Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Midrange & Mainframe systems for Security Policies compliance control Tool

The goal of this document, within the scope of the practical exam for the GSEC1 SANS2 option 2, is to present a solution for a Company, in order to be able to manage and apply computing security rules on Mainframe and Midrange systems, as well as Facilities Management systems complying with other security rules, specific to customers. With the help of a tool accepting the OS platform Z/OS MVS3, Z/OS VM, OS4004 and the security product: RACF5, ACF26, CA TSS7. This tool runs on a law table applicable on any computing sys...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Midrange & Mainframe systems for Security Policies compliance control Tool

© SANS Institute 2005, Author retains full rights.

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2

Submitted by: Pierre CAILLOUX, December 1, 2004
SANS Conference - London - June 2004.

© SANS Institute 2005 Author retains full rights.

ABSTRACT

The goal of this document, within the scope of the practical exam for the GSEC[1] SANS[2] option 2, is to present a solution for a Company, in order to be able to manage and apply computing security rules on Mainframe and Midrange systems, as well as Facilities Management systems complying with other security rules, specific to customers.

With the help of a tool accepting the OS platform Z/OS MVS[3], Z/OS VM, OS400[4] and the security product: RACF[5], ACF2[6], CA TSS[7]. This tool runs on a law table applicable on any computing system, or a set of systems, or a particular system. The tool creates executable commands on various systems managed by the tool, in order to have the security rules applied. Sending of controls by mail to the various individuals affected to their job, using an addressee table. As well as a part of the controls validation by ISPF/TSO[8] chosen within the tool.

Purpose

- Control the protection of sensitive security elements
- Provide facilities to manage events
- Analyze protection of the sensitive operating system resources
- Control compliance relationship rules
- Provide housekeeping[9] report (sub-system)
- Dispatch report to appropriate administrators

Methodology

- Store every sensitive records in DB2[10] tables
- Incorporate automatically sensitive operating system resources with an assigned level
- Dispatch reports via email
- Administrator's activity logs
- Archive reports for evidences of control

[1] GSEC (GIAC) Global Information Assurance Certification Security essential certification
[2] SANS institute
[3] Z/OS MVS multiple virtual storage, Z/OS VM virtual machine (IBM System 370 & 390)
[4] OS400 (Operating system 400) for midrange IBM system
[5] RACF (Resource Access Control Facility) IBM security software
[6] ACF2 (Computer associates) security software
[7] CA TSS (Computer Associate) security software
[8] ISPF / TSO (interactive system productivity facility, time sharing option) IBM software
[9] "Housekeeping" control ids found in a product sub-system (DB2, ….) and not found in the system security product.
[10] DB2 (database 2) an IBM relational database management system

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Table of Contents

Abstract…..……..... 2
Table Of Contents……... 3
List of Figures …..…….. 4
Problem Description…….…….…. 5
ntroduction…….……. 6-7
Overview Of The Tool…….……..... 8
The TOOL…….…. 9-21
Prerequisite …… 9
Tool concept …….. 10
Universal platform ……..…;. 11
Security Data ……..…… 11
Data extractor…… 11
Data centralization…… 12
Data modeling…….. 12-14
Data repository……..... 14
Checker …… 14
Reference validation……..... 14
ISPF interface ……..... 15-18
Output controls……..…… 18
Commands …… 18
Mails…….. 19
Compliance control report……. 19
Delta report…….…. 20
Report / Analysis…….. 20
Document management…….. 20
CBN (Continuous Business Need validation)…… 21-22
Flow…..…… 23-24
Qualities of the tool …… 25-28
Cost/Saving…….. 28
References …… 29
Summary……. 30
Annex 1: Data extractor …… 31
Annex 2: Modeling…….. 32
Annex 3: Example of Security data modeling …… 33

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

List of Figures

Figure 1 : Tool architecture…… 8
Figure 2 : Prerequisite standardization …… 9
Figure 3 : Tool concept …… 10
Figure 4 : Data centralization…… 12
Figure 5 : Data modeling…… 13
Figure 6 : ISPF Primary panel…… 15
Figure 7 : ISPF Focal Point monitoring …… 16
Figure 8 : ISPF Reference Table management …… 17
Figure 9 : ISPF Detail on one resource…… 18
Figure 10 : CBN (Continuous Business Need) …… 21
Figure 11 : Data flow…… 23
Figure 12 : Example of data flow…… 24
Figure 13 : Level of security period …… 25
Figure 14 : Example of 0S/400 systems …… 27

Trademarks

The following terms used in this publication, are trademarks of the IBM Corporation in the United States or other countries.

DB2 CICS IMS MVS NETVIEW OS/390 OS/400 ISPF
RACF QMF

IBM ® International Business Machines Corporation

And other following term used is trademark of Computer Associates, INC (CA).

Top secret ® ACF2 , TSS .

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

PROBLEM DESCRIPTION

Many Companies apply and manage their computing security rules as and when the need arises, most of the time when they have to prove compliance to an business control organization. The implementations review are becoming more and more important within the world of protection, referenced in the chapter « Defense-in-Depth » in the SANS[1] security course. The men/months had to be increased in order to cope with this surveillance and security rules application workload. In a first step, the companies create complete computing services. This is no longer dealing with security from time to time, but men are assigned to security duties on a full time basis. The main difficulty is to apply and maintain security rules rapidly, due to the number of systems increase, without waiting too long between the controls and the rules application.

How can we know a security rule is not applied on a set of computing systems?

For a new security rule, what are the systems in deviation, what is the impact on the whole computing stock managed by the tool?

All these questions are raised by the companies, delay to apply these new security rules is generally important. They are added to other existing rules which have not been applied yet.

Thus many companies leave their computing to professionals' care. It has become an emerging market for many companies called "Outsourcing".

The tool has to meet the security audits requirements. It may as well be used to answer some of the standards controls, like ISO9000[2], SAS70[3].

[1] SANS institute
[2] ISO9000 International Organization for Standardization
[3] SAS70 Statement on Auditing Standards Number 70 (internal control law "Sarbanes-Oxley")

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

INTRODUCTION

Policies and processes are vital to the security business. This software tool mainly running on Mainframe systems MVS[1] is able to make periodic and automatic health security review. Good data security practices are becoming increasingly important due to a number of trends such as:

- Large number of inter-connected systems
- Use of easy-to-use high level languages
- General familiarity with data processing
- Easy access to information stored in databases

Without the implementation of appropriate data-security practices these advances could result in a higher like hood of unauthorized persons accessing, modifying, or destroying data, either inadvertently or deliberately.

My purpose is to present this tool within its general aspect with some important detail points in particular.

The tool includes following phases:

- The extractor (Data collection)
- Data transfer
- The Focal Point processing
  - Modeling
  - Security rules implementation
  - Data processing
  - Controls
- Reports dispatching
  - Output controls
  - Report Analysis results
  - Document management
  - Available data
- Specific additional control (local control)

[1] MVS multiple virtual storage (IBM System 370 & 390)

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

This tool is dedicated to security. All reports sent by this tool are auditable. The responsibility of the addressees has to be emphasized. The email report sent to the appropriate security administrator. The administrators are considered as being responsible for the security items, of the associated target systems, that are detailed in the report. The tool sends automatically all modifications on a destination table for validation to each administrator. You may -and it is advised- use the development part locally to produce reports on-demand from users, administrators or customers. Whenever necessary, design DB2/QMF[1] procedures for a punctual use with an automatic submission daily, weekly or annually to an email address reference.

My Company has assigned me the role of elaborating this tool and develop processes to send automatically reports to concerned individuals including results found by the tool, non-compliant security rules, deviations as well as the computing devices annual inventory. Statistics have also to be produced to follow-up the security evolution of security on all the computing systems managed by the tool. A help to the administrators on the use of the tool, and on data manipulation is available by DB2/QMF requests. Since several years, I participated actively to the creation of this tool on the DB2/QMF part. Now, this tool is a European tool and I provide support to users to help them understand and develop local procedures and implement new policies.

