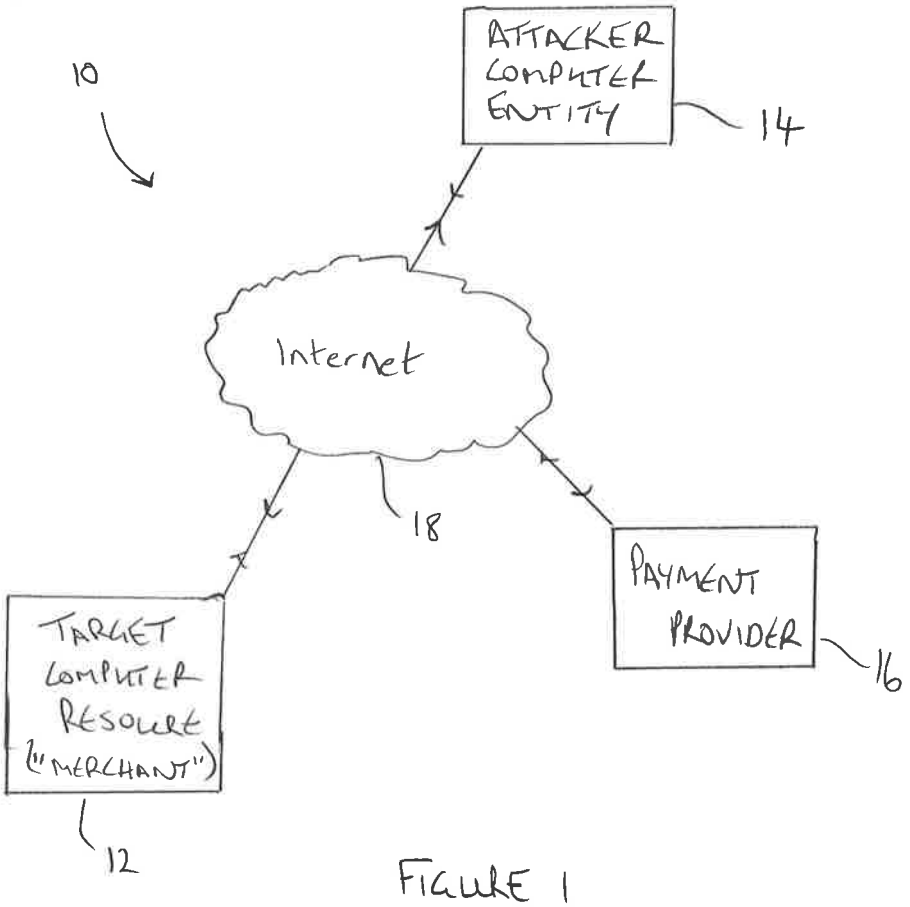
10
ATTACKER COMPUTER ENTITY
14
Internet
18
PAYMENT PROVIDER
16
TARGET COMPUTER RESOURCE ("MERCHANT")
12

