B PROJECT 1: SQL THREAT HUNTING & LOG ANALYSIS

Screenshot:

```
6e74 656e 742d 5479 7065 3a20 7465 7874
                                                                     ntent-Type:.text
         0x00f0:
         0x0100:
                    2f68 746d 6c3b 2063 6861 7273 6574 3d55
                                                                     /html;.charset=U
                    5446 2d38 0d0a 4c6f 6361 7469 6f6e 3a20
         0x0110:
                                                                     TF-8..Location:.
         0x0120:
                    6874 7470 733a 2f2f 6f70 656e 736f 7572
                                                                     https://opensour
                    6365 2e67 6f6f 676c 652f 0d0a 4461 7465 3a20 5765 642c 2031 3120 4a75 6e20 3230
         0x0130:
                                                                     ce.google/..Date
                                                                     :.Wed,.11.Jun.20
         0x0140:
                    3235 2030 303a 3531 3a30 3820 474d 540d
         0x0150:
                                                                     25.00:51:08.GMT.
                    0a53 6572 7665 723a 2073 6666 650d 0a43
         0x0160:
                                                                     .Server:.sffe..C
                    6f6e 7465 6e74 2d4c 656e 6774 683a 2032
         0x0170:
                                                                     ontent-Length:.2
         0x0180:
                   3233 0d0a 582d 5853 532d 5072 6f74 6563
                                                                     23..X-XSS-Protec
                    7469 6f6e 3a20 300d 0a0d 0a3c 4854 4d4c
         0x0190:
                                                                     tion:.0....<HTML
         0x01a0:
                    3e3c 4845 4144 3e3c 6d65 7461 2068 7474
                                                                     ><HEAD><meta.htt
         0x01b0:
                   702d 6571 7569 763d 2263 6f6e 7465 6e74
                                                                     p-equiv="content
         0x01c0: 2d74 7970 6522 2063 6f6e 7465 6e74 3d22
                                                                     -type".content="
                   7465 7874 2f68 746d 6c3b 6368 6172 7365
                                                                     text/html; charse
         0x01d0:
                   743d 7574 662d 3822 3e0a 3c54 4954 4c45
         0x01e0:
                                                                     t=utf-8">.<TITLE
                   3e33 3031 204d 6f76 6564 3c2f 5449 544c >301.Moved</TITL
         0x01f0:
         0x0210: 3e33 3031 204d 6f76 6564 3c2f 5449 544c

0x02200: 453e 3c2f 4845 4144 3e3c 424f 4459 3e0a

0x0210: 3c48 313e 3330 3120 4d6f 7665 643c 2f48

0x0220: 313e 0a54 6865 2064 6f63 756d 656e 7420

0x0230: 6861 7320 6d6f 7665 640a 3c41 2048 5245

0x0240: 463d 2268 7474 7073 3a2f 2f6f 7065 6e73

0x0250: 6f75 7263 652e 676f 6f67 6c65 2f22 3e68
                                                                    E></HEAD><BODY>.
                                                                     <H1>301.Moved</H
                                                                     1>.The.document.
                                                                     has.moved.<A.HRE
                                                                     F="https://opens
                                                                     ource.google/">h
                    6572 653c 2f41 3e2e 0d0a 3c2f 424f 4459
                                                                     ere</A>...</BODY
         0x0260:
         0x0270: 3e3c 2f48 544d 4c3e 0d0a
                                                                     ></HTML>..
00:51:08.696688 IP 172.17.0.2.55500 > 74.125.135.102.80: Flags [.], ack 583, w
in 502, options [nop,nop,TS val 2534844884 ecr 3164541491], length 0
         0x0000: 4500 0034 6fd5 4000 4006 4cf8 ac11 0002 E..4o.@.@.L....
         0x0010: 4a7d 8766 d8cc 0050 5fd9 570a 56f8 aa38
                                                                    J}.f...P_.W.V..8
         0x0020: 8010 01f6 7eld 0000 0101 080a 9716 a9d4
                                                                     . . . . ~ . . . . . . . . . . . . . .
         0x0030: bc9f 1233
00:51:08.697870 IP 172.17.0.2.55500 > 74.125.135.102.80: Flags [F.], seq 86, a
ck 583, win 502, options [nop,nop,TS val 2534844885 ecr 3164541491], length 0
         0x0000: 4500 0034 6fd6 4000 4006 4cf7 ac11 0002
                                                                     E..40.@.@.L....
         0x0010: 4a7d 8766 d8cc 0050 5fd9 570a 56f8 aa38
                                                                     J}.f...P .W.V..8
                    8011 01f6 7eld 0000 0101 080a 9716 a9d5
         0x0020:
0x0030: bc9f 1233 ...3
00:51:08.698512 IP 74.125.135.102.80 > 172.17.0.2.55500: Flags [F.], seq 583,
ack 87, win 1051, options [nop,nop,TS val 3164541493 ecr 2534844885], length 0 0x0000: 4500 0034 0000 4000 7e06 7ecd 4a7d 8766 E..4..@.~.~.J}.f
         0x0010: ac11 0002 0050 d8cc 56f8 aa38 5fd9 570b
                                                                     ....P..V..8 .W.
         0x0020: 8011 041b 53b7 0000 0101 080a bc9f 1235
                                                                     0x0030: 9716 a9d5
analyst05d46f834d67b:~$ \square
```