Attending SANS courses last June, was a great help to me. My mind has been opened to the other technical fields. Now I am able to see the connection between them.

[1] DB2/QMF Database 2 (an IBM relational database management system) Query management facility (an IBM software)

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

OVERVIEW OF THE TOOL

The tool comprises: (see figure 1 below)

- The target systems and the extractor
- The transfers of data security
- The focal point
- The communication

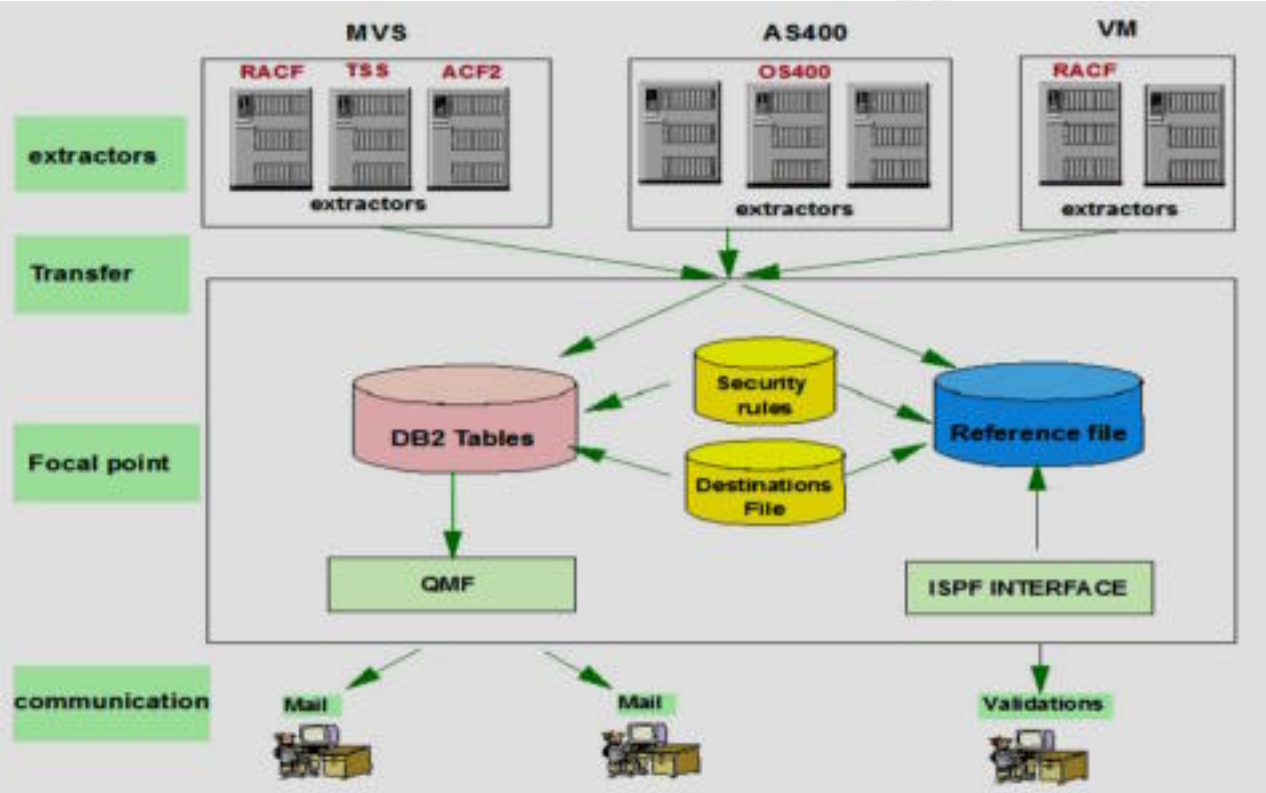


Figure1: tool architecture

The focal point, which runs in an MVS[1] environment, stores the security data in data repositories (DB2)[2] for analysis. Security analysis is done by comparing the data extracted from the target systems with general security rules stored in a security rules file.

[1] MVS multiple virtual storage (IBM system 370 & 390)
[2] DB2 (database 2) an IBM relational database management system

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

THE TOOL

Prerequisite

In a first step, each computing system has to support an architecture update including 10 "system standardization projects" phases. The tool enables this standardization, more easily on all centralized data.

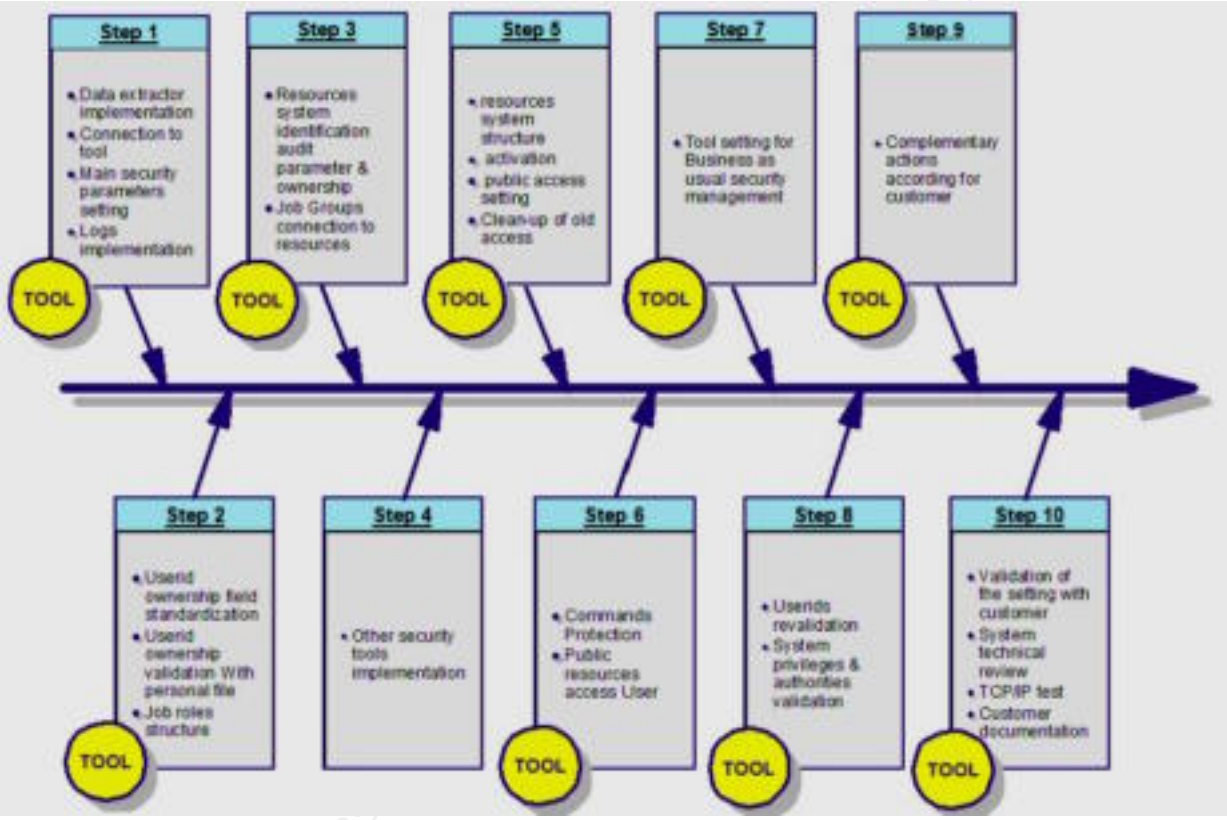


Figure 2: Prerequisite standardization[1]

Step 1 : Collect and store the security data

Step 2 : Userids[2] standardization for the tool

Step 3 : Operating system resources sensible standardization

Step 4 : Adapt records for control by the tool other security local tool

Step 5 : Standardize Operating system sensible resources

Step 6 : Apply command protection and public access with validation

Step 7 : Customize reference file

Step 8 : Validation of privileged userid and authorities

[1] reference: GSEC Practical Assignment of "Yves Depoorter" April, 2004
[2] "userid" the term « user id » is a general term for indicate the user, the group, the access id group or logon id

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Step 9 : Complementary projects with sub-systems

Step 10 : Validation of the security system management

Each step may be re-sequenced with the tool running after running.

