Summary Report: TESTBED

System: PUFFADDER (Snake.com)
Analysis Date: 08-Nov-2013 CONFIDENTIAL

Rating Against Industry Average

☺	😐	☹
	X	

Overall Comments

Overall, security is about average compared with other Active Directory domains used in the Manufacturing sector.

The machine has the latest Service Pack for Windows installed.

The main concern is that most users are not forced to change their passwords on a regular basis.

Report Highlights

Report Section / Comments	
1	**Summary Graphs** Graphical comparisons against the industry average and leading practice.
3	**Domain Accounts Policy** Some System policies are weak, for example: • Controls that reduce the risk of intruders gaining access to the system via repeated password guessing attempts could be strengthened • The client should consider renaming the Administrator (uid 500) and Guest (uid 501) accounts via policy See comment 15 also.
4.1	**Audit Policy Settings** The client is making good use of Windows' auditing features.
5	**Group Policy Objects** You should check the policies defined in the Group Policy Objects to ensure they are appropriate.
6	**Password Settings Objects (PSOs)** There is one Password Settings Object (PSO) defined on the system. See also SekChek's white paper: *MS-Windows Password Settings Objects (PSOs)*.
8	**User Accounts Defined In The Domain** There are 16 user accounts defined in the domain. Many accounts are not clearly assigned to specific people. This will cause accountability concerns if they have access to powerful functions or sensitive information. 13% (2) of accounts have security administration privileges. The Administrator account (uid 500) has not been renamed.

This report summary is provided to highlight some of the main issues detailed in the SekChek reports. The overall rating is against the industry average and not against leading practice. All comments are generic. For best results they should be considered together with an understanding of the client's own unique business and computer environments.

Report Section / Comments	
10	**Domain Local Groups and their Members** Note that 1 account from another domain is a member of a local group. This account will acquire the privileges of the local group it belongs to. See comment 24.5 also.
13	**Last Logons, 30 Days and Older** SekChek shows that 44% (7) of accounts have not been used in the last 3 months. However, most are disabled.
14	**Passwords, 30 Days and Older** Passwords for 44% (7) of accounts have not been changed in the last 3 months. However, most are disabled.
15	**Passwords that Never Expire** 88% (14) of users are not required to change their passwords due to settings at account level. Note that these settings override the system's Policy settings (see report section 3). This should be OK for service accounts.
16	**Accounts not Requiring a Password** One user account is allowed to logon with a zero length password due to security settings in the user account. See the report for implications and a detailed explanation. See also SekChek's white paper: *MS-Windows Accounts not Requiring a Password*.
18	**Users Not Allowed to Change Passwords** Passwords for 56% (9) of accounts can only be changed by a security administrator. This should be OK for service accounts.
20	**Disabled Accounts** 19% (3) of accounts, including the Guest account, are disabled.
23	**User Accounts Created in the Last 90 Days** 7 accounts were created in the last 90 days. You should confirm that the creation of these accounts was appropriately authorised by management.
24.5	**Rights Assigned to Users** The most powerful rights are restricted to the accounts with security administration privileges. Note that accounts from another domain will also acquire powerful privileges. See 10 above.
25	**Discretionary Access Controls (DACL) for Containers** The client should check that the listed permissions over objects are appropriate and in line with users' job functions.
26	**Trusted and Trusting Domains** The domain analysed has trust relationships with 2 other domain. *Note that security of the domain analysed is very dependent on the quality of security (particularly user authentication controls) on the trusted domain also. Similarly, security on the trusting domain is dependent on the quality of security on the domain being analysed.*

Report Section / Comments	
29	**Accounts Allowed to Dial In through RAS** 2 accounts can be used to dial-in to the domain via RAS. Dial-back controls are not fully implemented. SekChek could not determine whether there are any RAS servers on the network because the host system's Computer Browser service was not running during the Scan.
30	**Services and Drivers on the Machine** The system seems to be running the Sophos Sweep (service was running) anti-virus software.
36	**Logical Drives** The system is using the NTFS file system. All disks have at least 20% free space.

Tip: Make navigation easier by adding the back button to your Quick Access Toolbar in MS-Word.

This report summary is provided to highlight some of the main issues detailed in the SekChek reports. The overall rating is against the industry average and not against leading practice. All comments are generic. For best results they should be considered together with an understanding of the client's own unique business and computer environments.