RSH CONSULTING

RACF

Monitoring & Reporting

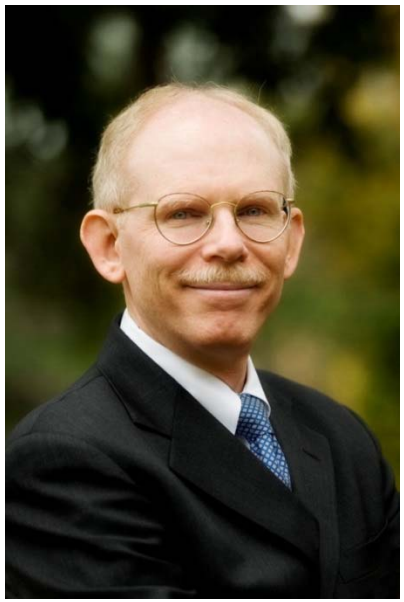
(Maximizing your SIEM ROI)

SHARE - 21250 - August 2017

RSH Consulting - Robert S. Hansel

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050



Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- http://twitter.com/RSH_RACF

Topics

- Monitoring Basics
- User Monitoring
- Resource Monitoring
- High Level Authority Monitoring
- Monitoring and SMF Record Considerations
- System Management Facilities (SMF)
- Reporting Tools

Monitoring Basics

- RACF terminology - AUDITING
- RACF auditing generates SMF records
- Auditing options can be specified in ...
  - RACROUTE Macro LOG= parameter
  - User profile
  - Resource profile
  - SETROPTS Options
- RACF authority to administer auditing
  - System-SPECIAL, Group-SPECIAL (within scope-of-groups), and Profile Owner can only view and set a resource profile's AUDIT option
  - System-AUDITOR, ROAUDIT (z/OS 2.2) , and Group-AUDITOR (within scope-of-groups) can view all SETROPTS and profile options, including those related to auditing
  - System-AUDITOR can set SETROPTS auditing options
  - System-AUDITOR and Group-AUDITOR (within scope-of-groups) can set UAUDIT and GLOBALAUDIT profile options

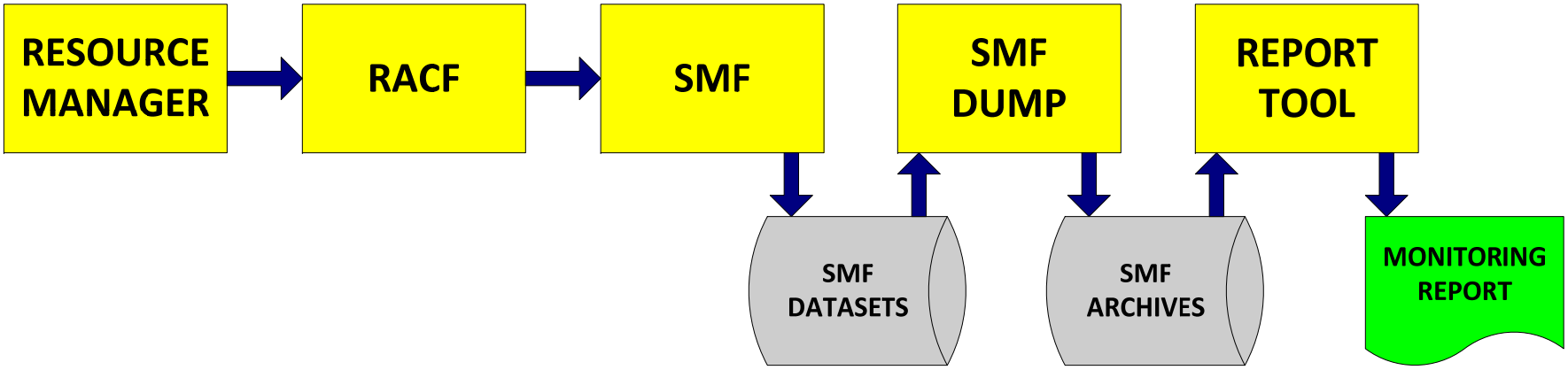
SMF Records

- RACF SMF records
  - 80 RACF Processing - Logged Events
  - 81 RACF Initialization - IPL
  - 83 RACF Audit - Subtypes:
    - 1 Dataset SECLABEL)
    - 2 Enterprise Identity Mapping (EIM)
    - 3 LDAP
    - 4 R-auditx
    - 5 WebSphere
    - 6 Tivoli Key Lifecycle Manager (TKLM)

