The **Alert Correlation Engine** works as follows:

1. **Groups Related Alerts**:
   * Alerts occurring within a specific **time window** (e.g., 5 minutes).
   * Alerts from the **same source** or with similar **event titles**.
   * Alerts of the **same severity level**.
2. **Summarizes Correlations**:
   * Generates a grouped summary showing how many related alerts occurred within each group.
3. **Visualizes Correlations**:
   * Creates a **heatmap** to show patterns across sources, severity levels, and event counts.
4. **Exports Reports**:
   * Provides a downloadable **CSV report** containing all grouped correlated alerts for further analysis.

This helps in understanding **alert patterns**, identifying **root causes**, and prioritizing actions.

Example to illustrate how the **"Groups Related Alerts"** feature works:

**Scenario:**

Your system generates alerts from various servers and applications. Here are some sample alerts:

| **Timestamp** | **EventSource** | **EventLevel** | **EventTitle** |
| --- | --- | --- | --- |
| 2024-12-05 14:00:10 | Server1 | Critical | CPU Usage High |
| 2024-12-05 14:01:15 | Server2 | Critical | Memory Usage High |
| 2024-12-05 14:02:05 | Server1 | Critical | CPU Usage High |
| 2024-12-05 14:03:40 | Server1 | Warning | Disk Space Low |
| 2024-12-05 14:04:50 | Server2 | Critical | Memory Usage High |

**Alert Correlation Output:**

**Group 1: Alerts from Server1 (CPU Usage High)**

* Alerts are grouped because they are:
  1. From the same source (Server1).
  2. Have the same event title (CPU Usage High).
  3. Occur within a short time window (e.g., 5 minutes).

| **Timestamp** | **EventSource** | **EventLevel** | **EventTitle** |
| --- | --- | --- | --- |
| 2024-12-05 14:00:10 | Server1 | Critical | CPU Usage High |
| 2024-12-05 14:02:05 | Server1 | Critical | CPU Usage High |

**Group 2: Alerts from Server2 (Memory Usage High)**

* These are grouped because they:
  1. Share the same event title (Memory Usage High).
  2. Occur within 5 minutes.

| **Timestamp** | **EventSource** | **EventLevel** | **EventTitle** |
| --- | --- | --- | --- |
| 2024-12-05 14:01:15 | Server2 | Critical | Memory Usage High |
| 2024-12-05 14:04:50 | Server2 | Critical | Memory Usage High |

**Group 3: Standalone Alert**

* The disk space alert doesn’t correlate with others.

| **Timestamp** | **EventSource** | **EventLevel** | **EventTitle** |
| --- | --- | --- | --- |
| 2024-12-05 14:03:40 | Server1 | Warning | Disk Space Low |