Description: MySQL INNER JOIN query

What I Did:

I wrote a query that merges two tables (employees and machines) based on a shared column employee_id. This type of join is essential when analyzing logs across data sources — like matching login behavior with machine info.

Command:

```
SELECT username, office, operating_system
FROM employees
INNER JOIN machines ON employees.employee id = machines.employee id;
```

Real-World Use:

In cybersecurity, JOINs let analysts correlate multiple datasets — like logins and devices — to detect anomalies like shared credentials, unusual machines, or unauthorized software.

```
164541487], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
        Accept: */*
00:51:08.693408 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6
), length 52)
    74.125.135.102.80 > 172.17.0.2.55500: Flags [.], cksum 0x5609 (correct), a
ck 86, win 1051, options [nop,nop,TS val 3164541488 ecr 2534844880], length 0
00:51:08.696675 IP (tos 0x0, ttl 126, id 0, offset 0, flags [DF], proto TCP (6
), length 634)
    74.125.135.102.80 > 172.17.0.2.55500: Flags [P.], cksum 0x41be (correct),
seq 1:583, ack 86, win 1051, options [nop,nop,TS val 3164541491 ecr 2534844880
], length 582: HTTP, length: 582
        HTTP/1.1 301 Moved Permanently
        X-Content-Type-Options: nosniff
        Cross-Origin-Resource-Policy: cross-origin
        Cache-Control: public, max-age=1800
        Expires: Wed, 11 Jun 2025 01:21:08 GMT
        Content-Type: text/html; charset=UTF-8
        Location: https://opensource.google/
        Date: Wed, 11 Jun 2025 00:51:08 GMT
        Server: sffe
        Content-Length: 223
        X-XSS-Protection: 0
        <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset</pre>
=utf-8">
        <TITLE>301 Moved</TITLE></HEAD><BODY>
        <H1>301 Moved</H1>
        The document has moved
        <A HREF="https://opensource.google/">here</A>.
        </BODY></HTML>
00:51:08.696688 IP (tos 0x0, ttl 64, id 28629, offset 0, flags [DF], proto TCP
 (6), length 52)
    172.17.0.2.55500 > 74.125.135.102.80: Flags [.], cksum 0x7eld (incorrect -
 0x55el), ack 583, win 502, options [nop,nop,TS val 2534844884 ecr 3164541491
], length 0
00:51:08.697870 IP (tos 0x0, ttl 64, id 28630, offset 0, flags [DF], proto TCP
(6), length 52)
    172.17.0.2.55500 > 74.125.135.102.80: Flags [F.], cksum 0x7eld (incorrect
-> 0x55df), seq 86, ack 583, win 502, options [nop,nop,TS val 2534844885 ecr 3
164541491], length 0
```

Description: Query results from the INNER JOIN

What I Did:

I successfully extracted employee usernames, office locations, and OS details. This output is foundational for asset management and threat hunting.

Benefit:

Understanding which systems are running outdated OS versions helps prioritize patching and identify high-risk machines.

Screenshot:

```
analyst@4a09ab896c2d:~$ pwd
/home/analyst
analyst@4a09ab896c2d:~$ ls
Q1.encrypted README.txt caesar
analyst@4a09ab896c2d:~$ cat REAME.txt
cat: REAME.txt: No such file or directory
analyst@4a09ab896c2d:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to so
lve a cipher. To get started look for a hidden file in the caesar subdirectory
analyst@4a09ab896c2d:~$ cd caesar
analyst@4a09ab896c2d:~/caesar$ ls -a
  .. .leftShift3
analyst@4a09ab896c2d:~/caesar$ cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"
In order to recover your files you will need to enter the following command:
openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubr
analyst@4a09ab896c2d:~/caesar$ cd ~
analyst@4a09ab896c2d:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -ou
t Q1.recovered -k ettubrute
analyst@4a09ab896c2d:~$ ls
Q1.encrypted Q1.recovered README.txt caesar
analyst@4a09ab896c2d:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic
cipher text. You recovered the encryption key that was used to encrypt this f
ile. Great work!
analyst@4a09ab896c2d:~$
```