- SMF records used for TSO, Batch, and Started Task logon information
  - 20 Job Initiation (RACFRW only)
  - 30 Common Address Space Work - Subtypes:
    - 1 Initiation
    - 5 Termination

SMF Generation and Reporting Process

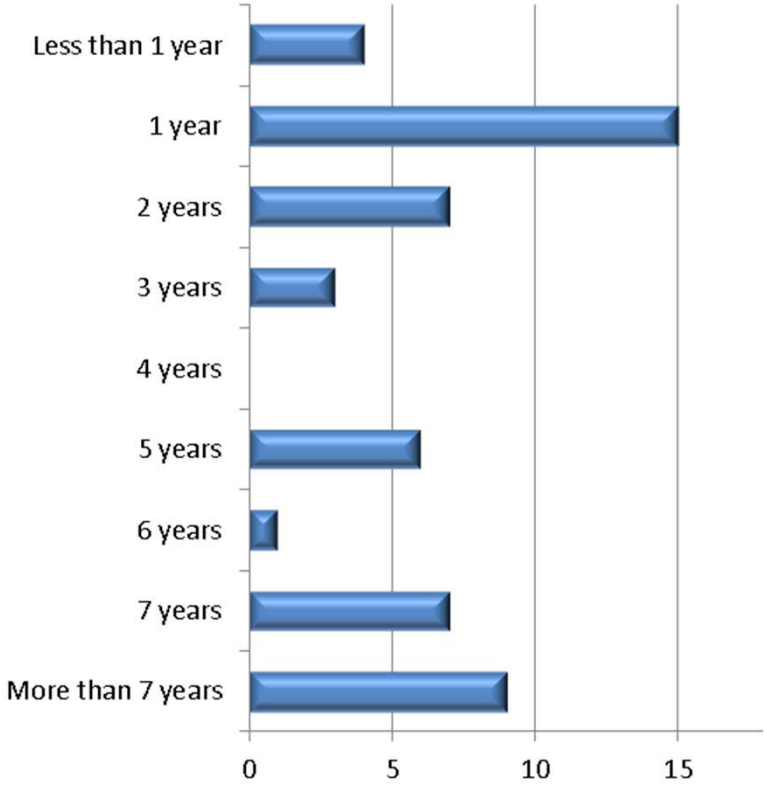
- Reporting tools require comprehensive SMF data collection and retention to be effective
- Log collection and reporting process
  - Resource Manager is configured to call RACF for an authorization check and does not suppress logging
  - RACF options are set to generate an SMF log record
  - SMF is configured to collect and save the log record
  - SMF records are dumped and archived for report processing
  - Software tools generate reports from the SMF record



RSH RACF Survey - April 2012

How long does your organization retain RACF-related SMF records?

Responses	Count	Percent %
Less than 1 year	4	7.7%
1 year	15	28.8%
2 years	7	13.5%
3 years	3	5.8%
4 years	0	0%
5 years	6	11.5%
6 years	1	1.9%
7 years	7	13.5%
More than 7 years	9	17.3%
Total	52	100%



Approximate Average - 4 years

RACROUTE LOG=

- RACROUTE Macro LOG= parameter
  - Can expand or suppress auditing
  - REQUEST=AUTH
    - NONE — No logging or console operator messages
    - NOSTAT — Same as NONE and no profile statistics are updated
    - NOFAIL — Do not log violations - log successes per ASIS
    - ASIS — Log in accordance with profile and SETROPTS audit settings
  - REQUEST=FASTAUTH
    - NONE — No logging or console operator messages
    - NOFAIL — Do not log violations - log successes per ASIS
    - ASIS — Log in accordance with profile and SETROPTS audit settings
  - REQUEST=VERIFY or VERIFYX
    - NONE — No logging or console operator messages
    - ASIS — Log logon failures
    - ALL — Log all logon events

