



Relatório de Inteligência de Dados: Auditoria de Ativos e Resposta a Incidentes com SQL

Analista: Roan Silva dos Anjos

Especialidade: Segurança de Dados & Análise de Vulnerabilidades



Objetivo Estratégico

Este projeto demonstra a aplicação de **SQL Avançado** como ferramenta de defesa cibernética. O foco foi a extração de inteligência a partir de bancos de dados relacionais para **identificar superfícies de ataque**, investigar tentativas de acesso não autorizadas e garantir o **compliance de segurança** da infraestrutura. Ao cruzar dados de RH e TI, transformei dados brutos em ações preventivas para mitigação de riscos.



1. Identificação de Máquinas Vulneráveis (INNER JOIN)

Cenário: Precisamos localizar funcionários de departamentos críticos (Vendas e Financeiro) que estão utilizando sistemas operacionais obsoletos (OS 1 e OS 2) para priorizar a atualização de segurança.

Query Utilizada:

```
SELECT e.username, e.department, e.employee_id, m.device_id,
m.operating_system
FROM employees AS e
INNER JOIN machines AS m ON e.device_id = m.device_id
WHERE (e.department = 'Sales' OR e.department = 'Finance')
AND m.operating_system NOT LIKE 'OS 3%';
```

```
MariaDB [organization]> SELECT e.username, e.department, e.employee_id, m.device_id, m.operating_system
->
-> FROM employees AS e
->
-> INNER JOIN machines AS m ON e.device_id = m.device_id
->
-> WHERE (e.department = 'Sales' OR e.department = 'Finance')
->
-> AND m.operating_system NOT LIKE 'OS 3%';
+-----+-----+-----+-----+-----+
| username | department | employee_id | device_id | operating_system |
+-----+-----+-----+-----+-----+
| wjaffrey | Finance | 1007 | h174i497j413 | OS 2 |
| abernard | Finance | 1008 | i858j583k571 | OS 2 |
+-----+-----+-----+-----+-----+
```

2. Auditoria de Tentativas de Login Suspeitas

Investigação focada em padrões de acesso que fogem à política de segurança da empresa.

A) Acessos Maliciosos Fora do Horário

Filtro aplicado para detectar tentativas de login que falharam após as 18:00, o que pode indicar tentativas de força bruta.

Query Utilizada:

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

```
MariaDB [organization]> SHOW TABLES;
+-----+
| Tables_in_organization |
+-----+
| employees              |
| log_in_attempts        |
| machines               |
+-----+
3 rows in set (0.001 sec)

MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE login_time > '18:00:00' AND success = 'FALSE'
-> ORDER BY login_time;
+-----+-----+-----+-----+-----+-----+-----+
| event_id | username | login_date | login_time | country | ip_address | success |
+-----+-----+-----+-----+-----+-----+-----+
| 104      | asundara | 2022-05-11 | 18:38:07  | US      | 192.168.96.200 | 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 |
| 18       | pwashing | 2022-05-11 | 19:28:50  | US      | 192.168.66.142 | 0 |
| 199      | yappiah | 2022-05-11 | 19:34:48  | MEXICO  | 192.168.44.232 | 0 |
```

B) Janela de Investigação de Incidente

Análise de todas as atividades ocorridas no período crítico de 08/05/2022 a 09/05/2022.

Query Utilizada:

```
SELECT *
FROM log_in_attempts
WHERE login_date BETWEEN '2022-05-08' AND '2022-05-09';
```

```
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE login_date BETWEEN '2022-05-08' AND '2022-05-09'
-> ORDER BY login_date, login_time;
+-----+-----+-----+-----+-----+-----+-----+
| event_id | username | login_date | login_time | country | ip_address | success |
+-----+-----+-----+-----+-----+-----+-----+
| 117      | bsand    | 2022-05-08 | 00:19:11  | USA     | 192.168.197.187 | 0 |
| 92       | pwashing | 2022-05-08 | 00:36:12  | US      | 192.168.247.219 | 0 |
| 8        | bisles   | 2022-05-08 | 01:30:17  | US      | 192.168.119.173 | 0 |
| 4        | dkot     | 2022-05-08 | 02:00:39  | USA     | 192.168.178.71  | 0 |
```

C) Filtragem por Origem Geográfica

Exclusão de tráfego vindo de regiões validadas (México) para focar a análise em IPs externos e desconhecidos.

Query Utilizada:

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

```
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

3. Gestão de Inventário por Localização Física

Cenário: Localização de dispositivos no departamento de Marketing situados especificamente no prédio Leste (East) para auditoria física.

Query Utilizada:

```
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

Hard Skills Demonstradas

- **Relacionamento de Dados:** Uso de **INNER JOIN** para vincular ativos a usuários.
- **Lógica Booleana:** Agrupamento de condições com **OR** e **AND** para filtros de precisão.
- **Análise de Padrões:** Uso de wildcards (%) para exclusão e inclusão de strings.
- **Compliance de TI:** Identificação proativa de máquinas fora do patch de segurança.