Appliquer des filtres aux requêtes SQL

Google Cybersecurity Certificate

Description du projet

L'entreprise pour laquelle je travaille s'efforce de renforcer la sécurité de son système. En tant que professionnelle de la sécurité, mon rôle est d'enquêter sur les problèmes de sécurité potentiels et de proposer des solutions pour protéger les données et les systèmes. Récemment, des incidents potentiels liés aux tentatives de connexion et aux ordinateurs des employés ont été détectés.

Pour mener à bien cette mission, j'ai utilisé SQL avec des filtres pour interroger les bases de données et identifier les données pertinentes.

Récupérer les tentatives de connexion échouées après les heures d'ouvertures

Un incident de sécurité potentiel s'est produit en dehors des heures de travail (après 18h00). Toutes les tentatives de connexion qui échouent en dehors des heures de travail doivent faire l'objet d'une enquête.

Pour identifier ces tentatives de connexion, j'ai utilisé la requête SQL suivante :

```
SELECT *
FROM log_in_attempts
WHERE login_time > '18:00:00' AND success = FALSE;
```

Cette requête permet de filtrer les tentatives de connexions qui ont échoué après 18h00. Elle sélectionne tous les enregistrements de la table `log_in_attempts` où l'heure de connexion (`login_time`) est supérieure à 18:00:00 et où la tentative de connexion a échoué (`success = FALSE`). Les résultats de la requête se trouvent dans la capture d'écran ci-dessous.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time > '18:00' AND success = FALSE;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.57   |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.17  |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.49  |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.153 |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.194  |       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.200  |       0 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.187 |       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27   |       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122  |       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.171 |       0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.176 |       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49  |       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.232  |       0 |
+----------+----------+------------+------------+---------+-----------------+---------+
19 rows in set (0.002 sec)
```

Récupérer les tentatives de connexion à des dates spécifiques

Un événement suspect s'est produit le 09/05/2022. Il est important d'analyser toute activité de connexion survenue le 09/05/2022 ou la veille.

Pour identifier ces tentatives de connexion, j'ai utilisé la requête SQL suivante :

```
SELECT *
FROM log_in_attempts
WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

Cette requête permet de filtrer les tentatives de connexion qui ont eu lieu le 09/05/2022 ou le 08/05/2022. Elle sélectionne tous les enregistrements de la table `logs_in_attempts` où la date de connexion (`login_date`) est égale à `"2022-05-09"` ou `"2022-05-08"`. Les résultats de la requête se trouvent dans la capture d'écran ci-dessous.

```
MariaDB [organization]> SELECT *
    -> 
    -> FROM log_in_attempts
    -> 
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+----------------+---------+
| event_id | username | login_date | login_time | country | ip_address     | success |
+----------+----------+------------+------------+---------+----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105 |       1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |       1 |
```

Récupérer les tentatives de connexion en dehors du Mexique

Après avoir examiné les données relatives aux tentatives de connexion, l'équipe a déterminé que le problème se situe au niveau des tentatives de connexion qui ont lieu en dehors du Mexique. Ces connexion doivent faire l'objet d'une enquête.

Pour identifier ces tentatives de connexion, j'ai utilisé la requête suivante :

```
SELECT *
FROM log_in_attempts
WHERE country NOT LIKE 'MEX%';
```

Cette requête permet de filtrer les tentatives de connexion qui ont eu lieu dans des pays autres que le Mexique. Elle sélectionne tous les enregistrements de la table `logs_in_attempts` où le pays (`country`) n'est pas `MEX` ou `MEXICO` (utilisant `LIKE` avec un caractère générique `%`). Les résultats de la requête se trouvent dans la capture d'écran ci-dessous.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.221 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81  |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |       1 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.135 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89   |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       19 | jhill    | 2022-05-12 | 13:09:04   | US      | 192.168.142.245 |       1 |
```

Récupérer les employés du service marketing

L'équipe souhaite effectuer des mises à jour sur les ordinateurs de certains employés du service marketing. Je dois obtenir des informations me permettant de déterminer quels ordinateurs mettre à jour.

Pour identifier ces employés, j'ai utilisé la requête SQL suivante :

