RAZ-LEE

SIEM & DAM Support

Sending IBM i Security Events

About Raz-Lee Security

Founded in 1983, Raz-Lee Security is one of the world's leading independent owned cybersecurity and compliance solution providers for IBM i servers (AS/400).

Raz-Lee's flagship iSecurity suite guards organizations against insider threats and unauthorized external access to business-critical information hosted on their IBM i. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

We build solutions that work with other companies' technologies allowing organizations to monitor IBM i activity via SIEM or DAM dashboards.

Technology Business Partners

imperva IBM McAfee™

Akamai RSA® SEA™ SOFTWARE ENGINEERING OF AMERICA

About iSecurity Suite

Advanced Threat Protection

- **Anti-Ransomware**
- **Antivirus** / Malware protection
  - **ICAP** Optional Client/Server for Antivirus

Authentication & Authorization

- **MFA** Multi Factor Authentication
- Self **Password Reset**
- **Authority On Demand**

Protection

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update** to protect production files

Evaluation, Reporting & Alerts

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence for Security

Score Cards

for GDPR, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Assessment

Encryption

- DB2 **Field Encryption** (FIELDPROC)
- **PGP File Encryption**

Data Base Solutions

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Secured file editor

Auditing & Response

- **Audit** Journal, System Values, Status…
- Proactive re-**Action** in real time
- **Capture** screen activity
- **Compliance** of Users, Objects, IFS
- **Change Tracker** watch Production Libraries

RAZ-LEE
iSecurity

SIEM & DAM Support

Sending IBM i Security Events

Syslog in Real Time

Real-time Syslog alerts sent from all iSecurity modules are fully integrated with leading SIEM/DAM products.

iSecurity SIEM/DAM works with every product that supports SYSLOG, like IBM QRadar, Splunk, McAfee, RSA, Datadog, GFI Solutions, ArcSight, Sumo HPOpenView, CA UniCenter and others.

Integration with Imperva SecureSphere DAM (OEM by Imperva) and McAfee Database Security DAM

Integration with SIEM products for forensic analysis of security-related events is an increasingly important requirement at companies worldwide; indeed, Raz-Lee's iSecurity suite has supported Syslog-to-SIEM for many years.

SIEM - Security Information and Event Management

DAM - Database Activity Monitoring

SIEM for System and User

We monitor and send the following simultaneously (not only QAUDJRN):

- Journals QAUDJRN, QVPN, QIPFILTER, QIPNAT, QACGJRN, QQOS, QSNMP, QDSNX, QZMF (Covering activity of System log, VPN, IP-Filter, IP-Nat, Quality-of-service, SNMP,…)
- Messages from QHST, QSYSOPR
- Messages from any message queue
- IFS logs – such as those of Apache, WebSphere
- Messages that user programs wish to send
- Messages from other iSecurity modules

