

Apply filters to SQL queries

Project description

Este proyecto tuvo como objetivo aplicar filtros SQL para investigar posibles incidentes de seguridad dentro de una organización. Utilizando las tablas log_in_attempts y employees, se realizaron consultas para analizar intentos fallidos de inicio de sesión, identificar accesos fuera de horario laboral, filtrar registros según fechas específicas y excluir países determinados. También se recuperó información de empleados de departamentos y oficinas concretas.

Retrieve after hours failed login attempts

Consulta usada:

```
SELECT *  
FROM log_in_attempts  
WHERE success = 0 AND login_time > '18:00:00';
```

```
MariaDB [organization]> SELECT *  
-> FROM log_in_attempts  
-> WHERE success = 0  
-> AND login_time > '18:00:00';
```

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	astrada	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	astrada	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 (0.017 sec)  
MariaDB [organization]>
```

Explicación: Esta consulta devuelve todos los intentos de inicio de sesión cuyo campo 'success' es 0 (Falso) y cuya hora (login_time) ocurrió después de las 18:00. Así se identificaron intentos sospechosos fuera del horario laboral.

Retrieve login attempts on specific dates

Consulta SQL usada:

```
SELECT *
```

```
FROM log_in_attempts
```

```
WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

```
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
32	acook	2022-05-09	02:52:02	CANADA	192.168.142.239	0
36	asundara	2022-05-08	09:00:42	US	192.168.78.151	1
38	sbaelish	2022-05-09	14:40:01	USA	192.168.60.42	1
39	yappiah	2022-05-09	07:56:40	MEXICO	192.168.57.115	1
42	cgriffin	2022-05-09	23:04:05	US	192.168.4.157	0
43	mcouliba	2022-05-08	02:35:34	CANADA	192.168.16.208	0
44	daquino	2022-05-08	07:02:35	CANADA	192.168.168.144	0
47	dkot	2022-05-08	05:06:45	US	192.168.233.24	1
49	asundara	2022-05-08	14:00:01	US	192.168.173.213	0
53	nmason	2022-05-08	11:51:38	CAN	192.168.133.188	1
56	acook	2022-05-08	04:56:30	CAN	192.168.209.130	1
58	ivelasco	2022-05-09	17:20:54	CAN	192.168.57.162	0
61	dtanaka	2022-05-09	09:45:18	USA	192.168.98.221	1
65	aalonso	2022-05-09	23:42:12	MEX	192.168.52.37	1
66	aestrada	2022-05-08	21:58:32	MEX	192.168.67.223	1
67	abernard	2022-05-09	11:53:41	MEX	192.168.118.29	1
68	mrah	2022-05-08	17:16:13	US	192.168.42.248	1
70	tmitchel	2022-05-09	10:55:17	MEXICO	192.168.87.199	1
71	mcouliba	2022-05-09	06:57:42	CAN	192.168.55.169	0
72	alevitsk	2022-05-08	12:09:10	CANADA	192.168.139.176	1
79	abernard	2022-05-09	11:41:15	MEX	192.168.158.170	0
80	cjackson	2022-05-08	02:18:10	CANADA	192.168.33.140	1
83	lrodriqu	2022-05-08	08:10:23	USA	192.168.67.69	1

Explicacion: Esta consulta recupera todos los registros de la tabla **log_in_attempts** cuyo valor en la columna **login_date** coincide con el 2022-05-09 o con el 2022-05-08. EL operador **OR** permite incluir mas de una condición de fecha, devolviendo los intentos de inicio de sesión que ocurrieron en cualquiera de los dos días.

Retrieve login attempts outside of Mexico

Consulta SQL usada:

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

```
MariaDB [organization]> SELECT *  
-> FROM log_in_attempts  
-> WHERE country NOT 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
21	iuduike	2022-05-11	17:50:00	US	192.168.131.147	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
29	bisles	2022-05-11	01:21:22	US	192.168.85.186	0
31	acook	2022-05-12	17:36:45	CANADA	192.168.58.232	0
32	acook	2022-05-09	02:52:02	CANADA	192.168.142.239	0
33	zbernal	2022-05-11	02:52:10	US	192.168.72.59	1
34	drosas	2022-05-11	21:02:04	US	192.168.45.93	0
36	asundara	2022-05-08	09:00:42	US	192.168.78.151	1
37	eraab	2022-05-10	06:03:41	CANADA	192.168.152.148	0
38	sbaelish	2022-05-09	14:40:01	USA	192.168.60.42	1
41	apatel	2022-05-10	17:39:42	CANADA	192.168.46.207	0
42	cgriffin	2022-05-09	23:04:05	US	192.168.4.157	0
43	mcouliba	2022-05-08	02:35:34	CANADA	192.168.16.208	0
44	daquino	2022-05-08	07:02:35	CANADA	192.168.168.144	0
45	dtanaka	2022-05-11	10:28:54	US	192.168.223.157	1
46	eraab	2022-05-11	11:29:27	CAN	192.168.24.12	0
47	dkot	2022-05-08	05:06:45	US	192.168.233.24	1
48	asundara	2022-05-11	03:18:45	USA	192.168.72.10	1
49	asundara	2022-05-08	14:00:01	US	192.168.173.213	0
50	jclark	2022-05-10	10:48:02	CANADA	192.168.174.117	0
51	jrafael	2022-05-10	22:40:01	CANADA	192.168.148.115	1
52	cjackson	2022-05-10	22:07:07	CAN	192.168.58.57	0

