Suspicious Login Attempts - Cybersecurity Analysis Demo

Wil Njeru

2025-07-10

Contents

0.1 Query 1 - Join login attempts with employee office information

- Compute location mismatches by comparing login country to office location

```sql
SELECT
    l.login_date,
    l.event_id,
    l.ip_address,
    l.username,
    l.country AS login_country,
    e.office,
    CASE
        WHEN e.office = 'New York' AND l.country != 'USA' THEN TRUE
        WHEN e.office = 'Toronto' AND l.country != 'Canada' THEN TRUE
        WHEN e.office = 'London' AND l.country != 'UK' THEN TRUE
        WHEN e.office = 'Berlin' AND l.country != 'Germany' THEN TRUE
        WHEN e.office = 'Singapore' AND l.country != 'Singapore' THEN TRUE
        WHEN e.office = 'Nairobi' AND l.country != 'Kenya' THEN TRUE
        ELSE FALSE
    END AS location_mismatch,
    l.success
FROM Employer_dataset.login_attempt l
JOIN Employer_dataset.employees e
ON l.username = e.username;
```

Figure 1: jointables

0.2 Query 2 - Suspicious login Mismatch

- Filter for failed login attempts with mismatched country/office locations

```
SELECT
login_date,
event_id,
ip_address,
login_country,
office,
location_mismatch,
success,
FROM Employer_dataset.joined_table
WHERE success = FALSE AND location_mismatch = TRUE;
```

Row	login_date	event_id	ip_address	login_country	office	location_mismatch	success
3	2025-06-30	15	183.48.75.77	USA	Berlin	true	false
4	2025-06-26	4	22.75.62.182	Canada	London	true	false
5	2025-06-29	8	70.190.109.190	Singapore	London	true	false
6	2025-06-24	11	7.153.248.116	UK	New York	true	false
7	2025-06-13	12	142.157.148.162	UK	New York	true	false
8	2025-06-12	13	86.126.253.140	Kenya	New York	true	false

Figure 2: failedlogin

0.3 Query 3 - Suspicious login counts by country

- Count the number of failed login with mismatches per country

```
SELECT
    login_country,
    COUNT(*) AS suspicious_count
FROM  Employer_dataset.joined_table
WHERE success = FALSE AND location_mismatch = TRUE
GROUP BY login_country;
```

Row	login_country	suspicious_count
1	Canada	3
2	USA	1
3	Singapore	1
4	UK	2
5	Kenya	1

Figure 3: login count

0.4 Visualization with Tableau

- Below is a Tableau-generated map showing where login attempts originate from, overlaid with expected office locations

Suspicious Login Attempts

Data

Login Country	Berlin	London	New York
Canada	Berlin	London	
Kenya			New York
Singapore	Berlin	London	
UK			New York
USA	Berlin		

.

0.5   Conclusion

Project Links

GitHub Repository: https://github.com/Wil421-hu/suspicious-login-analysis

Tableau Dashboard: https://public.tableau.com/app/profile/wil.jero/viz/SuspiciousLoginAttempts/
Dashboard1

This demo successfully highlights

- How login attempts from non-office locations can signal unauthorized access attempts.
- The power of simple SQL logic to reveal potentially malicious activity.
- Visualization strategies to support investigation and reporting.

Note: Data used is simulated. No real user data is included.