Access Management - Separation of Duties Tutorial

This tutorial shows the use of SODanalyse to identify Separation of Duties violations from an application dump of identities and their responsibilities. AMX tools such as identityReport can prepare these files from Resources such as the Active Directory.

AMX runs on Windows and must be setup as shown in the AMX Tutorial Setup document. In this tutorial identityReport and identitySync are run from the Command Line using AMXRun which sets the environment variables.

Identity and Responsibility Application Reports.

The AMX install has reports from an application for use with SODanalyse in the Tutorial4 directory.

1. Review the SODanalyzer Properties File

Open the SODanalyse.properties file. The full description of the properties are described in the AMX Role Management Document. The key ones are:

- SODmatrixFile, the name of the file containing the SOD rules matrix
- responsibilitiesFile a CSV file containing an account name and its responsibilities
- SODReport the filename for results of the analysis, a SOD analysis report.

2. Review the SOD rule matrix

Open the SOD rules matrix SODmatrix.xls using Excel.

Notice the Initiate Wire Transfer responsibility on row 35. It is incompatible with all the other responsibilities as you read across the page. When the line of symmetry is found the incompatible responsibilities become the column AI and reading down the column the only compatible responsibility is Payroll Bank Reconciliations.

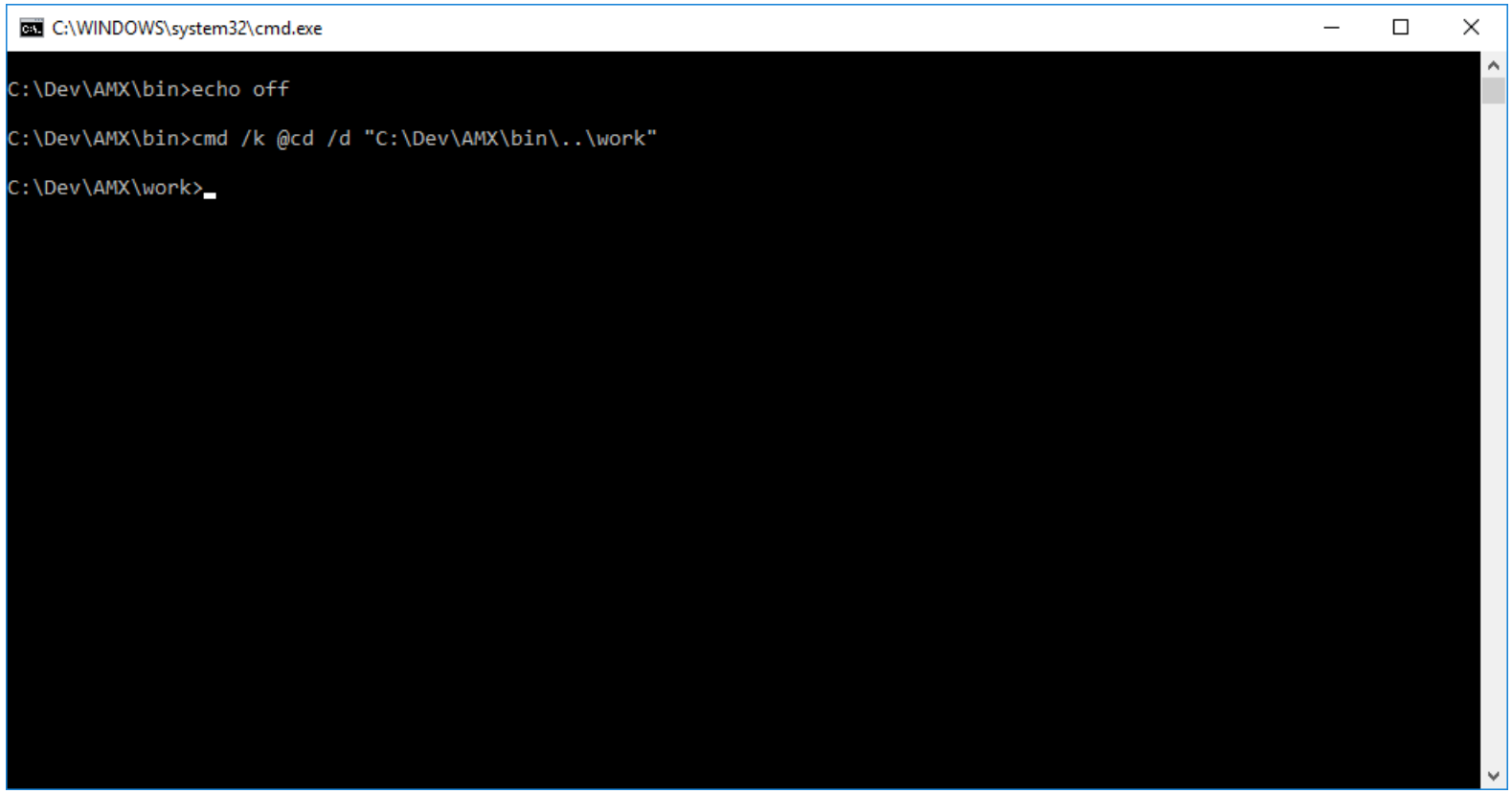
Only the left hand of the matrix is populated, and anything in the right hand side causes an error. This is the result of bad experience with asymmetric SOD rule definitions. SODanalyzer completes the full matrix internally in a consistent manner, something that is difficult to do manually.

