

# Integrating IBM i Security with Enterprise SIEM and Monitoring Solutions

Real-Time Monitoring of  
IBM i Security Events

**iSecurity**  
System i Security Solutions

# Company Overview



Software Engineering of America

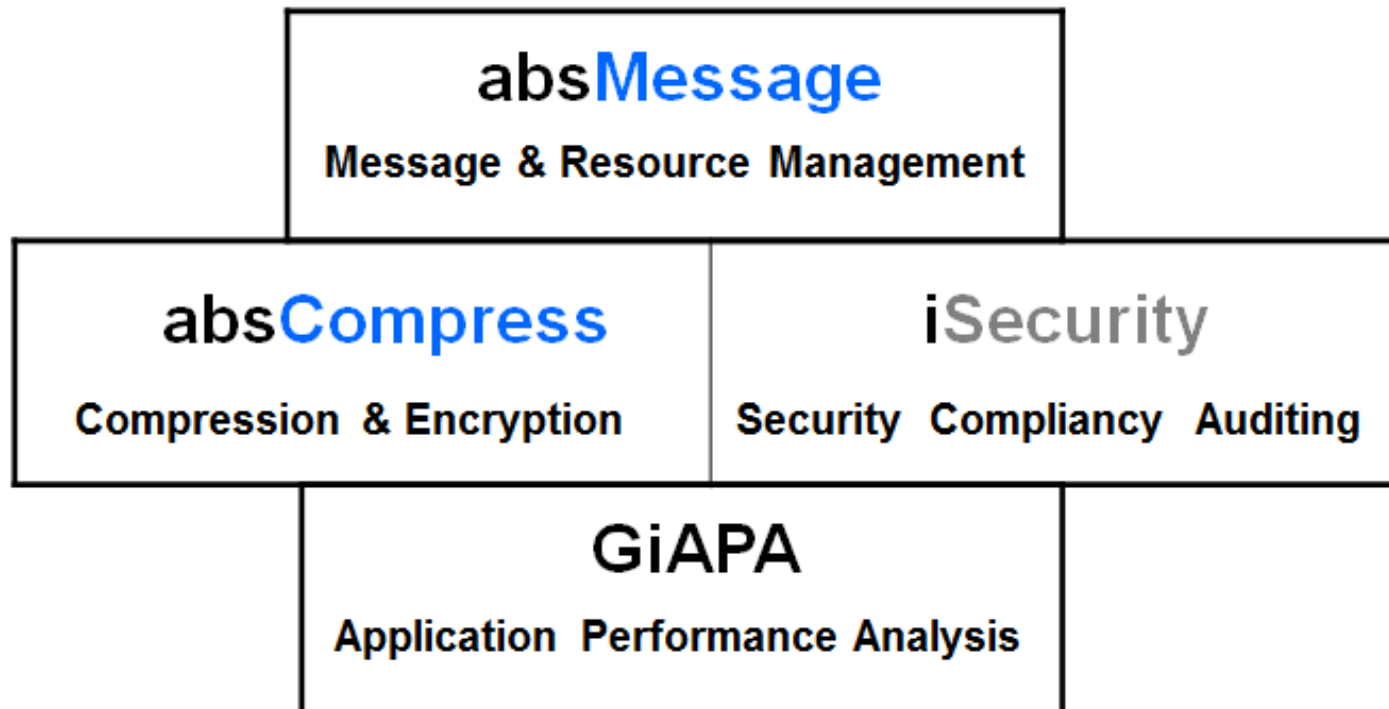
[www.seasoft.com](http://www.seasoft.com)

# Company Overview



- 30 Years of Excellence
- 9 of the Fortune 10
- 85% of the Fortune 500
- Licenses in over 50 Countries

# Company Overview





# Company Overview



- Support - Live Operator 24x7x365
- SEA Employee
- Training
- Conversions
- Consulting

# SIEM – What is it ?

---

- **Security information & event management**
  - solutions are a combination of the formerly disparate product categories of **SIM** (security information management) and SEM (security event management). **SIEM** technology provides real-time analysis of security alerts generated by network hardware and applications.
  - SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes

From Wikipedia, the free encyclopedia

# SIEM – What is it, really ?

(security information & event management)

---

- **Data Aggregation:** log management solution, aggregate data from many sources
- **Correlation:** looks for common attributes, and links events together into meaningful bundles.
- **Alerting:** the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues.
- **Retention:** SIEM/SIM solutions employ long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements.

