SIEM & DAM Support

DATASHEET (iSecurity Suite Evaluation Modules)

Integrating IBM i Security Events

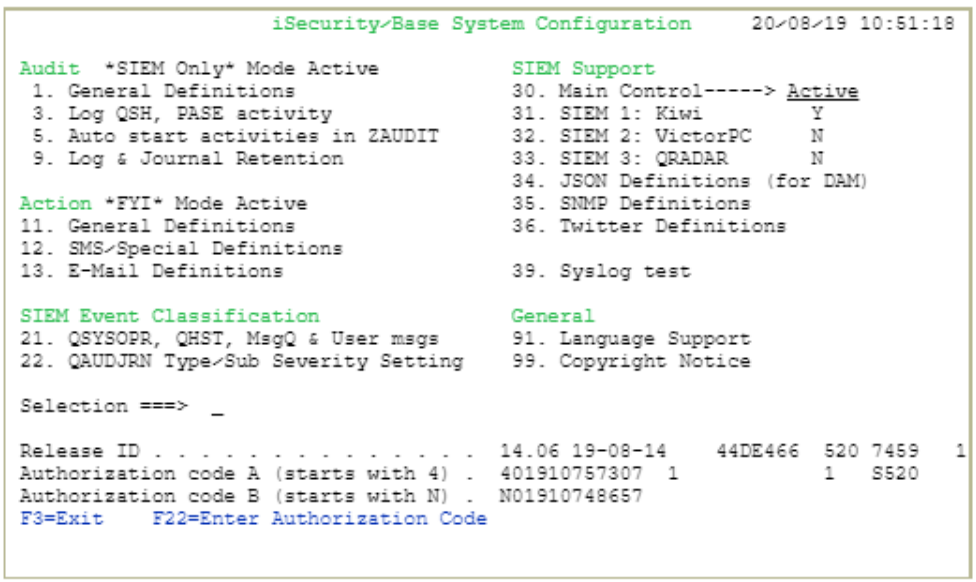
SIEM software matches events against rules and analytics engines and indexes them for sub-second search to detect and analyze advanced threats using globally gathered intelligence. This gives security teams both insight into and a track record of the activities within their IT environment by providing data analysis, event correlation, aggregation, reporting and log management.

A DAM solution streamlines asset management and optimizes the production of rich media, particularly within sales and marketing organizations, by creating a centralized management system for digital assets.

SIEM & DAM Support

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

- 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.
- 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.



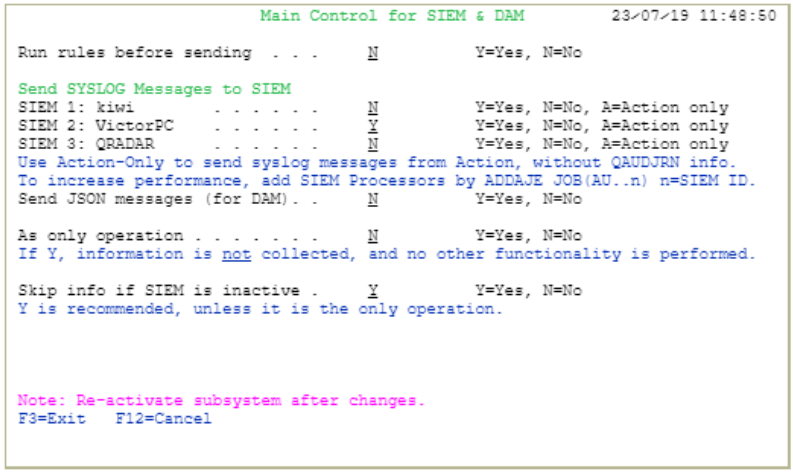
Key Features

- 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.

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.