple user profiles in a system.
3. Identification of generic user profiles.
4. Identification of dormant user profiles.
5. Identification of inactive user profiles.
6. Identification of terminated employees that still have access to systems.

Microsoft Baseline Network Configuration

7. Number of administrators are appropriately limited.
8. The local guest user profile on devices has been disabled.
9. Domain level auditing of security related events has been enabled.
10. Automatic logon has been disabled for all devices.
11. Windows systems do not use FAT or FAT32 file systems.
12. All local user profiles have passwords set to expire.
13. Anonymous user profiles have been restricted on the network.
14. Network shares are appropriately limited.

Password Configuration

15. User profiles are locked out after five (or less) failed sign-on attempts.
16. Password history has been enabled to prohibit the re-use of the previous six (or more) passwords.
17. Password complexity is enforced.
18. Password complexity rules enforce the use of upper- and lower-case characters (e.g. a z, A Z).
19. Password complexity rules enforce the use of alpha, numeric and special characters (e.g. 0 9,!@#$%^&*()_+|).
20. A password length of at least eight characters or more is enforced.
21. Anonymous user profiles have been restricted on the network.
22. The minimum password age is 48 hours or more.
23. All local user profiles have passwords set to expire.
24. User profiles do not bypass password controls.
25. There are no active user profiles with passwords that have not been reset in over 90 days.

Patch Management

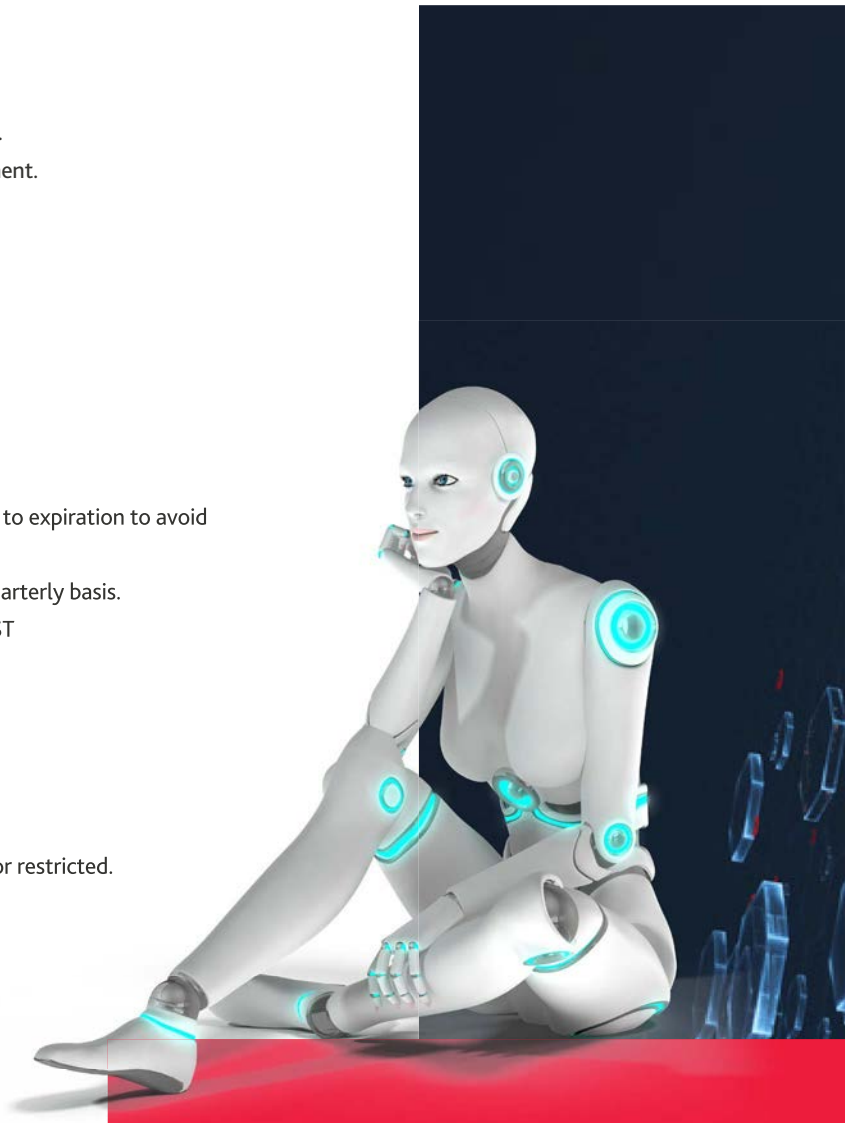
26. Dentification of duplicate usernames in a system.
27. Operational patches are up to date across the environment.
28. Critical security patches are up to date across the environment.
29. Security patches are up to date across the environment.
30. Service Packs are up to date across the environment.

Website & Certificate Management

31. Public facing websites utilize HTTPs.
32. HTTPs websites are utilizing a secure certificate.
33. The certificate has not expired.
34. Certificate and keys are replaced no less than 30 days prior to expiration to avoid unplanned downtime.
35. The websites are scanned for vulnerabilities at least on a quarterly basis.
36. Certificate validity periods (rotation periods) are within NIST recommendations unless specific exception is granted.

WordPress Management

37. A valid user profile cannot be determined from WordPress.
38. Access to the WordPress Readme.html has been removed or restricted.
39. WordPress plugins are up to date.
40. WordPress software is up to date.
41. WordPress themes are up to date.



WHAT DATA IS REQUIRED?

- AD extracts via a connector.
- System listings of users for the in-scope systems in required data schema.
- Employee listing of all active and terminated employees in required data schema.
- IP Range for in-scope websites and the ability to update the header tag of the website.
- IP ranges of the Windows environment for the patches and security connectors.

WHAT IS THE DELIVERABLE?

A user-friendly report indicating the status of the controls tested coupled with recommendations for improvement. This report can be used by all governance stakeholders, ranging from IT management to the members of the Board.

BENEFITS FOR YOU

- Quick and easy deployment.
- Minimal time and effort.
- Near real-time visibility into the basic security risks in the IT environment.
- Ability to re-run the assessment periodically, if required.
- Independent insights and recommendations for remediation.
- Easily consumed reporting by the C-Suite and members of the Board and Audit & Risk Committees.

FOR A CLEAR PERSPECTIVE, PLEASE CONTACT US:

NEVELLAN MOODLEY
Partner
nmoodley@bdo.co.za

/BDOSouthAfrica /bdoafrica /bdo_sa /company/bdo-south-africa

www.bdo.co.za