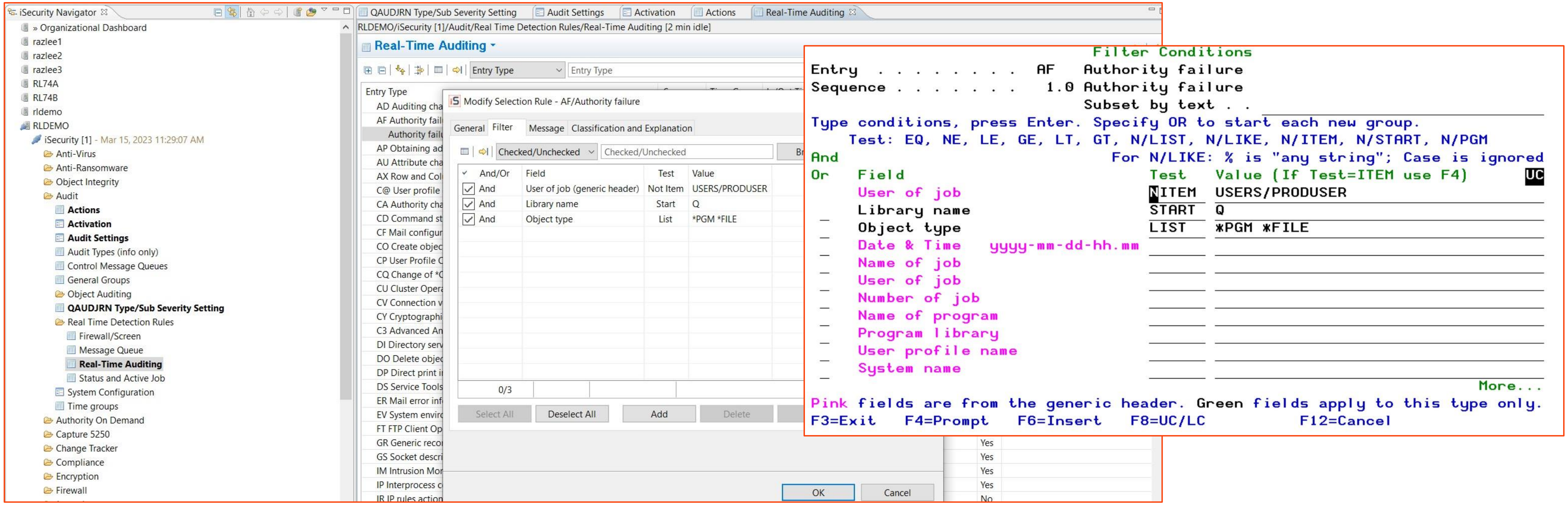
Key Features

- Supports CEF, LEEF and local structuring of the message format
- Sends Syslog messages in parallel to up to 3 SIEM products
- Transmission is supported via UDP, TCP or TLS (encrypted channel)
- Advanced filtering capabilities via specific severity code
- Syslog Self-Test facility. Receiving messages locally on the IBM i, to enable pre-check prior to sending to a remote syslog server
- Enables sending extremely high volumes of information with virtually no performance impact
- Advanced communication recovery
- Proven integration with all major SIEM products

Filtering Data by Field Values

- By Field values from the Journal Header and the Body fields
- With wide range of testing, trivial or advances, such as: Not/LIKE, Not/LIST, Not/ITEM in a table, group profile, by user profile special authority or having limited capability
- Comes in Native and GUI.