FIGURE 1

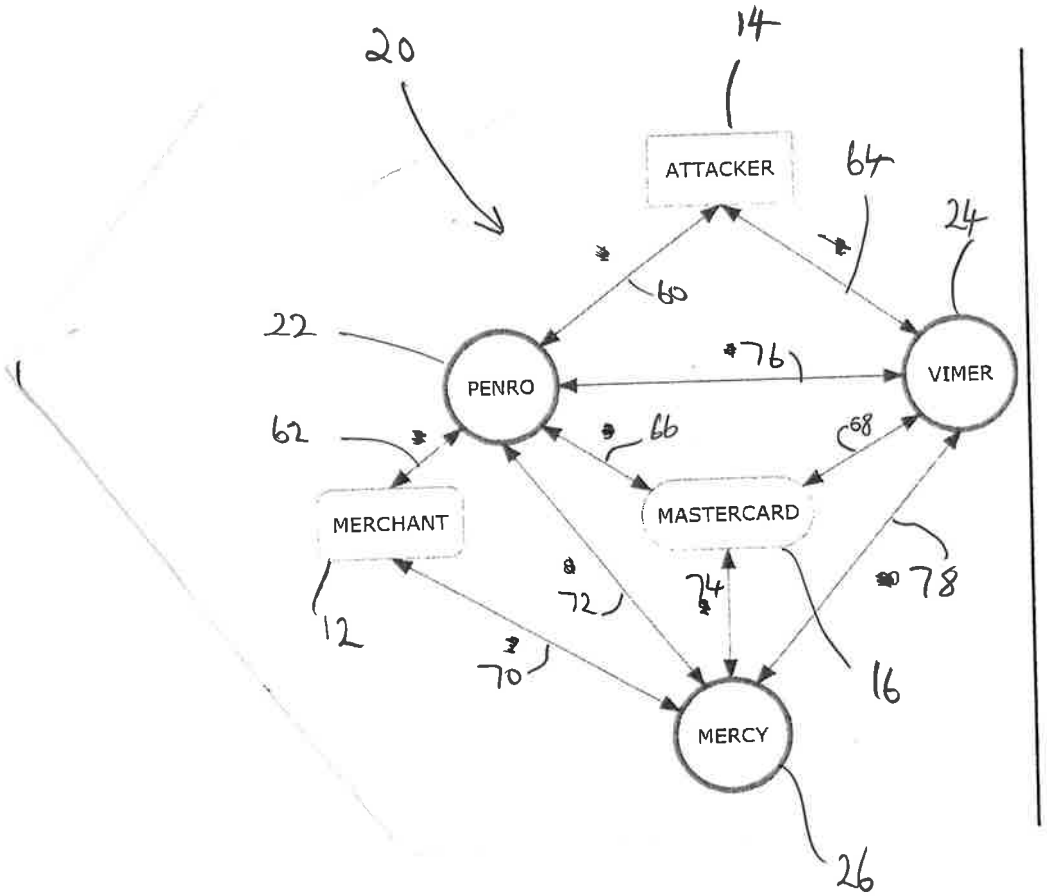
20
14
ATTACKER
64
24
60
22
PENRO
76
VIMER
62
66
68
MERCHANT
MASTERCARD
78
12
72
74
70
16
MERCY
26

FIGURE 2

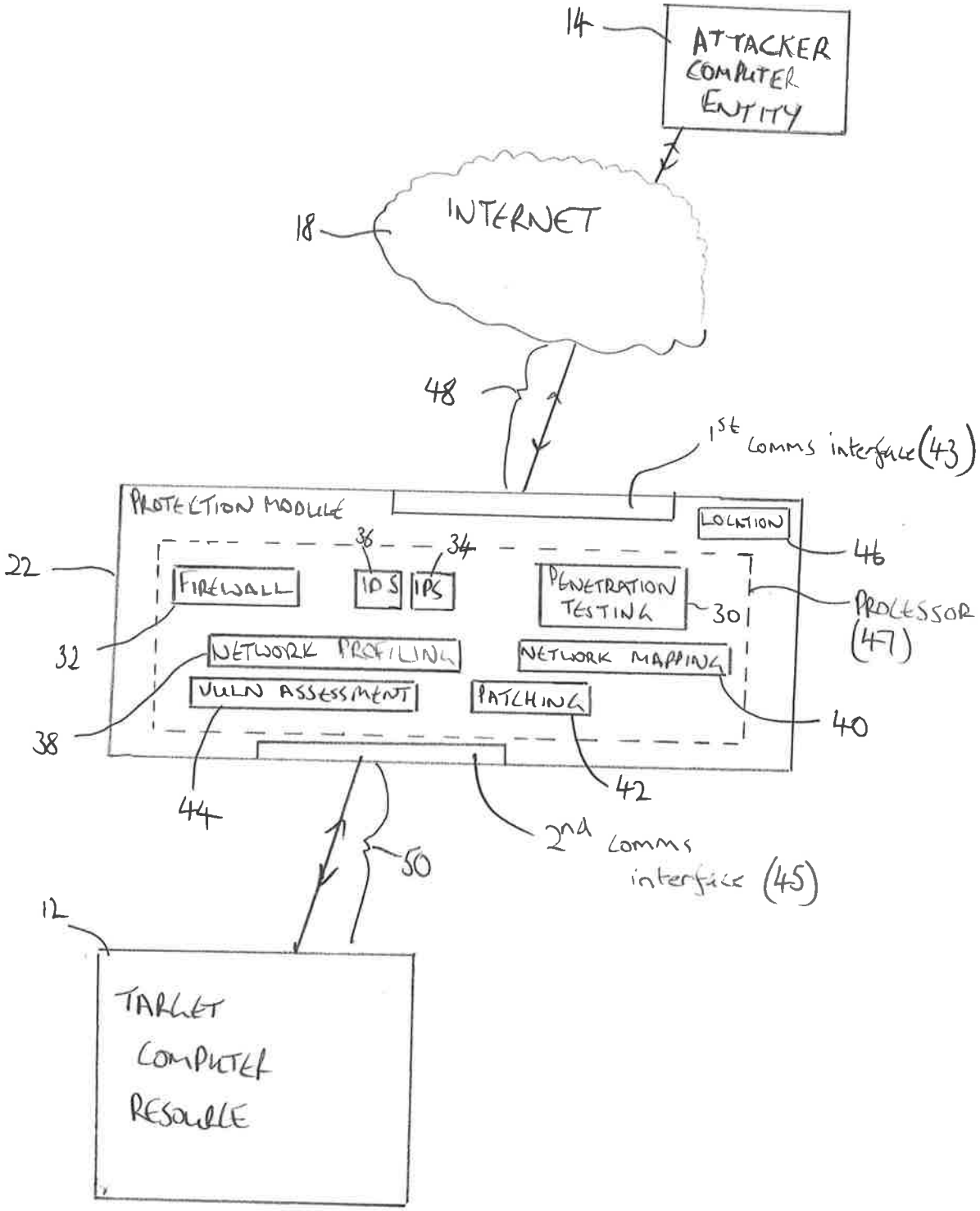
14
ATTACKER COMPUTER ENTITY
18
INTERNET
48
1st comms interface (43)
PROTECTION MODULE
LOCATION
46
22
36
34
FIREWALL
IDS
IPS
PENETRATION TESTING
30
PROCESSOR (47)
32
NETWORK PROFILING
NETWORK MAPPING
VULN ASSESSMENT
PATCHING
38
40
44
42
2nd comms interface (45)
50
12
TARGET COMPUTER RESOURCE

