Explanation/Trends	Rule Logic	Count	FP count	TP count	% Precision	% Recall	# Total count of fraud events
In order to run the querries add:	SELECT * FROM "Data"						
(Option 2#)	SELECT ROW_NUMBER()OVER()AS ROW_NUMBER, SUM(CASE WHEN fraud_label=TRUE THEN 1 ELSE 0 END)OVER()AS fraud_true,SUM(CASE WHEN fraud_label=FALSE THEN 1 ELSE 0 END)OVER()AS fraud_false,COUNT(*)OVER()AS total_rows, * FROM"Data"						
Events with product names combined with **specific OS and graphic cards** patterns were strongly linked to fraud and were blacklisted.	WHERE product_name='' AND(os_version='18.3.1' OR(os_version='19.0.0' AND graphic_card='ANGLE (NVIDIA, NVIDIA GeForce RTX 3070 (0x00002488) Direct3D11 vs_5_0 ps_5_0, D3D11)')OR (os_version='5.4.0' AND graphic_card='ANGLE (Google, Vulkan 1.3.0 (SwiftShader Device (Subzero) (0x0000C0DE)), SwiftShader driver)')OR (os_version='10' AND graphic_card=''))	151	30	121	80.13%	39.93%	303
A high number of **suspicious events in the last 30 minutes** often signals coordinated automated attacks - covering more than 1/3 of the cases.	WHERE suspicious_count_last_30m > 3	108	3	105	97.22%	34.65%	303

Explanation/Trends	Rule Logic	Count	FP count	TP count	% Precision	% Recall	# Total count of fraud events
A high number of **suspicious events in the last 30 minutes** often signals coordinated automated attacks - covering more than 1/3 of the cases.	WHERE suspicious_count_last_30m >0	171	16	155	90.64%	51.16%	303

Explanation/Trends	Rule Logic	Count	FP count	TP count	% Precision	% Recall	# Total count of fraud events
A few **devices** showed an unusually high number of users. (Here I first identified these devices using pivot tables, then wrote an SQL query to flag and blacklist them)	WHERE (device_id='eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI2MjNiYzM5OS03YjIwLTRiMDgtYTFjNy1hNjcyOTJjZmVhM2MiLCJ2ZXJzaW9uIjoxLCJpYXQiOjE3NDU2NzYxMDJ9.RqdIDOfXSiktpyIeclEibNw1hBa4S5h9h11Sel4zqOk' OR device_id='eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI4NjFkZjM5Ny0yNmJjLTQ0ODktYmNmNy03ZmZlZTI0OThiNGYiLCJ2ZXJzaW9uIjoxLCJpYXQiOjE3NDM3MDg0NTh9.bgk4vfW6qfgziME0WzqsOR1DWcfl2LNVvbnngIGusY4' OR device_id='eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI4OGZiMjQ0YS1kY2VmLTQ5ZTUtOGExMi1kYmI5MzMwZGZjNzkiLCJ2ZXJzaW9uIjoxLCJpYXQiOjE3NDM2Mjc5NTd9.Hp7tBjtX-LHqx9Q4-6km3GcNE3M7DHPHAS0OZlREHkE' OR device_id='eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI5ZTlhOTVjYi03ZDI2LTQyYjktOTFmMC04N2RhZDI4ZWFiZDYiLCJ2ZXJzaW9uIjoxLCJpYXQiOjE3NDU1NDU3NDN9.3BGl-u_M8dJ0FJKBgjd8a2DR5NIKc6fef9oGDWDRFNU' OR device_id='eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9	100	0	100	100.00%	33.00%	303