For clarity, the rest of presentation is in Native

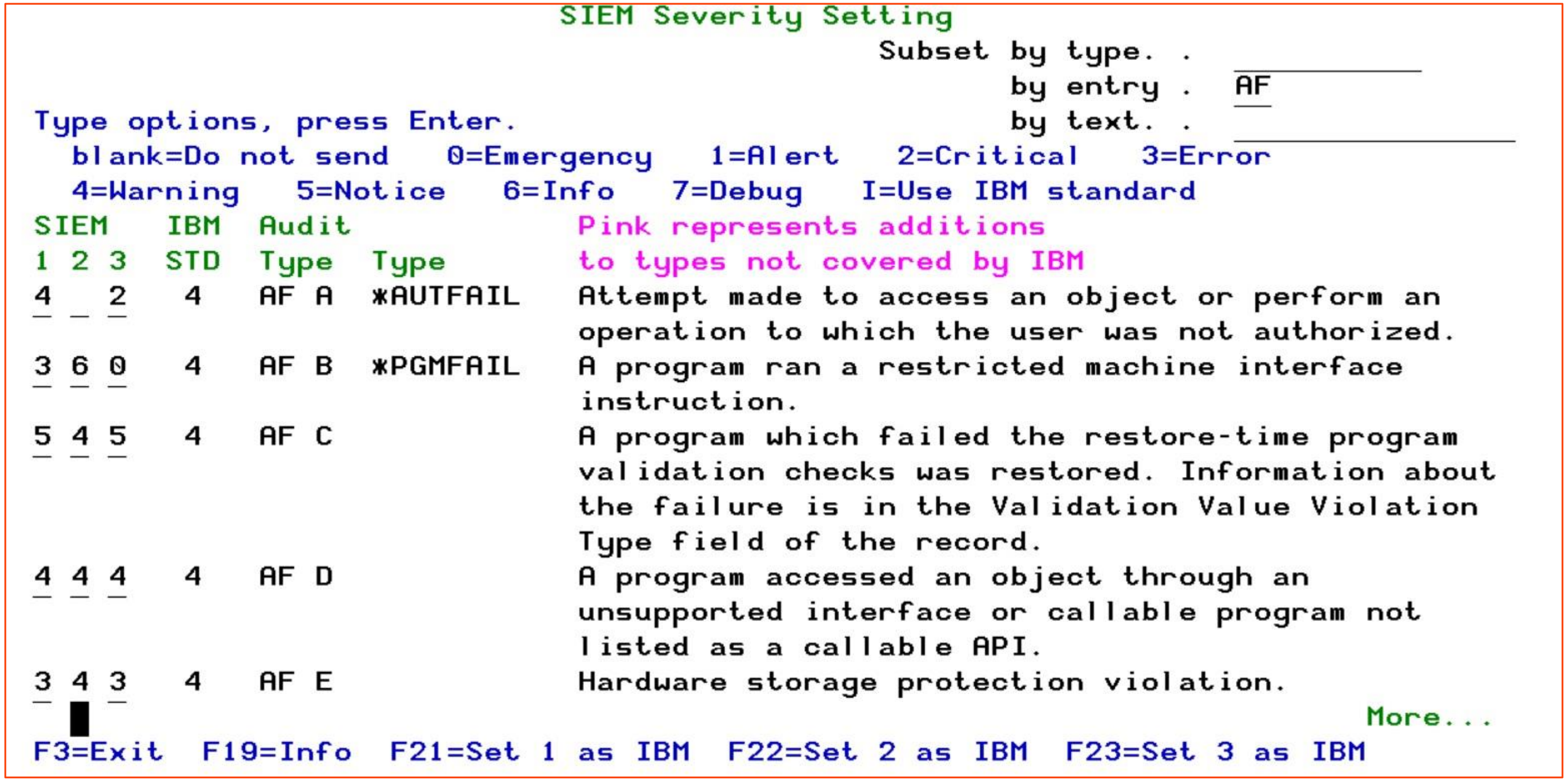


And/Or	Field	Test	Value
☑ And	User of job (generic header)	Not Item	USERS/PRODUSER
☑ And	Library name	Start	Q
☑ And	Object type	List	*PGM *FILE

```
                              Filter Conditions
Entry  . . . . . . . . .   AF   Authority failure
Sequence . . . . . . . .   1.0  Authority failure
                                Subset by text . .
Type conditions, press Enter. Specify OR to start each new group.
    Test: EQ, NE, LE, GE, LT, GT, N/LIST, N/LIKE, N/ITEM, N/START, N/PGM
And                           For N/LIKE: % is "any string"; Case is ignored
Or    Field                                Test    Value (If Test=ITEM use F4)      UC
      User of job                          NITEM   USERS/PRODUSER
      Library name                         START   Q
 _    Object type                          LIST    *PGM *FILE
 _    Date & Time    yyyy-mm-dd-hh.mm
 _    Name of job
 _    User of job
 _    Number of job
 _    Name of program
 _    Program library
 _    User profile name
 _    System name
 _                                                                        More...
Pink fields are from the generic header. Green fields apply to this type only.
F3=Exit   F4=Prompt   F6=Insert   F8=UC/LC        F12=Cancel
```