The tool proposes a set of standard security rules applicable to each platform managed by the tool ; a detection of the system sensible resources and proposes a protection for all of them.

Tool concept

The tool general principle is to extract security data on each system towards a focal point and to develop processes to send automatically reports to concerned individuals, including results found by the tool or to make controlled security data available for validation by the tool. Intermediate parts include data centralization in a specific format (modeling), a data manipulation with security rules table and the preparation of reports to send or validate.

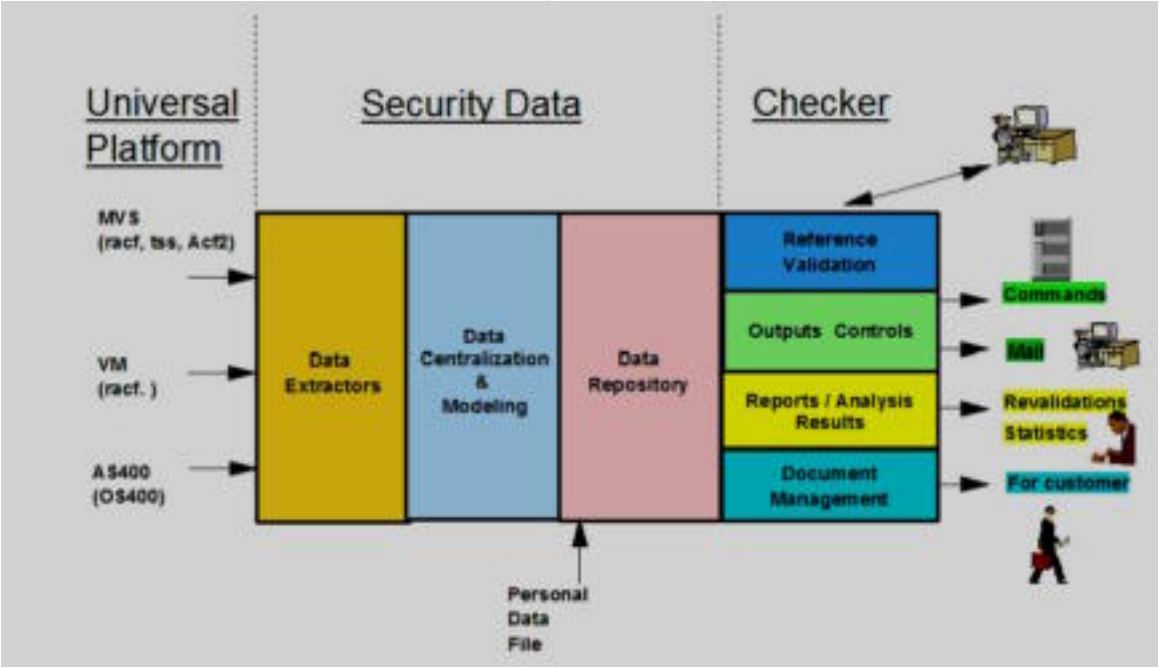


Figure 3: Tool concept

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Universal platform

The existing extractors are adapted to each platform mentioned in Figure 3. A new extractor could be easily developed as it has a basic conception for extracting all security data. The data will be "modelized" on the focal system to enter the application.

Security Data

Data extractor

Security data and system information are extracted and sent to a focal point. Various utilities are run, like RACF[1] utilities (DSMON, IRRDBU00)[2], as well as system commands (DISPLAY) and sub-system commands (HLIST USER)[3]. Data are extracted from these outputs, merged into a single DATA file and sent to the focal point of processing as a DFDSS DUMP[4] compressed format on OS/390 platforms and TERSED[5] file on VM/ESA[6] platforms. For the OS400 [7]system the file are not compress but the extractor run the command "save object" with compress = *yes option.
The tool support different operating system platforms and security products, so the following sub-components have been developed:

- RACF/VM[8] and RACF/MVS[9] extractor
- OS/400[10] extractor
- CA-TSS[11] OS/390[12] extractor

The extractor is executed on each system be managed by the tool. The aim is to capture maximum of data related to security even if they are not needed today and try to have the minimum of complexity to avoid having to update frequently the extractor.

An extractor is conceived per platform. Refer to "annex 1" the various data groups captured on each platform; the use of standard utilities to simplify maintenance.

[1] RACF (resource access control facility) IBM software of security
[2] DSMON IRRDBU00 extract data security monitor or RACF software
[3] HLIST USER command for RACF software
[4] DFDSS DUMP data facility data set services (IBM software product)
[5] Terse software compress file for VM system
[6] VM/ESA virtual machine/enterprise systems architecture (IBM)
[7] OS400 IBM operating system for AS/400
[8] RACF (resource access control facility) IBM software of security
[9] MVS multiple virtual storage (IBM System 370 & 390)
[10] OS400 IBM operating system for AS/400
[11] CA-TSS Computer Associates International, Inc.
[12] OS/390 IBM operating system 390

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Data centralization

The process of data centralization is to make a transfer within a short time and to use a standard transmission adapted on each platform or customer environment. The files are compressed on target system and decompressed on focal system. See the figure 4 below. A study is carried out with the customer to define the encryption method, mainly as concerns data transferred outside the Intranet.

Before to transfer the security data, ICSF[1] could be used to encrypt the data between remote systems and focal point system.

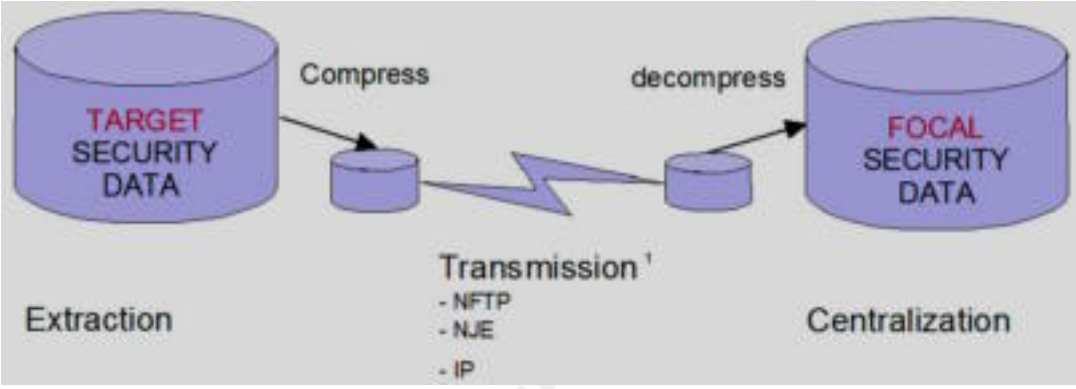


Figure 4: Data centralization

Data modeling

The set of data is modelized in order to distinguish the different computing systems, the various platform and the different sub-systems which compose the various specific entities for a precise control during the post treatment. The objective is to classify all data into boxes with an entity combined by convention.

The choice is to take 3 key words:

Domain category type ident

"**DOMAIN**" : We enter the name of the operating system or the name of the security software or sub system.
"**CATEGORY**" : For the operating system, we indicate computing objects depending on its vocation or the name of the sub system.
"**TYPE**" : Here, we indicate the type in the combined domain category type. Generally, we have here Authority, public access or setting notions.

