

SIEM & DAM Support



DATASHEET (iSecurity Suite Evaluation, Reporting & Alerts)

Integrating IBM i Security Events

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

SIEM - Security Information and Event Management

DAM - Database Activity Monitoring

SIEM & DAM Support



- Integration with IBM's Tivoli, McAfee, RSA enVision, Q1Labs, GFI Solutions, also tested with ArcSight, HPOpenView, CA UniCenter and others.
- iSecurity supports Imperva SecureSphere DAM.

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

- Journals QAUDJRN, QVFN, 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 other iSecurity modules

Key Features

- Advanced filtering capabilities via specific severity code, part of the syslog standard, for each event/message and specifying the range of messages to send to each SIEM. This controls which messages will be sent to each SIEM.
- Advanced communications recovery features handle network problems or SIEM unavailability
- Enables sending extremely high volumes of information with virtually no performance impact.
- Syslog Self-Test facility runs on the IBM i, receiving messages locally for syslog message pre-check prior to sending to a remote syslog server.
- Proven integration with all SIEM products.
- Field-mode support for the 2 major standards – LEEF (IBM QRadar) and CEF (ArcSight). These standards are supported in many other SIEM products as well.
- As an alternative to CEF and LEEF, iSecurity continues to support local structuring of the message format sent to a specific SIEM.
- Sends Syslog messages in parallel to up to 3 SIEM products.
- Transmission is supported via UDP, TCP or TLS (encrypted channel).
- Support in all iSecurity solutions enables infrastructure-related alerts and field-level application alerts on unauthorized data changes or access.

Installation Requirements

- Operating system 7.1 or higher
- 300 MB of disk space for initial installation

Integration at its Fullest

Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems.

Message alerts contain detailed event information about application data changes, deletes or reads of objects and files, emergency changes in user authorities, IFS viruses detected, malicious network access to the Series i, and more.

```

Main Control for SIEM & DAM                23/07/19 11:48:50

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

Send SYSLOG Messages to SIEM
SIEM 1: kiwi . . . . . N          Y=Yes, N=No, A=Action only
SIEM 2: VictorPC . . . . . Y          Y=Yes, N=No, A=Action only
SIEM 3: QRADAR . . . . . N          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.

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

```

```

iSecurity/Base System Configuration        20/08/19 10:51:18

Audit *SIEM Only* Mode Active              SIEM Support
1. General Definitions                    30. Main Control-----> Active
3. Log QSH, PASE activity                 31. SIEM 1: Kiwi          Y
5. Auto start activities in ZAUDIT        32. SIEM 2: VictorPC     N
9. Log & Journal Retention                33. SIEM 3: QRADAR       N
                                           34. JSON Definitions (for DAM)
                                           35. SNMP Definitions
                                           36. Twitter Definitions

Action *FYI* Mode Active
11. General Definitions                   39. Syslog test
12. SMS/Special Definitions
13. E-Mail Definitions

SIEM Event Classification                  General
21. QSYSOPR, QHST, MsgQ & User msgs      91. Language Support
22. QAUDJRN Type/Sub Severity Setting     99. Copyright Notice

Selection ==> -

Release ID . . . . . 14.06 19-08-14    44DE466 520 7459 1
Authorization code A (starts with 4) . 401910757307 1      1 8520
Authorization code B (starts with N) . N01910748657
F3=Exit  F22=Enter Authorization Code

```

Let's Get Started

Schedule your Demo and Integrate your Security Events with iSecurity SIEM & DAM Support.