Filtering Data by Severity

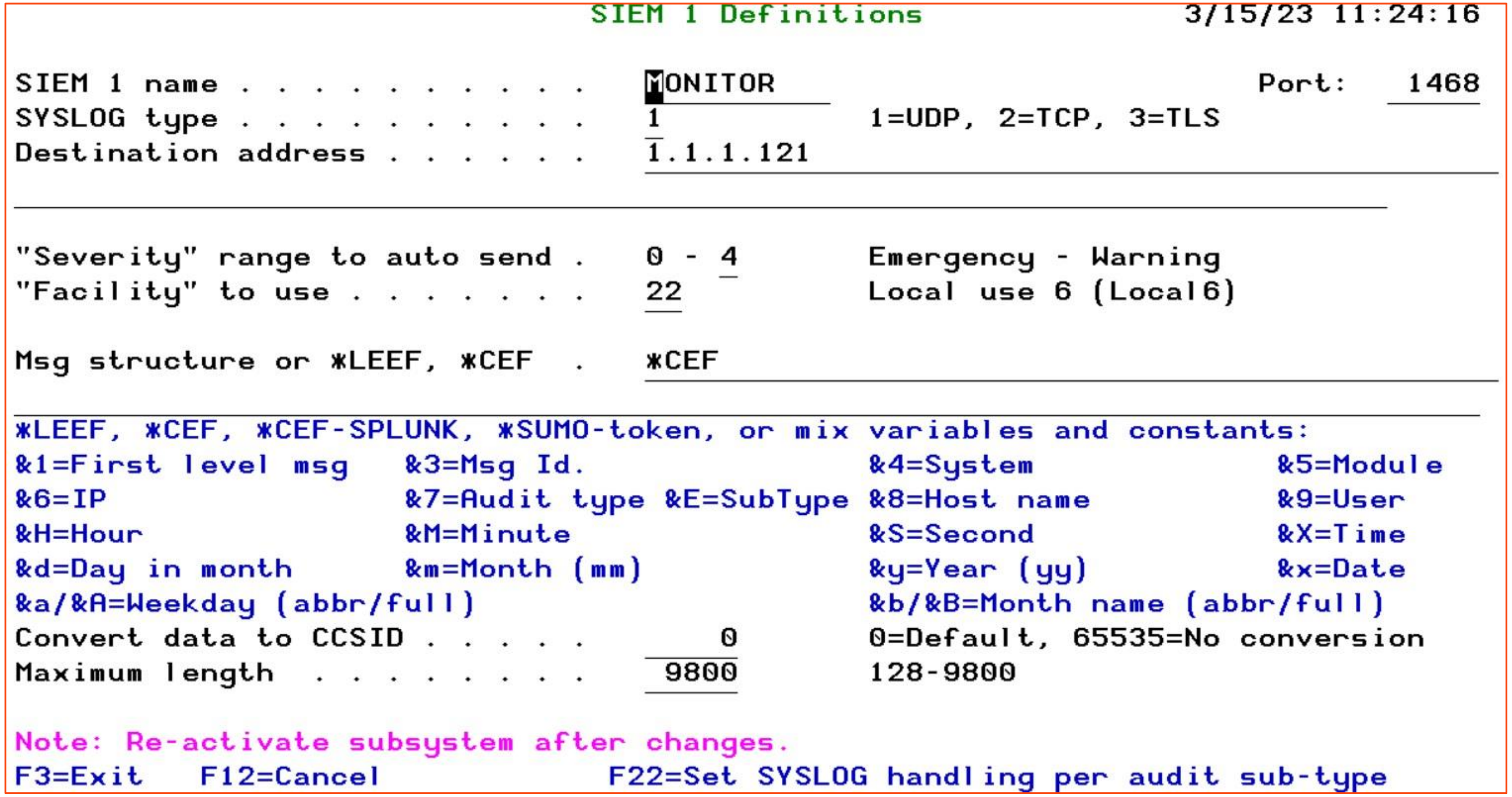
- Setting different severities for each SIEM



```
                              SIEM Severity Setting
                                              Subset by type. .  __________
                                                     by entry .  AF
Type options, press Enter.                           by text. .  ________________
  blank=Do not send   0=Emergency   1=Alert   2=Critical   3=Error
  4=Warning   5=Notice   6=Info   7=Debug   I=Use IBM standard
SIEM   IBM  Audit                   Pink represents additions
1 2 3  STD  Type  Type              to types not covered by IBM
4 _ 2   4   AF A  *AUTFAIL          Attempt made to access an object or perform an
                                    operation to which the user was not authorized.
3 6 0   4   AF B  *PGMFAIL          A program ran a restricted machine interface
                                    instruction.
5 4 5   4   AF C                    A program which failed the restore-time program
                                    validation checks was restored. Information about
                                    the failure is in the Validation Value Violation
                                    Type field of the record.
4 4 4   4   AF D                    A program accessed an object through an
                                    unsupported interface or callable program not
                                    listed as a callable API.
3 4 3   4   AF E                    Hardware storage protection violation.
                                                                          More...
F3=Exit  F19=Info  F21=Set 1 as IBM  F22=Set 2 as IBM  F23=Set 3 as IBM
```

