RAZ-LEE iSecurity

Audit

Raz-Lee Security

- Founded in 1983
- 100% focused on IBM i (AS/400)
- Corporate offices in: US, Italy, Germany
- Installed in more than 40 countries, over 12,000 licenses
- IBM Business Partner
- Partnerships with other major global SIEM & DAM solution providers:
  - Proven integration with McAfee, ArcSight, Qradar, HP OpenView, GFI, Splunk, Juniper, NNT
  - OEM by Imperva SecureSphere
- The widest security solution offer in the market
- Unique products: Anti-Ransomware, Change Tracker, Capture

iSecurity Suite of Products

Audit - Agenda

- Audit – What for?
- iSecurity Audit – Product characteristics
- Auditing of:
  - User Profiles, Objects, and other “entities”
  - Auditing the activities (Audit Journal, QHST)
- Ways to analyze – Log, Report Generator, Business Intelligence, SIEM
- Filtering capabilities – Reduce the overhead
- Automation, Tracking the Exceptions
- React upon event: SIEM, E-mail, Script of commands

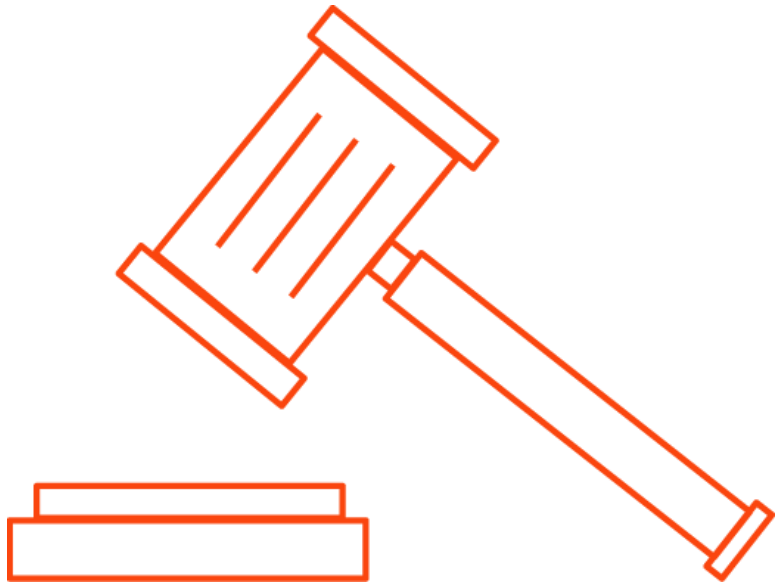
IT Audit – General Definition and Objectives

- The examination and evaluation of an organization's information technology infrastructure, policies and operations.
- It determine whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals.
- The primary objectives:
  - Evaluate the systems and processes in place that secure company data.
  - Determine risks to a company's information assets, and help identify methods to minimize those risks.
  - Ensure information management processes are in compliance with IT-specific laws, policies and standards.
  - Determine inefficiencies in IT systems and associated management.

