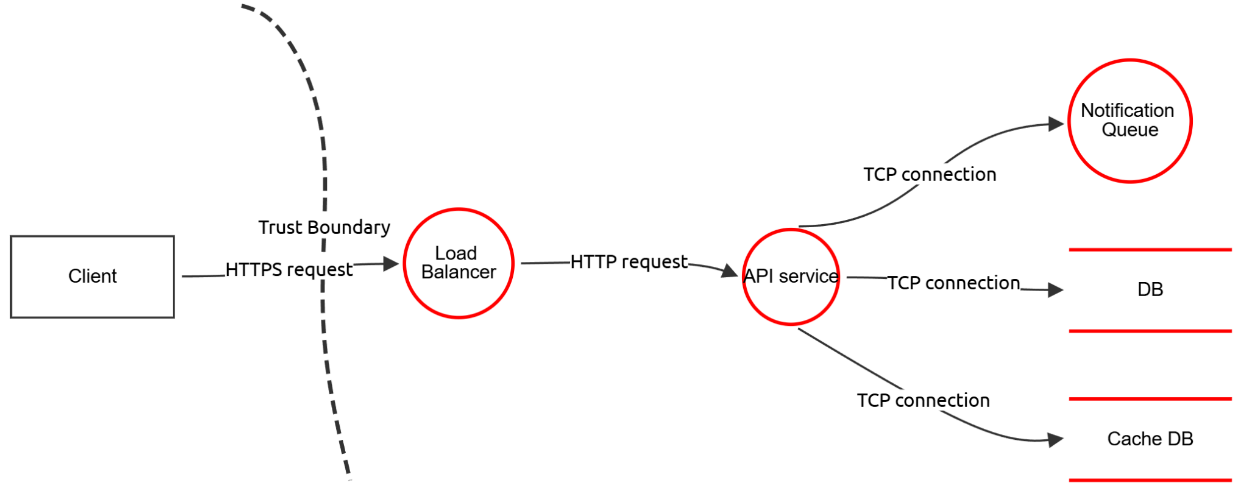
For the Threat Model we have used OWASP Threat Dragon.

Threat Model diagram with 5 interactions:

ID	Component / Dependency Interaction
1	Client -> API
2	Load Balancer -> API
3	API -> Notification Queue
4	API -> DB (PostgreSQL)
5	API -> Cache DB (Redis)



Flow ID	Flow name	Description	Interactions:
1	User Authentication & Authorization Flow	Authenticate users and allow access to protected API endpoints.	1. Client → Load Balancer 2. Load Balancer → API Service 3. API Service → Database

2	Ticket Purchase Flow	Allow authenticated users to purchase tickets and update system state.	1. Client → Load Balancer 2. Load Balancer → API Service 3. API Service → Cache Database 4. API Service → Database (cache miss fallback) 5. API Service → Notification Queue
3	Notification Delivery Flow	Deliver asynchronous notifications triggered by system events.	1. API Service → Notification Queue
4	View Event Details Flow	Allow users to retrieve event information and availability.	1. Client → Load Balancer 2. Load Balancer → API Service 3. API Service → Cache Database 4. API Service → Database (cache miss fallback)

We have got 16 threads from Threat Model diagram:

Id	Interaction ID	Flows affected	Type	Description	Mitigations	Score	Severity
1	1	Flow 1, Flow 2, Flow 4	Tampering	Using speed to violate explicit or implicit assumptions about the application’s normal use to achieve unfair individual gain	Defences include providing enforcement of behavioral workflow and anti-automation	7	High
2	1	Flow 1, Flow 2, Flow 4	Information Dis…	Using speed to violate explicit or implicit assumptions about the application’s normal use to achieve unfair individual gain	Defence includes providing anti-automation	3	Low
3	1	Flow 1, Flow 2, Flow 4	Elevation of Pri…	Usage may resemble legitimate application usage but leads to exhaustion of resources	Mitigation or prevention such as providing backoff, resource management and avoiding forced deadlock	8	High

4	2	Flow 1, Flow 2, Flow 4	Tampering	Using speed to violate explicit or implicit assumptions about the application’s normal use to achieve unfair individual gain	Defences include providing enforcement of behavioral workflow and anti-automation	9	Criti…
5	2	Flow 1, Flow 2, Flow 4	Information Dis…	Systematic enumeration and examination in order to find weaknesses and points where a security vulnerability might exist	Defence includes providing anti-automation	5	Med…
6	2	Flow 1, Flow 2, Flow 4	Elevation of Pri…	Usage may resemble legitimate application usage but leads to exhaustion of resources	Mitigation or prevention such as providing backoff, resource management and avoiding forced deadlock	6	Med…
7	2	Flow 1, Flow 2, Flow 4	Information Dis…	Information gathering with the objective of learning as much as possible about the composition, configuration and security mechanisms of the application	Defences include shutting down unnecessary services/ports and excluding information that could identify and compromise security of the organisation	2	Low
8	3	Flow 2, Flow 4	Tampering	Using speed to violate explicit or implicit assumptions about the application’s normal use to achieve unfair individual gain	Defences include providing enforcement of behavioral workflow and anti-automation	4	Med…
9	3	Flow 2, Flow 4	Information Dis…	Systematic enumeration and examination in order to find weaknesses and points where a security vulnerability might exist	Defence includes providing anti-automation	3	Low
10	3	Flow 2, Flow 4	Elevation of Pri…	Usage may resemble legitimate application usage but leads to exhaustion of resources	Mitigation or prevention such as providing backoff, resource management and avoiding forced deadlock	5	Med…
11	4	Flow 1, Flow 2, Flow 4	Information Dis…	Collecting accessible data and/or processed output from the application	Detect fake or compromised accounts, ensure information is accessible only with authentication and authorisation	10	Criti…
12	4	Flow 1, Flow 2, Flow 4	Elevation of Pri…	Automated repeated clicking or requesting or submitting content,	Defences include control of interaction frequency or proper	7	High

				affecting application based metrics such as counts, and measures of frequency and/or rate	enforcement of a single unique action		
13	4	Flow 1, Flow 2, Flow 4	Elevation of Pri… ▾	Storing malicious such as malware, Iframe distribution, photographs & videos, advertisements, referrer spam and tracking/surveillance code	Defences include detecting embedded malicious code, controling interaction frequency and enforcement of a single unique action	8	High ▾
14	5	Flow 2, Flow 3	Information Dis… ▾	Collecting accessible data and/or processed output from the application	Detect fake or compromised accounts, ensure information is accessible only with authentication and authorisation	8	High ▾
15	5	Flow 2, Flow 3	Elevation of Pri… ▾	Automated repeated clicking or requesting or submitting content, affecting application based metrics such as counts, and measures of frequency and/or rate	Defences include control of interaction frequency or proper enforcement of a single unique action	4	Med… ▾
16	5	Flow 2, Flow 3	Elevation of Pri… ▾	Storing malicious such as malware, Iframe distribution, photographs & videos, advertisements, referrer spam and tracking/surveillance code	Defences include detecting embedded malicious code, controlling interaction frequency and enforcement of a single unique action	6	Med… ▾