SIEM Definition

- Filtering by the range of severities.
- Only severe messages are sent



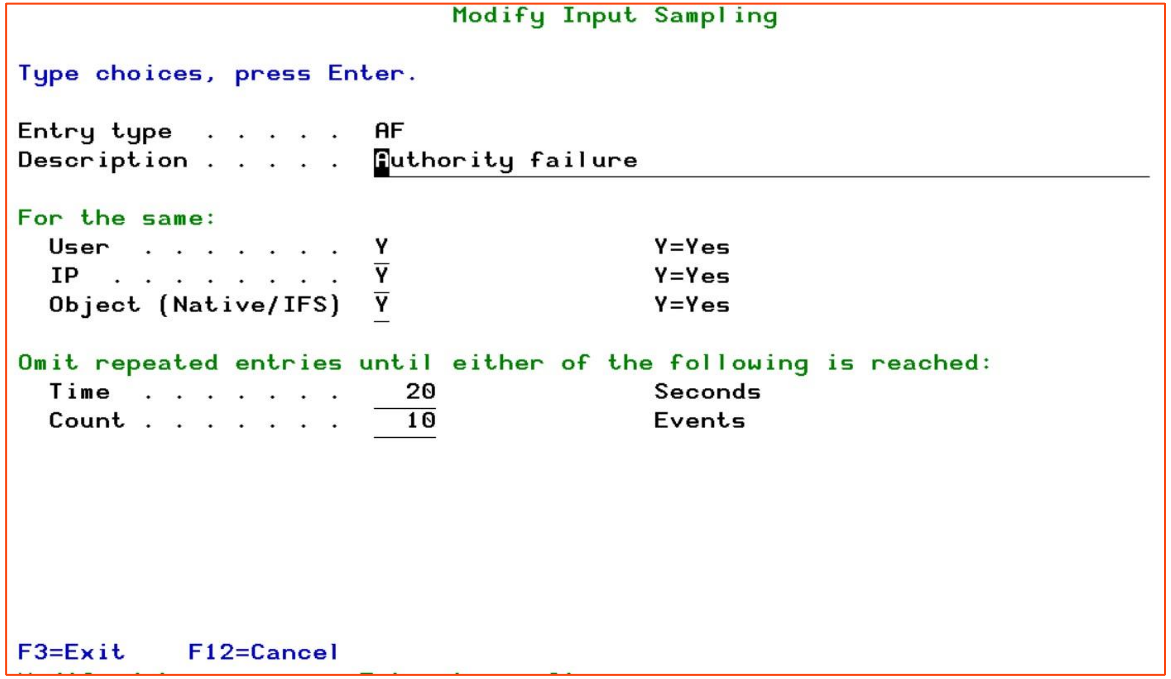
```
                               SIEM 1 Definitions                3/15/23 11:24:16

SIEM 1 name . . . . . . . . . . . .   MONITOR                         Port:   1468
SYSLOG type . . . . . . . . . . . .   1           1=UDP, 2=TCP, 3=TLS
Destination address . . . . . . . .   1.1.1.121


"Severity" range to auto send .       0 - 4       Emergency - Warning
"Facility" to use . . . . . . . .     22          Local use 6 (Local6)

Msg structure or *LEEF, *CEF  .       *CEF

*LEEF, *CEF, *CEF-SPLUNK, *SUMO-token, or mix variables and constants:
&1=First level msg     &3=Msg Id.                  &4=System                    &5=Module
&6=IP                  &7=Audit type &E=SubType    &8=Host name                 &9=User
&H=Hour                &M=Minute                   &S=Second                    &X=Time
&d=Day in month        &m=Month (mm)               &y=Year (yy)                 &x=Date
&a/&A=Weekday (abbr/full)                          &b/&B=Month name (abbr/full)
Convert data to CCSID . . . . . .          0       0=Default, 65535=No conversion
Maximum length  . . . . . . . . .       9800       128-9800

Note: Re-activate subsystem after changes.
F3=Exit    F12=Cancel           F22=Set SYSLOG handling per audit sub-type
```