FIGURE 3

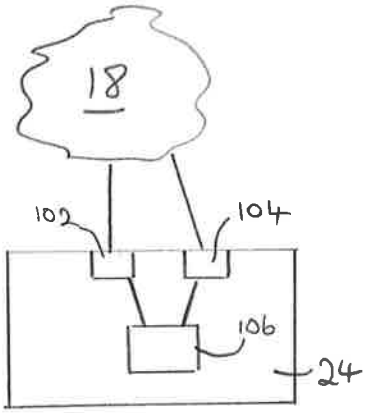

FIGURE 4

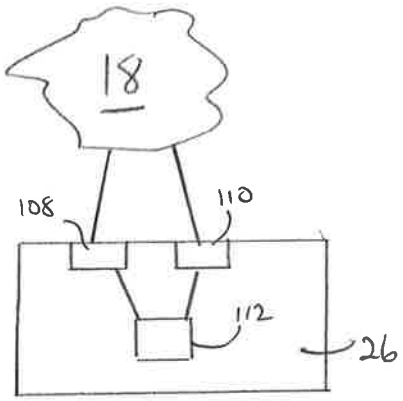

FIGURE 5

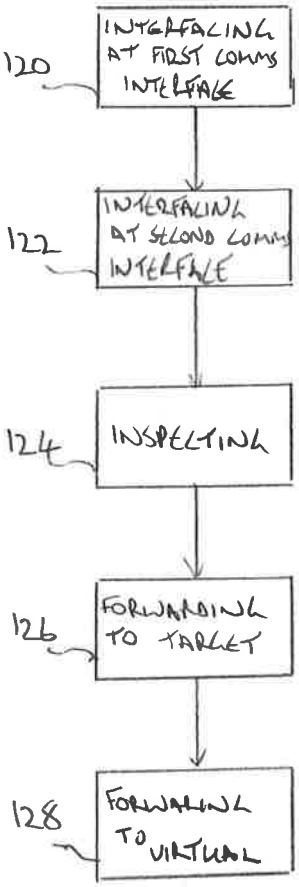

FIGURE 6

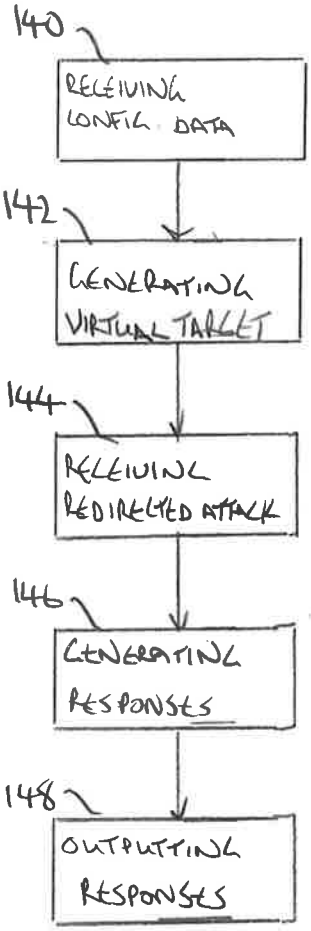

FIGURE 7

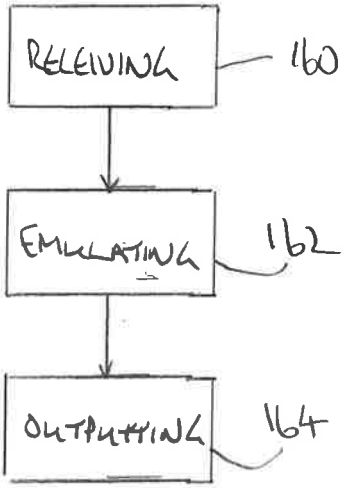

FIGURE 8