User Monitoring

- UAUDIT attribute on user profile
  - All accesses logged - unless granted by Global Access Table, PRIVILEGED Started Task, or caller specifies RACROUTE LOG=NONE
  - Used to selectively monitor untrusted/external users and TRUSTED Started Tasks
  - Useful in analyzing access activity in order to remediate access
  - Some IDs may generate a substantial number of SMF records, especially those accessing Unix
  - Requires AUDITOR authority to add and remove UAUDIT

```
LU RSHTEST
USER=RSHTEST  NAME=RSH RACF TEST ID      OWNER=RACFTEST  CREATED=09.292
 ...
 ATTRIBUTES=UAUDIT
```

Resource Monitoring

```
LISTDSD DATASET('SYS1.LIBS*') ALL
INFORMATION FOR DATASET SYS1.LIBS* (G)

LEVEL   OWNER    UNIVERSAL ACCESS   WARNING   ERASE
-----   -------- ----------------   -------   -----
 00     TECHSPT1         READ         NO      NO

AUDITING
--------
FAILURES(UPDATE)

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----------  --------------  ------------
   READ         TECHSPT1       NON-VSAM

GLOBALAUDIT
-----------
NONE
```

Resource Monitoring

Dataset and General Resource Profile

- Parameters
  - AUDIT(*options*(*level*))
    - Set by Profile owner or SPECIAL
    - Default: FAILURES(READ)
  - GLOBALAUDIT(*options*(*level*))
    - Set by AUDITOR
    - Default: NONE
  - Used in combination - event is logged if either requires it
- To log successes for sensitive resources
  - AUDIT(SUCCESS(UPDATE),FAILURES(READ))
  - AUDIT(ALL(READ))
- Use profile LEVEL(##) to tag ACCESS records for report selection

- Auditing *options*
  - SUCCESS — Authorized Access
  - FAILURES — Violation
  - ALL — Both
  - NONE — No Logging
- Auditing *levels* - at or above
  - ALTER
  - CONTROL
  - UPDATE
  - READ
- PRIVILEGED and TRUSTED Started Task access not logged

Resource Monitoring

```
SETROPTS LIST
ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) TERMINAL(READ) SAUDIT CMDVIOL OPERAUDIT
…
AUDIT CLASSES = DATASET USER GROUP DASDVOL GDASDVOL GTERMINL TERMINAL
…
LOGOPTIONS "ALWAYS" CLASSES =  SURROGAT
LOGOPTIONS "NEVER" CLASSES =  NONE
LOGOPTIONS "SUCCESSES" CLASSES =  NONE
LOGOPTIONS "FAILURES" CLASSES =  FACILITY
LOGOPTIONS "DEFAULT" CLASSES = DATASET ACCTNUM ACICSPCT ALCSAUTH APPCLU
                               ... VTAMAPPL VXMBR WIMS WRITER
```

High Level Authority Monitoring

- SAUDIT SETROPTS Option
  - Audit all RACF commands executed by SPECIAL user
  - Audit all resource access using SPECIAL authority
- OPERAUDIT SETROPTS Option
  - Audit all resource access using OPERATIONS authority
  - Audit all ADDSDs using OPERATIONS authority
  - Can generate massive amounts of SMF records if this authority is being relied on extensively
- CMDVIOL SETROPTS Option
  - Audit all violations using RACF commands by anyone
  - SEARCH and LIST-type command violations are not logged
  - Rarely invoked - most command 'violations' are treated as 'errors'

Profile Change Monitoring

- AUDIT(*resource-class*) SETROPTS Option
  - Audits all changes to RACF profiles in the associated resource class
  - Captures administrative events not covered by SAUDIT and OPERAUDIT
  - For certain classes, also logs:
    - DATASET Creation and deletion of datasets
    - FSOBJ Creation and deletion of UNIX file system objects
    - IPCOBJ Creation and deletion of UNIX objects (e.g., semaphores)
    - PROCESS Dubbing and undubbing of a process
    - USER All password changes, even those made during logon and auto-assignment of OMVS segments by BPX.UNIQUE.USER
    - GROUP Auto-assignment of OMVS segments by BPX.UNIQUE.USER
  - Recommended for <u>all</u> classes