Get Rid of Excess Repetitions

We provide Input Sampling per same audit type, user, IP, Object - within time or count.

- Some types of data may appear too many times, for example:
  - ZR Object accessed (read)
  - ZC Object accessed (change)
  - AP Obtaining adopted authority

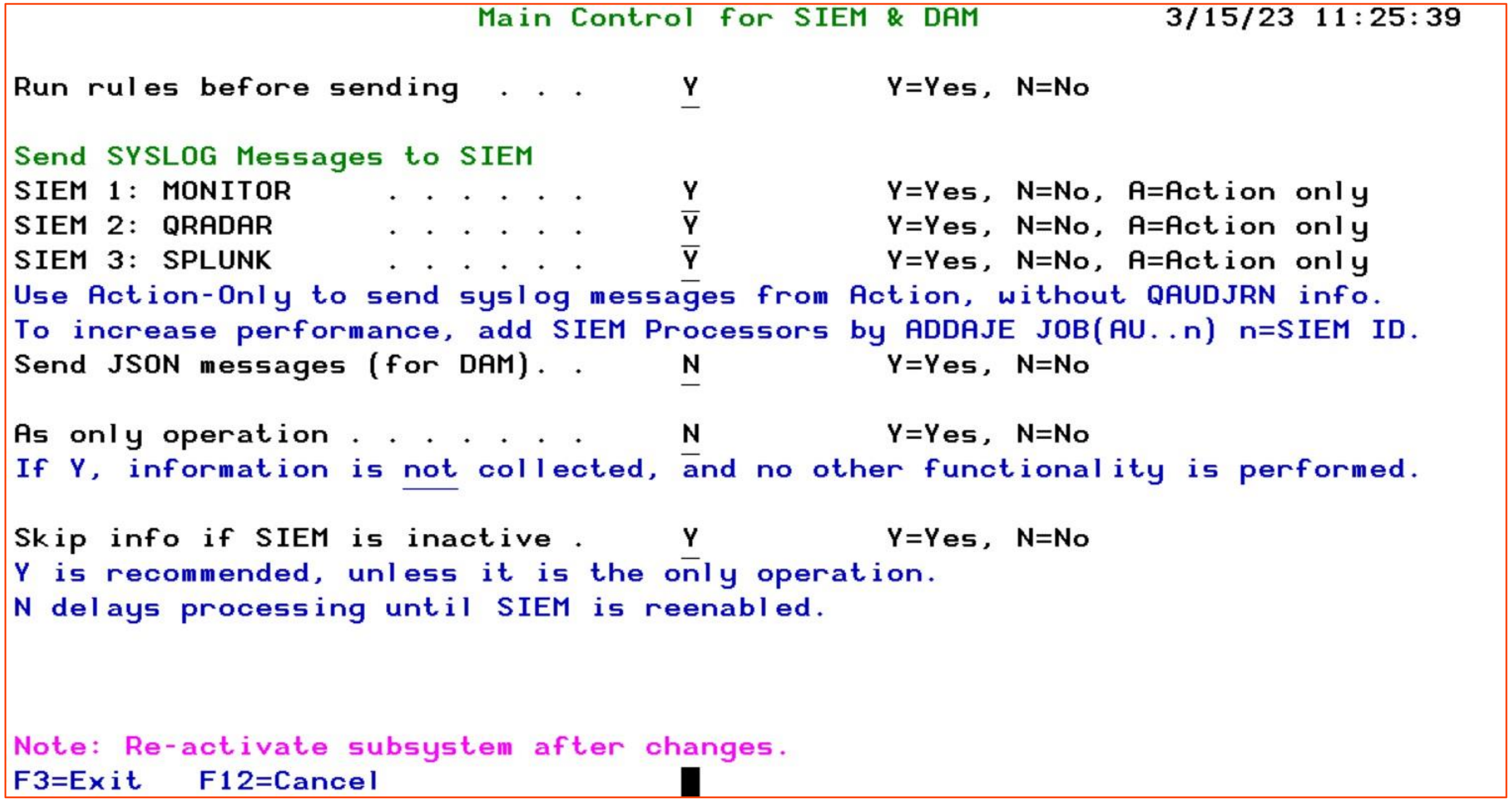
- Input sampling removes unneeded repetitions



```
                              Modify Input Sampling

Type choices, press Enter.

Entry type  . . . . . .   AF
Description . . . . . .   Authority failure

For the same:
  User  . . . . . . . .   Y                 Y=Yes
  IP  . . . . . . . . .   Y                 Y=Yes
  Object (Native/IFS)     Y                 Y=Yes

Omit repeated entries until either of the following is reached:
  Time  . . . . . . . .     20              Seconds
  Count . . . . . . . .     10              Events





F3=Exit     F12=Cancel
```

