RAZ-LEE

File Integrity Monitoring on **IBM i**:

Detecting Unauthorized Changes

Critical files, objects, applications, and data are constantly changing in an IBM i environment. The challenge is determining which changes are expected and which may indicate unauthorized activity, malware, ransomware, insider threats, or configuration problems.



The problem: What changed?

"If someone changes a critical IBM i object today, how quickly will you know?

File Integrity Monitoring (FIM)

provides the visibility needed to detect and investigate changes to critical resources.

What changed? Who changed it? What happened next?

RAZ-LEE iSecurity

What Is FIM?

FIM helps detect changes that may result from:

- Unauthorized user activity
- Compromised credentials
- Malware
- Ransomware
- Insider threats
- Application errors
- Configuration mistakes
- Administrative activity

Define it as:

"File Integrity Monitoring is the continuous monitoring of critical files, objects, and resources to identify unauthorized, unexpected, or suspicious changes. “

The key is not simply detecting ***any*** change.

"It is providing enough information to determine whether the change is expected, authorized, or suspicious.”

File Integrity Monitoring



RAZ-LEE iSecurity

Why IBM i Journaling Matters for FIM

IBM i provides powerful journaling capabilities that can capture changes and activities associated with journaled objects. For FIM, journal information can provide valuable evidence about changes occurring to critical resources.

IBM i already provides the foundation for monitoring many types of changes.

iSecurity AP-Journal helps turning that journal information into useful **Security Visibility**.

What Should you Monitor?

A practical FIM strategy should begin with the organization's most critical resources.

Potential targets include:



Critical application objects

Programs, libraries, and application components supporting important business processes.



Security-related resources

Objects and configurations where unauthorized changes could affect the security posture.



IFS files

Critical configuration and application files.



Privileged activity

Changes performed by highly privileged users or administrative processes.



Database-related resources

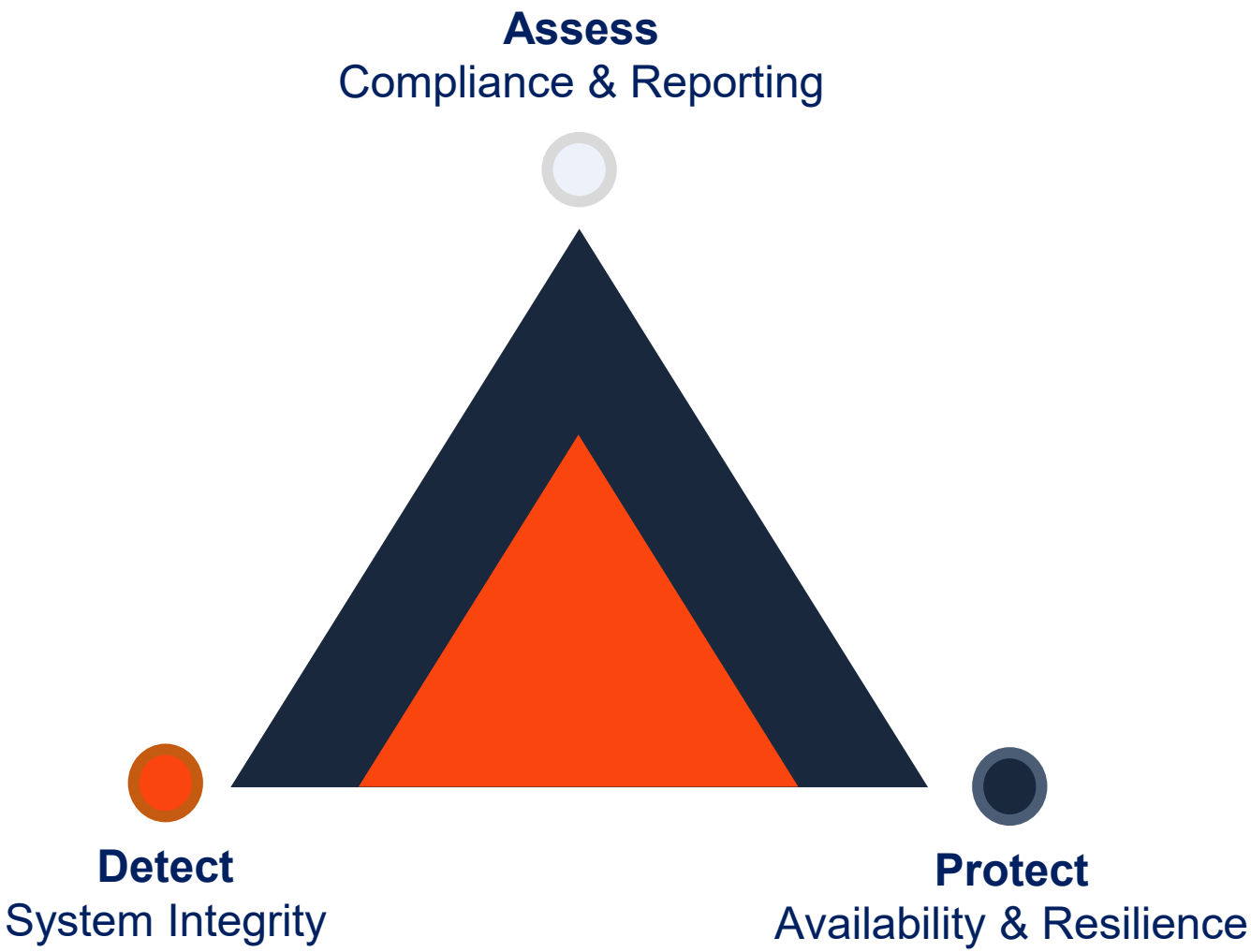
Resources containing sensitive or business-critical information.