# SIEM – Why and How?

---

- **Fact:** Multi-platform environments are the reality at nearly all companies.
- **Company Goal:** Consolidate relevant event information from multiple environments onto a single console → require a SIEM (Security Information & Event Manager solution). Optimally, security event information should be both infrastructure-related as well as application- related.
- **Method:** Syslog & SNMP are the most widely used protocol for sending alert messages in real time to SIEM solutions.

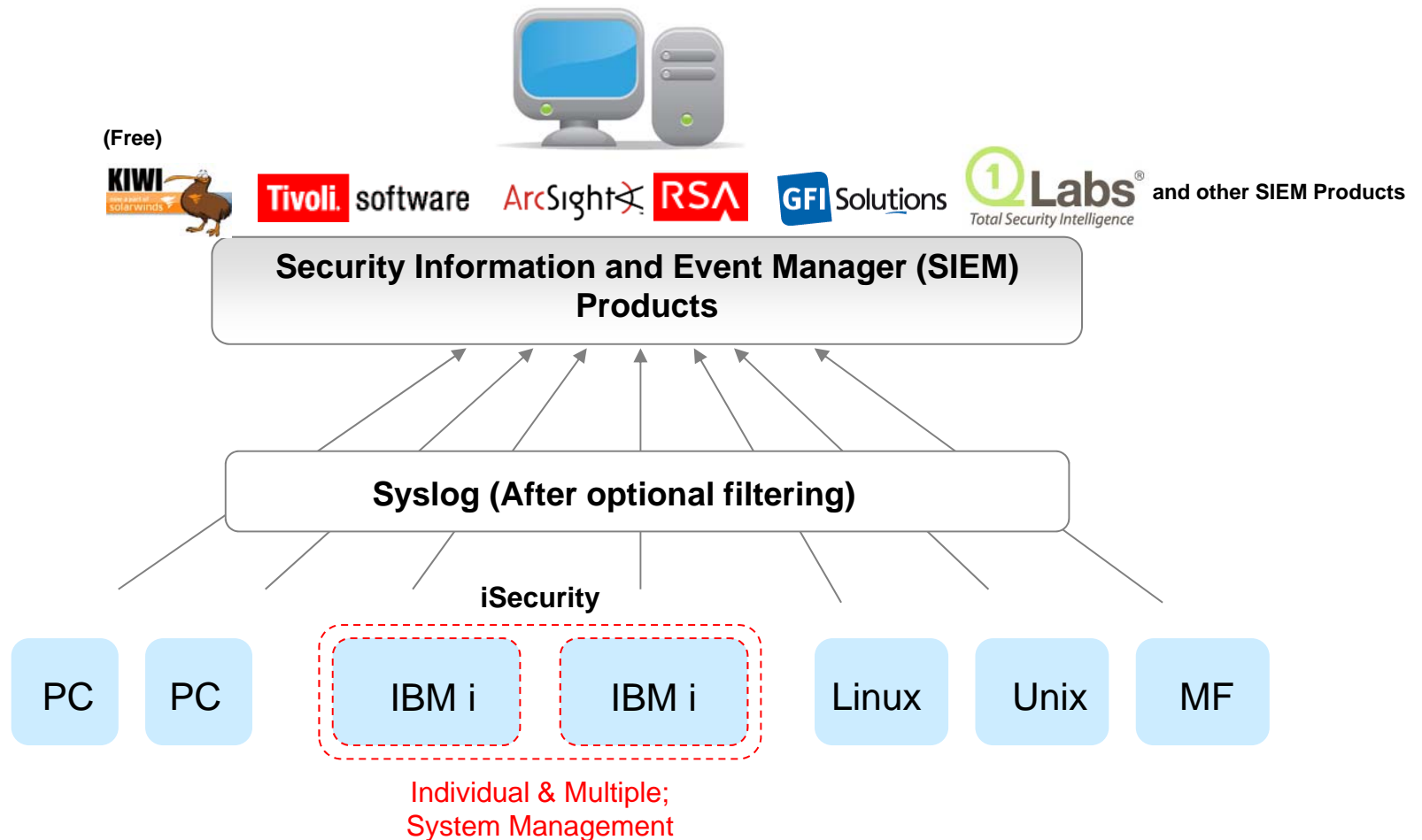


# iSecurity SIEM Partners

---

- IBM Tivoli Security Manager
- Q1Labs (recently purchased by IBM)
- RSA enVision
- GFI
- iSecurity also proven with Arcsight, HPOpenview, CA Unicenter and others

