Use Event Alerts to analyze audit data

You can use Event Alerts to identify any type of SQL Server event data you are currently auditing. Event Alerts allow you to track suspicious events collected in your audit data stream. You can use these alerts to warn about potentially malicious activity or record routine activity on an audited instance or database.

For example, when a suspicious event is discovered, you can be notified by email so you can immediately diagnose and resolve the issue. You can also configure IDERA SQL Compliance Manager to write a custom message to the application event log so you have an ongoing record.

Event Alert rule examples

Use the following examples to help you identify the alert criteria you need to define in the corresponding Event Alert rule to monitor a specific action.

Data you want to alert on …	Type of Event Alert rule criteria to set …
When a login fails to access a database containing customer information	• Failed Logins • Instance named SalesServer • Database named Customers
When any login performs a password change	• Security Changes • Any SQL Server instance • Successful Event is true • Exclude certain event types
When a non-privileged user attempts to add a login to role	• Security Changes • Any SQL Server instance • Successful Event is false • Privileged User is false • Exclude certain event types
When a login other than HR01 changes the Salary table	• Data Manipulation • Instance named HRServer • Database object named Salary • Login Name is not HR01 • Successful Event is true • Exclude certain event types