The goal is not necessarily to monitor everything equally.

A risk-based approach helps organizations focus monitoring where unauthorized changes would have the greatest impact.

RAZ-LEE iSecurity

How do we categorize the Needs for FIM?



RAZ-LEE iSecurity

File Integrity Monitoring & Compliance

	Regulation Section	Data Security Requirements	iSecurity Solution
DETECT	**Data Breach Notification** *__NIS2__ Art. 21(2)(a)(b)(f) *__GDPR__ Art. 30, 33 and 34 *__DORA__ Art. 1 and 2(a)(b)(c)(d)	Continuously monitor the implementation of the risk treatment measures.	▪ **Audit** ▪ **Action** ▪ **AP-Journal** ▪ **Capture** ▪ **Change Tracker** ▪ **SIEM / DAM Support**

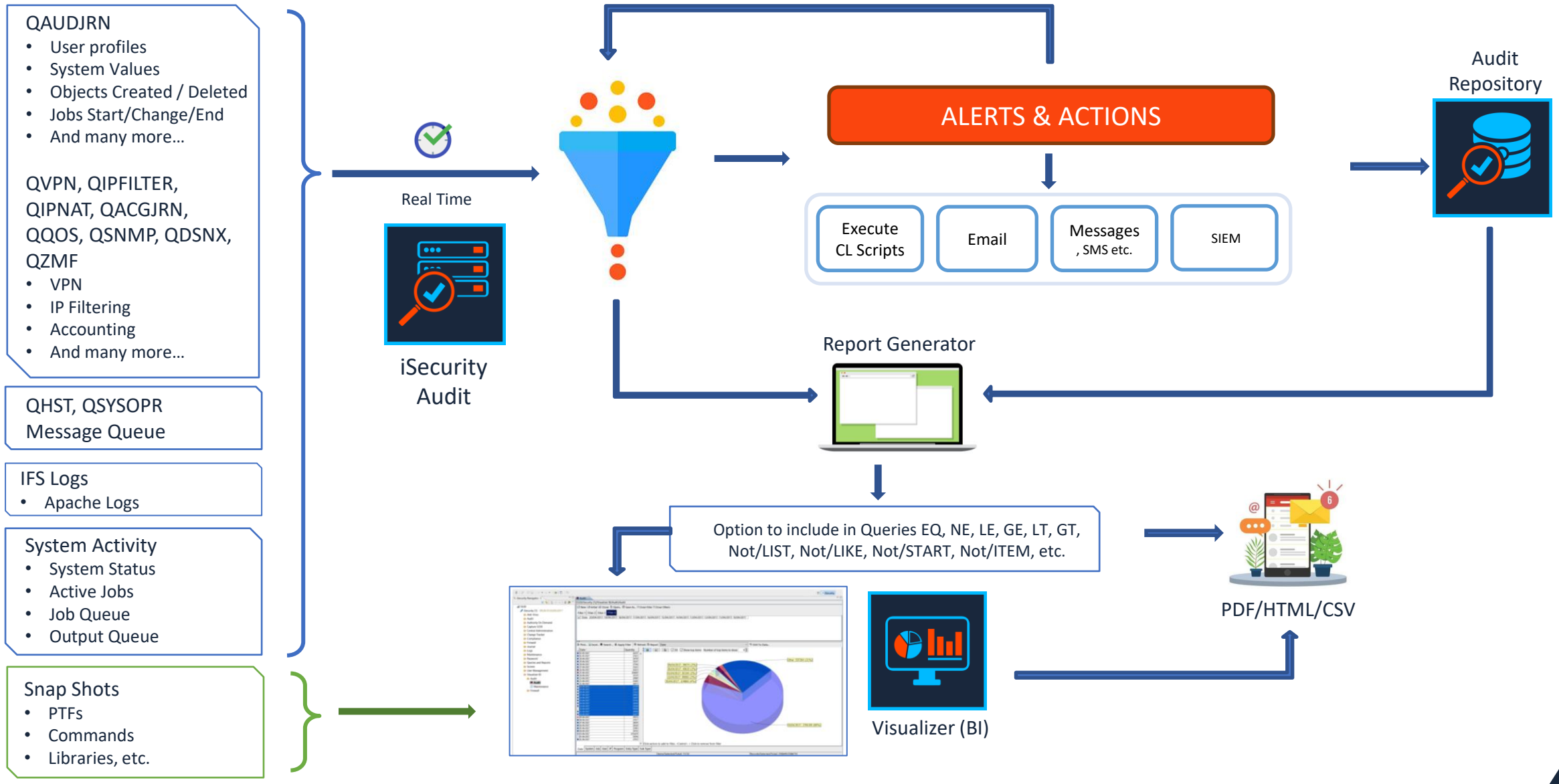
RAZ-LEE iSecurity

RAZ-LEE

iSecurity Audit



iSecurity Audit



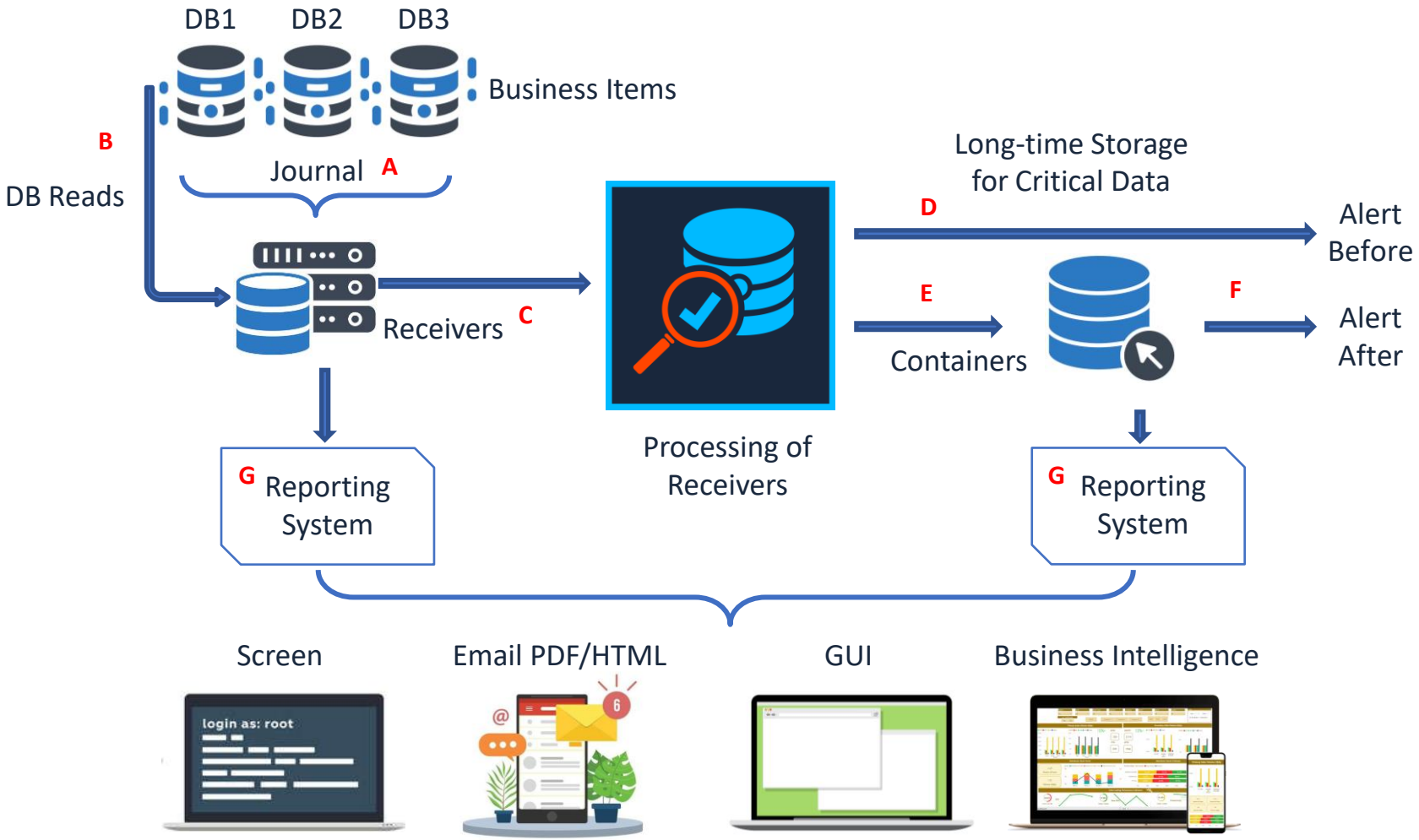
RAZ-LEE

iSecurity

AP-Journal



iSecurity AP-Journal



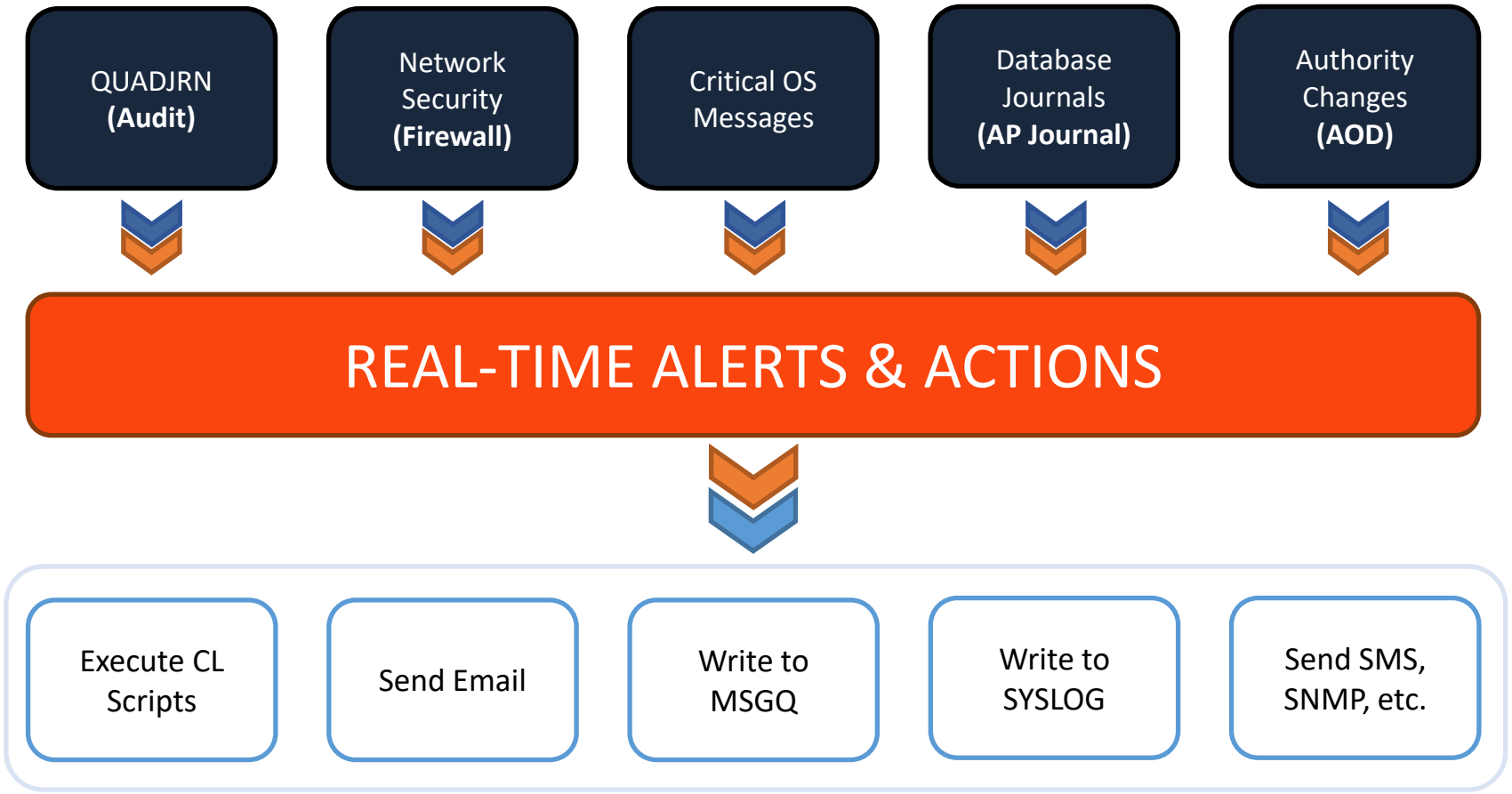