[1] ICSF integrated cryptographic service facility (IBM software)
[2] Transmission NFTP (NetView file transfer program) NJE (network job entry) IP (internet protocol)

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Forming an entity called « source », a system name and an image name are added to anticipate the system megaplex[1]. On Figure 6, we can notice all security data, wherever they come from, are subject to the « modeling » to enter the application.

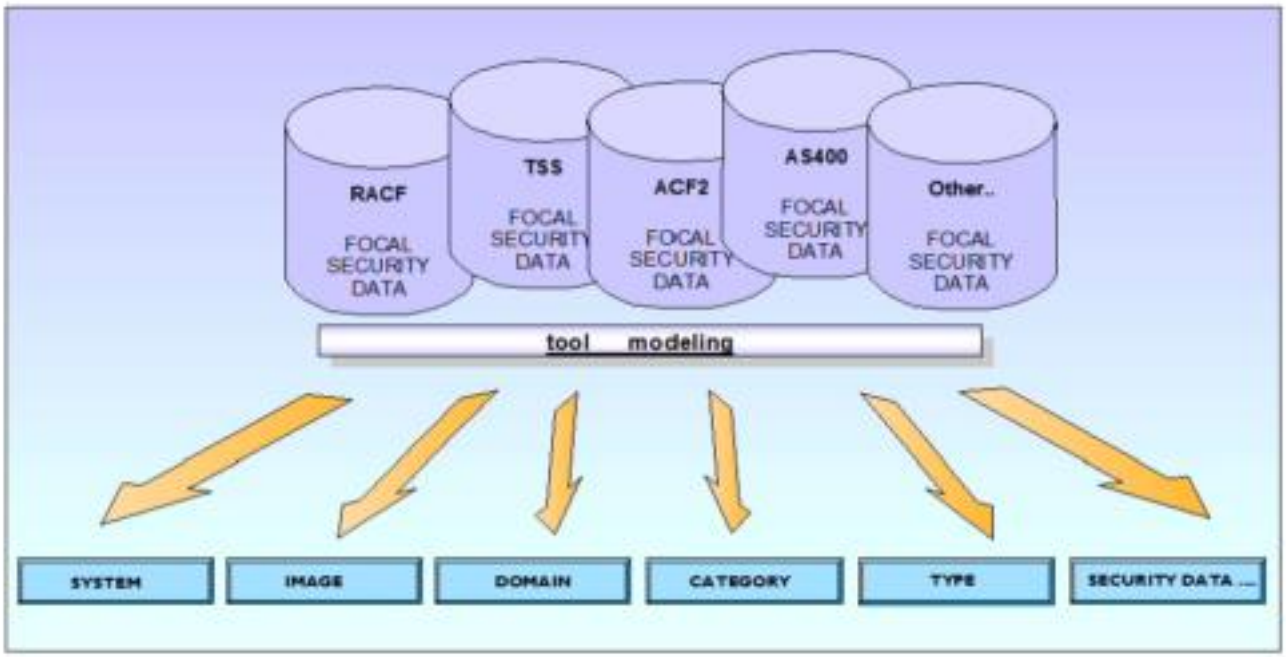


Figure 5: Data modeling

For example: If we use an MVS[2] operating system and RACF[3] security software, we will get for the USERID category.

SYSTEM	IMAGE	DOMAIN	CATEGORY	TYPE	VALUE
Systxx	Image2	RACF	USERID	BASIC	AUTOTASK1 ownership
Systyy	Image3	RACF	USERID	AUTH	AUTOTASK1 operation
Systzz					

Entities known as « source » may be built by the tool, these sources are useful to be able to apply the lows and to extract the deviations.

[1] megaplex one hardware system with several system here as in image
[2] MVS Multiple Virtual Storage (IBM System 370 & 390)
[3] RACF(Resource Access Control Facility) IBM security software

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

SYSTEM	IMAGE	DOMAIN	CATEGORY	TYPE	VALUE
Systxx	Image2	RACF	OSR	BASIC	name
Systyy	Image3	RACF	OSR	ACCESS	SYS1.* username READ
Systas400		OS400	OSR	BASIC	QSYS db2jobsec *lib

OSR: Operating system resources: sensible resources of the system and its accesses.

Refer to the various sources examples in Annex 2.
The example of a part of security data for Mainframe RACF setropts (global options) in Annex 3.
The list of the security data with the modeling RACF RACF SETTING SETROPTS. This example shows how it's possible to adapt a rule for applying a policy.
The option of setting setropts "addcreator" must be "active". The tool compares security data with the rules to be applied on them. If the security data is not in accordance with the rules, then a report is sent to the administrator corresponding to the DOMAIN CATEGORY TYPE indicated in the table of addressees.

SYST	SYSN	DOMAIN	CATEGORY	TYPE	DATA SECURITY		VALUE
SYSTMVS	MVSA	RACF	RACF	SETTING	SETROPTS	ADDCREATOR	INACTIVE

Data Repository

The « data repository » comprises 4 datasets, spread among a set of DB2/QMF tables:
A first dataset corresponds exactly to the system image.
A second one to the data built by the tool.
A third one to annex data « personnel organization » including internet addresses for mails, as well as the information from the collaborator to his manager and the manager's manager.
A fourth one for statistic data.

Checker

Reference Validation

Use of a law table (Security Information technology is a vital component of business success). The laws implementation by the administrator is ensured in a table, with the possibility to test the result of its implementation on the whole set of systems and to appreciate the impact.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

ISPF[1] Interface

The ISPF interface is used on the tool MVS[2] focal point. Specific panels for the tool have been created and only the elements concerning the administrator may be seen, with a possibility to switch for the administrators backups. The delta process proposes several pathswithin the different data sources. The non control, the logging, the mail sending and at least, the validation control in the ISPF panel; in the data validation panel for a specific source. We find again the entity called « source » with the indication of actions to take or current state. All security data are present in the ISPF interface, they may be consulted at any time. For each element, the administrator may select and see the details. Thus, he may take the decision on the action to be taken.

Source selection Panel

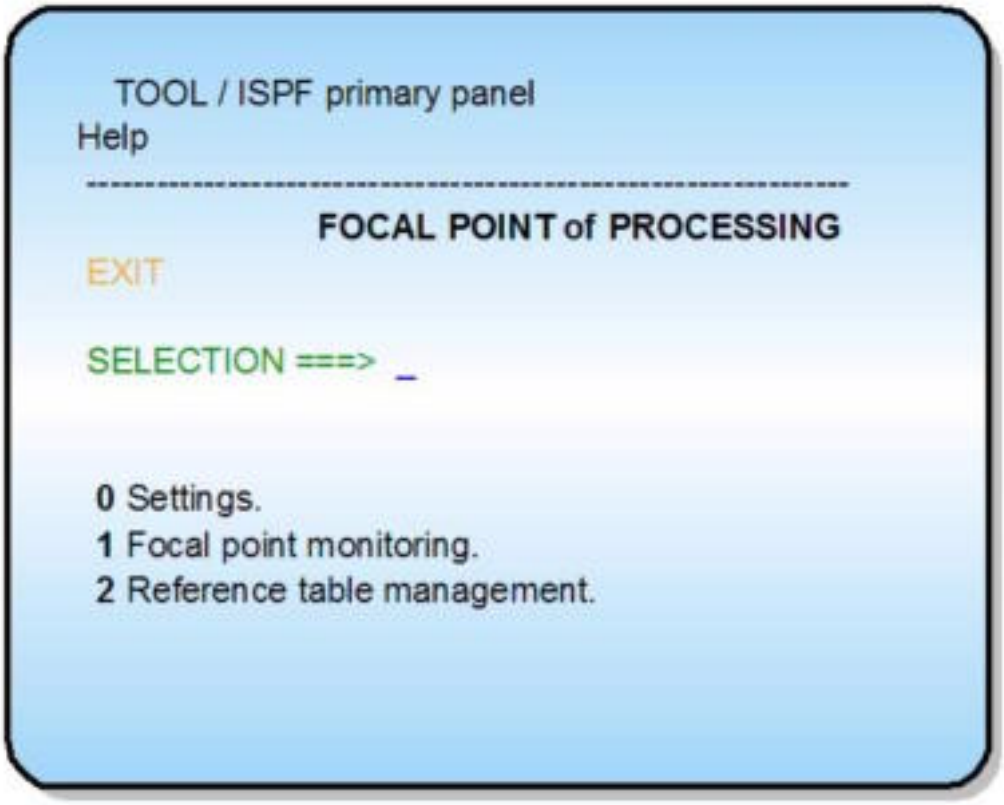


Figure 6 : ISPF primary panel

[1] ISPF interactive system productivity facility, an IBM software
[2] MVS multiple virtual storage (IBM system 370 & 390)

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

The ISPF primary panel shows the different selections that may be used.

