**Raw Data Previews** (not queries, just loading tables)

SELECT \* FROM users;

SELECT \* FROM devices;

SELECT \* FROM access\_logs;

SELECT \* FROM threat\_alerts;

0 1 jdoe IT 2022-08-05

1 2 asmith IT 2022-01-17

2 3 bwilliams HR 2022-01-16

3 4 mjohnson Finance 2022-02-17

4 5 klee Finance 2022-04-22

5 6 tjackson Finance 2022-04-30

6 7 hpatel IT 2022-09-16

7 8 cnguyen Marketing 2022-11-05

8 9 aroberts IT 2022-01-14

9 10 bwilson Marketing 2022-10-15

0 101 4 Desktop macOS

1 102 9 Desktop iOS

2 103 7 Laptop macOS

3 104 4 Laptop Windows 10

4 105 8 Desktop Android

5 106 10 Laptop iOS

6 107 5 Laptop Windows 10

7 108 1 Desktop Android

8 109 3 Laptop Windows 10

9 110 7 Desktop iOS

0 1001 105 2023-12-01 10:51:00 logout

1 1002 110 2023-12-01 09:08:00 login

2 1003 106 2023-12-01 10:59:00 login

3 1004 110 2023-12-01 10:54:00 login

4 1005 104 2023-12-01 10:45:00 logout

5 1006 102 2023-12-01 08:18:00 logout

6 1007 101 2023-12-01 10:35:00 logout

7 1008 104 2023-12-01 10:42:00 login

8 1009 105 2023-12-01 08:43:00 login

9 1010 102 2023-12-01 10:16:00 logout

10 1011 104 2023-12-01 09:02:00 login

11 1012 102 2023-12-01 08:41:00 logout

12 1013 107 2023-12-01 09:58:00 logout

13 1014 105 2023-12-01 09:37:00 logout

14 1015 108 2023-12-01 09:09:00 login

15 1016 106 2023-12-01 10:43:00 logout

16 1017 103 2023-12-01 10:56:00 login

17 1018 106 2023-12-01 10:22:00 login

18 1019 106 2023-12-01 08:56:00 logout

19 1020 104 2023-12-01 10:55:00 logout

0 2001 110 2023-12-01 09:04:00 low phishing

1 2002 107 2023-12-01 10:21:00 high malware

2 2003 106 2023-12-01 08:02:00 medium phishing

3 2004 104 2023-12-01 10:54:00 high malware

4 2005 103 2023-12-01 08:29:00 high malware

5 2006 109 2023-12-01 10:54:00 high ransomware

6 2007 108 2023-12-01 10:17:00 low malware

7 2008 102 2023-12-01 09:08:00 low phishing

8 2009 101 2023-12-01 10:44:00 medium phishing

9 2010 102 2023-12-01 09:27:00 low ransomware

10 2011 103 2023-12-01 08:28:00 high phishing

11 2012 103 2023-12-01 09:15:00 high unauthorized\_access

12 2013 107 2023-12-01 09:51:00 low ransomware

13 2014 110 2023-12-01 08:40:00 high phishing

14 2015 102 2023-12-01 09:56:00 medium phishing

15 2016 107 2023-12-01 08:00:00 medium unauthorized\_access

16 2017 107 2023-12-01 09:07:00 low ransomware

17 2018 110 2023-12-01 10:08:00 low unauthorized\_access

18 2019 108 2023-12-01 08:45:00 medium ransomware

19 2020 109 2023-12-01 10:09:00 medium ransomware

1)-List all users and the number of devices assigned to each---

SELECT u.username, COUNT(d.device\_id) AS device\_count

FROM users u

LEFT JOIN devices d ON u.user\_id = d.user\_id

GROUP BY u.username;

aroberts 1

asmith 0

bwilliams 1

bwilson 1

cnguyen 1

hpatel 2

jdoe 1

klee 1

mjohnson 2

tjackson 0

---2)-------. Show the number of access logs recorded for each device---

SELECT device\_id, COUNT(\*) AS log\_count

FROM access\_logs

GROUP BY device\_id;

aroberts 1

asmith 0

bwilliams 1

bwilson 1

cnguyen 1

hpatel 2

jdoe 1

klee 1

mjohnson 2

tjackson 0

--3)---Identify departments that have users with the most high severity threats

SELECT u.department, COUNT(\*) AS high\_threat\_count

FROM threat\_alerts t

JOIN devices d ON t.device\_id = d.device\_id

JOIN users u ON d.user\_id = u.user\_id

WHERE t.threat\_level = 'high'