RAZ-LEE iSecurity

RAZ-LEE

iSecurity Action



iSecurity Action



iSecurity
Action

Security Breach Response & Corrections

iSecurity Action brings Proactive Response in real-time to any security event by Email, SMS, Syslog, SNMP, and CL script processor.



RAZ-LEE

Taking Action in Real Time

In today's business environment, it is not enough to discover and report on a security problem after it occurs.

- ✓ Traditional audit software provides useful historical data after the fact but often lacks state-of-the-art functionality to provide relevant managers with alerts and enable corrective specific corrective actions.

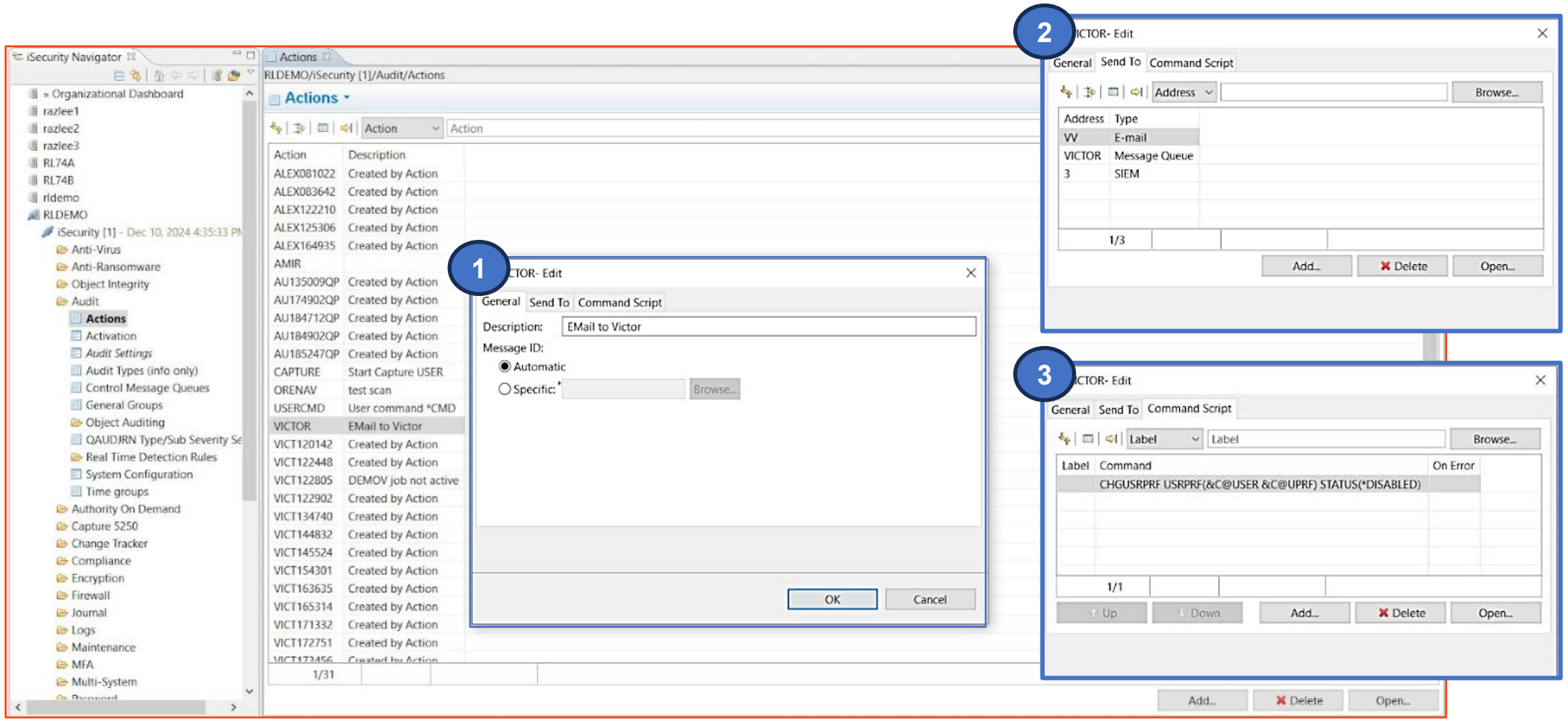
- ✓ **iSecurity Action** provides a comprehensive, easy-to-use solution. For example, if a user attempts to copy a critical file, Action can send an SMS message to the security officer's mobile phone and automatically sign off and disable the offending user.