Option 0 : Indicated the different libraries the tool needs. This option is a part of the tool customization at the installation time on the focal point.

Option 1: Focal point monitoring, this option enables the tool administrator to update the 3 main tables.

Rules Table
Destination Table
System Table

```
  TOOL / ISPF Panel option 1
   Help
-----------------------------------------------------------------
                         FOCAL POINT MONITORING

 COMMAND ===>

 Selection ( S  or  B  for Browse,  E  for Edit)
  !
! v ! Type file ! Data set name                                !
!***!************!*********************************************!
! - ! RULE       ! SYS1.USC.SUSCCNTL(RULES)                    !
! - ! DEST       ! USC.GDG.DEST                                !
! - ! SYST       ! USC.USC.LOCAL.CNTL(SYSTEM)                  !
!***!************!*********************************************!
```

Figure 7: ISPF Focal point monitoring

The selection may be a write or an update one. It is advised to restrict the access to these tables.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Source selection Panel

```
TOOL / ISPF Reference Table Management
*****************************************************************************
                         REFERENCE TABLE MANAGEMENT        Row 31 to 44 of 44
COMMAND ===========>                                          SCROLL==> PAGE
                                                   ISPF ID = USRADM1
S Select  J Joblog display
|                                                      TOTAL  PENDING CORRECTED
V SYSTEM   SYSN DOMAIN   CATEGORY  TYPE       DATE     REC    STATUS  STATUS
  ---1---- -2-- ---3---- ---4---- ---5---- -----6----  --7--    --8--    --9--
  JES2RINT RINT TSS      TSS      AUDIT    2004-10-22    24
  JES2RINT RINT TSS      TSS      PUBLIC   2004-10-22   244
  JES2RINT RINT TSS      TSS      SETTING  2004-10-22   179
  JES2TINT TINT TSS      ADMIN    AUTH     2004-10-22  1278        4
  JES2TINT TINT TSS      BYPASS   AUTH     2004-10-22    64
  JES2TINT TINT TSS      DATASET  ACCESS   2004-10-22  1045
S JES2TINT TINT TSS      DATASET  BASIC    2004-10-22   568
  JES2TINT TINT TSS      OMVS     AUTH     2004-10-22    53
  JES2TINT TINT TSS      RESOURCE ACCESS   2004-10-22    67
  JES2TINT TINT TSS      RESOURCE BASIC    2004-10-22     9
  JES2TINT TINT TSS      TSS      ACID     2004-10-22   620        1
  JES2TINT TINT TSS      TSS      AUDIT    2004-10-22    21
  JES2TINT TINT TSS      TSS      PUBLIC   2004-10-22   264
  JES2TINT TINT TSS      TSS      SETTING  2004-10-22   169
****************************** Bottom of data ******************************
```

Figure 8 : Reference Table management

This option allows viewing and managing the security data gathered from the target systems. In this source of security data, all the items are here; and the delta process indicates the records are changed.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Selection detail on one item

```
TOOL / ISPF Detail of source
  Help
 -------------------------   SELECTED ENTRY STATUS   -------------------------
 COMMAND ---------->                                          SCROLL==> PAGE
                                                   ISPF ID = USRADM1

SYSTEM= JES2PAS1 DOMAIN= TSS      CATEGORY= DATASET  TYPE= BASIC     2004-11-03

          RESOURCE =  'SYS1.LOGREC'
          CLASS    =  DATASET
          OWNER    =  OWNOSR
          LEVEL    =  A
```

Figure 9 : ISPF Detail on one source

The screen above is an example of the display when an S (Select) is entered; and if it's a delta generated by the tool, it may be accepted.

Output controls

Commands:

Executable correctives commands on each system are generated by the tool ; a first executable commands file not analyzed by the administrator and another file with executable commands proposition for each system.

For examples:

- An organization change command (new service number or next Manager for an individual account)

- A proposal for canceling someone's account who has left the Company.

- An ownership modification command for a sensible resource following a security rule written in the law table.

Mails :

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

The tool is configured for e-mail reports to the appropriate security administrators. The type, frequency and content of these reports is tailored to the specific requirement of the recipient. The tool proposes the choice of the form (plain text or html).

There are two different types of report:

- Compliance control report

The compliance control report is provided usually on a regular basis. This report is often referred to as the weekly report, however it may be done more, or less frequently.

This report is divided into the following sections:

1. Userid[1] Ownership control

This entire control is the detection of ownership discrepancies for access keys to the computing system. The accounts are recorded with an ownership key on security programs for each appropriate platform and a comparison Vs a personal organization file.

The keys recorded on security programs are part of the prerequisites prior to the correct running of controls by the tool.

2. Compliance control

The compliance control section is to verify the security settings with respect to those predefined rules and other for implementation of local rules.

3. OSR rules compliance

In the tool, a standard setting detection is implemented with a level assigned to the profile. The profile automatically enters the compliance control process.

For example: the process detects the operating system sensible resource if the parameter UACC (Universal Access) is different from “NONE”.

4. Housekeeping control

The housekeeping control is to indicate any discrepancies between security setting in the software running on the target system and the associated setting in the operating security system. This section identifies whenever a corrective action is necessary.

For example: the userid in the sub-system running on the target system must be identified on the security database.

5. Summary of deviations section

The purpose of the deviation summary section is to make the synthesis of all deviations found in the report.

[1] “userid” the term « user id » is a general term for indicate the user, the group, the access id group or logon id

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

- Delta report

The delta report indicates the changes in security settings between two consecutive runs. Before the run, a new result of extractor must be loaded on the focal point. Generally, this run is a daily process. But it may be run on another period.

This report comprises two sections:

1. The Delta process

This section indicates all differences from a run to another on all security data for information. This parameter is to be indicated on the destination table (I: for Information).

2. Statistics on waiting for validation under ISPF.

This section indicates the reports having security parameters changes that are waiting for manual validation via the ISPF[1] interface.

Rq: on a table destination, a column indicates for each source if the information goes to delta report, ISPF panel validation or no control. And the tool allows sending a report on a back-up administrator's email.

Reports / analysis Results

Revalidation

See chapter CBN

Statistics

Two types of statistics are produced by the tool:

- Statistics for a system where the system activity is generates list of activity.
- Statistics for a system where the results of the controls made by the tool are shown.

Document management

Document management is a synthesis of all data with a security level percentage, in order to show clearly the strong and weak points. This document is designed to be visualized by the customer and to discuss an improvement plan.

[1] ISPF : Interactive Structure Programmer Facility

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

CBN (Continuous Business Need validation)

The computing objects validation is a security rule. Periodically, a list has to be sent to the service managers for themselves and their collaborators. In order to make this revalidation possible, the ownership structure has to be implemented. A relation is established between security data implemented in the security software and personal data where email addresses may be found.

DB2 tables in the tool, on the focal point include all necessary data, their owners and their email addresses.