# Typical Syslog Environment



# What Auditors Are Looking For

---

## BEST PRACTICES

- Written Policy that all employees understand
- Continuous Monitoring of **Enterprise Security** Activity
- Rules to Enforce Security Policy
- Real-time Alerts of Exceptions to Policy

# What Auditors Are Looking For

---

## BEST PRACTICES

- Data Retention
- Relevant Reports for mgmt and auditors
- Being pro active

# What Auditors Are Looking For

---

## BEST PRACTICES

- Also be aware of other uses of this information
  - How your systems run
  - How your applications run
  - What your users are doing
  - Volume of remote and local activity

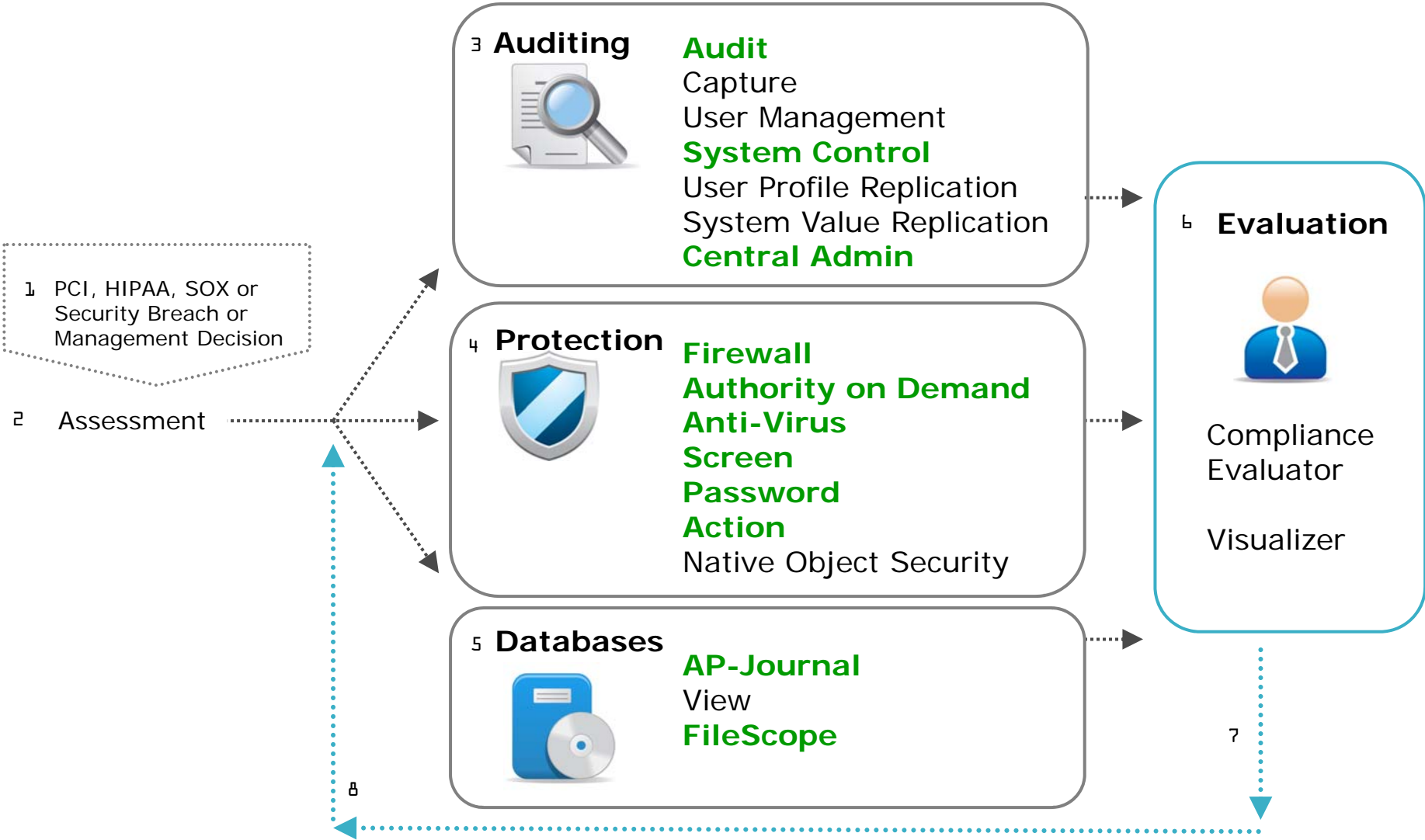
# Benefits of Integration

---

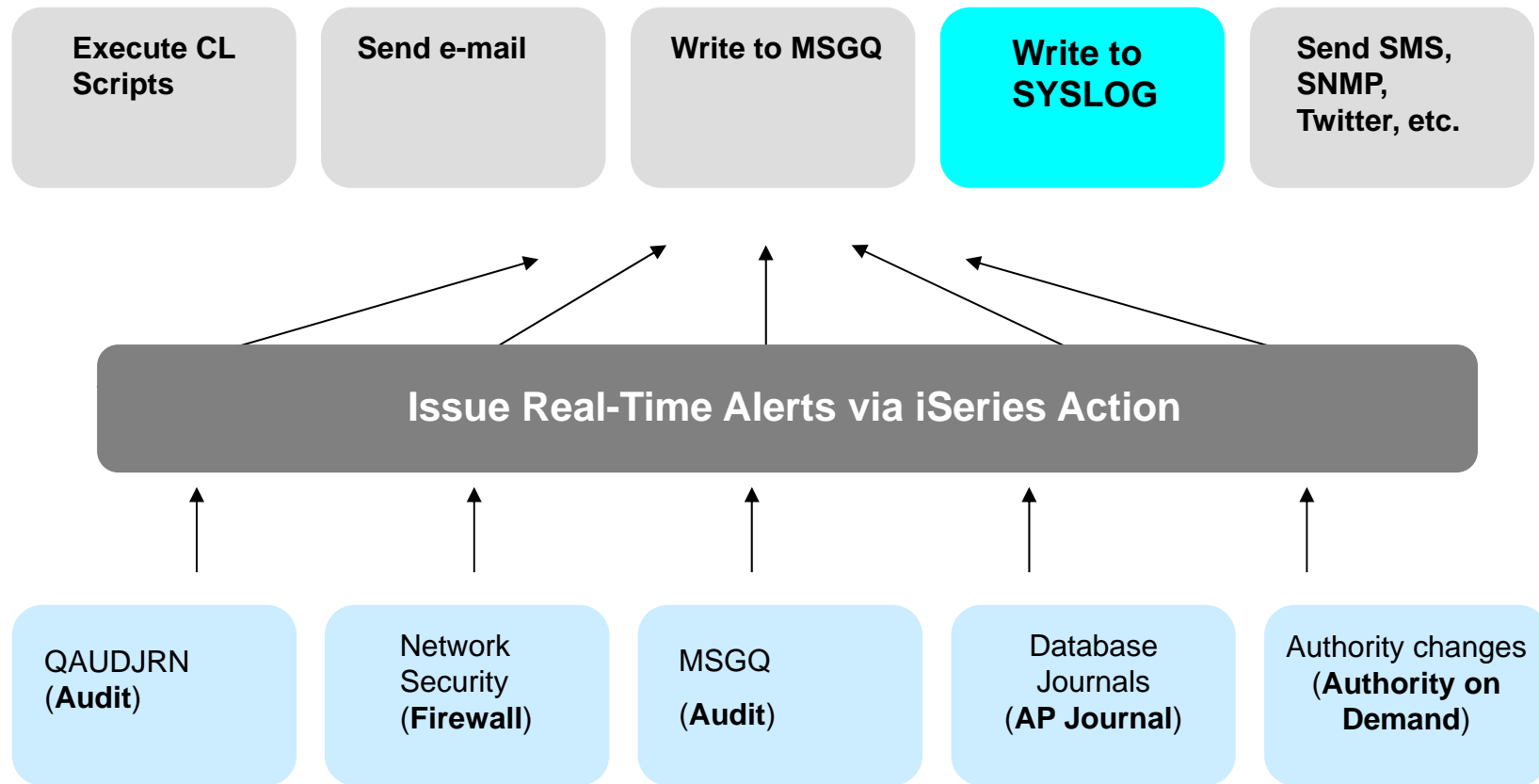
- Single SYSTEM for all audit & compliance recording
- Single APPLICATION for all audit & compliance
- Single TEAM to train and operate audit and compliance reporting
- Single LOOK & FEEL presented for reporting from multiple platforms
- Dependent upon source systems for data