3. Review the responsibilities File

This is synthetic data, the file users.csv contains the account names and their roles.

4. Run SODanalyze

Right click on AMX Run in the Start Programs menu or AMXRun.bat in the installation directory bin, and Run as Administrator.




```
C:\AMX\Tutorial4>SODanalyze SODanalyze.properties
Begins Mon, 04 Jan 2016 12:54:16 GMT
SOD error for BrownR
AP Payments,Sales Order Entry
AP Voucher Entry,Sales Order Entry
Bank Reconciliation AP,Sales Order Entry
Sales Order Entry,Vendor (add/delete/change)
```

```
Finished Mon, 04 Jan 2016 12:54:16 GMT

C:\AMX\Tutorial4>
```

5. Review the Results

The results of the analysis are also written to the file specified in the property “SODreport”.

The violations are reported once in pairs.

```
SOD error for BrownR
AP Payments,Sales Order Entry
AP Voucher Entry,Sales Order Entry
Bank Reconciliation AP,Sales Order Entry
Sales Order Entry,Vendor (add/delete/change)
```

AP Payments is not allowed with Sales Order Entry and vice versa. In the SOD rule matrix AP Payments is row 3 and column 3 (C). Scroll down column C and at row 27 the rule is established for Sales Order Entry.

Notice in the results, every violation involves Sales Order Entry. The violation could be cleared by removing that responsibility from BrownR.

6. Update the SOD Risk

The results are for all the SOD rules, open the SODmatrix.xlsx and notice that the rules are marked as H or M. On row 27 Sales Order Entry and Bank Reconciliation AP have a M risk. Open the SODanalyze.properties file and update SODrisk = H this will only report H SOD rule violations.

7. Review the Results

Run SODanalyze again, the reported violations are reduced to just:

```
SOD error for BrownR
AP Payments,Sales Order Entry
AP Voucher Entry,Sales Order Entry
Sales Order Entry,Vendor (add/delete/change)
```

8. Update the SOD Risk

Open the SODanalyze.properties file and update SODrisk = M this will only report M SOD rule violations.

9. Review the Results

Run SODanalyze again, the reported violations are reduced to just:

```
SOD error for BrownR
Bank Reconciliation AP,Sales Order Entry
```

Having various levels of risk in the SOD risk matrix during the introduction of SOD processes allows medium or low risk violations to be the subject of compensating controls and only the high risk violations remediated.

10. Update Responsibilities

Open Users.csv in a suitable editor and on line 14 remove the first responsibility Sales Order Entry from BrownR including the list delimiter ":". Save the file and re-run SODanalyzer

11. Review the Results

The results show no SOD violations.

This simple fix is never so simple in production. There are two scenarios.

a. SODanalyze is run on existing responsibilities, as is being done here. The intention is to clean up responsibilities and make sure there are no SOD violations. A discussion will have to be used so that the owner of account BrownR can choose which responsibility to remove. Experience with these sorts of meetings has been that the first response is "None of them", the second is that the SOD rules are wrong, and the third is that there must be some compensating control that can be used.
b. This is an access request for a new responsibility, in which case the response "denied" and the reason why is given to the requestor. This is often countered with responses 2 & 3 above.

Violations may not be resolvable, depending on the organisation and whether security trumps operations. It sometimes does. If you are an auditor, violations are audit comments, if you are an access manager they are a metric, and if you are a security manager they are a problem.