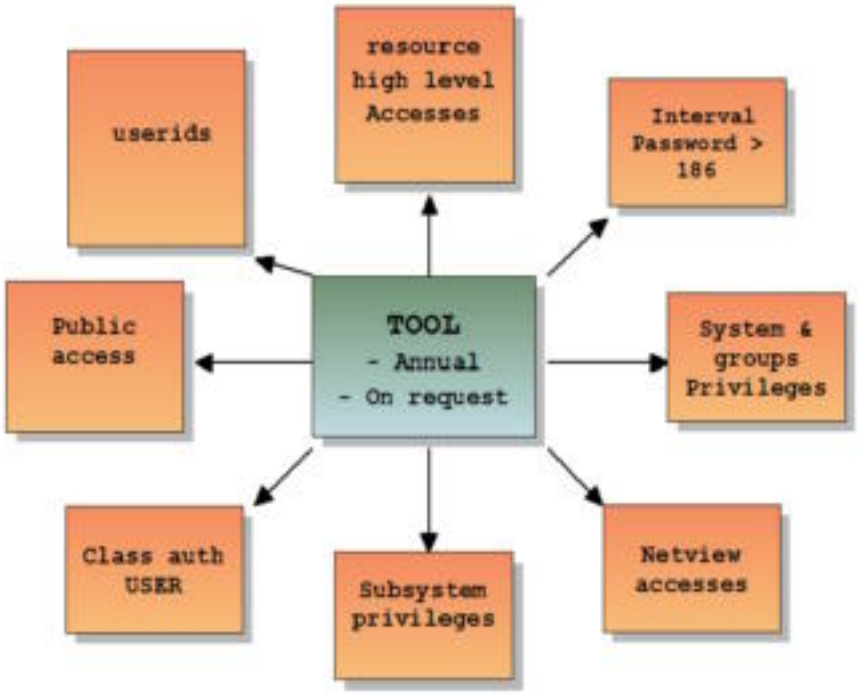


Figure 10: CBN (Continuous Business Need validation)

The CBN may be activated on-demand choosing a specific period, a group of systems or a unique system, as well as 2 format types.

An individual formal for each collaborator sent to his Manager, or a department format sent to the service Manager (the reports may be under the text or the HTML format).

To facilitate the understanding and the system administration, a job structure has to be implemented (see chapter prerequisite first). Jobs will be defined with a naming and access reference to the computing system objects.

For example, a group named « SUPTECH » will have the label 'Technical Support'. The user name connected to this group will have a unique reference, stating that this person has a 'Technical Support' job. Moreover, this architecture is already partially implemented because the administration is far more easy, then we assign a label to the group name already created on the security software.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

List of computing objects included in the inventory:

- USERID[1]

List of access keys to the systems.

- Resource level access

List of connections to a job group or list of system sensible resources out of the job group.

- Interval password

The interval password is a privilege because it is non interval, or because the interval limit is superior to a limit referenced in a law table in the tool (here it's 186 days maximum).

- System and group privileges

System privileges on the user or by the path of a group, as well as the user group privileges.

- Netview[2] access

Own a Netview access key is a privilege.

- Subsystem privileges

List of sub systems privileges (e.g. : DB2[3], CICS[4], ….)

- Class authority user

List of class authorities associated to userids.

- Public access

List of public access resources.

[1] USERID the term « user id » is a general term for indicating the user, the group, the accesser id group or logon id
[2] Netview network observation tool (IBM program product, note
[3] DB2 DATABASE 2 (an IBM relational database management system)
[4] CICS Customer Information Control System (IBM)

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

DATA FLOW

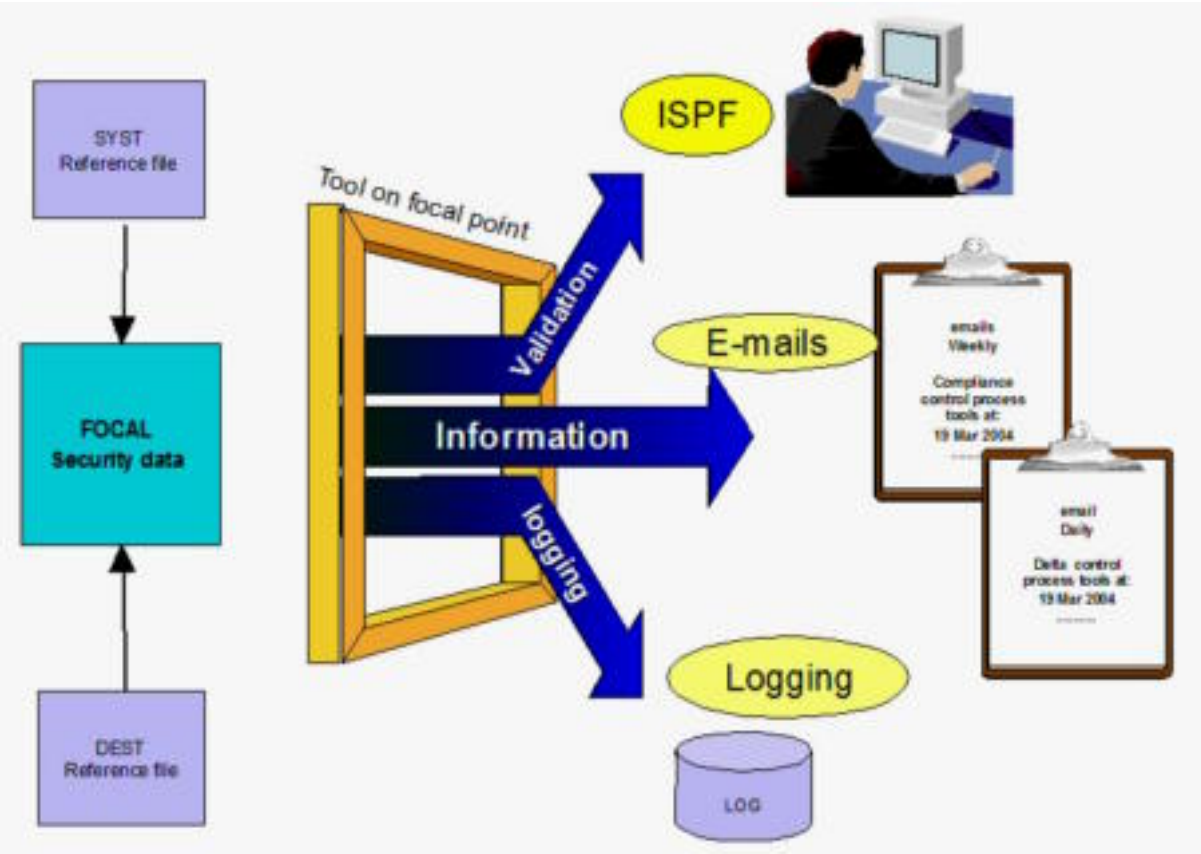


Figure 11: data flow

All security data are modelized and thanks to information in a control table, controls and delta take different paths.

- To be validated in the tool by the ISPF interface
- Information in a report by emails
- Event logged
- No control at all

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Example of data Flow

In the graph below, containing the figures by platform, is indicated the data flow in deviation sent by e-mail for a total systems amount only representing the information.