Resource Monitoring

- LOGOPTIONS SETROPTS Options
  - LOGOPTIONS(*level*(*class*)) - set for each individual class
  - Levels:
    - ALWAYS — Log all access
    - NEVER — Do not log
    - SUCCESSES — Log all authorized access
    - FAILURES — Log all violations (*recommended for most classes*)
    - DEFAULT — Use resource profile log options
  - SUCCESSES and FAILURES *augment* resource profile audit settings
  - ALWAYS and NEVER *override* resource profile audit settings
  - ALWAYS level
    - Logs all accesses for a given resource class, even when no profile is defined to RACF - class must also be active
    - Logs TRUSTED Started Tasks

Resource Monitoring

- LOGOPTIONS SETROPTS Options (continued)
  - Activates logging of certain z/OS Unix events
    - ALWAYS
      - FSSEC File system security changes
    - FAILURES
      - PROCESS Process UID or GID changes and privileged operations
      - PROCACT Functions effecting other processes (e.g., kill)
      - IPCOBJ Object access, UID or GID changes
  - NEVER does not suppress user UAUDIT logging
  - LOGOPTIONS is ignored when access is granted by:
    - Global Access Table
    - RACROUTE FASTAUTH processing (use profile auditing (e.g., UNIXPRIV, VTAMAPPL))
    - RACROUTE LOG=NONE
  - LOGOPTIONS(ALWAYS(PROCACT)) required to log 'w_getpsent'

APPC and MLS Auditing

- APPLAUDIT SETROPTS Option
  - Allows user verification auditing at the beginning and ending of a user's transaction processing
  - Must also specify AUDIT(ALL) or GLOBALAUDIT(ALL) on the APPL class profile associated with the APPC/MVS LU
  - Can produce excessive SMF data if the APPL profile specifies AUDIT(SUCCESS(READ)) or ALL(READ)) and the application does not support persistent verification

- SECLEVELAUDIT(*seclevel*) | NOSECLEVELAUDIT SETROPTS Option
  - Activates auditing of all access attempts to resources at or above a specified security level
  - Security level must be defined in SECDATA SECLEVEL profile

- SECLABELAUDIT | NOSECLABELAUDIT SETROPTS Option
  - Specified that SECLABEL profile auditing options are to be used in addition to the resource profile auditing options in logging access

Additional Monitoring

- Real Time Notification
  - NOTIFY(*userid*) - Messages to *single* TSO user
  - Security Console
    - Defined in PARMLIB(CONSOLxx) - MCS or SMCS
    - Route code 2, 9, and 11 messages
    - Recommend require logon if outside computer room

- SETROPTS STATISTICS(*class*)
  - Access counts kept on Discrete profiles
  - Counts not incremented for Global Access Table or RACLIST access
  - Activated by class
  - Little value and performance drag

Monitoring Considerations

- LIST and SEARCH command usage is not logged
- All SETROPTS command execution is automatically logged
- PRIVILEGED Started Task access is never logged
- Global Access Table (GAT) authorized access is never logged
  - Dataset creation is logged if SETROPTS AUDIT(DATASET) is in effect
- RACF exits can expand or suppress auditing
- Access granted during Failsoft is logged
- RACF RACROUTE TYPE=AUDIT - generates log records

Logging & SMF Record Considerations

- RSH RACF Tips - July 2017 - RACF SMF Factoid - TRUSTED

  Certain audit settings result in SMF 80 ACCESS event records being generated for access by a TRUSTED Started Task. When access is granted by TRUSTED authority, a bit in the header section of the SMF record is set ON, and the field ACC_AUTH_TRUSTED in the corresponding SMF Unload record contains YES. This bit is not set ON for DEFINE, ADDVOL, DELVOL, RENAME, or DELRES events. However, the SMF 80 record for all these events has a UTOKEN relocate section, and this section has a bit which is set ON if the user had TRUSTED authority. If the bit is ON, the field event_UTK_TRUSTED in the corresponding SMF Unload record contains YES. This field is cryptically documented in the RACF Macros and Interfaces manual as "Is this user a part of the trusted computing base (TCB)?" It can be used to determine if any of these events were allowed because of TRUSTED authority.

- RSH RACF Tips - January 2017 - WARNING SMF Records

  Access allowed by WARNING always generates an ICH408I message, but a corresponding SMF record will not be generated unless auditing options are set correctly. To ensure an SMF record is created, either SUCCESS or FAILURES in either AUDIT or GLOBALAUDIT must be set to log the intended level of access associated with the WARNING event. For example, if FAILURES is set to UPDATE, but the WARNING access intent was READ, no record will be generated. The same is true if AUDIT is set to NONE.

