ID Incident Management Process

This dataset is an event log of an incident management process, extracted from data gathered from the audit system of an instance of the ServiceNow platform used by an IT company over the course of approximately one year. The event log is enriched with data loaded from a relational database. The dataset contains vectors representing 141,712 events, covering 24,918 distinct incidents. Relevant attributes include:

* Caller ID (identifier of user affected)
* Category (descriptive identifier of affected service
* Dates of incident opening, system update, incident resolution, and incident closing
* Users responsible for incident opening, system update, incident resolution, and incident closing
* Level of impact (three-tier scale)
* Level of urgency (three-tier scale)
* Level of priority (four-tier scale based on impact and urgency)
* Close code (identifier of resolution of incident)

Using data visualization, we observed the frequency of different levels of impact and urgency, and which users were most responsible for updating that information. We also analyzed the which callers had the most affected services to evaluate how the priority of an incident relates to its duration. Finally, we observed the most frequent combinations of categories and close codes, and which users were most frequently responsible for resolving those incidents.

Chart, histogram

Description automatically generated

This column chart shows the number of incidents at each level of urgency, broken down by level of impact. The vast majority of incidents were considered medium-urgency, medium-impact.

Chart, treemap chart

Description automatically generatedThis treemap shows the number of incidents that users updated (i.e., generated the current log record) during each month. It is filtered to display only medium-urgency, medium-impact cases.

Chart, bubble chart

Description automatically generatedThis packed bubble chart shows the number of medium-urgency, medium-impact incidents updated by each user during March.

Chart, treemap chart

Description automatically generatedThis treemap shows the ten callers who had the longest total case duration for problems affecting them. The duration was calculated as the number of days between a user initially reporting the incident and a user closing the case. The value is reflected by both the size and color of each region.

Chart, bar chart

Description automatically generatedThis column chart shows the number of incidents called in by the ten callers with the longest total duration, the same ones as the previous chart. Each divided by color based on the number of incidents assigned to each priority level.

Chart

Description automatically generatedThis bar graph shows the number of distinct incidents that were called in by particular callers, filtered to show the ten with the highest amount.

Chart, scatter chart

Description automatically generatedThis scatter plot shows the average number of system updates for each category (first-level description of the affected service), based on levels of urgency, impact, and priority. The priority level is based on a calculation involving the urgency and impact levels.

Chart, treemap chart

Description automatically generatedThis treemap shows the average duration of incidents assigned to each category of severity. The duration is reflected by both the size and color of each region.

Chart, bubble chart

Description automatically generatedThis chart shows the average duration of incidents assigned to each priority level. Larger circles represent longer durations.

Chart

Description automatically generated with medium confidenceThis chart shows the average duration of incidents in each category, filtered by the level of priority. It seems that higher priority generally results in less time needed to solve the incident.

Chart, scatter chart

Description automatically generatedThis graph shows the number of distinct cases reported in certain categories, filtered down to those with 500 or more cases. It is then broken down by close code, which is an identifier of the resolution of the incident.

Chart, line chart

Description automatically generatedThis graph shows the number of distinct incidents resolved by different users. Specifically, these are incidents marked by Category 42 and Close Code 6, the most frequently occurring combination. It is also filtered to users who resolved at least 20 of these incidents.

Chart, treemap chart

Description automatically generatedThis table shows how many Category 42 incidents different users resolved with Close Code 6 during March, April, and May. The table shows users who resolved at least 10 distinct cases, with higher amounts indicated by a darker colored cell.