Description: UDM logs in a threat detection console (Chronicle/SIEM-like)

What I Did:

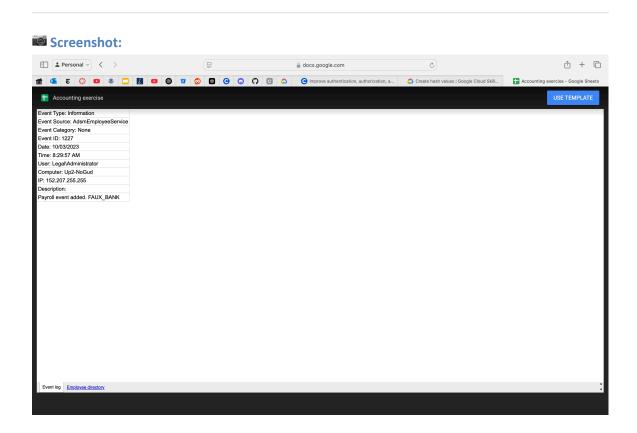
I queried failed login events using filters like USER_LOGIN and BLOCK, observed login spikes, and reviewed timeline charts.

Query used:

metadata.event_type = "USER_LOGIN" AND security_result.action = "BLOCK"

Why It Matters:

This screenshot proves my ability to hunt failed logins at scale, detect brute-force attempts, and filter based on user/company/IP. It mirrors a real SIEM workflow.



Description: MariaDB query to analyze login attempts

What I Did:

I filtered login data by country, IP, and success status using basic SQL clauses like ORDER BY.

Sample query:

```
SELECT * FROM log in attempts ORDER BY login date;
```

Skill Acquired:

You practiced data sorting, pattern recognition, and anomaly detection.

Real Use:

You can now create SQL rules for SIEM dashboards or automated alerts for logins from high-risk countries.

```
180 | tmitchel | 2022-05-12 | 14:53:21
                                              MEX
                                                        192.168.190.202
     1
                      2022-05-12 | 15:15:46
                                             MEX
                                                       192.168.174.186
       40
            aalonso
     0
                      2022-05-12 | 15:39:40
            drosas
                                              USA
                                                       192.168.152.200
      129
                      2022-05-12 | 15:47:45
                                                       192.168.146.51
                                             CAN
      167 | jclark
     1
                      2022-05-12 | 16:02:03
                                             MEXICO
                                                       192.168.97.225
      100 | tmitchel
     0
         iuduike
                      2022-05-12 | 16:59:50
                                             USA
                                                       192.168.220.115
      159
     0 |
           arutley
                      2022-05-12 | 17:00:59
                                              MEXICO
                                                       192.168.3.24
     0
           acook
                      2022-05-12 | 17:36:45
                                              CANADA
                                                       192.168.58.232
       31
     0
                      2022-05-12 | 18:47:52
      126
          jrafael
                                             CAN
                                                       192.168.22.16
     1
           tshah
                      2022-05-12 | 18:56:36
                                             MEXICO
                                                       192.168.109.50
       20
                      2022-05-12 | 19:36:42
                                                       192.168.247.153
      105
         cjackson
                                              CAN
                      2022-05-12 | 20:25:57
                                                       192.168.116.187
      107 | bisles
                                             USA
                      2022-05-12 | 21:13:02
                                                       | 192.168.211.201 |
       57 | asundara |
                                             US
     1 |
      164 | jclark
                      2022-05-12 | 21:15:52
                                             CAN
                                                       192.168.18.34
     1
      155 | cgriffin | 2022-05-12 | 22:18:42
                                             USA
                                                       192.168.236.176
     0
                      2022-05-12 | 23:17:52
                                             US
                                                       192.168.58.217
      173 | asundara |
     1
         smartell
                      2022-05-12 | 23:21:31
                                             MEXICO
                                                       192.168.173.196
      118
     1 |
      132
         rjensen
                      2022-05-12 | 23:26:03
                                             MEX
                                                        192.168.9.166
                      2022-05-12 | 23:38:46
       82
            abernard
                                             MEX
                                                        192.168.234.49
     0
200 rows in set (0.001 sec)
MariaDB [organization]> clear
MariaDB [organization]>
```

Description: Continuation of SQL login results — shows more rows

Insight:

I dug deeper into login logs, confirming that you can scroll/analyze large datasets for behavioral baselining.