Platform	NB systems	NB users	NB records run	NB of reports recipient [1]
ACF2	1	1 201	3 667	1
OS400	261	130 989	931 973	25
RACF	198	499 597	4 187 853	78
TSS	11	53 003	118 931	6
TOTAL	471	684 800	5 242 424	110

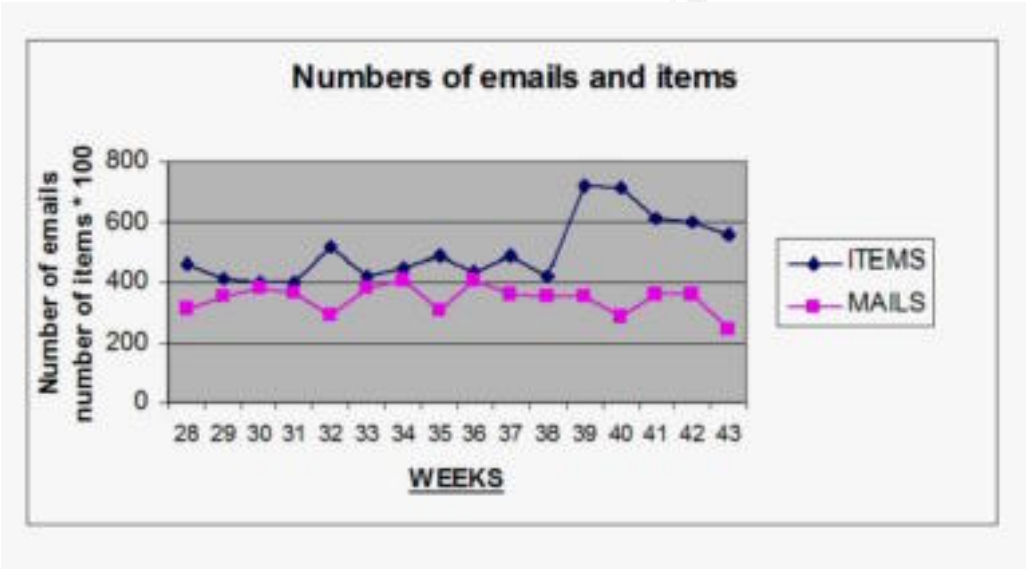


Figure 12: Example of data flow

Traffic increases correspond to the system integrations which are really helpful to the administrators for implementing security rules.

[1] Reports recipient: is a people in charge of software

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Qualities of the TOOL

Adaptabilities

The concept of the tool is capable in a short period of time to control all elements. Between two runs, the administrator has to validate or correct the policy. The administrator adapts specific rules to customer's requests in the contract with him.

- Able to manage different levels of security required by our customers
- Able to manage security according to real risk
- Able to create a specific report for manager or customer

Security Level

The tool proposes us to run the application on different periods of time. The obtention of a maximum security is to be able to run the application as often as possible.
The closer the period is, the easier it is to reach rapidly a high security level.
The more important the period is, the more work we will have to obtain a high security level, as during the long intermediary period, the level was deteriorated.

The long interval time between two runs supplements the vulnerability and we are not in compliance with the high ratio. For example, if the run is annual, the compliance is for during six month. When you decide another run, you have a lot of deviations on your system and you have a lot of work to get a good compliance. If you want a high security level, the tool runs a delta process on a daily basis and compliance process weekly. The administrator will have a short report for each week.

Fig 13: Level of security period

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Efficiency

When the new rule is installed, the administrator can create a request on the DB2/QMF environment to see the impact of the new rules on all systems managed by the tool, and with another request he creates a specific command for different software of security then executes it on the target system.

- Controls regularly all security items
- Involves all actors to be more pro-active
- The course and documentation are available

Transparency

The tool reports the statistics indicator to the management.

- Provide accurate and precise reporting which reflects the real situation
- Provide clear message when we address them to other organizations or to customer.

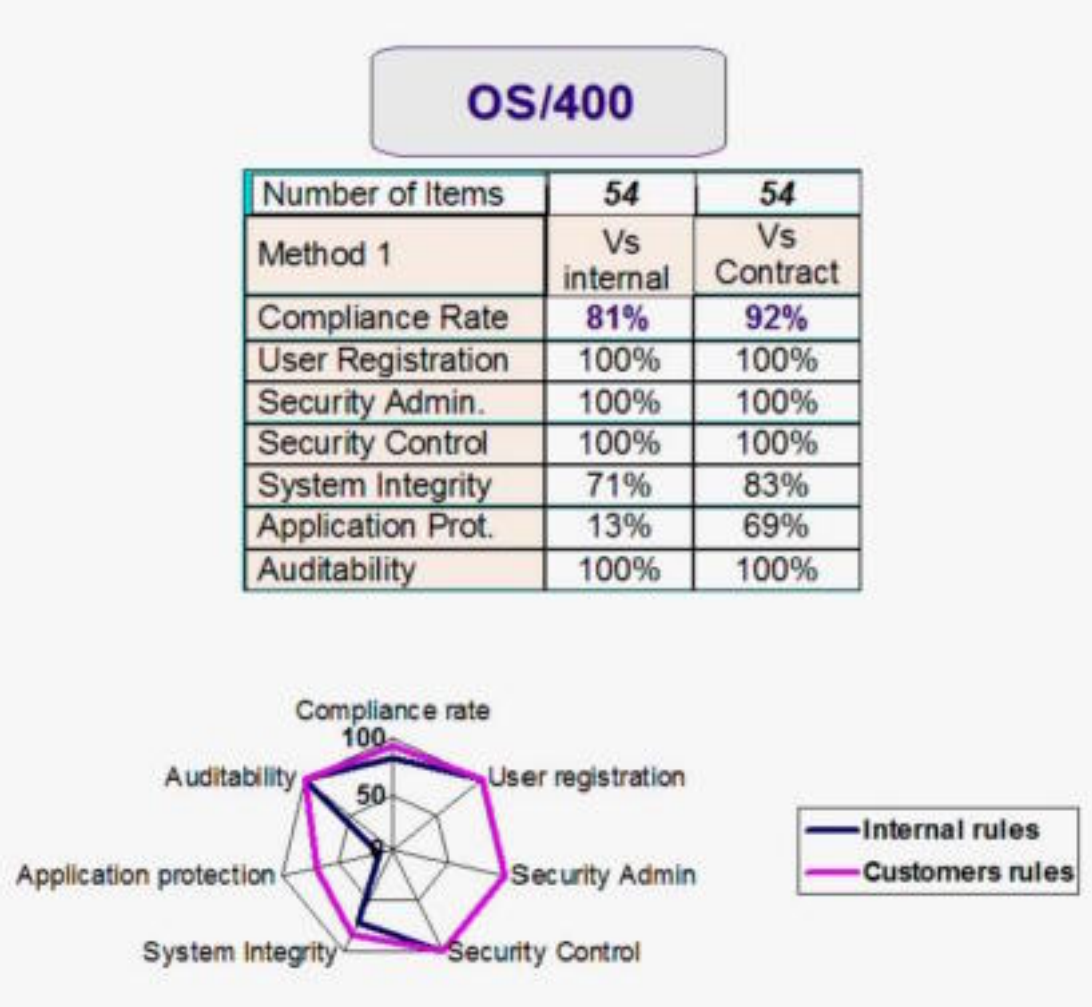
To illustrate the transparency with the statistics on OS400 systems (see figure: 14). The first method takes into account the company internal security rules and the other method , the customer security rules. On the graph, we see the different security levels and each domain for two different groups of security rules (internal rules and standard rules)

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Compliance rate calculation

All references on this graph are calculated with the activities of the tool and for all figures, an importance coefficient is applied.



OS/400

Number of Items	54	54
Method 1	Vs internal	Vs Contract
Compliance Rate	81%	92%
User Registration	100%	100%
Security Admin.	100%	100%
Security Control	100%	100%
System Integrity	71%	83%
Application Prot.	13%	69%
Auditability	100%	100%

Figure 14: Example of OS400 systems statistics

© SANS

Productivity

- Automation of the operations allows administrator to work on events that require analysis, decision, intelligence.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Auditability

Tool activity must be auditable:

Tool files are managed as OSR/E

All actions through ISPF are logged

Programs write AUDIT TRAIL

LOGs & AUDIT trails are kept 6 months

Cost

For example in my environment the tool is installed for managing 198 MVS VM/RACF systems and 261 OS400 systems.

Administration of the tool.