```
SELECT *
FROM employees
WHERE department = 'Marketing' AND office LIKE 'East%';
```

Cette requête permet de filtrer les employés qui travaillent au sein du service marketing et dans le bâtiment Est. Elle sélectionne tous les employés de la table `employees` qui travaillent dans le département `Marketing` et dont le bureau se trouve dans le bâtiment Est (`office LIKE 'East%'`). Les résultats de la requête se trouvent dans la capture d'écran ci-dessous.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE department = 'Marketing' AND office LIKE 'East%';
+-------------+-------------+----------+------------+----------+
| employee_id | device_id   | username | department | office   |
+-------------+-------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157 |
|        1103 | NULL         | randerss | Marketing  | East-460 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+-------------+----------+------------+----------+
7 rows in set (0.001 sec)
```

Récupérer les employés du service financier (Finance) ou commercial (Sales)

Les ordinateurs des employés des services financier et commercial doivent également être mis à jour. Étant donné qu'une mise à jour de sécurité distincte est nécessaire, je dois obtenir des informations me permettant de déterminer uniquement les employés travaillant au sein de ces deux services.

Pour identifier ces employés, j'ai utilisé la requête SQL suivante :

```
SELECT *
FROM employees
WHERE department = 'Finance' OR department = 'Sales';
```

Cette requête permet de filtrer les employés qui travaillent dans le département `Finance` ou dans le département `Sales`. Elle sélectionne tous les employés de la table `employees` qui travaillent dans le département `Finance` ou `Sales`. Les résultats de la requête se trouvent dans la capture d'écran ci-dessous.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE department = 'Finance' OR department = 'Sales';
+-------------+-------------+----------+------------+-------------+
| employee_id | device_id   | username | department | office      |
+-------------+-------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1011 | l748m120n401 | drosas   | Sales      | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales      | South-215   |
|        1025 | z381a365b233 | jhill    | Sales      | North-115   |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156    |
```

Récupérer tous les employés, en dehors de ceux qui travaillent au service informatique (IT)

L'équipe doit effectuer une mise à jour de sécurité supplémentaire sur les ordinateurs des employés qui ne font pas partie du service informatique. Pour cela, je dois d'abord obtenir des informations me permettant de déterminer quels employés sont concernés.

Pour identifier ces employés, j'ai utilisé la requête SQL suivante :

```
SELECT *
FROM employees
WHERE NOT department = 'Information Technology';
```

Cette requête permet de filtrer les employés qui ne font pas partie du service informatique. Elle sélectionne tous les employés de la table `employees` qui ne font pas partie du département Information Technology (`NOT department = 'Information Technology'`). Les résultats de la requête se trouvent dans la capture d'écran ci-dessous.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE NOT department = 'Information Technology';
+-------------+--------------+----------+-----------------+-------------+
| employee_id | device_id    | username | department      | office      |
+-------------+--------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
|        1003 | d394e816f943 | sgilmore | Finance         | South-153   |
|        1004 | e218f877g788 | eraab    | Human Resources | South-127   |
|        1005 | f551g340h864 | gesparza | Human Resources | South-366   |
|        1007 | h174i497j413 | wjaffrey | Finance         | North-406   |
|        1008 | i858j583k571 | abernard | Finance         | South-170   |
|        1009 | NULL         | lrodriqu | Sales           | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance         | South-109   |
|        1011 | l748m120n401 | drosas   | Sales           | South-292   |
```

Synthèse

J’ai appliqué des filtres aux requêtes SQL pour obtenir des informations spécifiques sur les tentatives de connexion et les ordinateurs des employés. J’ai utilisé deux tables différentes : logs_in_attempts et employees. J’ai utilisé les opérateurs AND, OR et NOT pour filtrer les informations spécifiques nécessaires à chaque tâche. J’ai aussi utilisé LIKE et le symbole de pourcentage (%) pour filtrer les modèles.