GROUP BY u.department

ORDER BY high\_threat\_count DESC;

IT 4

Finance 2

HR 1

---4. Show users whose devices have had more than one high severity threat

SELECT u.username, COUNT(\*) AS high\_threat\_count

FROM threat\_alerts t

JOIN devices d ON t.device\_id = d.device\_id

JOIN users u ON d.user\_id = u.user\_id

WHERE t.threat\_level = 'high'

GROUP BY u.username

HAVING COUNT(\*) > 1;

hpatel 4

5. Identify all users who experienced a high severity threat on one of their devices within 10 minutes after a login event

SELECT

u.user\_id,

u.username,

u.department,

d.device\_id,

d.device\_type,

a.access\_time AS login\_time,

t.detected\_time AS threat\_time,

t.threat\_type,

t.threat\_level,

CASE

WHEN t.threat\_level = 'high'

AND a.access\_type = 'login'

AND t.detected\_time BETWEEN a.access\_time AND DATEADD(MINUTE, 10, a.access\_time)

THEN 'Threat After Login (Within 10 min)'

ELSE 'No Immediate Threat'

END AS threat\_status

FROM

access\_logs a

JOIN

devices d ON a.device\_id = d.device\_id

JOIN

users u ON d.user\_id = u.user\_id

LEFT JOIN

threat\_alerts t ON a.device\_id = t.device\_id

WHERE

a.access\_type = 'login'

ORDER BY

u.username, a.access\_time;

10 bwilson Marketing 106 Laptop 2023-12-01 10:22:00 2023-12-01 08:02:00 phishing medium No Immediate Threat

10 bwilson Marketing 106 Laptop 2023-12-01 10:59:00 2023-12-01 08:02:00 phishing medium No Immediate Threat

8 cnguyen Marketing 105 Desktop 2023-12-01 08:43:00 NULL NULL NULL No Immediate Threat

7 hpatel IT 110 Desktop 2023-12-01 09:08:00 2023-12-01 09:04:00 phishing low No Immediate Threat

7 hpatel IT 110 Desktop 2023-12-01 09:08:00 2023-12-01 08:40:00 phishing high No Immediate Threat

7 hpatel IT 110 Desktop 2023-12-01 09:08:00 2023-12-01 10:08:00 unauthorized\_access low No Immediate Threat

7 hpatel IT 110 Desktop 2023-12-01 10:54:00 2023-12-01 09:04:00 phishing low No Immediate Threat

7 hpatel IT 110 Desktop 2023-12-01 10:54:00 2023-12-01 08:40:00 phishing high No Immediate Threat

7 hpatel IT 110 Desktop 2023-12-01 10:54:00 2023-12-01 10:08:00 unauthorized\_access low No Immediate Threat

7 hpatel IT 103 Laptop 2023-12-01 10:56:00 2023-12-01 08:29:00 malware high No Immediate Threat

7 hpatel IT 103 Laptop 2023-12-01 10:56:00 2023-12-01 08:28:00 phishing high No Immediate Threat

7 hpatel IT 103 Laptop 2023-12-01 10:56:00 2023-12-01 09:15:00 unauthorized\_access high No Immediate Threat

1 jdoe IT 108 Desktop 2023-12-01 09:09:00 2023-12-01 10:17:00 malware low No Immediate Threat

1 jdoe IT 108 Desktop 2023-12-01 09:09:00 2023-12-01 08:45:00 ransomware medium No Immediate Threat

4 mjohnson Finance 104 Laptop 2023-12-01 09:02:00 2023-12-01 10:54:00 malware high No Immediate Threat

4 mjohnson Finance 104 Laptop 2023-12-01 10:42:00 2023-12-01 10:54:00 malware high No Immediate Threat