QUANTUMFALCON
Summarization to support QUANTUM Targeting

Overview

Overview

Challenges

- Triage selectors for potential QUANTUM targeting
- Enrich with strongly correlated selectors
- Possible manually with MARINA with multiple queries (no workflows)

Overview

Overview

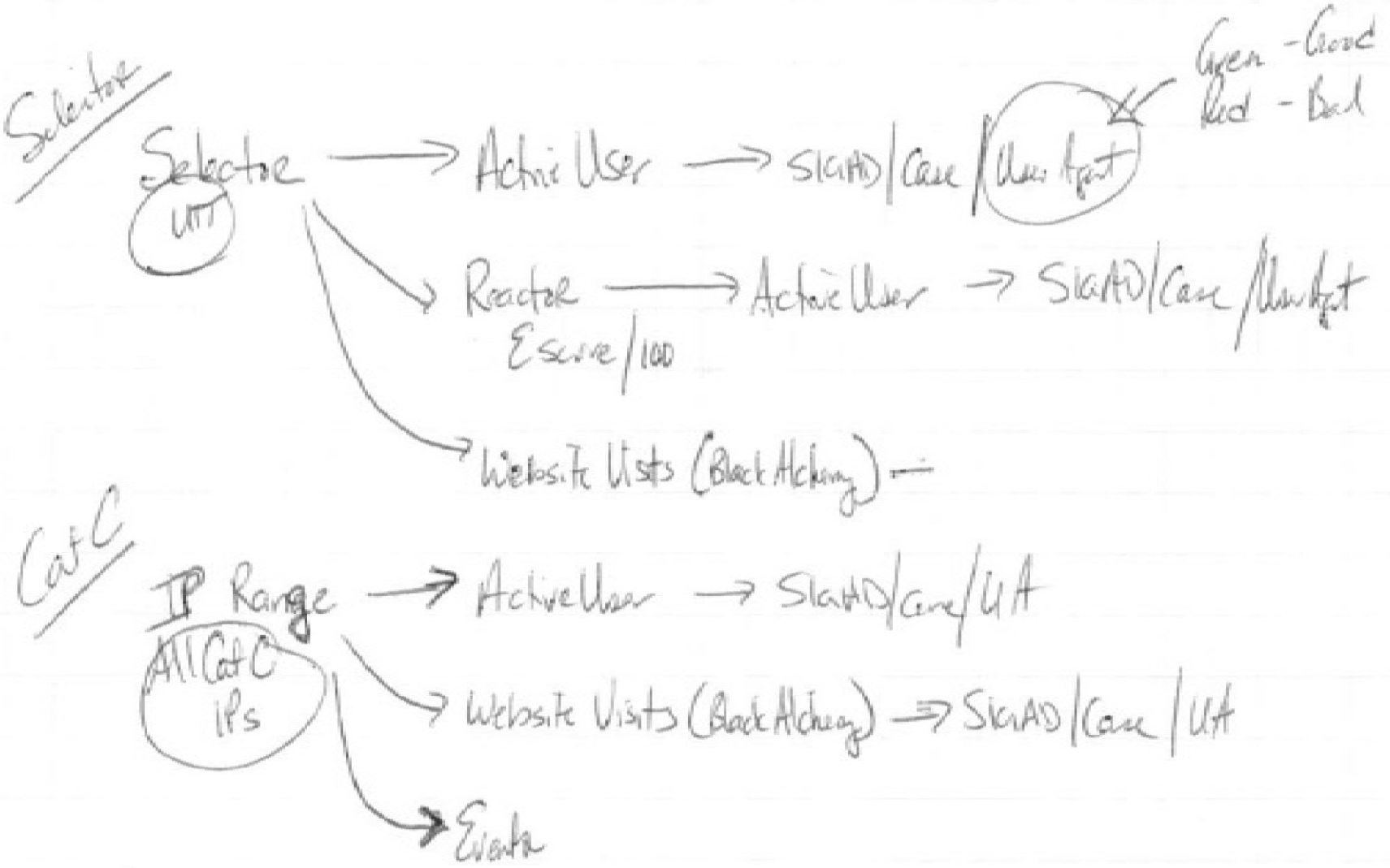
Solution

- Cloud analytic developed to support targeting
- Map/Reduce ideal for counting activity

- Using corporate resources to perform activities
  - Seed selector list – INQUIRY service
  - Summary of ASDF data already on GHOSTMACHINE
  - REACTOR E score data inside ASDF records (User = User Atom)
  - UTT sent daily to GHOSTMACHINE

Overview

The Napkin



Results

What does it look like?

