Integrity Check Results window

The Integrity Check Results window allows you to review the results of your audit data integrity check.

If your audit data fails the integrity check, the integrity check returns a list of events that were inserted, modified, or deleted from the selected Repository or archive database. These events are considered compromised. The integrity check also analyzes the additional data associated with Before-After and Sensitive Column auditing of DML and SELECT events, and indicates whether this data is compromised as well.

The integrity check results indicate:

- How many individual event entries are compromised
- How many entries of Before-After change data and column data are compromised
- How many Sensitive Column entries are compromised

You can choose whether to mark each compromised event entry in the audit data. Marking these events changes the event class to reflect the compromise and changes the event category to Integrity Check. Use the marked audit data to help diagnose the issues and begin a forensic analysis.

Type of Compromise	New Event Class	New Event Category
Events were added to the audit data stream after archival using another application	Events inserted	Integrity Check
Events stored in the selected Repository or archive database were modified using another application	Events modified	Integrity Check
Events previously stored in the selected Repository or archive database were deleted using another application	Missing events	Integrity Check

To mark the compromised events as they occur in the audit data, click **Mark Events**.