FFG

Incident timeline

This test will simulate some small part of our SOAR (Security Operation Automation and Response) system. SOAR system provides an ability to manage security incidents, document the process and manage analyst's collaboration.

In scope of this test you are required to implement Incident page that includes incident details and incident timeline.

1. Assume following data is preloaded to the system (Create some seed script to load data)

{"name":"Incident 1", "id":1, "status":"Open", "priority":"Low", "country":"us"},

{"name":"Incident 2", "id":2, "status":"Open", "priority":"Medium" , "country":"cn"},

{"name":"Incident 3", "id":3, "status":"Open", "priority":"High" , "country":"de"},

{"name":"Incident 4", "id":4, "status":"Closed", "priority":"Critical" , "country":"il"},

{"name":"Incident 5", "id":5, "status":"Closed", "priority":"Low" , "country":"us"},

{"name":"Incident 6", "id":6, "status":"Closed", "priority":"Medium" , "country":"cn"},

{"name":"Incident 7", "id":7, "status":"Open", "priority":"High" , "country":"cn"},

2. Implement page that will represent single incident in the system, so we will able to navigate directly to this page.
   http://localhost:8080/incident/[id]
3. The page will show incident name and ID and will allow changing incident status, priority and location (country).
4. System will record every change in the DB, the record will include timestamp, incident ID and operation details.
5. System will provide timeline component. Timeline component will show all recorded events as well will allow adding manual events by user. Events should be sorted chronologically most recent record should appear first.
6. A bonus – Implement adding manual event to the timeline – An event should include:
   a. Caption
   b. Description
   c. Reported time

Use the following images as a mockup for the application.

Priority	Status	Country		Created
CRITICAL ⌄	CLOSED ⌄	🇺🇸 US ⌄		5 minutes ago

Timeline

Incident closed
Incident status from OPEN to CLOSED
a few seconds ago

Location changed
Incident location changed from 🇨🇳 to 🇺🇸
a few seconds ago

Important manual note
Important Important Important
a minute ago

Priority changed
Incident priority changed from MEDIUM to CRITICAL
5 minutes ago

⊕ Add Event

Below design for available Priority levels

LOW   MEDIUM

HIGH   CRITICAL

Below design for available Statuses

OPEN   CLOSED

Use this mockup for a bonus question

CyberProof ™

Add event ✕

Name *

> Important note

Description

> Optional description

Reported time *

> 09.09.2020 10:12

Cancel **Upload**

Extra Points:

1. Create unit tests.
2. Use a linting utility.
3. Document your code.
4. Use source control.