- ✓ Scripts can even initiate actions that execute if an appropriate response does not occur within a specified period of time!



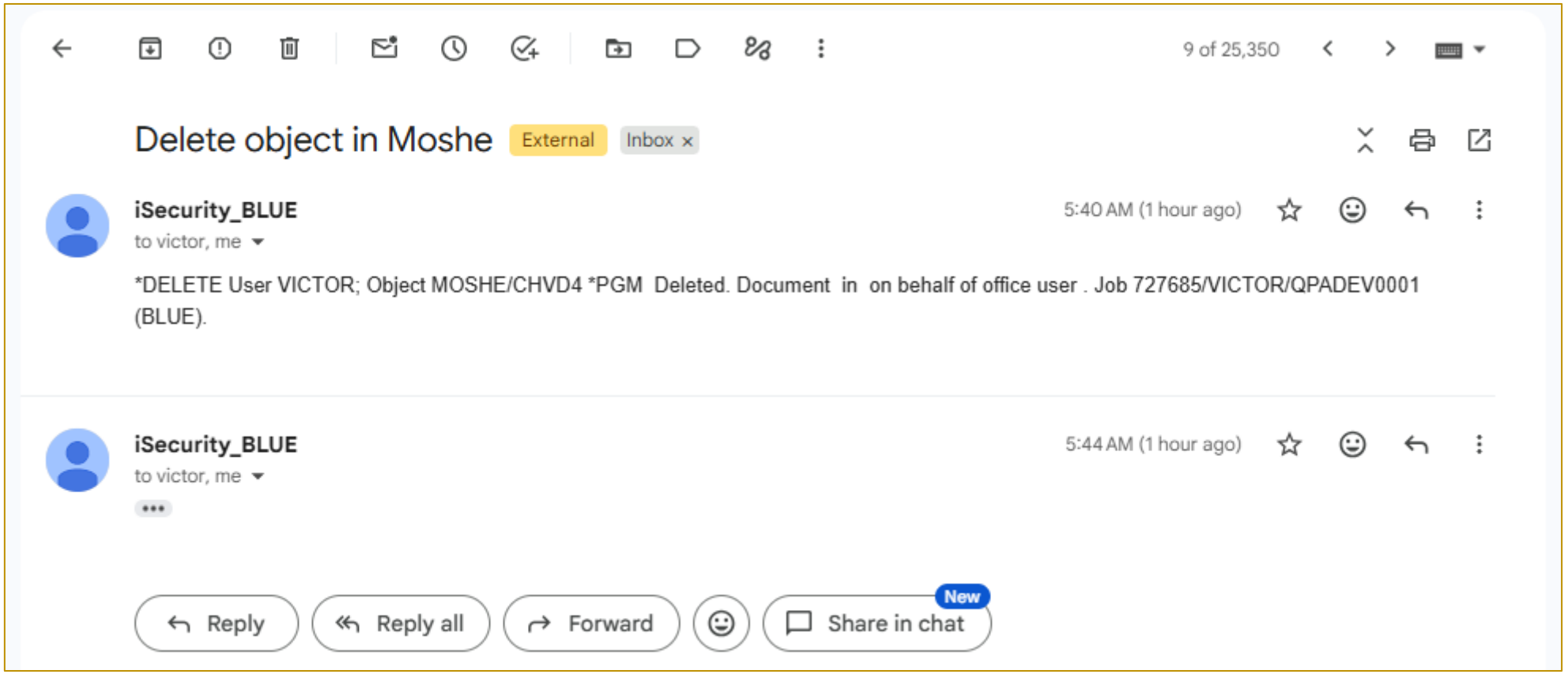
RAZ-LEE iSecurity

Defining Action that Sends Email and Blocks a User (GUI)



