

SQL Filtering & Asset Investigation

Assignment Overview

In this lab, I assumed the role of a security analyst responsible for locating targeted employee, device, and department information to support operational and security actions. The goal was to efficiently retrieve specific records from an organizational database by applying filters to SQL queries.

This assignment focused on using the `WHERE` clause and the `LIKE` operator to narrow large datasets into actionable insights, skills that are essential for real-world security operations, asset management, and incident response.

Scenario Context

The organization maintains multiple interconnected tables containing employee, device, and departmental data. The security team relies on this information to:

- Identify machines that require updates
- Notify employees affected by device issues
- Distribute compliance and privacy notices to specific departments

The analysis was performed using the following tables in the `organization` database:

- **machines** – device inventory and operating systems
 - **employees** – employee identity, department, and office location
-

Task 1: Listing Organization Machines

Objective

Retrieve a clear inventory of all organization machines and their operating systems.

Approach

Using a targeted **SELECT** statement, I returned only the device identifiers and operating systems from the machines table. This allowed for a concise system inventory without unnecessary data.

Outcome

- Confirmed the total number of devices in the organization
- Established a baseline inventory for follow-on filtering and analysis

This mirrors common asset management tasks performed by security and IT teams.

Task 2: Identifying Machines Running OS 2

Objective

Locate all machines running a specific operating system that requires an update.

Approach

I applied a **WHERE** filter to return only machines with the operating system value of **OS 2**. This narrowed the dataset to only the systems requiring attention.

Outcome

- Identified the exact number of machines running OS 2
- Produced a focused list suitable for patching or remediation workflows

This task reflects how analysts scope vulnerability exposure during update cycles.

Task 3: Filtering Employees by Department

Objective

Identify employees working in departments handling sensitive information.

Approach

Using the **WHERE** clause, I filtered employee records by department, first isolating Finance employees and then modifying the query to retrieve Sales employees.

Outcome

- Retrieved employee records for Finance and Sales departments
- Determined employee counts and identifiers for departmental notifications

Department-based filtering is a common requirement for compliance, audits, and targeted security communications.

Task 4: Identifying Employees by Office Location

Objective

Determine which employees are affected by machine issues in a specific building.

Approach

- Queried the employees table to identify the user assigned to a specific office
- Expanded the query using the `LIKE` operator and wildcard (%) to retrieve all employees located in the South building

Outcome

- Identified the employee using the affected machine in South-109
- Retrieved a list of all employees located in the South building
- Determined departmental ownership for impacted staff

This mirrors real-world incident response scenarios where physical location data is critical for targeted alerts.

Key Skills Demonstrated

- Filtering SQL queries using the `WHERE` clause
 - Pattern matching with the `LIKE` operator and wildcards
 - Translating business and security needs into precise queries
 - Investigating asset and employee data efficiently
-

Conclusion

This lab strengthened my ability to retrieve precise, actionable data from relational databases using SQL filters. By narrowing results based on operating systems, departments, and physical locations, I demonstrated how SQL supports security operations, asset tracking, and incident response.