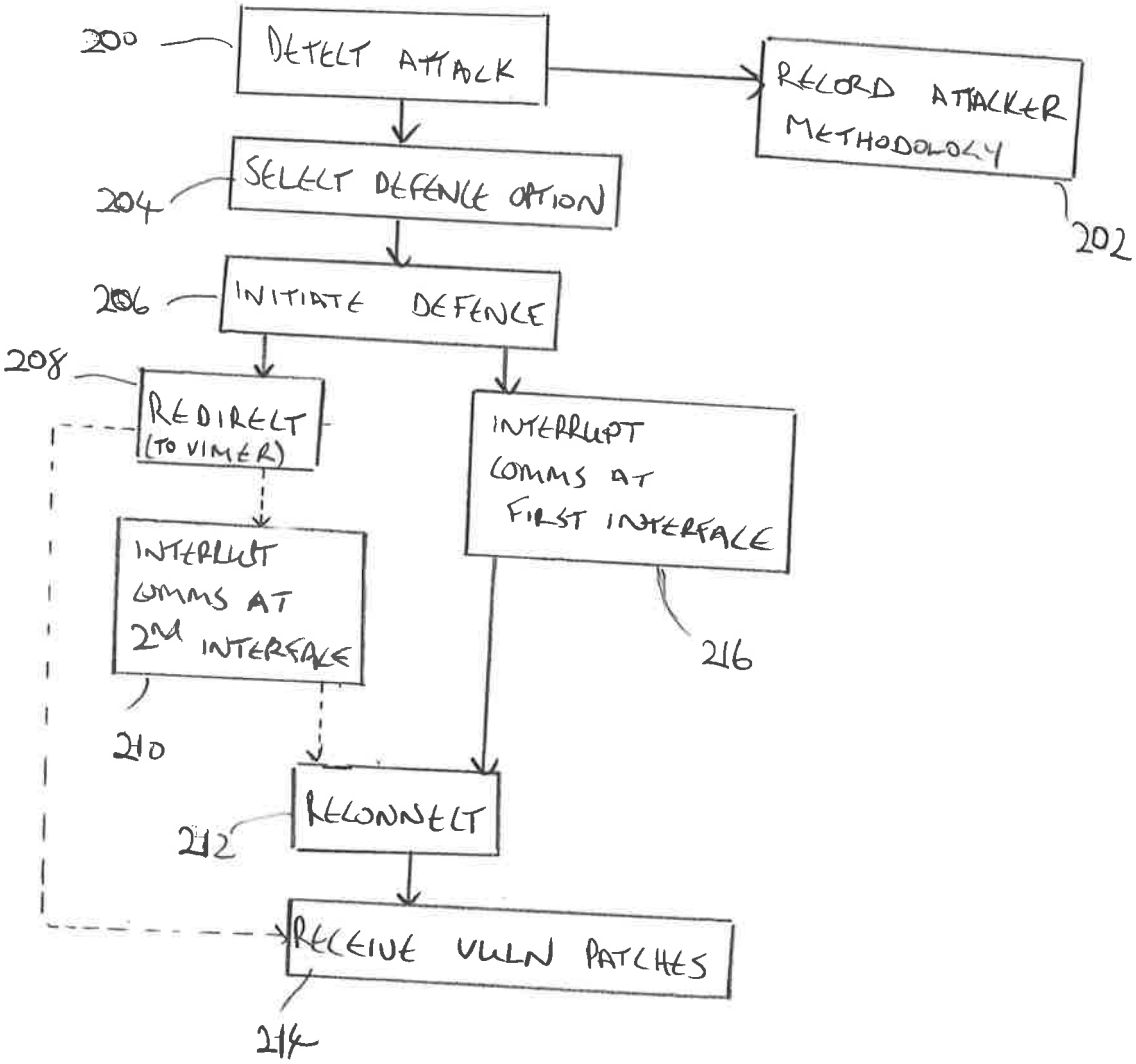
200
DETECT ATTACK
RECORD ATTACKER METHODOLOGY
202
204
SELECT DEFENCE OPTION
206
INITIATE DEFENCE
208
REDIRECT (TO VIMER)
INTERRUPT COMMS AT FIRST INTERFACE
216
INTERRUPT COMMS AT 2ND INTERFACE
210
212
RECONNECT
RECEIVE VULN PATCHES
214

