SQL Assignment:

You are a Senior Specialist at MMC Cyber Risk Intelligence Center. The team is building threat intelligence cyber quantification model. Your task is to analyze system data to understand recent trends.

**Available Tables:**

1. users.tsv

* user\_id (INT): Unique ID of the user.
* username (VARCHAR): Username of the employee.
* department (VARCHAR): Department the user belongs to.
* join\_date (DATE): When the user joined the company.

1. devices.tsv

* device\_id (INT): Unique ID of the device.
* user\_id (INT): Owner of the device.
* device\_type (VARCHAR): Type of device (e.g., Laptop, Desktop).
* os (VARCHAR): Operating system installed on the device.

1. access\_logs.csv

* log\_id (INT): Log entry ID.
* device\_id (INT): Device from which access occurred.
* access\_time (TIMESTAMP): Timestamp of the access event.
* access\_type (VARCHAR): Either login or logout.

1. threat\_alerts.csv

* alert\_id (INT): Unique ID of the alert.
* device\_id (INT): Affected device.
* detected\_time (TIMESTAMP): When the threat was detected.
* threat\_level (VARCHAR): Severity of the threat (low, medium, high).
* threat\_type (VARCHAR): Type of threat (e.g., malware, phishing, unauthorized\_access).

Please generate SQL queries to address the following questions:

* List all users and the number of devices assigned to each.
* Show the number of access logs recorded for each device.
* Identify departments that have users with the most high severity threats.
* Show users whose devices have had more than one high severity threat.
* Identify all users who experienced a high severity threat on one of their devices within 10 minutes after a login event. Include: username, department, device\_type, access\_time(login), detected\_time(threat), threat\_type.

**Please zip your SQL queries and the relevant output before sharing them with us.**