How Data Alerts work

IDERA SQL Compliance Manager can generate a Data Alert when it finds a suspicious data manipulation in your audit trail. Alert rules define what a suspicious data manipulation is and how SQL Compliance Manager should respond. For example, you can create a rule to alert you when data in sensitive columns has been accessed. You can configure SQL Compliance Manager to write a custom alert message to the application event log and send an alert email notification to your corporate and personal SMTP accounts when the alert is triggered. For more information, see Use Data Alerts to perform forensics.

SQL Compliance Manager only alerts on the data you select for an audited SQL Server instance and database. After the Collection Server processes the raw event data sent by the SQL Compliance Manager Agent, the Collection Server uses the criteria defined by your alert rules to search for suspicious manipulations. When a matching event is found, the alert is triggered.

If you specified a message for this alert, SQL Compliance Manager saves the alert message in the SQLcompliance Repository database. You can view alert messages and the corresponding events using the Data Alerts tab on the Select SQL Server Instance view. Depending on the amount of alert activity your environment generates, you may want to groom alert messages on a routine basis. For more information, see Groom alerts.