  Regardless of the profile settings, WARNING events will always be logged if the user has UAUDIT or if SETROPTS LOGOPTIONS for the class is set to either SUCCESSES or ALWAYS.

  To log all WARNING events, ensure all profiles have at least AUDIT(FAILURES(READ)).

- Visit www.rshconsulting.com to find other RSH RACF Tips articles related to logging

System Management Facilities (SMF)

- Record Collection
- Record Dumping
- Monitoring and Integrity

Factors Affecting SMF Logging

- SMF collects and saves log records
  - SMF parameters can ignore record types
  - SMF exits can suppress records
- SMF records are dumped for archive and for report processing
  - Live SMF datasets must be dumped to archive datasets when they fill
  - SMF dump utility and its exit can ignore records
  - Datasets holding dumped archive SMF records can be manipulated or deleted

SMF - Record Collection

- Parameters
  - PARMLIB(IEASYSxx)
  - PARMLIB(SMFPRMxx)

- Exits
  - IEFU83 - Receives control before record is written to the SMF dataset; can suppress record
  - IEFU84 - Receives control when SMF Writer Routine is branch-entered and is not entered in cross-memory mode, before record is written to the SMF dataset; can suppress record
  - IEFU85 - Receives control when SMF Writer Routine is branch-entered and is entered in cross-memory mode, before record is written to the SMF dataset; can suppress record

- Many SIEMs install SMF exits to capture records as they are being generated

SMF - Record Collection - IEASYSxx

- SMF=xx SMFPRMxx member director
- OPI=YES | NO IPL Operator Intervention

- To display current options via the console, issue command:

  DISPLAY SMF,O

```
IEE967I 15.38.31 SMF PARAMETERS 373
        MEMBER = SMFPRMB1
        INTVAL(30) -- DEFAULT
        SUBSYS(STC,TYPE(0:98,100:255)) -- SYS
        SUBSYS(STC,NOINTERVAL) -- SYS
        SUBSYS(STC,NODETAIL) -- SYS
        SUBSYS(STC,EXITS(IEFUSO)) -- PARMLIB
        SUBSYS(STC,EXITS(IEFUJP)) -- PARMLIB
        SUBSYS(STC,EXITS(IEFU84)) -- PARMLIB
        SUBSYS(STC,EXITS(IEFU83)) -- PARMLIB
        SUBSYS(STC,EXITS(IEFU29)) -- PARMLIB
        SID(RSHB) -- PARMLIB
        JWT(0400) -- PARMLIB
        NOPROMPT -- PARMLIB
        DSNAME(SYS1.RSHB.MAN3) -- PARMLIB
        DSNAME(SYS1.RSHB.MAN2) -- PARMLIB
```

SMF - Record Collection - SMFPRMxx

- ACTIVE | NOACTIVE — SMF recording active
- RECORDING(DATASET | LOGSTREAM) — Where to record SMF records
- DSNAME [(*dsnames*)] — SMF datasets (defaults - SYS1.MANX and SYS1.MANY)
- SID(*processer-model#* | *sysid*) — System Identifier (up to 4 characters)
- PROMPT(ALL | *option* | NOPROMPT) — Operator intervention at IPL allowed
  - IPLR — Enter reason for IPL
  - LIST — Change Options
  - ALL — IPLR + LIST
- SYS(*options*) — Global Options
  - TYPE(0:255|#,#:#) — Type records collected
  - NOTYPE(#,#:#) — Type records excluded
  - EXITS(*name*,*name*) — Exits invoked
- SUBSYS(*name*,*options*) — Subsystem options
  - [Same as SYS] — Supersede SYS
- BUFSIZMAX(128M | nnnnM) — Maximum size of SMF buffers - up to 1024M (1G)
- BUFUSEWARN(25 | 10 to 90) — Begin issuing warnings when buffers to nn% full

SMF - Record Dumping

▪ Dump Exit	IEFU29	Automatic dump and switch
▪ Dump Utility	IFASMFDP	Dump SMF datasets
	IFASMFDL	Dump SMF logstream