Explicación: Esta consulta devuelve todos los intents de inicio de sesión de la tabla **log_in_attempts** donde el valor de la columna **country** no empieza con "MEX". El comodín % permite abarcar tanto **MEX** como **MEXICO**, y el operador **NOT LIKE** asegura que esos registros queden excluidos de los resultados

Retrieve employees in Marketing

Consulta SQL usada:

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

```
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 | k865l965m233 | 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)
```

Explicacion: Esta consulta selecciona todos los registros de la tabla **employees** cuyo departamento es "Marketing" y cuya oficina comienza con "East". El operador **AND** garantiza que ambas condiciones se cumplan, de modo que solo se muestran empleados de Marketing que trabajan en las oficinas del edificio Este.

Retrieve employees in Finance or Sales

Consulta SQL usada:

```
SELECT *
```

```
FROM employees
```

```
WHERE department = 'Finance' OR department = 'Sales';
```

```
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	k242l212m542	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
1035	j236k303l245	bisles	Sales	South-171
1039	n253o917p623	cjackson	Sales	East-378
1041	p929q222r778	cgriffin	Sales	North-208
1044	s429t157u159	tbarnes	Finance	West-415
1045	t567u844v434	pwashing	Finance	East-115
1046	u429v921w138	daquino	Finance	West-280
1047	v109w587x644	cward	Finance	West-373
1048	w167x592y375	tmitchel	Finance	South-288

Explicación: Esta consulta selecciona todos los registros de la tabla **employees** cuyo valor en la columna **department** sea "Finance" o "Sales". El operador **OR** permite combinar dos condiciones distintas y recuperar los empleados de cualquiera de los dos departamentos.

Retrieve all employees not in IT

Consulta SQL usada:

```
SELECT *
```

```
FROM employees
```

```
WHERE NOT department = 'Tecnología de la información';
```

```
MariaDB [organization]> SELECT *
-> FROM employees
-> WHERE NOT department = 'Tecnologa de la informacin';
```

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
1006	g329h357i597	alevitsk	Information Technology	East-320
1007	h174i497j413	wjaffrey	Finance	North-406
1008	i858j583k571	abernard	Finance	South-170
1009	NULL	lrodriqu	Sales	South-134
1010	k242l121m542	jlansky	Finance	South-109
1011	l748m120n401	drosas	Sales	South-292
1012	m756n668o146	nmason	Information Technology	North-160
1013	n205o559p243	zbernal	Information Technology	South-229
1014	NULL	asundara	Information Technology	West-219
1015	p611q262r945	jsoto	Finance	North-271
1016	q793r736s288	sbaelish	Human Resources	North-229
1017	r550s824t230	jclark	Finance	North-188
1018	s310t540u653	abellmas	Finance	North-403
1019	t815u205v470	mcouliba	Information Technology	North-108
1020	u899v381w363	arutley	Marketing	South-351
1021	v200w121x977	smartell	Information Technology	South-138
1022	w237x430y567	arusso	Finance	West-465
1023	x253y759z103	aalonso	Information Technology	West-393
1024	y976z753a267	iuduike	Sales	South-215
1025	z381a365b233	jhill	Sales	North-115
1026	a998b568c863	apatel	Human Resources	West-320

Explicación:

Esta consulta devuelve todos los registros de la tabla **employees** en los que el valor de la columna **department** no coincide con “Tecnología de la información”. El operador **NOT** invierte la condición, lo que permite excluir a los empleados de IT y mostrar al resto de la organización.

Summary

Durante la actividad ejecuté varias consultas SQL que me permitieron filtrar datos de seguridad relevantes. Identifiqué intentos de inicio de sesión fallidos fuera del horario laboral y en fechas específicas, así como accesos desde fuera de México. Además, filtré información de empleados de Marketing en oficinas del edificio Este, de empleados de Finanzas o Ventas, y de todos aquellos que no pertenecen al departamento de TI. Estas consultas demostraron la utilidad de los filtros SQL para analizar datos, detectar patrones de riesgo y fortalecer la postura de ciberseguridad de la organización.