FIGURE 9

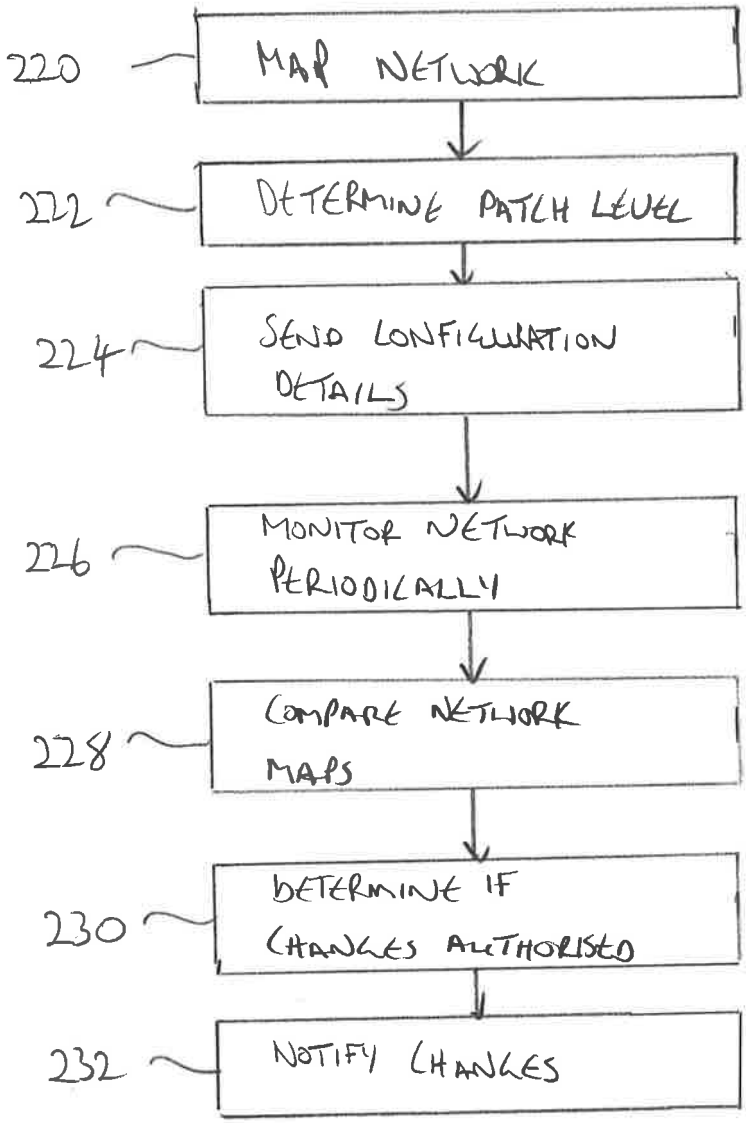
220
MAP NETWORK
222
DETERMINE PATCH LEVEL
224
SEND CONFIGURATION DETAILS
226
MONITOR NETWORK PERIODICALLY
228
COMPARE NETWORK MAPS
230
DETERMINE IF CHANGES AUTHORISED
232
NOTIFY CHANGES