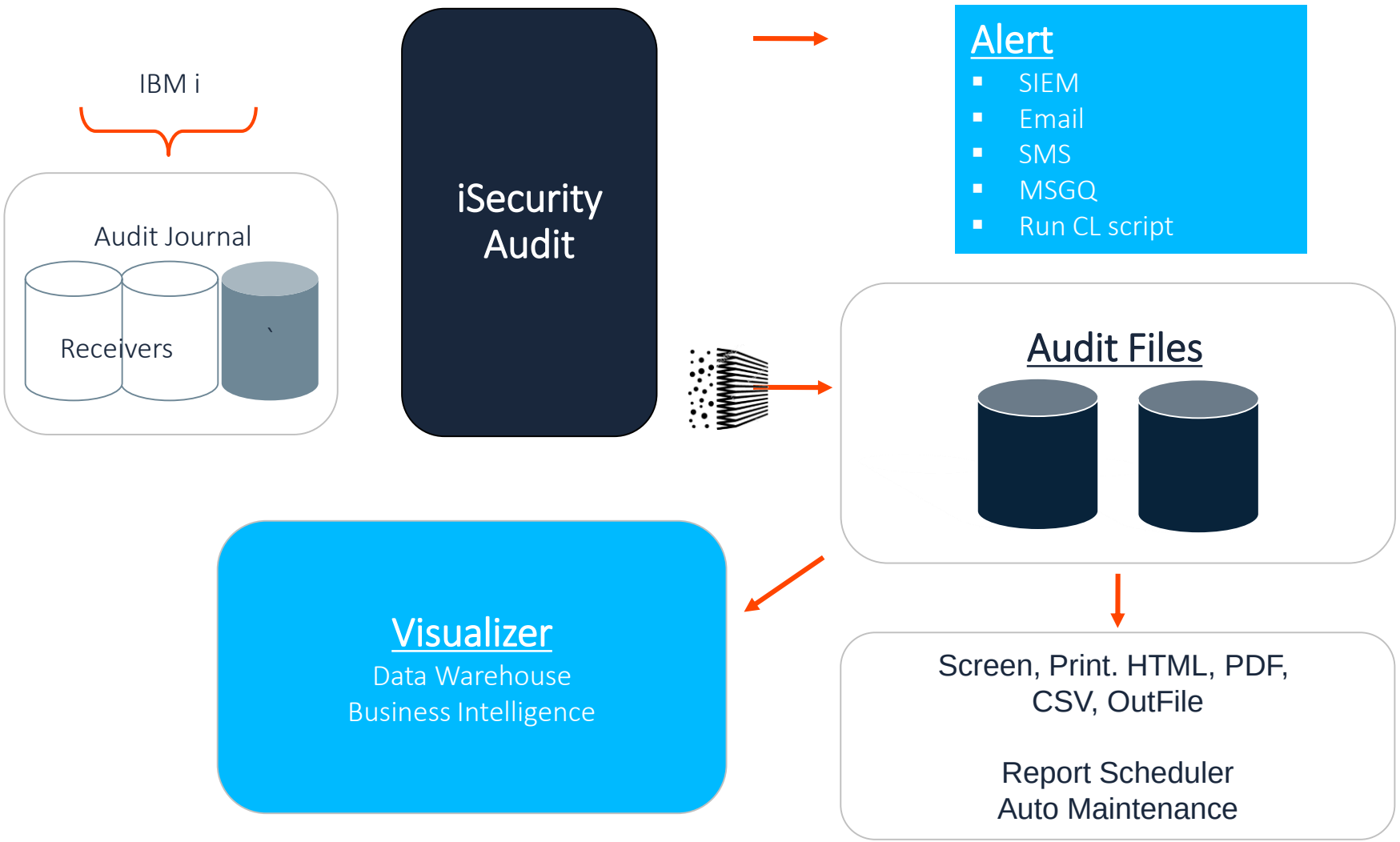
The need to Audit

- To ensure IT systems are reliable, secure and not vulnerable to computer attacks.
- To reduce risks of data tampering, data loss or leakage, service disruption, and poor management of IT systems.
- Mandatory Security Regulations
  - GDPR, NIS Directive, HIPAA, SOX
- Event and User Activity Tracking
- External auditor's demands
- Internal security policies

- But – isn't what IBM provides enough?



Audit Journal Flow Diagram



Characteristics of iSecurity Audit

- User-friendly display and process of Audit Journal, QHST and Message Queues
- Process of Open Logs (Apache, WebSphere, Others)
- Status snapshots of User profiles, System Values, Objects, etc.
- Advanced filtering capabilities, eliminating unneeded data
- Powerful Report Generator allows to create queries quickly without programming
  - Various report formats; HTML, PDF, CSV, OUTFILE, Visualized as statistical data
- Base line to compare changes of System Values, Network Attributes
- Business Intelligence; graphical analysis of data
- Advanced scheduler runs reports at specified times, e-mailing results to your desktop
- Real-time responses to potential threats and security violations

New Features

- New sources of information for queries were added
- Triple SIEM support with full CEF and LEEF format
- QHST support, including break of messages to its parameters
- Query generator enhanced to support user defined groups of summaries
- Supports of IASP
- Export single query to a remote system
- ZIP several reports into a single file
- Email subject name contains *NO DATA* to say - No exception found
- Optional enhanced auto disable of user profile with generic names
- Auto delete of dormant or disabled user profiles
- Support of generic options in general groups

Auditing of User Profiles, Objects, and other “entities”

- Attributes of definitions of user profiles, object authority, system values, etc. control the actual security and capabilities of accessing and using objects and applications.
- This is the bases of providing proper security
- It is important to ensure settings are properly defined and protected against changes

Auditing the activities

- The system provides an audit journal
- A wide set of audit information will be placed in it subject to proper settings mainly based on system values
- There is a communication message que named QSYSOPR that is used to raise important events
- The information in QSYSOPR is preserved in QHST (system history log) as well

Ways to analyze

The Audit journal is filtered and stored in regular database files (which cannot be overwritten)

Log

- The display log command can show the information in tables structure or as text messages (similar to the standard Display Log or Display Job Log)

Query generator

- Works on the pre-filtered Audit journal info (Authority failures, Creates, Deletes…)
- Works on subjects to be audited (User Profiles, System values, Object authorities…)

Business intelligence

- Data warehouse of statistical info from the Audit journal
- Result of any report output (or Audit journal or Subjects)

SIEM

Filtering capabilities – Reduce the overhead

Usage of filters

- Use the Business Intelligence to analyze and define
- Can reduce up to 95% of QAUDJRN size when stored in Audit
- Real time reactions
- Query generator
- Boolean rules
  - EQ, NE, LE, GE, LT, GT
  - N/LIST, N/LIKE, N/ITEM, N/START, N/PGM
- Item groups: Predefined, Time, User defined

Automation, Tracking the Exceptions

- Daily, Weekly, Monthly reports
- Package reports output to a single ZIP
- Search for Exceptions – Mail subject tells you “No data”
- Store old reports for later reference

React upon event: SIEM, E-mail, Script of commands

- In Real-Time, over Audit journal, Message queues, IFS logs
- On demand, over any Query report (even static info).

Example: Regulation says: Allow updates only by pre-confirmed programs

- Prepare PRODDTA group of production data libraries using ITEM
- Prepare PRODPGM group of production program libraries using ITEM
- Add a rule of ZC-Object changed:
  - If file is in PRODDTA, and program is NOT in PRODPGM
  - Send message
  - Send Email
  - Send SIEM
  - Run a Command Script

Thank You

For more information, visit us at

www.razlee.com