SIEM Main Control

- Main Control Screen



```
                         Main Control for SIEM & DAM          3/15/23 11:25:39

Run rules before sending  . . .       Y           Y=Yes, N=No

Send SYSLOG Messages to SIEM
SIEM 1: MONITOR      . . . . . .      Y           Y=Yes, N=No, A=Action only
SIEM 2: QRADAR       . . . . . .      Y           Y=Yes, N=No, A=Action only
SIEM 3: SPLUNK       . . . . . .      Y           Y=Yes, N=No, A=Action only
Use Action-Only to send syslog messages from Action, without QAUDJRN info.
To increase performance, add SIEM Processors by ADDAJE JOB(AU..n) n=SIEM ID.
Send JSON messages (for DAM). .       N           Y=Yes, N=No

As only operation . . . . . . .       N           Y=Yes, N=No
If Y, information is not collected, and no other functionality is performed.

Skip info if SIEM is inactive .       Y           Y=Yes, N=No
Y is recommended, unless it is the only operation.
N delays processing until SIEM is reenabled.



Note: Re-activate subsystem after changes.
F3=Exit   F12=Cancel
```

SIEM for Database Journals

To support database journals we have the product AP-Journal. This product, relevant to SIEM, provides:

- Advanced filtering based on journal header, file fields, and the relation between the “before” or “after” values of each database field by percentage or absolute value changes
- Supports also Not/LIKE, Not/LIST, Not/ITEM (in external table or by user profile qualification such as special authority of limited capability)
- Can send only Committed transactions
- Supports 3 SIEMs in parallel
- Use of TLS, TCP, UDP
- Can run on a High Availability system, reducing performance impact on Production Systems

RAZ-LEE

Thank You

For more information about our company and products please visit

www.razlee.com