SIEM & DAM Support

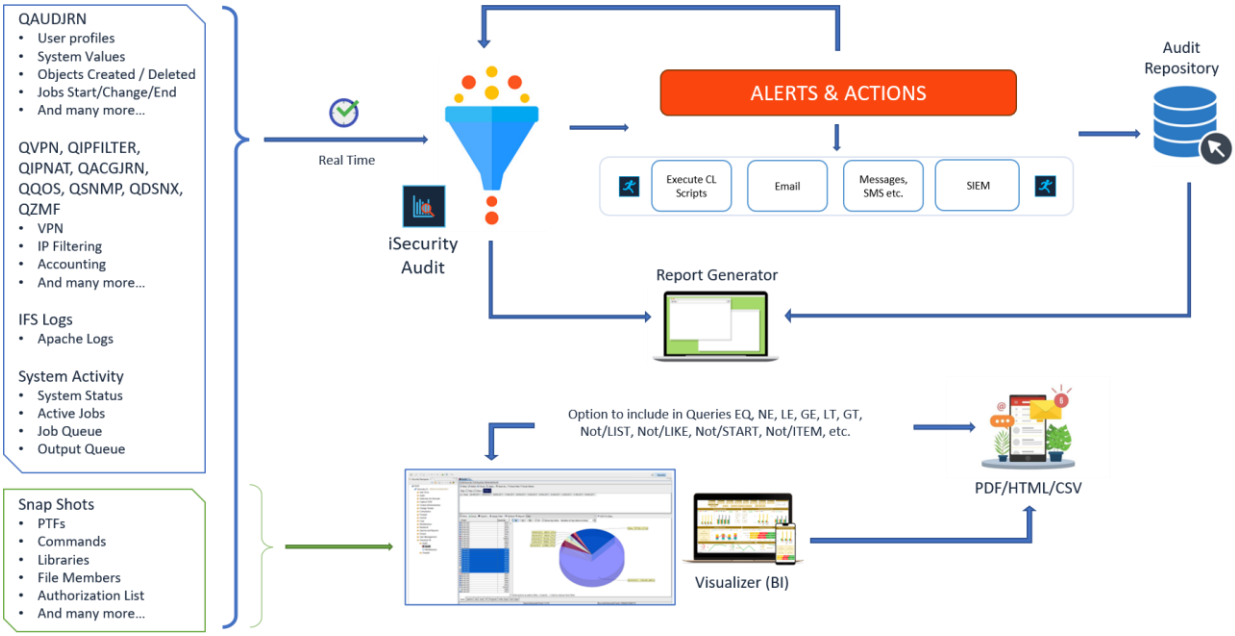
DATASHEET (iSecurity Suite Evaluation, Reporting & Alerts)

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, 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 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.

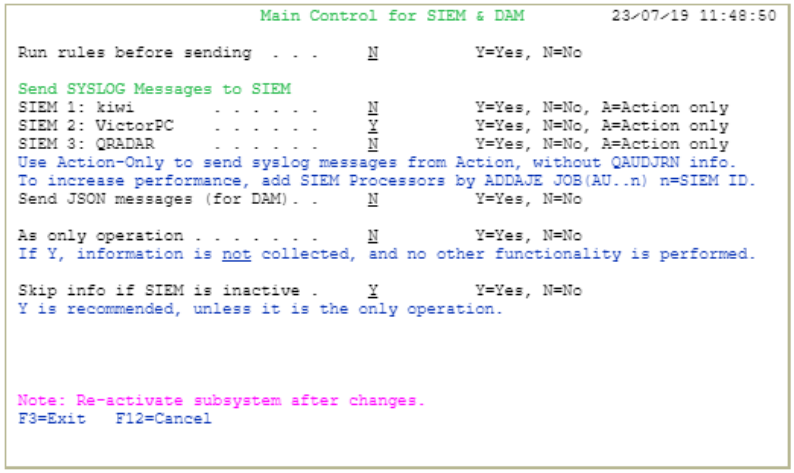
Installation Requirements

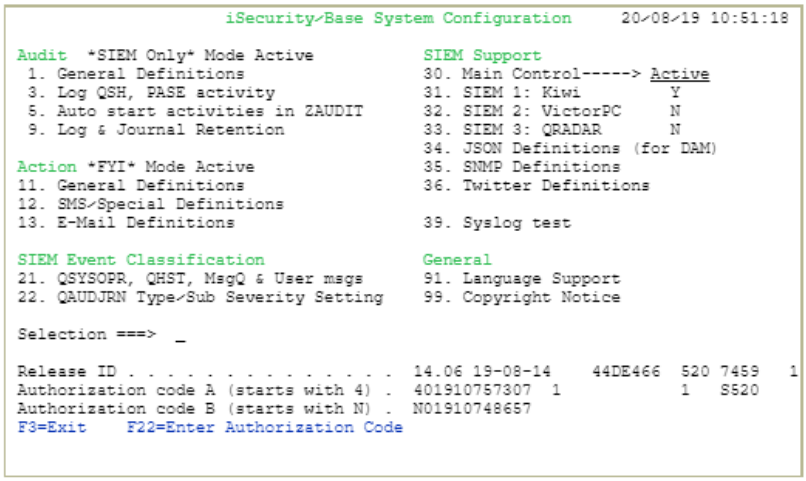
- Operating system 7.1 or higher
- 300 MB of disk space for initial installation

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.





Let's Get Started

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

RAZ-LEE iSecurity