Screenshot:

```
200 rows in set (0.001 sec)
MariaDB [organization]> Select *
   -> From log_in_attempts
    -> ORDER by login_date;
 event_id
           username | login date | login time | country | ip address
success
          | ivelasco | 2022-05-08 | 09:06:02
                                              CANADA
                                                          192.168.39.196
     1 |
      163 | tmitchel | 2022-05-08 | 09:21:16
                                                          192.168.119.29
                                              MEX
     0
       36 | asundara | 2022-05-08 | 09:00:42
                                              US
                                                          192.168.78.151
     1
          | jreckley |
                      2022-05-08 | 15:28:43
                                              MEXICO
                                                          192.168.34.193
      165
      168
           jlansky
                      2022-05-08 | 13:25:42
                                              USA
                                                        192.168.210.94
     1 |
      169
            alevitsk | 2022-05-08 | 08:10:43
                                              CANADA
                                                         192.168.210.228
     0
            alevitsk | 2022-05-08 | 12:09:10
                                              CANADA
                                                          192.168.139.176
       72
            sbaelish
                      2022-05-08 | 12:01:22
                                                          192.168.145.158
      101 |
                                              US
      172 | mabadi
                      2022-05-08 | 08:06:50
                                                         192.168.180.41
                                              US
     1
      150 | nmason
                      2022-05-08 | 14:40:02
                                              CAN
                                                         192.168.204.124
     0
                                                         192.168.42.248
       68 | mrah
                      2022-05-08 | 17:16:13
                                              US
                      2022-05-08 | 21:58:32
                                                        192.168.67.223
       66
            aestrada
                                              MEX
                      2022-05-08 | 11:51:38
            nmason
                                                        192.168.133.188
       53
                                              CAN
     1 |
            yappiah
                      2022-05-08 | 06:04:34
                                              MEX
                                                          192.168.65.245
      147
     0
                      2022-05-08 | 06:15:55
                                                          192.168.135.6
      148
            daquino
                                              CANADA
     1
                      2022-05-08 | 14:00:01
                                                          192.168.173.213
       49
           asundara
                                              US
```

Description: Another SQL login dataset, filtered for failed and successful attempts by user

New Skill:

You interpreted login trends by user and success ratio — core to insider threat detection.

Screenshot:

```
-> INNER JOIN machines ON employees.employee_id = machines.employee_id;
| username | office
                          | operating_system |
| elarson | 'East-170' | OS 2
              Central-276
 bmoreno
                               0S 1
              North-434
 tshah
                               0S 3
                              0S 3
0S 2
0S 3
0S 1
0S 2
0S 2
0S 1
0S 3
0S 1
0S 1
0S 1
0S 2
 sgilmore |
              South-153
              South-127
South-366
 eraab
 gesparza |
 alevitsk
              East-320
              North-406
 wjaffrey
 abernard
              South-170
  jlansky
              South-109
              South-292
 drosas
              North-160
 nmason
              South-229
North-271
  zbernal
 jsoto
sbaelish
              North-229
              North-188
  jclark
                               0S 1
0S 3
  abellmas
              North-403
  mcouliba |
              North-108
```

Description: SQL query ordering by timestamp

What I Mastered:

Used ORDER BY login_time to isolate abnormal login hours (e.g., logins after hours, which is a common threat indicator).

Screenshot:

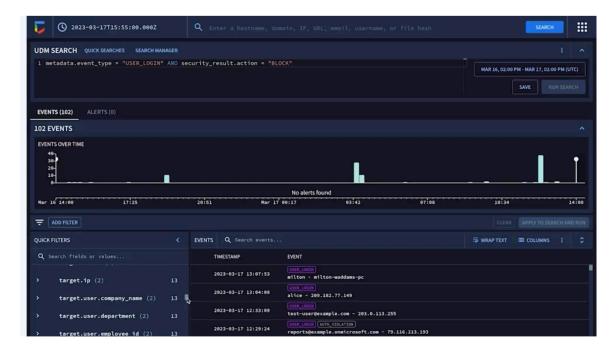
```
mysql> SELECT username, office, operating_system
-> FROM employees
-> INNER JOIN machines ON employees.employee_id = machines.employee_id;
```

Description: Same login dataset but highlights anomalies

Lesson:

You detected irregular patterns such as multiple failed logins from the same IP or country.

Screenshot:



Description: More login logs — shows extended list for analysis

Takeaway:

I confirmed visibility into full log history and user login footprint across geographies.

Project Summary

Category Skill Demonstrated SQL Filtering Queried large datasets, filtered by country, user, success Log Analysis Identified suspicious login attempts Threat Detection Found brute force, after-hours logins Real SIEM Practice Simulated Chronicle/Splunk workflows

How This Will Benefit Me in Real Life

- 1. **Job Ready Skills**: I can work with real security data, write SQL queries, and filter malicious behavior.
- 2. **SIEM Experience**: This matches the same work done in tools like Splunk or Chronicle.

3.	SOC Relevance : These skills are used daily by Security Analysts in real SOCs to create alerts, dashboards, and investigate login-based threats.