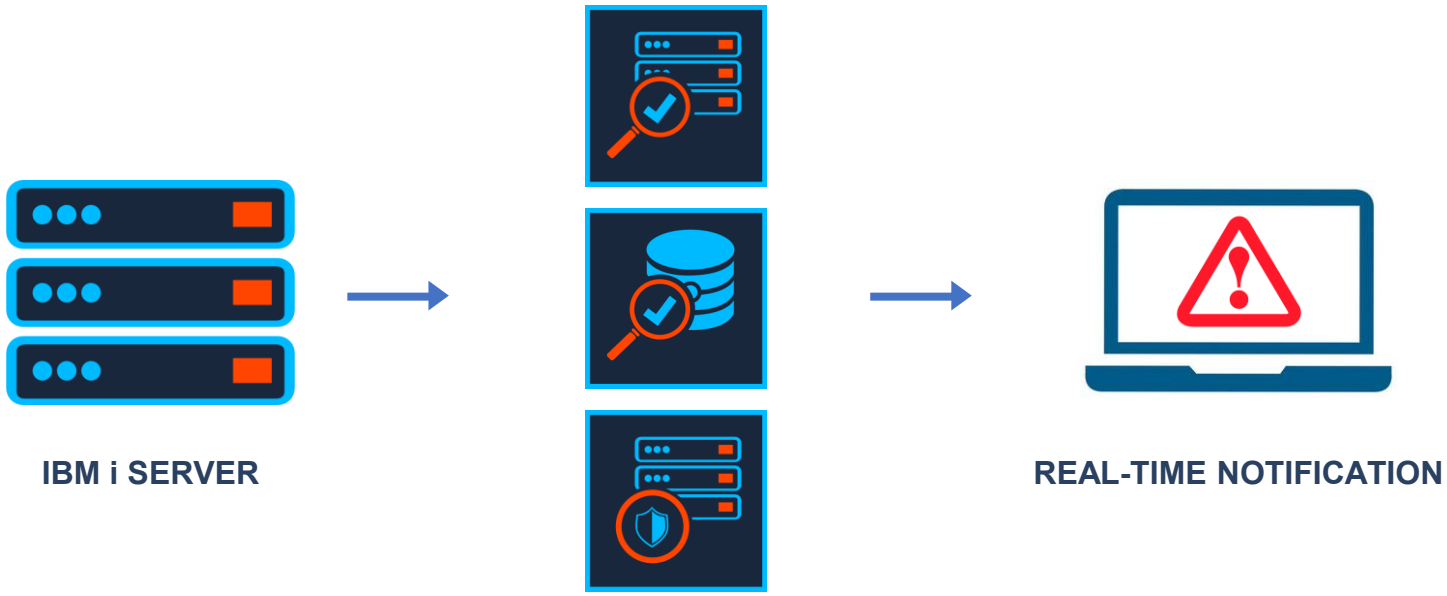
RAZ-LEE iSecurity

e-mail Alert



RAZ-LEE iSecurity

File Integrity Monitoring on IBM i



RAZ-LEE iSecurity

iSecurity Action Advantages

- ✓ Responds to events detected by **Audit**, **Firewall**, **AP-Journal**, etc.
- ✓ Alert messages sent via **Syslog, SNMP, e-mail, SMS, MSGQ or Twitter**.
- ✓ Automatically takes corrective actions by running command scripts or programs.
- ✓ **Rule Wizard** makes definition process simple for non-technical users.
- ✓ Rules can use many different selection criteria.
- ✓ Built-in command script interpreter with replacement variable support.
- ✓ Responds to current system status parameters and active jobs.
- ✓ Restrict user access during vacations, holidays and other planned absences.
- ✓ Automatically **Disables Inactive User Profiles**.
- ✓ Tight **Control over Authority Adoption**.



RAZ-LEE iSecurity

RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com



RAZ-LEE

See you Soon!

Thanks for your Attention

Marketing Manager

Moshe Sofer

Visit our Website for more Information

www.razlee.com