# iSecurity Overview – Syslog Coverage



# Real-Time Alert handling in iSeries



# Syslog in iSecurity

---

- **iSecurity sends Syslog security event information originating from:**
  - the system's infrastructure (QAUDJRN, network access, virus detection product, user profile changes including requests for stronger authorities, etc.)
  - business-critical applications (not only field level writes & updates but also unauthorized READ accesses to sensitive data)

# Syslog in iSecurity (cont'd)

---

- iSecurity includes advanced filtering capabilities to select which events are sent to SIEM for analysis → can control Syslog “traffic”
- “Super fast” iSecurity Syslog implementation enables sending extremely high volumes of information with virtually no performance impact.
- Syslog message structure is easily definable by each site and can include event-specific values such as user profile name, field-level “before” value, etc.

# Use Cases

(names available upon request)

---

- Large insurance company

- Sends all field-level data changes via **AP-Journal's** Syslog facility to RSA enVision
- Monitors changes to ensure that only authorized PROD\* users who also have “change” authority change data by more than X% or Y (amount)
- >1000 transactions/second are sent via Syslog; CPU overhead <1%
- Manage journal change file on PC rather than on IBM i

# Use Cases

(names available upon request)

---

- Large insurance company (cont'd)
  - Planned integration of Syslog from iSecurity Audit (based on QAUDJRN system journal) and iSecurity Firewall in 4Q11-1Q12
  - Provides field-level change reports to corporate and application managers



# Use Cases

(names available upon request)

---

- Very large mortgage bank
  - Monitors all **Firewall** rejects
  - Monitors all **QAUDJRN** system journal activities via **Audit**
  - Syslog sent to Arcsight for Firewall+Audit forensic analysis
  - Used for providing reports to internal and external auditors

# Use Cases

(names available upon request)

---

- A large airport authority
  - Sent alerts to internal AS/400 message queues for years. Now they use SNMP to send to their SIEM
  - All definitions of new user profiles with high authorities, or changes to such user profiles, are sent via SNMP.
  - They will soon implement the "mass SNMP" capability, i.e. they will define which audit types NOT to send SNMP traps for, and all QAUDJRN entries with the other audit types will automatically be sent, en masse

# Syslog Attribute Definitions

SYSLOG Definitions		3/11/11 17:10:39
<b>SYSLOG Support</b>		
Send SYSLOG messages . . . . .	<input checked="" type="checkbox"/>	Y=Yes, N=No, A=Action only
SYSLOG type . . . . .	1	1=UDP, 2=TCP      Port: 514
Destination address . . . . .	1.1.1.155	
<hr/>		
"Facility" to use . . . . .	20	LOCAL USE 4 (LOCAL4)
"Severity" range to auto send .	0 - 7	Emergency - DEBUG
Sends QAUDJRN edited messages. Use F22 to set.		
In range-Send All or LOG=Y only	A	A=All, F=Filtered to be logged
Convert data to CCSID . . . . .	0	0=Default, 65535=No conversion
Maximum length . . . . .	1024	128-9800
Message structure . . . . .	&d/&m/&y &X &8 &9 &1	
<hr/>		
Mix Variables and constants (except &, %) to compose message:		
&1=First level msg	&3=Msg Id.	&4=System      &5=Module
&6=Prod Id.	&7=Audit type	&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)
<hr/>		
F3=Exit    F12=Cancel		F22=Set SYSLOG handling per audit sub-type

Syslog Severity range can be defined.

For each alert message, the "First level message" (&1) is appended to the pre-defined Message Structure.

This option shown on following slide.