Explanation/Trends	Rule Logic	Count	FP count	TP count	% Precision	% Recall	# Total count of fraud events
(Option 2#)	--#1 SELECT device_id,COUNT(*)AS total_rows,SUM (CASE WHEN fraud_label=TRUE THEN 1 ELSE 0 END)AS fraud_true,SUM(CASE WHEN fraud_label=false THEN 1 ELSE 0 END)AS fraud_false FROM"Data" GROUP BY device_id HAVING COUNT(*)>2 AND SUM(CASE WHEN fraud_label=TRUE THEN 1 ELSE 0 END)>0 ORDER BY fraud_true DESC; --#2 SELECT*FROM"Data" WHERE device_id IN ('eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJzdWIiOiI2MjNiYzM5OS03YjIwLTRiMDgtYTFjNy 1hNjcyOTJjZmVhM2MiLCJ2ZXJzaW9uIjoxLCJpYX QiOjE3NDU2NzYxMDJ9. RqdIDOfXSiktpyIeclEibNw1hBa4S5h9h11Sel4zqOk' ,'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJzdWIiOiJmZDBhOGI0OC1mNDFiLTRkMDAtYjQ 5NC1iNmVmZGIwMmE2MTAiLCJ2ZXJzaW9uIjoxL CJpYXQiOjE3MzU2MjkxMDk1MDZ9. 3uI1uIDHv4FpkrdTDqx70jMk4luvPEeJaG59mdu5Q 7s','eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJzdWIiOiI4OGZiMjQ0YS1kY2VmLTQ5ZTUtOGEx Mi1kYmI5MzMwZGZjNzkiLCJ2ZXJzaW9uIjoxLCJp YXQiOjE3NDM2Mjc5NTd9.Hp7tBjtX-LHqx9Q4- 6km3GcNE3M7DHPHAS0OZlREHkE','eyJhbGciOiJI UzI1NiIsInR5cCI6IkpXVCJ9. eyJzdWIiOiI1NDUyZDYxYy0yNzM3LTRlMDctODBm Yi1hNzU5MjFlYTlkNGYiLCJ2ZXJzaW9uIjoxLCJpYX QiOjE3NDQ1ODQzNzR9	136	6	130	95.59%	42.90%	303

Explanation/Trends	Rule Logic	Count	FP count	TP count	% Precision	% Recall	# Total count of fraud events
Some events originated from **IP addresses registered in Canada**, but their **timezones** were inconsistent, suggesting possible VPN or proxy use.	WHERE ip_country = 'CA' AND timezone NOT LIKE '%America%'	91	20	71	78.02%	23.43%	303

Explanation/Trends	Rule Logic	Count	FP count	TP count	% Precision	% Recall	# Total count of fraud events
An IP generating **more than 10 actions** within one minute likely indicates automated bot activity.	WHERE ip_action_count_last_minute > 10	88	16	72	81.82%	23.76%	303
Although high connection RTT values alone are uncommon, **combining RTT higher than 100 with 'hosting' IP types** helps identify suspicious activity more effectively.	WHERE connection_rtt >= 100 AND ip_type='hosting'	84	34	50	59.52%	16.50%	303
Devices associated with **3 or more users in the past 7 days** may indicate shared or fraudulent device usage.	WHERE user_on_device_7d >= 3	71	24	47	66.20%	15.51%	303
A high action rate on mobile devices often indicates bot activity and helped detect about 1/5 of fraud cases in this dataset.	WHERE high_action_rate_mob=TRUE	64	5	59	92.19%	19.47%	303
Devices associated with **3 or more users in the past day** may indicate shared or fraudulent device usage.	WHERE user_on_device_1d >= 3	58	12	46	79.31%	15.18%	303
The current automation tests detected a relatively small number of cases but proved to be reliable indicators of fraud	WHERE (automation_test_1 = TRUE OR automation_test_2 = TRUE OR automation_test_3 = TRUE OR automation_test_4 = TRUE)	47	2	45	95.74%	14.85%	303
Hosting' IP types linked to more than two users within a day often indicate fraud, with minimal risk of false positives.	WHERE user_on_device_1d >2 AND ip_type='hosting'	45	0	45	100.00%	14.85%	303