FIGURE 10

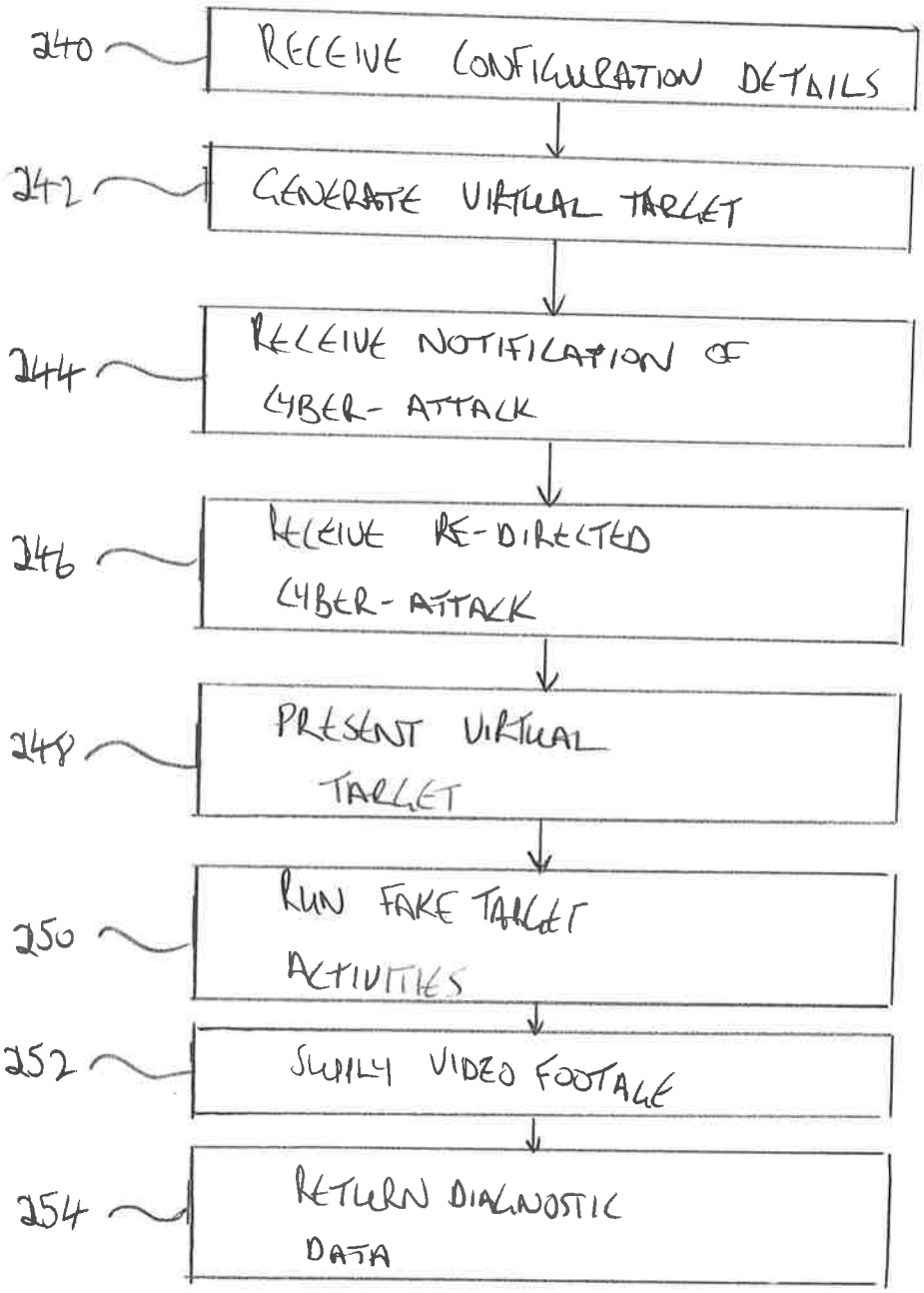
240
RECEIVE CONFIGURATION DETAILS
242
GENERATE VIRTUAL TARGET
244
RECEIVE NOTIFICATION OF CYBER-ATTACK
246
RECEIVE RE-DIRECTED CYBER-ATTACK
248
PRESENT VIRTUAL TARGET
250
RUN FAKE TARGET ACTIVITIES
252
SUPPLY VIDEO FOOTAGE
254
RETURN DIAGNOSTIC DATA

FIGURE 11