# Set Syslog handling per Audit sub-type

Severity level can be set for each audit entry-type/sub-type combination.

```

QAUDJRN Type/Sub Severity Setting
                                     Position to . . . _____
Type options, press Enter.           Subset . . . . . _____
blank=Do not send  0=Emergency  1=Alert  2=Critical  3=Error
4=Warning  5=Notice  6=Info  7=Debug

      Audit      Entry Sub
Opt  Type      Type Type Description
  1  *ATNEVT    IM  P  A potential intrusion has been detected. Further
      evaluation is required to determine if this is an
      actual intrusion or an expected and permitted
      action.
  3  *AUTFAIL   AF  A  Attempt made to access an object or perform an
      operation to which the user was not authorized.
  6      AF  F  ICAPI authorization error
  6      AF  G  ICAPI authentication error
  6      AF  H  Scan exit program action.
  6      AF  I  An attempt was made to proceed with a System Java
      inheritance which was not allowed
  6      AF  J  Attempt made to submit or schedule a job under a
      More...

Settings are used to specify range of severities to send to SIEM.
F3=Exit  PgUp/PgDn=Update
    
```

# Defining Syslog message format

## Message to send

```
Application &APP  SPAIN      Demo Application containing 5 files
File . . . &FILE JDORDDT
  Library . &LIB  SMZJDTA
BEFORE          1.0      "SYSLOG demo: Price of item changed by > 15 cents"
```

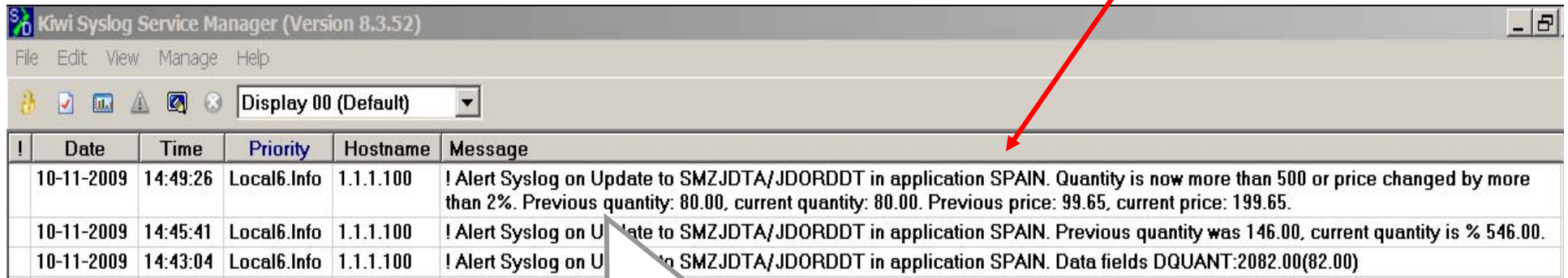
Type the message to send. Use F7 to select file or event-description fields.

Message: &OPERATION=Write, Update..., &FIELDS=All fields.

User &JOUSPF, Alert &DESC on &OPERATION to &LIB/&FILE in application &APP. Current Price: &DPRICE, Previous Price: &DPRICE(B) for Order Number: &DORDNO

Variables beginning with & are replaced with actual event values. &DPRICE(B) is the previous price ("before value") of the item.

# Syslog Messages in (free) Kiwi Syslog Daemon



!	Date	Time	Priority	Hostname	Message
	10-11-2009	14:49:26	Local6.Info	1.1.1.100	! Alert Syslog on Update to SMZJDTA/JDORDDT in application SPAIN. Quantity is now more than 500 or price changed by more than 2%. Previous quantity: 80.00, current quantity: 80.00. Previous price: 99.65, current price: 199.65.
	10-11-2009	14:45:41	Local6.Info	1.1.1.100	! Alert Syslog on Update to SMZJDTA/JDORDDT in application SPAIN. Previous quantity was 146.00, current quantity is % 546.00.
	10-11-2009	14:43:04	Local6.Info	1.1.1.100	! Alert Syslog on Update to SMZJDTA/JDORDDT in application SPAIN. Data fields DQUANT:2082.00(82.00)

**Note real-time user-defined messages from AP-Journal containing previous and new quantity and price values.**



# Syslog Messages in (free) Kiwi Syslog Daemon

Kiwi Syslog Service Manager (Version 8.3.52)

File Edit View Manage Help

Display 00 (Default)