Target system : 0.5 day / system / year

Extractor management

Focal point : 20 days / year

DESTINATION file
RULES file
SYSTEM file

Saving

The saving is mostly linked to the reaction time during an event. The analyse is really important when the problem is solved later. Why and how the event occurred, and who is the problem originator. The correction is difficult when as time goes by.
For example:
At a sub-system installation time to support a new application. If a security rule is not applied, the correction would be immediately applied if we are informed at the same time. Whilst six months later, the application will be installed, operational for many users, and to apply the security rule in deviation, we will have to plan a study and an analyse of the impact for users. The security level would then me qualified as medium.
In an environment identical the one described in the above chapter, a saving of 108 people is estimated, including all administrators (administrators, technical supports, etc.) for a high security level.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

References

GIAC. Global Information Assurance Certification

(The industry standard for security knowledge)

http://www.giac.org/admin_22.php

SANS Institute, The SANS Security Project Policies

http://www.sans.org/resources/policies

Yves Depoorter, GSEC Practical Assignment, Enhance mainframe system security while standardizing it.

http://www.giac.org/practical/GSEC/Yves_Depoorter_GSEC.pdf

ISO 9000: ISO standards which identify the requirements for an effective quality management system
http://www.iso.org/iso/en/ISOOnline.openerpage

ISO 17790:
http://www.iso-17799.com/

SAS 70: (about SAS 70)

http://www.sas70.com/about.htm

Sarbanes_Oxley:
http://www.pwcglobal.com/Extweb/NewCoAtWork.nsf/docid/D0D7F79003C6D64485256CF30074D66C

Outsourcing:

http://www.cio.com/research/outsourcing/

http://www.outsourcing-law.com/what_is_outsourcing.htm

IBM Corporation, OS/390: RACF macros and interfaces,

Document number: SA22 7682-05

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Summary

In this document, I present a tool dedicated to declare, and to control the compliance of security rules on mainframe and midrange systems. This tool controls security settings based on security rules which may be different from a customer system to another. Auditable reports are sent to e-mail addresses with an addressees table. It allows answering security audits. The tool provides the possibility to reach a high level of security on an important stock of systems.
The automated process generates saving. For the same number of people, it allow to manage more systems with a better reactivity, liability, security level, and an archival system which helps us to meet an business control organization requests on a set of different platforms.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Annex 1: Data extractor

Data are collected from:

- Security server unload (standard utility)
- SETROPTS, RVARY list, TSS, ACF2 lists
- MVS / VM dataset monitor output
- MVS / JES display commands list
- SDSF interface lists
- JES proclib' scanning
- IEHLIST (APF/LNK)
- SVCCHECK output
- Subsystems lists (DB2, IMS, CICS, NETVIEW, VMBARS …)
- VM list (SETEVENT, DIRECTORY, ..)
- OS/400 JOBSEC (User profile, authorization list, group list, directories, public access, network attributes, job description, system values, default password, object list, ..)

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Annex 2: Modeling

Find the principal source of DOMAIN, CATEGORY and TYPE

DOMAIN	CATEGORY	TYPE
OS400	OSR	BASIC
OS400	OSR	PUBLIC
OS400	JOBD	BASIC
TOOL	CONTROL	DEST
DFSMS	DFSMS	AUTH
DFSMS	DFSMS	SETTING
OS400	GROUP	ACCESS
OS400	GROUP	SYS_AUTH
MVS	MVS	PPT
MVS	MVS	SVC
MVS	RETAINED	LOG
MVS	STC	SETTING
MVS	STC	USER
MVS	TSO	SETTING
MVS	UADS	USER
NFTP	NFTP	CONTROL
NFTP	NFTP	SETTING
NFTP	NFTP	USER
NVAS	NVAS	USER
OS400	OBJECT	LIB
OMVS	OMVS	PUBLIC
OMVS	OMVS	SETTING
OS400	OBJECTS	CMD
OS400	OBJECTS	NETATTR
OS400	OBJECTS	SYSVAL
RACF	CLASS	AUTH
RACF	DATASET	ACCESS
RACF	DATASET	BASIC
RACF	DATASET	CATEGORY
RACF	DATASET	PUBLIC
RACF	GROUP	ACCESS
RACF	GROUP	AUTH
RACF	OMVS	AUTH
RACF	RACF	CDT
RACF	RACF	EXIT
RACF	RACF	SETTING
RACF	RESOURCE	ACCESS
RACF	RESOURCE	APPCLU
RACF	RESOURCE	BASIC
RACF	RESOURCE	CATEGORY
RACF	RESOURCE	GLOBAL
RACF	RESOURCE	OSR_CTL
RACF	RESOURCE	PROGRAM
RACF	RESOURCE	PUBLIC
RACF	RESOURCE	VMXEVENT
RACF	USERID	ACCESS
RACF	USERID	AUTH
RACF	USERID	SETTING
TCPIP	TCPIP	SETTING
TSS	ADMIN	AUTH
TSS	BYPASS	AUTH
TSS	RESOURCE	BASIC
TSS	TSS	ACID
TSS	TSS	AUDIT
TSS	TSS	PUBLIC
TSS	TSS	SETTING
OS400	USERID	BASIC
OS400	USERID	NOINTER
OS400	USERID	OBJECT
OS400	USERID	PSWD
OS400	USERID	SYS_AUTH
OS400	USERID	USAUDIT
VM	AUTHDASD	SETTING
VM	AUTHFOR	USER
VM	DIRMAINT	AUTH
VM	DIRMAINT	SETTING

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

```
VM        DIRMAINT  USER
```

Annex 3: Example of security data modeling

DOMAIN	CATEGORY	TYPE	DATA SECURITY		VALUE	DATE_OF_RUN
RACF	RACF	SETTING	SETROPTS	ADDCREATOR	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	APPLAUDIT	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	AUTOMATIC DATASET PRO	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	CATALOGUED DATA SETS	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	CMDVIOL	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	COMPATIBILITY MODE	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	CONSECUTIVE UNSUCCESS	4	2004-10-22
RACF	RACF	SETTING	SETROPTS	DATA SET MODELING	BEING DONE FOR	2004-10-22
RACF	RACF	SETTING	SETROPTS	EIM REGISTRY	NONE	2004-10-22
RACF	RACF	SETTING	SETROPTS	ENHANCED GENERIC NAMI	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	ERASE-ON-SCRATCH	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	ERASE-ON-SCRATCH BY S	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	GENERIC OWNER ONLY	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	GROUP DATA SET MODELL	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	INACTIVE USERIDS AUTO	186	2004-10-22
RACF	RACF	SETTING	SETROPTS	INITSTATS	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	INSTALLATION PASSWORD	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	JES-BATCHALLRACF OPTI	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	JES-EARLYVERIFY OPTIO	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	JES-XBMALLRACF OPTION	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	KERBLVL	0	2004-10-22
RACF	RACF	SETTING	SETROPTS	LIST OF GROUPS ACCESS	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS	MULTI-LEVEL ACTIVE	INACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS àMAJOPTS	CLASS	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS àMAJOPTS	GENERIC COMMAND	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS àMAJOPTS	GENERIC PROFILE	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS àMAJOPTS	LOGOPTIONS	ALWAYS	2004-10-22
RACF	RACF	SETTING	SETROPTS àMAJOPTS	RACLIST	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCLU	GENERIC PROFILE	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCLU	LOGOPTIONS	DEFAULT	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCPORT	AUDIT	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCPORT	CLASS	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCPORT	GENERIC COMMAND	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCPORT	GENERIC PROFILE	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCPORT	LOGOPTIONS	DEFAULT	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCSERV	AUDIT	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCSERV	LOGOPTIONS	DEFAULT	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCSI	AUDIT	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCSI	CLASS	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCSI	GENERIC COMMAND	ACTIVE	2004-10-22
RACF	RACF	SETTING	SETROPTS APPCSI	GENERIC PROFILE	ACTIVE	2004-10-22

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2004. As a part of GIAC Practical repository. Author retains full rights.
© SANS Institute 2005 Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**