SMF - Record Dumping - IFASMFDP

```
//DUMPSMFR JOB (001),'HANSEL RS',CLASS=A,NOTIFY=&SYSUID
//STEP0001 EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//SYSMANDS DD DSN=SYS1.MAN1,DISP=SHR
//SMFMTHLY DD DSN=SMF.MONTHLY.DUMP.FEB,DISP=SHR
//RWDATA   DD DSN=RSH.RACF.SMF.FEB,DISP=(NEW,CATLG,DELETE),UNIT=SYSDA,
//            SPACE=(CYL,(100,10),RLSE),DCB=(LRECL=32767,RECFM=VBS)
//SYSIN    DD *
     INDD(SYSMANDS,OPTIONS(DUMP))
     INDD(SMFMTHLY,OPTIONS(DUMP))
     OUTDD(RWDATA,TYPE(30(1,5),80,81,83))
     DATE(2006040,2006043) START(0800) END(1600)
     SID(MVSA)
     ABEND(NORETRY)
-------------------------------------------------------------------------------
     USER2(IRRADU00) USER3(IRRADU86)                          <<< SMF Unload
//ADUPRINT DD SYSOUT=*
//XMLFORM  DD DSN=RSH.SMF.XMLFORM,DISP=(NEW,CATLG,DELETE),          <<< XML #1
//            SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=12888,RECFM=VB)
//XMLOUT   DD DSN=RSH.SMF.XMLOUT,DISP=(NEW,CATLG,DELETE),          <<< XML #2
//            SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=12888,RECFM=VB)
//OUTDD    DD DSN=RSH.SMF.UNLOAD,DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(100,10),RLSE),UNIT=SYSDA,DCB=(LRECL=12888,RECFM=VB)
```

SMF - Monitoring and Integrity

- SMF Record Type
  - 7 Lost Data
  - 90 System Status

- SMFPRMxx
  - NOBUFFS and LASTDS parameters - HALT option
  - Can be used to prevent SMF record loss

Reporting Tools

▪ RACF Report Writer	RACFRW (stabilized 1992)
▪ RACF SMF Unload	IFASMFDx User Exits IRRADU00 and IRRADU86
▪ SMF Unload Processing	DFSORT / ICETOOL - see SYS1.SAMPLIB(IRRICE) REXX DB2 SQL
▪ SMF Unload Facilitator	RSH Software - RSMFSEL
▪ SMF Reporting	IBM - IBM Security zSecure Audit Vanguard Integrity Professionals - Advisor Allen Systems Group - ASG-Audit EKC - E-SRF Beta Systems - Beta 88 z/Security Auditor Software Engineering of America - RA7
▪ SIEM Reporting	Syncsort - Ironstream SDS - VitalSigns SIEM Agent for z/OS (formerly SMA_RT) Correlog - Correlog SIEM Agent for z/OS IBM - QRadar

Reporting Tools

- SMF Unload
  - Creates text and XML formatted data from unformatted SMF data
  - Invoked through user exits in the SMF Dump Utility (IFASMFDP or IFASMFDL)
  - No pre-unload record selection capability
  - DB2 table load SQL provided
  - Text data can be browsed
  - XML data can be viewed in an HTML browser
  - Requires programming skills to generate reports
    - DB2 SQL queries
    - DFSORT and ICETOOL
    - SAS, REXX, or other report writer

Effective Reporting

- Correct, comprehensive SMF archive datasets must be included for processing
  - All pertinent SMF record types must be processed
  - Data from all system images must be included
- Reporting tool must be properly coded to select desired records for reporting
  - Ensure all Violation events are requested
  - Ensure Warnings and Successes are selected
- Reports on important types of activities should be generated
  - Access to sensitive and critical resources
  - Warnings
  - Activities of UAUDIT users
  - Logons by undefined users
  - OPERATIONS and Storage Admin authority use
  - Security administration actions
- Reports must be organized for efficient review
- Reports must be disseminated to user and resource owners

Reporting Resources

- RSH - www.rshconsulting.com
  - Presentations
    - RACF Utilities
    - DFSORT and ICETOOL
    - RACF and REXX
  - RACF Tips Newsletters
  - RACF Surveys
    - SETROPTS LOGOPTIONS
    - RACF-related SMF Record Retention
- SYS1.SAMPLIB(IRRICE)
- Nigel Pentland - http://www.racf.co.uk/
- Steve Neeland - http://www.oocities.org/steveneeland/Sort_Reports.html