I	Date	Time	Priority	Hostname	Message
	05-14-2009	09:36:39	Local6.Alert	1.1.1.100	S720 iSecurity/ /FW/04/S720.RAZLEE.COM/JAVA1 /*SQL *FYI* Denied for JAVA1 to SMZ4DTA/AUSTTS *FILE. SQL: SELECT STDATE,SUM(STCOUN) FROM SMZ4DTA/AUSTTS WHERE STDATE BETWEEN 90320 AND 90514 GROUP BY STDATE ORDER BY STDATE.
	05-14-2009	09:35:46	Local6.Alert	1.1.1.100	S720 iSecurity/ /FW/03/S720.RAZLEE.COM/AV /*FTPSRV *FYI* Denied for AV to HOME AV/EX2_BERT.C type *IFS. Function RCV_FILE. Function RCV_FILE. IP address 1.1.1.229.
	05-14-2009	09:35:43	Local6.Alert	1.1.1.100	S720 iSecurity/ /FW/32/S720.RAZLEE.COM/JAVA1 /*TCPSTGN *FYI* Denied for JAVA1. Function RTVSGONINF.
	05-14-2009	09:35:26	Local6.Info	1.1.1.100	S720 iSecurity/ /FW/03/S720.RAZLEE.COM/AV /*FTPSRV *FYI* Allowed for AV. Function CHG_DIR. IP address 1.1.1.229.
	05-14-2009	09:35:02	Local6.Alert	1.1.1.100	S720 iSecurity/ /FW/02/S720.RAZL
	05-14-2009	09:33:42	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd /GT/OD/s44k1246.razlee.il/ELI /ELI Start add authority of user QSECOFR in job 247689/ELI/QPADEV0002.
	05-14-2009	09:32:53	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd /RL/OD/s44k1246.razlee.il/ELI /ELI End add authority of user QSECOFR in job 247689/ELI/QPADEV0002.

100% 0 MPH 09:38 05-14-2009

Syslog messages written when special user authority added or removed. Note **multi-product**, **multi-system** & **multi-IP** messages.

# Syslog Messages in a console

The screenshot displays a Syslog console interface. On the left is a navigation sidebar with sections: Monitor, Admin, Menu, Explorer, Dashboard, Events, Service Views, Hyper Map, About, Host/Group/Service filters, Service Views, Status, Groups, Reports, Availability, Event Levels, History, and Inventory. The main area shows a list of messages:

Timestamp	Severity	Message
Thu 12:01:45	NOTIFICATION	iSecurity! : MCO1400 *CREATE User QSYS.
26-01-2012 Thu 12:02:15	SERVICE ALERT	sea4001b.seapub.com iSecurity! : MCO1400 *CREATE User QSYS.
26-01-2012 Thu 12:02:15	SERVICE ALERT NOTIFICATION	sea4001b.seapub.com iSecurity! : MCO1400 *CREATE User QSYS.
26-01-2012 Thu 12:02:46	SERVICE ALERT	sea4001b.seapub.com iSecurity! : MCO1400 *CREATE User QSYS.
26-01-2012 Thu 12:02:46	SERVICE ALERT NOTIFICATION	sea4001b.seapub.com iSecurity! : MCO1400 *CREATE User QSYS.
26-01-2012 Thu 12:03:16	SERVICE ALERT	sea4001b.seapub.com iSecurity! : MCA0100 *SECURITY Authority Access code (A-Added R-Removed N-None). *ADD- *UPD- *DLT- *EXCLUDE- *EXECUTE-Y* Personal status changed . QOpenSys\root o
26-01-2012 Thu 12:03:16	SERVICE ALERT NOTIFICATION	sea4001b.seapub.com iSecurity! : MCA0100 *SECURITY Authority Access code (A-Added R-Removed N-None). *ADD- *UPD- *DLT- *EXCLUDE- *EXECUTE-Y* Personal status changed . QOpenSys\root o
26-01-2012 Thu 12:03:16	SERVICE ALERT	sea4001b.seapub.com iSecurity! : MCO1400 *CREATE User QSYS.
26-01-2012	SERVICE ALERT	sea4001b.seapub.com

# Review

---

- Single:
  - SYSTEM for all audit & compliance recording
  - APPLICATION for all audit & compliance
  - TEAM to train and operate audit and compliance reporting
  - LOOK & FEEL presented for reporting from multiple platforms
  - Dependent upon source systems for data

---

# Thank You!

Visit us at

[WWW.SEASOFT.COM](http://WWW.SEASOFT.COM)

[sales@seasoft.com](mailto:sales@seasoft.com)

516-328-7000

Software Engineering of America

[www.seasoft.com](http://www.seasoft.com)