Selector	AltID	UTTCategory	SIGAD	CASENOTATION	IPDirecti	From	FromASN	To	ToASN	#TRSI	#DaysSe	La
100000227785040<facebook>	[redacted]	6587:FGS2A4	US-972U	AF.QXAPOS000000	C->S	AF	38742	US	32934	1	1	20
100000227785040<facebook>		6587:FGS2A4	US-972U	AF.QXAPOS	C->S	AF	38742	US	32934	1	1	20
100000603891507<facebook>		-	UKC-302A	PKCSE035K000HD0	C->S	PK	45595	US	26101	2	1	20
100000603891507<facebook>		-	UKC-302A	PKCSE035L000HD0	C->S	PK	45595	US	26101	2	2	20
100000677501875<facebook>		-	UKC-302A	PKCSE068A000HD0	C->S	PK	45595	BG	32934	1	1	20
100000677501875<facebook>		-	UKC-302A	PKCSE068A000HD0	C->S	PK	45595	US	32934	8	2	20
100000677501875<facebook>		-	UKC-302A	PKCSE068A000HD0	S->C	US	32934	PK	45595	1	1	20
100000692006670<facebook>		60:S2A13	USD-1079	H5V035343960000	S->C	US	32934	SG	7700	9	2	20
100000727045165<facebook>		1860:S2A63 238(	UKC-302A	PKCSE035L000HD0	C->S	PK	45595	US	26101	2	1	20
100000727045165<facebook>		1860:S2A63 238(	UKC-302A	PKCSE039K000HD0	C->S	PK	45595	US	14778	66	2	20
100000727045165<facebook>		1860:S2A63 238(	UKC-302A	PKCSE039K000HD0	C->S	PK	45595	US	36646	28	3	20
100000727045165<facebook>		1860:S2A63 238(	UKC-302A	PKCSE039L000HD0	C->S	PK	45595	US	14778	81	4	20
100000727045165<facebook>		1860:S2A63 238(	UKC-302A	PKCSE039L000HD0	C->S	PK	45595	US	36646	40	4	20
100000820627286<facebook>		-	USJ-759A	5BDAZ00000M0000	S->C	BG	32934	IQ	16212	26	1	20
100000820627286<facebook>		-	USJ-759A	5BDAZ00000M0000	S->C	US	32934	IQ	16212	215	4	20
100000820627286<facebook>		-	USJ-759	5BDAZ00000MID03	C->S	IQ	16212	BG	32934	36	3	20
100000820627286<facebook>		-	USJ-759	5BDAZ00000MID03	C->S	IQ	16212	US	32934	70	4	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	S->C	US	8075	XX	-	531	6	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	null	-	-	-	-	9	1	20
100001442593682<facebook>		2783:F74	US-966A	E2H1154346000TD	C->S	XX	-	IE	32934	5	1	20
100001442593682<facebook>		2783:F74	US-966A	E2H1154346000TD	C->S	XX	-	US	32934	2	1	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	S->C	IE	32934	XX	-	49	4	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	S->C	US	32934	XX	-	50	6	20
100001450912744<facebook>		-	UKC-302A	PKCSE035K000HD0	C->S	PK	45595	US	26101	2	2	20
100001450912744<facebook>		-	UKC-302A	PKCSE035L000HD0	C->S	PK	45595	US	26101	1	1	20
100001751863833<facebook>		-	UKC-302A	PKCSE035K000HD0	C->S	AF	55330	US	26101	1	1	20
100001751863833<facebook>		-	US-968Z	K5H110900004144	S->C	US	32934	AF	23649	5	1	20
100002135632573<facebook>		2381:SV 4318:S2	UKC-302A	PKCSE072A000HD0	C->S	PK	45595	US	32934	5	1	20
100002135632573<facebook>		2381:SV 4318:S2	UKC-302A	PKCSE072A000HD0	S->C	US	32934	PK	45595	1	1	20

Results

What does it look like?

Selector	AltID	SIGAD	CASENOTATION	IPDirecti	FromIP	From	ToIP	To	#TRSI	#DaysSe
100000227785040<facebook>	[redacted]	US-972U	AF.QXAPOS000000	C->S	[redacted]	AF	[redacted]	US	1	
100000227785040<facebook>		US-972U	AF.QXAPOS	C->S		AF		US	1	
100000692006670<facebook>		USD-1079	H5V035343960000	S->C		US		SG	1	
100000692006670<facebook>		USD-1079	H5V035343960000	S->C		US		SG	3	
100000692006670<facebook>		USD-1079	H5V035343960000	S->C		US		SG	5	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	152	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	35	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		BG		IQ	26	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	9	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	19	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	5	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	34	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	24	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		BG	2	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		BG	31	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		BG	3	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	2	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	3	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	1	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	8	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	63	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	4	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	127	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	17	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	28	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	90	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	21	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	24	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	6	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	9	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	61	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	10	

Hits | CaseNotationCounts | IPHits

1105 of 31950 records found Average: 10060205.58 Count: 14378 Sum: 44466108682 100%

Issues

Issues

Questions